Elementary Number Theory

David Pierce

September 20, 2012

Mathematics Department
Mimar Sinan Fine Arts University
Istanbul
dpierce@msgsu.edu.tr
http://mat.msgsu.edu.tr/~dpierce/

This work is licensed under the
Creative Commons
Attribution-NonCommercial-ShareAlike 3.0
Unported License.
To view a copy of this license, visit
http://creativecommons.org/licenses/by-nc-sa/3.0/
or send a letter to
Creative Commons,
444 Castro Street, Suite 900,
Mountain View, California, 94041, USA.

Bu çalışma
Creative Commons Attribution-Gayriticari-ShareAlike 3.0
Unported Lisansı ile lisanslı.
Lisansın bir kopyasını görebilmek için,
http://creativecommons.org/licenses/by-nc-sa/3.0/
adresini ziyaret edin ya da mektup atın:
Creative Commons,
444 Castro Street, Suite 900,
Mountain View, California, 94041, USA.

David Austin Pierce

Matematik Bölümü
Mimar Sinan Güzel Sanatlar Üniversitesi
Bomonti, Şişli, İstanbul, 34380

dpierce@msgsu.edu.tr
http://mat.msgsu.edu.tr/~dpierce/

Contents

Preface **8**

1. Proving and seeing **11**
1.1. The look of a number 11
1.2. Patterns that fail 15
1.3. Incommensurability 20

2. Numbers **25**
2.1. The natural numbers 25
2.2. The integers 30
2.3. The rational numbers 32
2.4. Other numbers 33

3. Divisibility **36**
3.1. Division 36
3.2. Congruence 37
3.3. Greatest common divisors 41
3.4. Least common multiples 44
3.5. The Euclidean algorithm 46
3.6. The Hundred Fowls Problem 49

4. Prime numbers **51**
4.1. The Fundamental Theorem of Arithmetic 51
4.2. Irreducibility 53
4.3. The Sieve of Eratosthenes 54
4.4. The infinity of primes 57
4.5. Bertrand's Postulate 59

5. Computations with congruences **64**
5.1. Exponentiation 64
5.2. Inversion 64
5.3. Chinese remainder problems 66

6. Powers of two **69**
6.1. Perfect numbers 69
6.2. Mersenne primes 70

7. Prime moduli **72**
7.1. Fermat's Theorem . . . 72
7.2. Carmichael numbers . . . 75
7.3. Wilson's Theorem . . . 77

8. Arithmetic functions **84**
8.1. Multiplicative functions . . . 84
8.2. The Möbius function . . . 87
8.3. Convolution . . . 89

9. Arbitrary moduli **93**
9.1. The Chinese Remainder Theorem . . . 93
9.2. Euler's Theorem . . . 95
9.3. Gauss's Theorem . . . 97

10. Primitive roots **102**
10.1. Order . . . 102
10.2. Groups . . . 106
10.3. Primitive roots of primes . . . 107
10.4. Discrete logarithms . . . 109
10.5. Composite numbers with primitive roots . . . 113

11. Quadratic reciprocity **118**
11.1. Quadratic equations . . . 118
11.2. Quadratic residues . . . 120
11.3. The Legendre symbol . . . 121
11.4. Gauss's Lemma . . . 124
11.5. The Law of Quadratic Reciprocity . . . 127
11.6. Composite moduli . . . 131

12. Sums of squares **135**

A. Foundations **139**
A.1. Construction of the natural numbers . . . 139
A.2. Why it matters . . . 142

B. Some theorems without their proofs **144**

C. Exercises **145**

D. 2007–8 examinations **156**
D.1. In-term examination . . . 156
D.2. In-term examination . . . 162

D.3. In-term examination 168
D.4. Final Examination 173

E. 2010–1 examinations **178**
E.1. In-term examination 178
E.2. In-term examination 182
E.3. Final examination 187

Bibliography **190**

Index **194**

List of Figures

1.1. Triangular numbers 11
1.2. A pair of equal triangular numbers 12
1.3. A pair of consecutive triangular numbers 12
1.4. Consecutive odd numbers 13
1.5. Consecutive odd numbers, without one 14
1.6. Consecutive even numbers 14
1.7. Partitions of circles by straight lines 17
1.8. Incommensurability of diagonal and side 21

3.1. Divisors of 60 38
3.2. Common divisors of 12 and 30 41
3.3. Divisors of 60, again 44
3.4. gcd and lcm 46
3.5. The Euclidean algorithm 46
3.6. Diagonal and side 48

7.1. The integers *modulo* 13, or $\mathbb{Z}_{13}$ 74

11.1. Two ways of counting, for the Law of Quadratic Reciprocity 129
11.2. Example of the proof of quadratic reciprocity 129

List of Tables

1.1. The number 9 as the sum of odd numbers of summands 17
1.2. The number 11 as the sum of odd numbers of summands 18
1.3. Pascal's Triangle 19

4.1. The Sieve of Eratosthenes 55
4.2. Composite numbers less than 1369 with least prime factor 17 or more 57

6.1. Mersenne primes and perfect numbers 71

7.1. Successive differences of powers 78
7.2. The inductive step for $\Delta^n f(x)$ 83

9.1. Exponentiation *modulo* 1000 97
9.2. Numbers according to gcd with 16, 18, and 21 99

10.1. Orders *modulo* 19 105
10.2. Powers of 3 *modulo* 17 110

11.1. Computation of (365/941) 130

D.1. Powers of 3 *modulo* 257 174

Preface

This book started out as a record of my lectures in the course called Elementary Number Theory I (Math 365) at Middle East Technical University in Ankara in 2007–8. When I was to teach the same course in 2010–1, I revised my lecture-notes and made them the official text for the course. That text, dated September 29, 2011, was 139 pages long. After the course, filled with enthusiasm, I made many revisions and additions. The result is this book.

The standard text for Math 356 at METU was Burton's *Elementary Number Theory* [7]. My lectures of 2007–8 more or less followed this. The catalogue description of the course was:

> Divisibility, congruences, Euler, Chinese Remainder and Wilson's Theorems. Arithmetical functions. Primitive roots. Quadratic residues and quadratic reciprocity. Diophantine equations.

In 2010–1, without realizing that *I* had written the course textbook, one student complained that it was hard to read. I am glad he felt free to criticize. But I had not aimed to create a textbook that could replace classroom lectures. I had written summarily, without trying to give all of the explanations that anybody could possibly want.

Among the many changes I have made since the 2010–1 course, I have:

1) put proofs of theorems *after* their statements, and not before as is sometimes natural in lectures (an omitted proof in the present text is left to the reader as an exercise);
2) removed the Fermat factorization method [7, §5.4] as being out of the main stream of the course;
3) added Dirichlet convolution, which gives a streamlined way of understanding Möbius inversion *and* of defining the phi-function;
4) added forward references, to show better how everything is interconnected;
5) added citations for the theorems, when I have been able to find them.

Precisely because these changes are significant, the book must still be considered as a work in progress, a rough draft.

As I suggested, Burton's text was the original model for this book,—but not in style, only in arrangement of topics. Models for style, as well as sources of content, include the sparer texts of Landau [25] and Hardy and Wright [21]. Much of the mathematics in the present text can be found in Gauss's *Disquisitiones Arithmeticae* [16] of 1801, written when Gauss was the age of many undergraduate students. Some of the mathematics is two thousand years older than Gauss.

I have made some attempt to trace theorems to their origins; but this work is not complete. I prefer to see the primary source myself before attributing a theorem. In this case, I cite the source *near* the theorem itself, possibly in a footnote, and not in some extra section at the end of the chapter. Even when I can find the primary source, usually a secondary source has led me there. The secondary source helps to determine what the primary source *is*. The best history would arise from reading all *possible* primary sources; but I have not done this.

Full names and dates of mathematicians named in the text are generally taken from the MacTutor History of Mathematics archive,[1] or from Wikipedia.

I ask students to learn something of the logical foundations of number theory. Section 2.1 contains an account of these foundations, namely a derivation of basic arithmetic from the so-called Peano Axioms. This section was originally an appendix, but I have decided that it belongs in the main body of text, even if most number theory texts do not have such a section. Chapter 2 is filled out with a summary review of the constructions of the other standard number systems, of integers, rationals, reals, and complex numbers. All of these systems have their place in number theory. Their constructions alone could constitute a course, and I do not expect number theory students as such to go through them all; but students should be aware that the constructions *can* be done, and they themselves can do them.

Readers will already know most of the *results* of Chapter 2. Assuming some of these results, the preceeding Chapter 1 is a general exploration of what *can* be done with numbers and, in some cases, what *has* been done for over two thousand years. The chapter begins with the *visual* display of certain numbers as triangles or squares. Throughout the text, where it makes sense, I try to display the mathematics in pictures or tables, as for example in the account of the Chinese Remainder Theorem in §9.1.

Appendix A begins with the *construction* of the natural numbers by von Neumann's method. This is a part of set theory and is beyond the scope of the course as such, but it is good for everybody to know that the construction can be done. The appendix continues with a discussion of common misunderstandings of foundational matters.

I do not like to quote a theorem without either proving it or being able to expect readers to prove it for themselves. In the original course, I did quote theorems, some recent, without myself knowing the proofs; I have now relegated these to Appendix B.

Appendix C consists of exercises, most of which were made available in installments to the students in the 2007/8 class. I have not incorporated the exercises into the main text. One reason for this is to make it less obvious how the exercises should be done. The position of an exercise in a text is often a hint as to how the

[1] `http://www-gap.dcs.st-and.ac.uk/~history/index.html`

exercise should be done; and yet there are no such hints on examinations. The exercises here are strung together in one numbered sequence. (So, by the way, are the theorems in the main text.)

Appendices D and E contain the examinations given to the 2007–8 and 2010–1 classes, along with my solutions and remarks on students' solutions.

In 2007–8, I treated 0 as a natural number; in 2010–1, I did not. In the present book, I intend to use the symbol $\mathbb{N}$ for the set $\{1, 2, 3, \dots\}$; if a symbol for the set $\{0, 1, 2, \dots\}$ is desired, this symbol can be ω. I have tried to update Appendix D (as well as my original lecture-notes from 2007–8) accordingly.

1. Proving and seeing

1.1. The look of a number

What can we say about the following sequence of numbers?

$$1, 3, 6, 10, 15, 21, 28, \ldots$$

The terms increase by 2, 3, 4, and so on. A related observation is that the numbers in the sequence can be given an appearance, a **look,** as shown in Figure 1.1. In

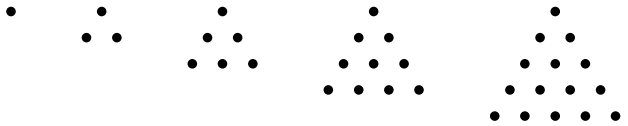


Figure 1.1. Triangular numbers

particular, the numbers are the **triangular numbers.** Let us designate them by t_1, t_2, t_3, and so on. Then they can be given **recursively** by the equations

$$t_1 = 1, \qquad t_{n+1} = t_n + n + 1.$$

This definition can be abbreviated as

$$t_n = \sum_{k=1}^{n} k.$$

The triangular numbers can also be given non-recursively, in **closed form** (so that t_n can be calculated directly):

Theorem 1. *For all numbers n,*

$$t_n = \frac{n(n+1)}{2}. \qquad (*)$$

Proof. We prove the claim $(*)$ for all n by **induction:**

1. The claim is true when $n = 1$.

2. If the claim is true when $n = k$, so that $t_k = k(k+1)/2$, then

$$\begin{aligned} t_{k+1} &= t_k + k + 1 \\ &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+2)(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

so the claim is true when $n = k + 1$.

By induction then, $(*)$ is true for all n. □

So equation $(*)$ *is* true; but we might ask further: *why* is it true? One answer can be seen in a picture. First rewrite $(*)$ as

$$2t_n = n(n+1).$$

Two copies of t_n do indeed fit together to make an $n \times (n+1)$ array of dots, as

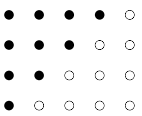


Figure 1.2. A pair of equal triangular numbers

in Figure 1.2. One may establish other identities in the same way. For example,

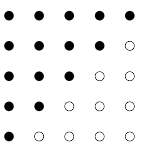


Figure 1.3. A pair of consecutive triangular numbers

Figure 1.3 suggests the next theorem.[1]

[1] The theorem is mentioned by Nicomachus of Gerasa (c. 60–c. 120) in his *Introduction to Arithmetic* [28, II.XII.1–2, p. 247]. For him, the picture alone seems to have been sufficient proof. (Gerasa is now Jerash, in Jordan.)

Theorem 2. *For all numbers n,*

$$t_{n+1} + t_n = (n+1)^2.$$

Proof. Just compute:

$$t_{n+1} + t_n = \frac{(n+1)(n+2)}{2} + \frac{n(n+1)}{2} = \frac{n+1}{2}(n+2+n) = (n+1)^2. \quad \square$$

What can we say about the following sequence?

$$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, \ldots$$

It is the sequence of odd numbers. Also, the first n terms seem to add up to n^2. Indeed we do have:

Theorem 3. *For all numbers n,*

$$\sum_{k=1}^{n} (2k-1) = n^2. \qquad (\dagger)$$

Proof. We use induction.

1. The claim is true when $n = 1$.
2. If the claim is true when $n = k$, then

$$\sum_{j=1}^{k+1} (2j-1) = \sum_{j=1}^{k} (2j-1) + 2k + 1 = k^2 + 2k + 1 = (k+1)^2,$$

so the claim is true when $n = k + 1$.

Therefore (†) is true for all n. $\square$

Figure 1.4 shows why the theorem is true. The point here is that, once a

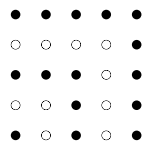


Figure 1.4. Consecutive odd numbers

numerical sequence is defined recursively, then identities involving the sequence can be *proved* by induction; but the identities will probably be first *discovered* in other ways, possibly through pictures.

Figure 1.5. Consecutive odd numbers, without one

From figure 1.4, we may derive two more observations.[2] The rearrangement shown in Figure 1.5 suggests the identity

$$n^2 - 1 = (n+1)(n-1),$$

while Figure 1.6 suggests

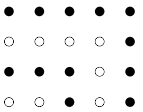


Figure 1.6. Consecutive even numbers

$$\sum_{k=1}^{n} 2k = n(n+1).$$

Observe finally:

$$1, \underbrace{3,5}_{8}, \underbrace{7,9,11}_{27}, \underbrace{13,15,17,19}_{64}, \underbrace{21,23,25,27,29}_{125}, \ldots$$

Does the pattern continue? As an exercise, write the suggested equation,

$$n^3 = \sum_{\cdots}^{\cdots} \cdots,$$

[2]These observations are suggested by two possible interpretations of a passage in Aristotle's *Physics.* In *A History of Greek Mathematics* [22, p. 77], Thomas Heath asserts that Aristotle (384–322) alludes to Figure 1.4 in that passage. Here is Apostol's translation of the passage [2, Γ 4]: 'Moreover, the Pythagoreans posit the infinite as being the *Even;* for they say that it is this which, when cut off and limited by the *Odd,* provides [as matter] for the infinity of things. A sign of this, they say, is what happens to numbers; for if gnomons are placed around the one and apart, in the latter case the form produced is always distinct, but in the former it is unique.' Here a *gnomon* is apparently a figure in the shape of the letter L (the word originally refers to the part of a sundial whose shadow shows the time). So Figure 1.4 results from placing gnomons around one dot. If we then remove the dot, we get Figure 1.5; if we start with two dots rather than one, we get Figure 1.6.

A few centuries later, Theon of Smyrna (c. 70–c. 135) states Theorem 3 in his *Mathematics useful for understanding Plato* [35, pp. 52–55]. (Smyrna is today's İzmir.)

and prove it.[3]

1.2. Patterns that fail

The following passage from V. I. Arnol′d's talk 'On the teaching of mathematics' [4] seems to provide a reasonable description of how mathematics (and in particular number theory) is done.[4]

> Mathematics is a part of physics. Physics is an experimental science, a part of natural science. Mathematics is the part of physics where experiments are cheap...
>
> The scheme of construction of a mathematical theory is exactly the same as that in any other natural science. First we consider some objects and make some observations in special cases. Then we try and find the limits of application of our observations, look for counter-examples which would prevent unjustified extension of our observations onto a too wide range of events (example: the number of partitions of consecutive odd numbers 1, 3, 5, 7, 9 into an odd number of natural summands gives the sequence 1, 2, 4, 8, 16, but then comes 29).
>
> As a result we formulate the empirical discovery that we made (for example, the Fermat conjecture or Poincaré conjecture) as clearly as possible. After this there comes the difficult period of checking as to how reliable are the conclusions.
>
> At this point a special technique has been developed in mathematics. This technique, when applied to the real world, is sometimes useful, but can sometimes also lead to self-deception. This technique is called modelling. When constructing a model, the following idealisation is made: certain facts which are only known with a certain degree of probability or with a certain degree of accuracy, are considered to be 'absolutely' correct and are accepted as 'axioms'. The sense of this 'absoluteness' lies precisely in the fact that we allow ourselves to use these 'facts' according to the rules of formal logic, in the process declaring as 'theorems' all that we can derive from them.

Arnol′d's parenthetical example is apparently the following. For each number n, we consider the number of ways to write the odd number $2n-1$ as a sum

$$t_1 + \cdots + t_{2k-1},$$

where k is an arbitrary number (so that $2k-1$ is an arbitrary odd number), but $t_1 \geqslant \cdots \geqslant t_{2k-1}$. Let us call the number of such sums a_n. Immediately $a_1 = 1$;

[3] This theorem too was apparently known to Nicomachus [28, II.XX.5, p. 263].

[4] A footnote explains the origin of the text: 'This is an extended text of an address at a discussion on the teaching of mathematics in Palais de Découverte in Paris on 7 March 1997.' The text is on line at `http://pauli.uni-muenster.de/~munsteg/arnold.html` (accessed November 14, 2010). I do not actually agree that mathematics is a part of physics.

and since

$$3 = 1 + 1 + 1, \qquad 5 = 3 + 1 + 1 = 2 + 2 + 1 = 1 + 1 + 1 + 1 + 1,$$

we have $a_2 = 2$ and $a_3 = 4$. To find a_4, we note

$$\begin{aligned} 7 &= 3 + 2 + 2 \\ &= 5 + 1 + 1 & &= 3 + 1 + 1 + 1 + 1 \\ &= 4 + 2 + 1 & &= 2 + 2 + 1 + 1 + 1 \\ &= 3 + 3 + 1 & &= 1 + 1 + 1 + 1 + 1 + 1 + 1, \end{aligned}$$

so $a_4 = 8$; and $a_5 = 16$, by the computations in Table 1.1 below. Thus the equation

$$a_n = 2^{n-1} \tag{‡}$$

is correct when n is 1, 2, 3, 4, or 5. However, there is no obvious reason why it should be true when $n > 5$. In fact it *fails* when $n = 6$. We have $a_6 = 29$, by counting the sums listed in Table 1.2. If one is so inclined, one can find further information on these numbers a_n in the *The On-Line Encyclopedia of Integer Sequences*.[5]

Another failed pattern is shown in Chapter 3, 'Proofs', of Timothy Gowers's *Mathematics: A Very Short Introduction* [18]. Suppose n distinct points are chosen on a circle, and each pair of the n points are connected by a straight line, and no three of those straight lines have a common point. Then the circle is divided into a number of regions, say a_n regions. Figure 1.7 shows that (‡) now holds when n is one of the numbers 1, 2, 3, 4, and 5; but when $n = 0$, then there is 1 region, not 1/2; and when $n = 6$, there are 31 regions, not 32.

Is there a formula for the number a_n here? When we add a new point, so that there are $n + 1$ points in all, then the new point will be connected to n other points. Suppose we number those n points with the numbers from 1 to n inclusive. Then the line going to point j has $j - 1$ points on one side, and $n - j$ on the other, so it crosses $(j - 1)(n - j)$ lines. So this new line is divided into $(j-1)(n-j)+1$ segments, and each of these corresponds to a new region. Thus

$$a_1 = 1, \qquad a_{n+1} = a_n + \sum_{j=1}^{n} \big((j-1)(n-j)+1\big);$$

this is a recursive definition of the numbers a_n, but it is perhaps not a very attractive definition. We can rewrite the last equation as

$$a_{n+1} = a_n + n + \sum_{j=2}^{n-1} (j-1)(n-j).$$

[5] `http://oeis.org/`, accessed November 14, 2010.

9	$= 4+2+1+1+1$
$= 7+1+1$	$= 3+3+3$
$= 6+2+1$	$= 3+3+1+1+1$
$= 5+3+1$	$= 3+2+2+1+1$
$= 5+2+2$	$= 3+1+1+1+1+1+1$
$= 5+1+1+1+1$	$= 2+2+2+2+1$
$= 4+4+1$	$= 2+2+1+1+1+1+1$
$= 4+3+2$	$= 1+1+1+1+1+1+1+1+1$

Table 1.1. The number 9 as the sum of odd numbers of summands

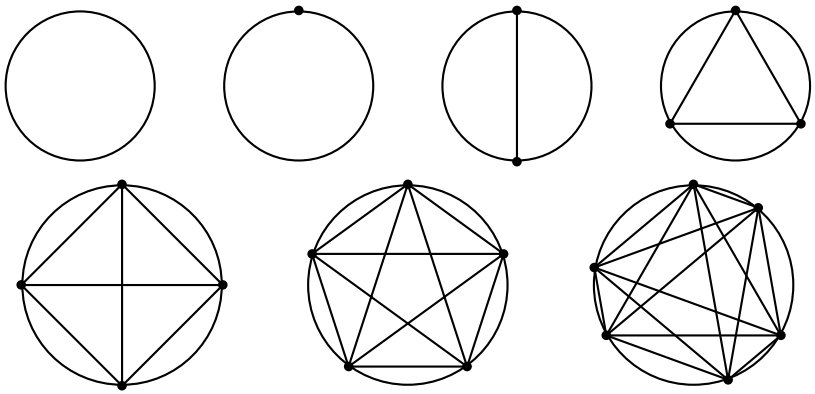


Figure 1.7. Partitions of circles by straight lines

$11 = 9 + 1 + 1$	$= 4 + 4 + 3$
$= 8 + 2 + 1$	$= 4 + 4 + 1 + 1 + 1$
$= 7 + 3 + 1$	$= 4 + 3 + 2 + 1 + 1$
$= 7 + 2 + 2$	$= 4 + 2 + 2 + 2 + 1$
$= 7 + 1 + 1 + 1 + 1$	$= 4 + 2 + 1 + 1 + 1 + 1 + 1$
$= 6 + 4 + 1$	$= 3 + 3 + 3 + 1 + 1$
$= 6 + 3 + 2$	$= 3 + 3 + 2 + 2 + 1$
$= 6 + 2 + 1 + 1 + 1$	$= 3 + 3 + 1 + 1 + 1 + 1 + 1$
$= 5 + 5 + 1$	$= 3 + 2 + 2 + 2 + 2$
$= 5 + 4 + 2$	$= 3 + 2 + 2 + 1 + 1 + 1 + 1$
$= 5 + 3 + 3$	$= 3 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$
$= 5 + 3 + 1 + 1 + 1$	$= 2 + 2 + 2 + 2 + 2 + 1$
$= 5 + 2 + 2 + 1 + 1$	$= 2 + 2 + 2 + 1 + 1 + 1 + 1 + 1$
$= 5 + 1 + 1 + 1 + 1 + 1 + 1$	$= 2 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1.$

Table 1.2. The number 11 as the sum of odd numbers of summands

The sum $\sum_{j=2}^{n-1}(j-1)(n-j)$ can be understood as the number of ways to choose 3 points out of n points. Indeed, if the points are again numbered from 1 to n inclusive, then for each j, there are $(j-1)(n-j)$ ways to choose i and k so that $i < j < k \leqslant n$. Therefore we have

$$a_{n+1} = a_n + n + \binom{n}{3} = a_n + \binom{n}{1} + \binom{n}{3}.$$

Recall that in the so-called Pascal's Triangle (Table 1.3) if we start counting with 0, then entry i in row j is $\binom{j}{i}$; in particular, $\binom{j}{i} + \binom{j}{i+1} = \binom{j+1}{i+1}$. Hence we have

$$a_{n+1} = a_n + \binom{n-1}{0} + \binom{n-1}{1} + \binom{n-1}{2} + \binom{n-1}{3}.$$

Then by induction,

$$a_n = \binom{n-1}{0} + \binom{n-1}{1} + \binom{n-1}{2} + \binom{n-1}{3} + \binom{n-1}{4}.$$

Here we should understand $\binom{n-1}{j} = 0$ if $n-1 < j$.

For an alternative derivation of the last formula for a_n, we can consider the following.

1. Even if there are no points, there is 1 region.
2. When a new line is drawn, one new region is created near one endpoint of the new line; and there are $\binom{n}{2}$ lines.
3. In addition, whenever the new line crosses an old line, a new region is created; and there are $\binom{n}{4}$ crossings.
4. Every region can be understood as arising in exactly one of the foregoing ways.

								1												
							1		1											
						1		2		1										
					1		3		3		1									
				1		4		6		4		1								
			1		5		10		10		5		1							
		1		6		15		20		15		6		1						
	1		7		21		35		35		20		7		1					
. . . . .																				

Table 1.3. Pascal's Triangle

Therefore, again,

$$a_n = 1 + \binom{n}{2} + \binom{n}{4} = \binom{n}{0} + \binom{n}{2} + \binom{n}{4} = \sum_{j=0}^{4} \binom{n-1}{4}.$$

1.3. Incommensurability

A **Diophantine equation**[6] is a polynomial equation with integral coefficients. If such a solution has no *integral* solutions, way to prove this is the method of **infinite descent,** which is attributed to Pierre de Fermat (1601–65).[7] A simple application of the method is the following.

Theorem 4. *No integers solve the equation*

$$x^2 = 2y^2.$$

Proof. Suppose $a^2 = 2b^2$, and a and b are positive. Then $a > b$. Also, a must be even. Say $a = 2c$. Consequently $4c^2 = 2b^2$, so $b^2 = 2c^2$. Thus we obtain a sequence

$$a, b, c, \ldots, k, \ell, \ldots,$$

where always $k^2 = 2\ell^2$. But we have also $a > b > c > \cdots$, which is absurd; there is no infinite descending sequence of positive integers. Therefore no positive a and b exist such that $a^2 = 2b^2$. □

In geometric form, the theorem is that the side and diagonal of a square are **incommensurable:** there is no one line segment that **measures,** or evenly

[6] So called after Diophantus of Alexandria (c. 200–c. 284), whose *Arithmetica,* comprising 13 books, treated such problems as, 'To divide a given square number into two squares' [37, pp.550–553]. Diophantus works out an example when the given square number is 16. The aim then is to find x such that $16 - x^2$ is a square. We try letting this square have the form $(mx - 4)^2$, presumably so that 16 will cancel from the resulting equation. In case $m = 2$, we solve

$$\begin{aligned} 16 - x^2 &= (2x - 4)^2 \\ &= 4x^2 - 16x + 16, \end{aligned} \qquad 16x = 5x^2, \qquad \frac{16}{5} = x,$$

so that $16 = (16/5)^2 + (12/5)^2$. Thus Diophantus is interested in *rational* solutions: in the present example, solutions to the equation $x^2 + y^2 = z^2$. It was in the margin next to this problem, in his own copy of the *Arithmetica,* that Fermat (see below) wrote the claim that $x^n + y^n = z^n$ has no [rational] solution when $n > 2$. This claim is the so-called *Fermat's Last Theorem,* although Fermat did not publish a proof, and he almost certainly did not know a correct proof.

[7] In his *History of Mathematics* [5, §XVII.16, p. 387], Boyer writes: 'Some of his theorems he [Fermat] proved by a method that he called his "infinite descent"—a sort of inverted mathematical induction, a process that Fermat was among the first to use.'

divides, each of them. We can see this as follows, using propositions from Euclid's *Elements* [13].[8] In Figure 1.8, there is a square, $ABCD$ (constructed by I.46).

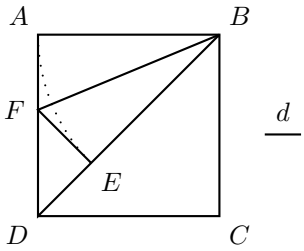


Figure 1.8. Incommensurability of diagonal and side

On the diagonal BD, the distance BE is marked equal to AB (as by drawing a circle with center B, passing through A). The perpendicular at E (constructed by I.11) meets AD at F. The straight line BF is drawn. Then triangles ABF and EBF are congruent, and in particular $EF = AF$ (by I.4, I.16, and I.32). Also, triangle DEF is similar to DAB (by VI.4, since angle DEF is equal to angle DAB, and angle EDB is common), so $DE = EF$. Suppose a straight line G measures both AB and BD. Then it measures ED and DF, since

$$ED = BD - AB, \qquad DF = AB - ED.$$

The same construction can be performed with triangle DEF in place of DAB. Since $DE < DF$ (by I.19 and I.32), so that $2ED < AB$, there will eventually be segments that are shorter than G (by X.1), but are measured by it, which is absurd. So such G cannot exist.

If we consider DA as a unit, then we can write DB as $\sqrt{2}$. In two ways then, we have shown then the **irrationality** of $\sqrt{2}$. For yet another proof, suppose $\sqrt{2}$ *is* rational. Then there are numbers a_1 and a_2 such that

$$\frac{a_1}{a_2} = \sqrt{2} + 1.$$

Consequently

$$\frac{a_2}{a_1} = \frac{1}{\sqrt{2}+1} = \frac{\sqrt{2}-1}{(\sqrt{2}+1)(\sqrt{2}-1)} = \sqrt{2} - 1 = \frac{a_1}{a_2} - 2 = \frac{a_1 - 2a_2}{a_2}.$$

Now let $a_3 = a_1 - 2a_2$, so that

$$\frac{a_2}{a_1} = \frac{a_3}{a_2}.$$

[8] The method is discussed in Heath's edition of the *Elements* [12, v. III, p. 19].

Continue recursively by defining

$$a_{n+2} = a_n - 2a_{n+1}.$$

Then by induction

$$\frac{a_{n+1}}{a_{n+2}} = \frac{a_1}{a_2} = \sqrt{2} + 1.$$

But $a_n = 2a_{n+1} + a_{n+2}$, so $a_1 > a_2 > a_3 > \cdots$, which again is absurd.

The same argument, adjusted, gives us a way to *approximate* $\sqrt{2}$. Suppose there are b_1 and b_2 such that

$$\frac{b_1}{b_2} = \sqrt{2} - 1.$$

Then

$$\frac{b_2}{b_1} = \sqrt{2} + 1 = \frac{b_1}{b_2} + 2 = \frac{b_1 + 2b_2}{b_2}.$$

If we define

$$b_{n+2} = b_n + 2b_{n+1}, \tag{§}$$

then by induction

$$\frac{b_{n+1}}{b_{n+2}} = \sqrt{2} - 1.$$

Now however the sequence $b_1, b_2, \ldots$, increases, so there is no obvious contradiction. But the definition (§) alone yields

$$\begin{aligned}
\frac{b_3}{b_2} &= 2 + \frac{b_1}{b_2}, \\
\frac{b_4}{b_3} &= 2 + \frac{b_2}{b_3} = 2 + \frac{1}{2 + \dfrac{b_1}{b_2}}, \\
\frac{b_5}{b_4} &= 2 + \frac{b_3}{b_4} = 2 + \frac{1}{2 + \dfrac{b_2}{b_3}} = 2 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{b_1}{b_2}}},
\end{aligned}$$

and so on. If we just let $b_1 = 1$ and $b_2 = 2$, then by (§) we sequence of the b_n is the increasing sequence

$$1, 2, 5, 12, 29, 70, \ldots$$

Then the sequence

$$\frac{2}{1}, \frac{5}{2}, \frac{12}{5}, \frac{29}{12}, \frac{70}{29}, \ldots$$

of fractions converges to $\sqrt{2} + 1$. That is, we have the following.

Theorem 5. *When the sequence b_1, b_2, ..., is defined recursively by*

$$b_1 = 1, \qquad b_2 = 2, \qquad b_{n+2} = b_n + 2b_{n+1},$$

then

$$\lim_{n\to\infty} \frac{b_{n+1}}{b_n} = \sqrt{2} + 1. \tag{¶}$$

Proof. Considering successive differences, we have

$$\frac{b_{n+2}}{b_{n+1}} - \frac{b_{n+1}}{b_n} = 2 + \frac{b_n}{b_{n+1}} - \frac{b_{n+1}}{b_n} = \frac{{b_n}^2 + 2b_n b_{n+1} - {b_{n+1}}^2}{b_n b_{n+1}}.$$

Replacing n with $n+1$ gives

$$\begin{aligned}
\frac{b_{n+3}}{b_{n+2}} - \frac{b_{n+2}}{b_{n+1}} &= \frac{{b_{n+1}}^2 + 2b_{n+1}b_{n+2} - {b_{n+2}}^2}{b_{n+1}b_{n+2}} \\
&= \frac{{b_{n+1}}^2 + 2b_{n+1}(2b_{n+1} + b_n) - (2b_{n+1} + b_n)^2}{b_{n+1}b_{n+2}} \\
&= -\frac{{b_n}^2 + 2b_n b_{n+1} - {b_{n+1}}^2}{b_{n+1}b_{n+2}} \\
&= -\Big(\frac{b_{n+2}}{b_{n+1}} - \frac{b_{n+1}}{b_n}\Big).
\end{aligned}$$

By induction then,

$$\frac{b_{n+2}}{b_{n+1}} - \frac{b_{n+1}}{b_n} = \frac{(-1)^{n+1}}{b_n b_{n+1}}, \tag{‖}$$

since this holds when $n = 1$. The sequence of products $b_n b_{n+1}$ is positive an strictly increasing; so we have

$$\begin{gathered}
\frac{b_2}{b_1} < \frac{b_3}{b_1}, \\
\frac{b_2}{b_1} < \frac{b_4}{b_3} < \frac{b_3}{b_1}, \\
\frac{b_2}{b_1} < \frac{b_4}{b_3} < \frac{b_5}{b_4} < \frac{b_3}{b_1}, \\
\frac{b_2}{b_1} < \frac{b_4}{b_3} < \frac{b_6}{b_5} < \frac{b_5}{b_4} < \frac{b_3}{b_1},
\end{gathered}$$

and in general

$$\frac{b_2}{b_1} < \frac{b_4}{b_3} < \frac{b_6}{b_5} < \cdots < \frac{b_7}{b_6} < \frac{b_5}{b_4} < \frac{b_3}{b_1}.$$

A consequence of this and (‖) is that the sequence of fractions b_{n+1}/b_n must be a *Cauchy sequence*. The limit is $\sqrt{2}+1$, since

$$\begin{aligned}
\frac{b_{n+2}}{b_{n+1}} < \sqrt{2}+1 &\iff \left(\frac{b_{n+2}}{b_{n+1}} - 1\right)^2 < 2 \\
&\iff \left(\frac{b_n}{b_{n+1}} + 1\right)^2 < 2 \\
&\iff \frac{b_n}{b_{n+1}} < \sqrt{2}-1 \\
&\iff \frac{b_{n+1}}{b_n} > \sqrt{2}+1.
\end{aligned}$$

□

The limit equation (¶) is written more suggestively as

$$\sqrt{2}+1 = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}}.$$

2. Numbers

2.1. The natural numbers

Theorems about natural numbers have been known for thousands of years. Some of these theorems come down to us in Euclid's *Elements* [13], for example, or Nicomachus's *Introduction to Arithmetic* [28], which were referred to in the last chapter. Certain underlying assumptions on which the proofs of these theorems are based were apparently not worked out until more recent centuries.

It turns out that all theorems about the natural numbers are logical consequences of the Axiom below. The Axiom lists five conditions that the natural numbers meet. Richard Dedekind published these conditions in 1888 [9, II, §71, p. 67]. In 1889, Giuseppe Peano [29, §1, p. 94] repeated them in a more symbolic form, along with some logical conditions, making nine conditions in all, which he called axioms. Of these, the five specifically number-theoretic conditions have come to be known as the **Peano Axioms.**

The foundations of number-theory are often not well understood, even today. Some books give the impression that all theorems about natural numbers follow from the so-called 'Well Ordering Principle' (Theorem 15). Others suggest that the possibility of definition by recursion (Theorem 6) can be proved by induction (part (e) of the Axiom) alone. These are mistakes about the foundations of number-theory. They are perhaps not really mistakes about number-theory itself; still, they are mistakes, and it is better not to make them. This is a reason why I have written this chapter.

An admirable development of the material in this chapter and more is found in Edmund Landau's book *Foundations of Analysis: The Arithmetic of Whole, Rational, Irrational, and Complex Numbers: A Supplement to Text-Books on the Differential and Integral Calculus* [26].

In the present chapter, *when proofs of lemmas and theorems here are not supplied, I have left them to the reader as exercises.*

An expression like '$f\colon A \to B$' is to be read as the statement 'f is a function from A to B.' This means f is a certain kind of subset of the Cartesian product $A \times B$, namely a subset that, for each a in A, has exactly one element of the form (a, b); then one writes $f(a) = b$. The function f can also be written as $x \mapsto f(x)$.

Axiom and definition. *The set of* ***natural numbers,*** *denoted by*

$$\mathbb{N},$$

meets the following five conditions.

a) *There is a* ***first*** *natural number, called* 1 *(****one****).*
b) *Every* n *in* $\mathbb{N}$ *has a unique* ***successor,*** *denoted (for now) by* $\mathrm{s}(n)$*.*
c) *The first natural number is not a successor: if* $n \in \mathbb{N}$*, then* $\mathrm{s}(n) \neq 1$*.*
d) *Distinct natural numbers have distinct successors: if* $n \in \mathbb{N}$ *and* $m \in \mathbb{N}$ *and* $n \neq m$*, then* $\mathrm{s}(n) \neq \mathrm{s}(m)$*.*
e) *Proof by* ***induction*** *is possible: Suppose* $A \subseteq \mathbb{N}$*, and two conditions are met, namely*
   (i) *the* ***base condition:*** $1 \in A$*, and*
   (ii) *the* ***inductive condition:*** *if* $n \in A$ *(the* ***inductive hypothesis****), then* $\mathrm{s}(n) \in A$*.*

   Then $A = \mathbb{N}$*.*

The natural number $\mathrm{s}(1)$ *is denoted by* 2*; the number* $\mathrm{s}(2)$*, by* 3*; &c.*

Remark. Again, the five conditions satisfied by $\mathbb{N}$ are the *Peano axioms.* Parts (c), (d) and (e) of the axiom are conditions concerning a set with a first element and an operation of succession. For each of those conditions, there is an example of such a set that meets that condition, but not the others. In short, the three conditions are logically independent.

Lemma. *Every natural number is either* 1 *or a successor.*

Proof. Let A be the set comprising every natural number that is either 1 or a successor. In particular, $1 \in A$, and if $n \in A$, then (since it is a successor) $\mathrm{s}(n) \in A$. Therefore, by induction, $A = \mathbb{N}$. □

Theorem 6 (Recursion)**.** *Suppose a set* A *has an element* b*, and* $f\colon A \to A$*. Then there is a* unique *function* g *from* $\mathbb{N}$ *to* A *such that*
a) $g(1) = b$*, and*
b) $g(\mathrm{s}(n)) = f(g(n))$ *for all* n *in* $\mathbb{N}$*.*

Proof. The following is only a sketch. One must prove existence and uniqueness of g. Assuming existence, one can prove uniqueness by induction. To prove existence, let $\mathcal{S}$ be the set of subsets R of $\mathbb{N} \times A$ such that
a) if $(1, c) \in R$, then $c = b$;
b) if $(\mathrm{s}(n), c) \in R$, then $(n, d) \in R$ for some d such that $f(d) = c$.

Then $\bigcup \mathcal{S}$ is the desired function g. □

Remark. In its statement (though not the proof), the Recursion Theorem assumes only parts (a) and (b) of the Axiom. The other parts can be proved as consequences of the Theorem. Recursion is a method of *definition;* induction is a method of *proof.* There are sets (with first elements and successor-operations) that allow proof by induction, but not definition by recursion. In short, induction is logically weaker than recursion.

Definition (Addition)**.** For each m in $\mathbb{N}$, the operation $x \mapsto m + x$ on $\mathbb{N}$ is the function g guaranteed by the Recursion Theorem when A is $\mathbb{N}$ and b is m and f is $x \mapsto \mathrm{s}(x)$. That is,

$$m + 1 = \mathrm{s}(m), \qquad\qquad m + \mathrm{s}(n) = \mathrm{s}(m + n).$$

Lemma. *For all n and m in $\mathbb{N}$,*
a) $1 + n = \mathrm{s}(n)$*;*
b) $\mathrm{s}(m) + n = \mathrm{s}(m + n)$.

Theorem 7. *For all n, m, and k in $\mathbb{N}$,*
a) $n + m = m + n$*;*
b) $(n + m) + k = n + (m + k)$*;*

Remark. It is possible to prove by induction alone that there is a unique operation of addition satisfying the definition and Theorem 7.

Definition (Multiplication)**.** For each m in $\mathbb{N}$, the operation $x \mapsto m \cdot x$ on $\mathbb{N}$ is the function g guaranteed by the Recursion Theorem when A is $\mathbb{N}$ and b is 1 and f is $x \mapsto x + m$. That is,

$$m \cdot 1 = m, \qquad\qquad m \cdot (n + 1) = m \cdot n + m.$$

Lemma. *For all n and m in $\mathbb{N}$,*
a) $1 \cdot n = n$*;*
b) $(m + 1) \cdot n = m \cdot n + n$.

Theorem 8. *For all n, m, and k in $\mathbb{N}$,*
a) $n \cdot m = m \cdot n$*;*
b) $n \cdot (m + k) = n \cdot m + n \cdot k$*;*
c) $(n \cdot m) \cdot k = n \cdot (m \cdot k)$*;*

Remark. As with addition, so with multiplication, one can prove by induction alone that there is a unique operation satisfying the definition and Theorem 8. However, the next theorem requires also parts (c)–(d) of the Axiom.

Theorem 9 (Cancellation)**.** *For all n, m, and k in $\mathbb{N}$,*
a) *if $n + k = m + k$, then $n = m$;*
b) *if $n \cdot k = m \cdot k$, then $n = m$.*

Definition (Exponentiation)**.** For each m in $\mathbb{N}$, the operation $x \mapsto m^x$ on $\mathbb{N}$ is the function g guaranteed by the Recursion Theorem when A is $\mathbb{N}$ and b is m and f is $x \mapsto x \cdot m$. That is,

$$m^1 = m, \qquad\qquad m^{n+1} = m^n \cdot m.$$

Theorem 10. *For all n, m, and k in $\mathbb{N}$,*
a) $n^{m+k} = n^m \cdot n^k$;
b) $(n \cdot m)^k = n^k \cdot m^k$;
c) $(n^m)^k = n^{m \cdot k}$.

Remark. In contrast with addition and multiplication, exponentiation requires more than induction for its existence.

Definition (Ordering)**.** If $n, m \in \mathbb{N}$, and $m + k = n$ for some k in $\mathbb{N}$, then this situation is denoted by $m < n$. That is,

$$m < n \iff \exists x\, m + x = n.$$

If $m < n$, we say that m is a **predecessor** of n. If $m < n$ or $m = n$, we write

$$m \leqslant n.$$

Theorem 11. *For all n, m, and k in $\mathbb{N}$,*
a) $1 \leqslant n$;
b) $m \leqslant n$ *if and only if* $m + k \leqslant n + k$;
c) $m \leqslant n$ *if and only if* $m \cdot k \leqslant n \cdot k$.

Theorem 12. *For all m and n in $\mathbb{N}$,*
a) $m < n$ *if and only if* $m + 1 \leqslant n$;
b) $m \leqslant n$ *if and only if* $m < n + 1$.

Theorem 13. *The binary relation leq is a* ***linear ordering:*** *for all n, m, and k in $\mathbb{N}$,*
a) $n \leqslant n$;
b) *if* $m \leqslant n$ *and* $n \leqslant m$, *then* $n = m$;
c) *if* $k \leqslant m$ *and* $m \leqslant n$, *then* $k \leqslant n$;
d) *either* $m \leqslant n$ *or* $n \leqslant m$.

We may say then that $<$ is a **strict linear ordering,** because

$$n \not< n,$$
$$k < m \ \&\ m < n \implies k < n,$$
$$m \not< n \ \&\ m \neq n \implies n < m.$$

Theorem 14 (Strong Induction)**.** *Suppose $A \subseteq \mathbb{N}$, and one condition is met, namely*

- *if all predecessors of n belong to A (the* ***strong inductive hypothesis****), then $n \in A$.*

Then $A = \mathbb{N}$.

Proof. Let B comprise the natural numbers whose predecessors belong to A. As 1 has no predecessors, they belong to A, so $1 \in B$. Suppose $n \in B$. Then all predecessors of n belong to A, so by assumption, $n \in A$. Thus, by Theorem 12 (b), all of the predecessors of $n+1$ belong to A, so $n+1 \in B$. By induction, $B = \mathbb{N}$. In particular, if $n \in \mathbb{N}$, then $n+1 \in B$, so n (being a predecessor of $n+1$) belongs to A. Thus $A = \mathbb{N}$. □

Remark. In general, strong induction is a proof-technique that can be used with some *ordered* sets. By contrast, 'ordinary' induction involves sets with first elements and successor-operations, but possibly without orderings. Strong induction does not follow from ordinary induction alone; neither does ordinary induction follow from strong induction.

Theorem 15. *The set of natural numbers is* ***well ordered*** *by* $<$*: that is, every non-empty subset of* $\mathbb{N}$ *has a least element with respect to* $\leqslant$.

Proof. Use strong induction. Suppose A is a subset of $\mathbb{N}$ with no least element. We shall show A is empty, that is, $\mathbb{N} \setminus A = \mathbb{N}$. Let $n \in \mathbb{N}$. Then n is not a least element of A. This means one of two things: either $n \notin A$, or else $n \in A$, but also $m \in A$ for some predecessor of n. Equivalently, if no predecessor of n is in A, then $n \notin A$. In other words, if every predecessor of n is in $\mathbb{N} \setminus A$, then $n \in \mathbb{N} \setminus A$. By strong induction, we are done. □

Remark. We have now shown, in effect, that if a linear order $(A, \leqslant)$ admits proof by strong recursion, then it is well-ordered. The converse is also true.

Theorem 16 (Recursion with Parameter)**.** *Suppose* A *is a set with an element* b*, and* $F\colon \mathbb{N} \times A \to A$*. Then there is a* unique *function* G *from* $\mathbb{N}$ *to* A *such that*

a) $G(1) = b$*, and*
b) $G(n+1) = F(n, G(n))$ *for all* n *in* $\mathbb{N}$.

Proof. Let $f\colon \mathbb{N} \times A \to \mathbb{N} \times A$, where $f(n, x) = (n+1, F(n, x))$. By recursion, there is a unique function g from $\mathbb{N}$ to $\mathbb{N} \times A$ such that $g(1) = (1, b)$ and $g(n+1) = f(g(n))$. By induction, the first entry in $g(n)$ is always n. The desired function G is given by $g(n) = (n, G(n))$. Indeed, we now have $G(1) = b$; also, $g(n+1) = f(n, G(n)) = (n+1, F(n, G(n)))$, so $G(n+1) = F(n, G(n))$. By induction, G is unique. □

Remark. Recursion with Parameter allows us to define the set of predecessors of n as $\mathrm{pred}(n)$, where $x \mapsto \mathrm{pred}(x)$ is the function G guaranteed by the Theorem when A is the set of subsets of $\mathbb{N}$, and b is the empty set, and F is $(x, Y) \mapsto \{x\} \cup Y$. Then we can write $m < n$ if $m \in \mathrm{pred}(n)$ and prove the foregoing theorems about the ordering.

Definition (Factorial)**.** The operation $x \mapsto x!$ on $\mathbb{N}$ is the function G guaranteed by the Theorem of Recursion with Parameter when A is $\mathbb{N}$ and b is 1 and F is $(x, y) \mapsto (x + 1) \cdot y$. That is,

$$1! = 1, \qquad (n + 1)! = (n + 1) \cdot n!$$

2.2. The integers

Number theory is fundamentally about the natural numbers, but it is sometimes useful to consider natural numbers simply as **integers.** These compose the set

$$\mathbb{N} \cup \{0\} \cup \{-x \colon x \in \mathbb{N}\}, \tag{$*$}$$

which is denoted by

$$\mathbb{Z}.$$

One may ask what these new elements 0 and $-x$ are. In that case, one can define $\mathbb{Z}$ as the quotient

$$\mathbb{N} \times \mathbb{N}/\!\sim,$$

where $\sim$ is the equivalence relation given by

$$(a, b) \sim (x, y) \iff a + y = b + x.$$

The equivalence class of (a, b) is denoted by

$$a - b.$$

There are three cases:

1. If $a < b$, then $a + c = b$ for some unique c, and
$$a - b = 1 - (c + 1).$$
2. If $a = b$, then
$$a - b = 1 - 1.$$
3. If $b < a$, then $b + c = a$ for some unique c, and
$$a - b = (c + 1) - 1.$$

Then $\mathbb{N}$ embeds in $\mathbb{Z}$ under the the map $x \mapsto (x + 1) - 1$, and one can define

$$0 = 1 - 1, \qquad -((x + 1) - 1) = 1 - (x + 1).$$

One can then identify $\mathbb{N}$ with its image in $\mathbb{Z}$. Then again $\mathbb{Z}$ can be understood as in $(*)$.

We extend multiplication to $\mathbb{Z}$ by defining

$$0 \cdot x = 0, \qquad -x \cdot y - (x \cdot y), \qquad -x \cdot -y = x \cdot y.$$

It is to be understood that multiplication is still to be commutative, so that also $x \cdot 0 = 0$ and $y \cdot -x = -(x \cdot y)$.

We extend the ordering to $\mathbb{Z}$ by defining

$$-x < 0, \qquad 0 < y, \qquad -x < -y \iff y < x.$$

Here of course x and y are elements of $\mathbb{N}$, and the two inequalities $-x < 0$ and $0 < y$ are taken to imply $-x < y$.

Now we can extend addition by defining

$$-x + -y = -(x + y), \qquad -x + y = \begin{cases} z, & \text{if } x < y \text{ and } x + z = y \\ 0, & \text{if } x = y, \\ -z, & \text{if } y < x \text{ and } y + z = x. \end{cases}$$

Finally, we define

$$--x = x.$$

Now one proves the following, where the letters range over $\mathbb{Z}$. First,

$$\begin{aligned} a + (b + c) &= (a + b) + c, \\ b + a &= a + b, \\ a + 0 &= a, \\ a + (-a) &= 0, \end{aligned}$$

so that $\mathbb{Z}$ is an **abelian group** with respect to addition. Next,

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c, \\ a \cdot 1 &= a, \\ 1 \cdot a &= a, && (\dagger) \\ a \cdot (b + c) &= a \cdot b + a \cdot c, \\ (a + b) \cdot c &= a \cdot c + b \cdot c, && (\ddagger) \end{aligned}$$

so $\mathbb{Z}$ is a **ring.** But we need not show (†) and (‡) in particular, because we have finally

$$a \cdot b = b \cdot a,$$

so $\mathbb{Z}$ is a **commutative ring.** Moreover,

$$\begin{aligned} a < b &\implies a + c < b + c, \\ 0 < a \ \&\ 0 < b &\implies 0 < a \cdot b, \end{aligned}$$

so $\mathbb{Z}$ is an **ordered** commutative ring. In particular, if $a \cdot b = 0$, then one of a and b is 0; so $\mathbb{Z}$ is an **integral domain.**

An integer a is called **positive** if $a > 0$, that is, if $a \in \mathbb{N}$; but a is **zero,** if $a = 0$, and a is **negative,** if $a < 0$.

2.3. The rational numbers

It is also useful in number theory to be aware that integers are **rational numbers.** In order to define these precisely, it is useful to begin (as one does in school) with the **positive rational numbers.** These compose the quotient

$$\mathbb{N} \times \mathbb{N}/\approx,$$

where $\approx$ is the equivalence relation defined by

$$(a, b) \approx (x, y) \iff a \cdot y = b \cdot x.$$

The equivalence class of (a, b) is denoted by

$$\frac{a}{b}$$

or a/b. Let us denote the set of positive rational numbers by

$$\mathbb{Q}^+.$$

On this set, one shows that the following are valid definitions:

$$\frac{a}{b} + \frac{x}{y} = \frac{ay + bx}{by}, \qquad \frac{a}{b} \cdot \frac{x}{y} = \frac{ab}{xy}, \qquad \frac{a}{b} < \frac{x}{y} \iff ay < bx.$$

We can also define

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a};$$

then $\mathbb{Q}^+$ is an abelian group with respect to multiplication. One shows that $\mathbb{Z}$ embeds in $\mathbb{Q}^+$ under the map $x \mapsto x/1$. Now we can identify $\mathbb{N}$ with its image in $\mathbb{Q}^+$. Letting letters stand now for positive rationals, we have, just as in $\mathbb{N}$,

$$r < s \iff \exists x \; r + x = s.$$

Now we can obtain the set $\mathbb{Q}$ of **rational numbers** from $\mathbb{Q}^+$ just as we obtained $\mathbb{Z}$ from $\mathbb{N}$ in the last section. In particular, $\mathbb{Q}$ is a commutative ring; it is moreover a **field,** because

$$a \neq 0 \implies \exists x \; ax = 1.$$

Since also $\mathbb{Q}$ is, like $\mathbb{Z}$, an *ordered* commutative ring, $\mathbb{Q}$ is an **ordered field.** Finally, $\mathbb{Z}$ is an ordered commutative sub-ring of this ordered field.

2.4. Other numbers

As a linear order, $\mathbb{Q}$ is **dense,** that is, between any two distinct elements lies a third:

$$a < b \implies \exists x\, (a < x \ \&\ x < b).$$

Moreover, $\mathbb{Q}$ has no **endpoints,** that is, no greatest or least element.

An order is called **complete** if every nonempty subset with an upper bound has a **supremum,** namely a least upper bound. Then $\mathbb{Q}$ is not complete, since the set $\{x\colon 0 < x \ \&\ x^2 < 2\}$ has no supremum.

If a dense linear order without endpoints is given, and a is an element, we can define

$$\mathrm{pred}(a) = \{x\colon x < a\}.$$

The union of any collection of such subsets is an **open** subset of the order.[1] In particular, the whole set and the empty set are open; all other open subsets are called **cuts** of the order. The set of all cuts of the order is the **completion** of the order. The completion is itself linearly ordered by inclusion ($\subseteq$), and the original order embeds in its completion under the map $x \mapsto \mathrm{pred}(x)$. In case the original order is $\mathbb{Q}$, the completion is denoted by

$$\mathbb{R}.$$

This is the set of **real numbers.** The operations on $\mathbb{Q}$ extend to $\mathbb{R}$ in such a way that $\mathbb{R}$ is also an ordered field. then $\mathbb{R}$ is a **complete ordered field,** and every complete ordered field is isomorphic to $\mathbb{R}$.

However, all of this takes quite a bit of work to prove. One approach is to consider first the completion of $\mathbb{Q}^+$. If X and Y are cuts of $\mathbb{Q}^+$, one can define

$$X + Y = \bigcup\{\mathrm{pred}(x+y)\colon\ \mathrm{pred}(x) \subseteq X \ \&\ \mathrm{pred}(y) \subseteq Y\},$$
$$X \cdot Y = \bigcup\{\mathrm{pred}(x\cdot y)\colon\ \mathrm{pred}(x) \subseteq X \ \&\ \mathrm{pred}(y) \subseteq Y\}.$$

Then one can obtain $\mathbb{R}$ from the completion of $\mathbb{Q}^+$, just as one obtains $\mathbb{Z}$ from $\mathbb{N}$, and $\mathbb{Q}$ from $\mathbb{Q}^+$.

Given a commutative ring, we can form 2×2 matrices whose entries are from the ring. These are added and multiplied by the rules

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}.$$

[1] The open sets, so defined, do indeed compose a *topology* for the order, but it is not the usual **order topology.** In the latter, the open sets are unions of sets $\{x\colon a < x \ \&\ x < b\}$.

Then the set of these matrices is a ring, but usually not a commutative ring. We define $\mathbb{C}$ as the set of 2×2 matrices

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}, \tag{§}$$

where x and y range over $\mathbb{R}$. One shows that $\mathbb{C}$ is a field. We identify $\mathbb{R}$ with its image in $\mathbb{C}$ under the map

$$x \mapsto \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix},$$

and we define

$$\mathrm{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then every element of $\mathbb{C}$ is uniquely $x + y\mathrm{i}$ for some x and y in $\mathbb{R}$; moreover, $\mathrm{i}^2 = -1$.

One shows that every positive real number x has a **square root,** namely the positive number $\sqrt{x}$ such that $(\sqrt{x})^2 = x$. Then we define

$$|x + \mathrm{i}y| = \sqrt{(x^2 + y^2)}.$$

The field $\mathbb{C}$ is **complete** in a new sense: every *Cauchy sequence* of complex numbers converges. Recall that a sequence $(a_n : n \in \mathbb{N})$ of complex numbers is a **Cauchy sequence** if for every positive real number ε, there is a positive integer k such that, if $n > k$ and $m > k$, then

$$|a_n - a_m| < \varepsilon.$$

Then $\mathbb{R}$ itself is also complete in this sense.

The field of complex numbers also has the convenient property of being **algebraically closed:** it contains a solution of every polynomial equation

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n = 0, \tag{¶}$$

for every n in $\mathbb{N}$, where of course the coefficients a_k range over $\mathbb{C}$. But there are other algebraically closed fields.

The field $\mathbb{Q}$ is **countable,** that is, there is a bijection between $\mathbb{Q}$ and $\mathbb{N}$. The same is not true for $\mathbb{R}$ or $\mathbb{C}$: they are **uncountable.** If we select from $\mathbb{C}$ the solutions of the equations (¶) such that the coefficients are *rational,* the result is the set of **algebraic numbers.** This set is a countable algebraically closed subfield of $\mathbb{C}$.

Every equation $a + bx = 0$, where a and b are integers and $b \neq 0$, has a solution in $\mathbb{Q}$, namely $-a/b$ (that is, $-ab^{-1}$). In particular, there is a solution when $b = 1$; but then the solution is just $-a$, an integer. More generally, if

the coefficients in (¶) are integers, then a solution to the equation is called an **algebraic integer.** In particular, $\sqrt{2}$ is an algebraic integer, being a solution of $x^2-2=0$. The algebraic integers are the subject of **algebraic number theory;** so we have had a taste of this in §1.3. The only algebraic integers in $\mathbb{Q}$ are the usual integers—which in this context may be called **rational integers.**

The study of $\mathbb{R}$ and $\mathbb{C}$ is **analysis.** There is a part of number theory that makes use of analysis; this is **analytic number theory.** We shall not try to do it here, but if one does prove the Prime Number Theorem (Theorem 105) for example, then the **Gamma function** may be useful: this is the function Γ given by

$$\Gamma(x) = \int_0^\infty \mathrm{e}^{-t} t^{x-1} \,\mathrm{d}\, x$$

when $x \geqslant 1$. You can show that $\Gamma(n+1) = n\Gamma(n)$, and $\Gamma(1) = 1$, so that $G(n+1) = n!$.

Our subject is mainly **elementary number theory.** This means not that the subject is easy, but that our integers are just the rational integers, and we shall not use analysis. However, the proof of Bertrand's Postulate in §4.5 gives a taste of analysis.[2]

[2] For an overview of algebraic numbers, analytic number theory, and other areas of mathematics, an excellent print reference is *The Princeton Companion to Mathematics,* edited by Timothy Gowers with June Barrow-Green and Imre Leader [19].

3. Divisibility

3.1. Division

Henceforth minuscule letters will usually denote integers. If n is such, let the set $\{nx\colon x \in \mathbb{Z}\}$ be denoted by $\mathbb{Z}n$ or $n\mathbb{Z}$ or

$$(n).$$

To give it a name, we may call (n) the **ideal**[1] of $\mathbb{Z}$ generated by n. Note that

$$(-n) = (n).$$

Moreover,

$$a \in (n) \iff (a) \subseteq (n).$$

It is not strictly necessary to introduce ideals, but they may clarify some arguments. By definition, if $a \in (n)$, that is, if $a = nx$ for some integer x, then n **divides** a, or n is a **divisor** of a; this situation is denoted by

$$n \mid a.$$

Then the following holds, simply because $\mathbb{Z}$ is a commutative ring in the sense of §2.2.

Theorem 17. *In $\mathbb{Z}$:*

$$\begin{gathered}
a \mid 0, \\
0 \mid a \iff a = 0, \\
1 \mid a, \\
a \mid a, \\
a \mid b \ \&\ b \mid c \implies a \mid c, \\
a \mid b \ \&\ c \mid d \implies ac \mid bd, \\
a \mid b \implies a \mid bx, \qquad (*) \\
a \mid b \ \&\ a \mid c \implies a \mid b + c. \qquad (\dagger)
\end{gathered}$$

[1] In the original terminology, (n) was an *ideal number*.

In particular, if $a \mid b$, then both a and $-a$ divide both b and $-b$. Every divisor of an integer b is a **proper** divisor if it is not $\pm b$ (this notion will be useful when we discuss *prime numbers* in Chapter 4).

We have an additional property because $\mathbb{Z}$ is an *ordered* commutative ring in which every positive element is 1 or greater; the following does not hold in $\mathbb{Q}$ or $\mathbb{R}$.[2]

Theorem 18. *In $\mathbb{Z}$,*

$$a \mid b \ \&\ b \neq 0 \implies |a| \leqslant |b|.$$

In particular,

$$a \mid b \ \&\ b \mid a \implies a = \pm b.$$

Proof. If $a \mid b$, and $b \neq 0$, then $n \cdot |a| = |b|$ for some positive n, so $1 \leqslant n$ and hence $|a| \leqslant n \cdot |a| = |b|$. □

We have now shown, in effect:

Theorem 19. *The relation $\mid$ of divisibility is an **ordering** of $\mathbb{N}$ that is refined by the linear ordering $\leqslant$, that is, if k, m, and n are in $\mathbb{N}$, then*

$$\begin{gathered} n \mid n, \\ m \mid n \ \&\ n \mid m \implies m = n, \\ k \mid m \ \&\ m \mid n \implies k \mid n, \\ m \mid n \implies m \leqslant n. \end{gathered}$$

Ordered sets can be depicted in so-called **Hasse diagrams.** Consider for example the positive divisors of 60, namely 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60: these twelve numbers can be arranged as in Figure 3.1. Here a line is drawn from a number a up to a number b if $a \mid b$, but there is no c distinct from a and b such that $a \mid c$ and $c \mid b$. In general, $a \mid b$ if and only if there is a path upwards from a to b.

3.2. Congruence

If $a - b \in (n)$, then we may also write

$$a \equiv b \pmod{n} \qquad (\ddagger)$$

[2] It does hold in other ordered commutative rings, such as $\mathbb{Z}[X]$, the ring of polynomials in a single variable X with integer coefficients, ordered so that X is greater than every constant polynomial.

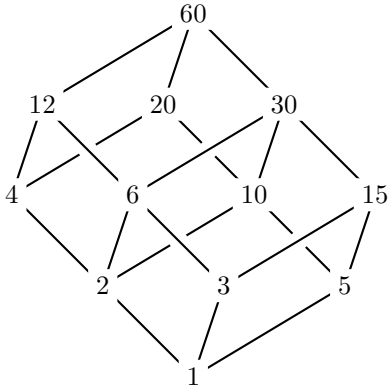


Figure 3.1. Divisors of 60

or $a \equiv b \ (n)$, saying a and b are **congruent** with respect to the **modulus** n, or a and b are congruent ***modulo*** a; also b is a **residue** of a, and a is a residue of b, *modulo* n.[3] If the modulus n is understood, we might write simply

$$a \equiv b.$$

Congruence with respect to a given modulus is an equivalence-relation. The congruence-class of a *modulo* n is

$$\{x \in \mathbb{Z} \colon a - x \in (n)\}.$$

If $n = 0$, then congruence *modulo* n is equality. In any case, congruence *modulo* n is the same as congruence *modulo* $-n$. So we usually need only be concerned with positive moduli.[4]

Lemma. *For every positive modulus n, for every integer a, distinct elements of the n-elemment set $\{a, a+1, \ldots, a+n-1\}$ are incongruent.*

[3]The notation of (‡) is introduced by Johann Carl Friedrich Gauss (1777–1855) in ¶2 of his *Disquisitiones Arithmeticae* [16], first published in 1801. Gauss notes that Legendre uses the same sign for both equality and congruence, because they are analogous concepts. Gauss writes in Latin, and Latin nouns, like Turkish nouns, have *cases.* In particular, the Latin noun *modulus,* meaning literally 'small measure', has the cases *modulum, moduli, modulo, modulo,* corresponding respectively (albeit roughly) to the Turkish *modülü, modülün, modüle, modülden.* However, Gauss does not use a form like '*modulo* 5', at least not in the first two paragraphs of the *Disquisitiones*; he says instead '*secundum modulum* 5', that is, with respect to the modulus 5, or in Turkish 5 *modülüne göre.* (I took Gauss's Latin text from `http://resolver.sub.uni-goettingen.de/purl?PPN235993352`, December 7, 2010; the link was in the Wikipedia article on the *Disquisitiones.*)

[4]Gauss writes in a footnote to his ¶1, 'The modulus must obviously be taken *absolutely,* i.e. without sign.' This suggests to me the picture in which -5 is 'really' 5, from a special point of view.

Proof. If i and j are distinct elements of the set, then $0 < |i - j| < n$, so $n \nmid i - j$ by Theorem 18. □

We want now to show that every integer is congruent to *some* element of $\{a, a+1, \ldots, a+n-1\}$. To do so, we shall use the *greatest integer in* a rational number. This notion applies to arbitrary real numbers as well, through the following:

Theorem 20. *For every real number x, there is a unique integer k such that*

$$k \leqslant x < k + 1.$$

Proof. Assume first $x \geqslant 0$. By the construction in §2.4, there is a rational number a/b such that $x < a/b$; and then $x < a$. By the Well Ordering Principle (Theorem 15), there is a *least* integer m such that $x < m$. Then $m - 1$ is the desired integer k. If $x < 0$, we let m be the least integer such that $-x \leqslant m$, and then $-m$ is the desired integer k.

In either case, the integer k is unique by Theorem 12 (though again, cases must be considered). □

In the theorem, the integer k is the **greatest integer in** x and can be denoted by

$$[x].$$

Its existence for all x in $\mathbb{R}$ is expressed by saying $\mathbb{R}$ is **archimedean** (as an ordered commutative ring).[5]

Lemma. *For every positive modulus n, every integer has a unique residue in $\{0, 1, \ldots, n-1\}$.*

Proof. For any integer a, we just compute

$$\begin{aligned} \left[\frac{a}{n}\right] \leqslant \frac{a}{n} &< \left[\frac{a}{n}\right] + 1, \\ \frac{a}{n} - 1 &< \left[\frac{a}{n}\right] \leqslant \frac{a}{n}, \\ 1 &> \frac{a}{n} - \left[\frac{a}{n}\right] \geqslant 0, \\ n &> a - n\left[\frac{a}{n}\right] \geqslant 0. \end{aligned}$$

So $a - n[a/n]$ belongs to the desired set; and it is an integer congruent to a. □

[5] Another way to say $\mathbb{R}$ is archimedean is that if a and b are positive real numbers, then for some positive integer n, $na > b$. This principle is used by Archimedes (c. 287–212 BCE) to show, for example, that the surface of a sphere is equal to a circle of twice the radius [3]. An example of a nonarchimedean ordered commutative ring is $\mathbb{Z}[X]$, defined in note 2 on page 37 above. We can characterize $\mathbb{Z}$ as the unique archimedean ordered commutative ring with no positive elements less than 1.

The following theorem is basically a restatement of the last lemma. It is called the Division Algorithm, though it is not really an algorithm; it is the observation that finding a quotient (with remainder) of one integer after division by a nonzero integer is always *possible*. So-called *long division* is an algorithm for doing this that is learned in school.

Theorem 21 (Division Algorithm)**.** *For every positive integer q, for every integer a, there are unique integers k and r such that*

$$a = kq + r, \qquad 0 \leqslant r < q.$$

As a consequence of the last two lemmas, we have:

Theorem 22. *For every positive modulus n, for every integer a, every integer has a unique residue in the set $\{a, a+1, \ldots, a+n-1\}$.*

Proof. Every integer x has a unique residue $f(x)$ in $\{0, 1, \ldots, n-1\}$. Let g be the restriction of f to the set $\{a, a+1, \ldots, a+n-1\}$. Then g is injective, and its domain and codomain are finite sets of the same size; therefore g is surjective onto $\{0, 1, \ldots, n-1\}$. Then $g^{-1}(f(x))$ belongs to $\{a, a+1, \ldots, a+n-1\}$ and is a residue of x; moreover, it is unique. □

In the theorem, $\{a, \ldots, a+n-1\}$ is called a **complete set of residues** *modulo* n. We shall be interested mainly in the cases

$$\{0, \ldots, n-1\}, \qquad \left\{-\left[\frac{n-1}{2}\right], \ldots, \left[\frac{n}{2}\right]\right\},$$

the latter set being $\{-m+1, \ldots, m\}$, if $n = 2m$, and $\{-m, \ldots, m\}$, if $n = 2m+1$.

Theorem 23. *If $a \equiv b$ and $c \equiv d$, then*

$$a + c \equiv b + d, \qquad ac \equiv bd.$$

Proof. If $n \mid b - a$ and $n \mid d - c$, then, by Theorem 17, we have $n \mid b - a + d - c$, that is,

$$n \mid b + d - (a + c),$$

and also $n \mid (b-a)c + (d-c)b$, that is,

$$n \mid bd - ac.$$

□

A first application of this is an ancient theorem, found in the work of Theon of Smyrna [36, pp. 102–5].

Theorem 24. *Every square is congruent to* 0 *or* 1 modulo 3 *and* 4.

Proof. By the last theorem, if two integers are congruent, then their squares are congruent. So it is enough to observe the following: The set $\{-1, 0, 1\}$ is a complete set of residues *modulo* 3, and the square of each element is congruent to 0 or 1. The set $\{-1, 0, 1, 2\}$ is a complete set of residues *modulo* 3, and the square of each element is congruent to 0 or 1. □

The set of congruence-classes of integers *modulo* n is denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$ or simply

$$\mathbb{Z}_n.$$

Then Theorem 23 is that addition and multiplication are well-defined on $\mathbb{Z}_n$; so this becomes a commutative ring.

3.3. Greatest common divisors

A **common divisor** of a and b is any j such that $j \mid a$ and $j \mid b$. If one of a and b is not 0, then $|j| \leqslant \min(|a|, |b|)$ by Theorem 18. In this case, a and b have a common divisor that is greatest with respect to the linear ordering $\leqslant$. This common divisor is called simply the **greatest common divisor** of a and b and is denoted by

$$\gcd(a, b).$$

If c is a common divisor of a and b, then $c \leqslant \gcd(a, b)$.

We immediately have an algorithm for finding $\gcd(a, b)$. If one of a and b is 0, then the absolute value of the other is the greatest common divisor. Otherwise:

a) List the elements of $\{1, \ldots, |a|\}$ that divide a.
b) List the elements of $\{1, \ldots, |b|\}$ that divide b.
c) Find the greatest number that is common to both lists.

For example, we can read $\gcd(12, 30) = 6$ off the Hasse diagram in Figure 3.1. See Figure 3.2. For large numbers, this algorithm is impractical; we shall develop

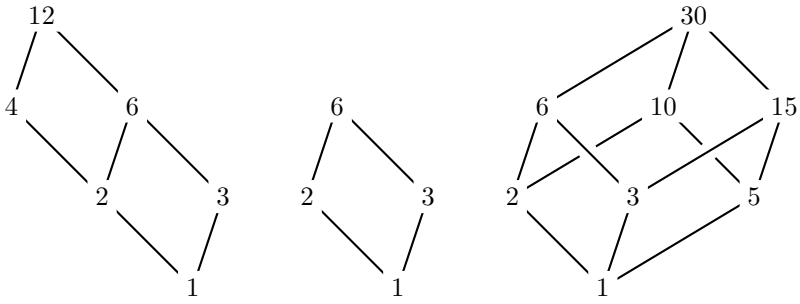


Figure 3.2. Common divisors of 12 and 30

the Euclidean Algorithm, which is far superior, in §3.5 below. Meanwhile, note that every common divisor of 12 and 30 divides 6. We shall show that this is always true: $\gcd(a, b)$ is a common divisor of a and b that is greatest with respect to the ordering $|$ of divisibility; that is, if c is a common divisor of a and b, then $c \mid \gcd(a, b)$.

To prove this result, we may note that, by $(*)$ and $(\dagger)$ in Theorem 17, if $a \mid b$ and $a \mid c$, then a divides every **linear combination,**

$$ax + by,$$

of a and b. Let the set $\{ax+by\colon x, y \in \mathbb{Z}\}$ of these linear combinations be denoted by

$$(a, b);$$

this is the **ideal** of $\mathbb{Z}$ generated by a and b. Then

$$(a) \subseteq (j) \ \ \& \ \ (b) \subseteq (j) \iff (a, b) \subseteq (j).$$

That is, the common divisors of a and b are those j such that $(a, b) \subseteq (j)$. In fact we have not introduced any new ideals, by the following:

Lemma. *For all integers a and b, for some unique non-negative integer k,*

$$(a, b) = (k).$$

Proof. Immediately $(0, 0) = (0)$. Now suppose one of a and b is not 0. Then (a, b) has positive elements, and we may let k be the least of these. Then $(k) \subseteq (a, b)$. We establish the reverse inclusion by showing k divides a and b. By Theorem 21 (the Division Algorithm), we have $a = kq + r$ and $0 \leqslant r < k$ for some q and r. Then

$$r = a - kq = a - (ax + by)q = a(1 - qx) + b(-qy)$$

for some x and y, so $r \in (a, b)$, and hence $r = 0$ by minimality of k. So $k \mid a$. By symmetry, $k \mid b$. □

Theorem 25. *If a and b are integers, not both 0, then*

$$(a, b) = \big(\gcd(a, b)\big),$$

that is, $\gcd(a, b)$ is the unique positive integer k such that $(a, b) = (k)$. Hence every common divisor of a and b divides $\gcd(a, b)$.

Proof. We know $(a, b) \subseteq (j)$ if and only if j is a common divisor of a and b. In particular, if $(a, b) = (k)$, then k is a common divisor of a and b, and if j is also a common divisor, then $(k) \subseteq (j)$, so $j \mid k$, and therefore $|j| \leqslant |k|$. □

The theorem is the reason why the notation (a, b) is sometimes used in place of $\gcd(a, b)$. The following is immediate.

Corollary (Bézout's Lemma[6])**.** *If a and b are not both 0, the diophantine equation*

$$ax + by = \gcd(a, b)$$

is soluble.

The following is sometimes useful:

Theorem 26. *For all integers a, b, and c, if one of a and b is not 0, then*

$$\gcd(ac, bc) = \gcd(a, b) \cdot c.$$

In particular, if $\gcd(a, b) = \ell$, and $k \mid \ell$, then

$$\gcd\Big(\frac{a}{k}, \frac{b}{k}\Big) = \frac{\ell}{k}.$$

If $\gcd(a, b) = 1$, then a and b together are called either **relatively prime** or **co-prime;** also, each of a and b is **prime to** the other. This is the case if the equation

$$ax + by = 1 \tag{§}$$

is soluble. Conversely, if a and b are co-prime, then (§) *must* have a solution, by Bézout's Lemma. If $\gcd(a, b) = k$, then a/k and b/k are co-prime, by the last theorem.

Gauss proves the following in ¶19 of the *Disquisitiones Arithmeticae* [16], but he uses the Fundamental Theorem of Arithmetic (Theorem 34 below) in his proof.

Theorem 27. *If a and b are co-prime, and each divides c, then $ab \mid c$.*

Proof. Under the hypothesis, $c = bs = ar$ for some s and r, and then the following equations are soluble:

$$\begin{aligned} ax + by &= 1, \\ acx + bcy &= c, \\ absx + bary &= c, \\ ab(sx + ry) &= c. \end{aligned}$$

□

Euclid proves the following in Proposition VII.30 of the *Elements* [12, 13], though his *statement* of the theorem assumes a is *prime* (see p. 51).

Theorem 28. *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

[6] `http://en.wikipedia.org/wiki/Bezout's_identity` (accessed December 13, 2010).

Proof. Again, as in the proof of the last theorem, the following have solutions:

$$ax + by = 1,$$
$$acx + bcy = c.$$

Since $a \mid ac$ and $a \mid bc$, we are done by Theorem 17. □

3.4. Least common multiples

The Hasse diagram of divisors of 60 in Figure 3.1 is symmetrical: if we interchange n and $60/n$, the result is the same diagram, reflected, as on the right of Figure 3.3. The general result is the following.

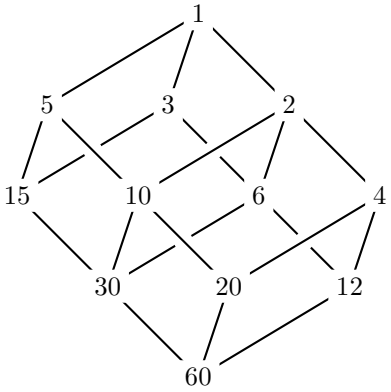


Figure 3.3. Divisors of 60, again

Theorem 29. *If d and e are divisors of some nonzero integer n, then*

$$d \mid e \iff \frac{n}{e} \mid \frac{n}{d}.$$

Proof. We have $d \mid e$ if and only if $dx = e$ for some x; but

$$dx = e \iff ndx = ne \iff \frac{nx}{e} = \frac{n}{d}.$$ □

The theorem leads to a notion that is 'dual' to the greatest common divisor. A **common multiple** of a and b is any j such that $a \mid j$ and $b \mid j$, that is, $(j) \subseteq (a) \cap (b)$. If $ab \neq 0$, then $(a) \cap (b)$ has a positive element (either ab or $-ab$), so it has a *least* positive element; this is the **least common multiple** of a and b, denoted by

$$\operatorname{lcm}(a, b).$$

The greatest common divisor of a and b is the common divisor of a and b that is greatest among all common divisors—greatest with respect to the linear ordering $\leqslant$, but also with respect to divisibility. The least common multiple of a and b has the corresponding property:

Theorem 30. *If $ab \neq 0$, then*

$$\big(\operatorname{lcm}(a,b)\big) = (a) \cap (b). \tag{¶}$$

In particular, $\operatorname{lcm}(a,b)$ *divides all common multiples of a and b. Moreover,*

$$\operatorname{lcm}(a,b) = \frac{|ab|}{\gcd(a,b)}. \tag{‖}$$

Proof. Let c and d be common multiples of a and b. Then $\gcd(c,d)$ must also be a common multiple of a and b. That is, under the assumption $(c) \subseteq (a) \cap (b)$ and $(d) \subseteq (a) \cap (b)$, we have $(c,d) \subseteq (a) \cap (b)$, and therefore $\big(\gcd(c,d)\big) \subseteq (a) \cap (b)$. In particular, if $d \notin (c)$, then

$$(c) \subset (c,d) = \big(\gcd(c,d)\big) \subseteq (a) \cap (b),$$

so $|c| \neq \operatorname{lcm}(a,b)$. This establishes (¶) and the conclusion that $\operatorname{lcm}(a,b)$ divides all common multiples of a and b.

As a special case, $\operatorname{lcm}(a,b)$ divides ab. By Theorem 29, if x is an arbitrary divisor of ab, then x is a common multiple of a and b if and only if ab/x is a common divisor of ab/a and ab/b, which are just b and a. Hence $|ab|/\gcd(a,b)$ must be the least common multiple of a and b *among the divisors of ab.* But we already know that the least of all common multiples of a and b is among the divisors of ab. Therefore we have (‖). □

Corollary. *If $ab \neq 0$, and c is a common multiple of a and b, then*

$$\operatorname{lcm}(a,b) = \frac{|c|}{\gcd(c/a, c/b)}.$$

Proof. Theorem 26. □

For example, since $\gcd(12,30) = 6$, we have that the least common multiple of $60/12$ and $60/30$ is $60/6$, that is,

$$\operatorname{lcm}(5,2) = 10.$$

In general, we have a Hasse diagram as in Figure 3.4.

Another corollary of the theorem is the following:

Corollary. *If $ab \neq 0$, and $x \equiv y$* modulo *both a and b, then*

$$x \equiv y \pmod{\operatorname{lcm}(a,b)}.$$

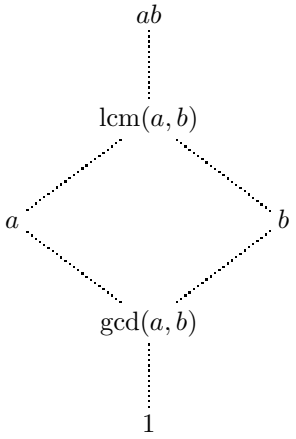


Figure 3.4. gcd and lcm

3.5. The Euclidean algorithm

We have observed that every common divisor of a and b divides every linear combination of a and b. In particular, it divides the remainder of dividing a by b. For example, let $d = \gcd(63, 23)$. Then d divides $63 - 23 \cdot 2$, which is 17. But then $23 - 17$ or 6 is another linear combination of 63 and 23, so d divides this. Similarly d divides $17 - 6 \cdot 2$ or 5. Finally, d divides $6 - 5$ or 1. Then d must *be* 1; that is, $\gcd(63, 23) = 1$, and so 63 and 23 are relatively prime. The computations are shown in Figure 3.5. The general method for finding greatest

$$
\begin{aligned}
63 &= 23 \cdot 2 + 17, \\
23 &= 17 \cdot 1 + 6, \\
17 &= 6 \cdot 2 + 5, \\
6 &= 5 \cdot 1 + 1,
\end{aligned}
$$

Figure 3.5. The Euclidean algorithm

common divisors is given by Euclid in Propositions VII.1 and 2 of the *Elements*. In modern notation, we have the following.

Theorem 31 (Euclidean Algorithm)**.** *Suppose $a_1 > a_2 \geqslant 0$. There are unique sequences $(a_n : n \in \mathbb{N})$ and $(q_n : n \in \mathbb{N})$ such that, if $a_{n+1} \neq 0$, then*

$$a_n = a_{n+1} \cdot q_n + a_{n+2}, \qquad 0 \leqslant a_{n+2} < a_{n+1}, \qquad (**)$$

but if $a_{n+1} = 0$, then $a_{n+2} = 0 = q_n$. Then the sequence $(a_n : n \in \mathbb{N})$ is eventually 0, and if a_m is the last nonzero entry, then

$$\gcd(a_0, a_1) = a_m.$$

Proof. The given conditions amount to a definition by recursion of the function $n \mapsto (a_n, a_{n+1})$. In the notation of Theorem 6, the set A is $\mathbb{Z}\times\mathbb{Z}$, and $b = (a_1, a_2)$, while f is given by $f(x, y) = (y, z)$, where z is the least nonnegative residue of x *modulo* y, if $y \neq 0$, but $z = 0$ if $y = 0$. (The function f is well defined by Theorem 22.)

We now have that, if $a_{n+1} \neq 0$, then $a_{n+2} < a_{n+1}$; also, the common divisors of a_n and a_{n+1} are just the common divisors of a_{n+1} and a_{n+2}, so that

$$\gcd(a_n, a_{n+1}) = \gcd(a_{n+1}, a_{n+2}).$$

In particular, if a_m is the least of the positive numbers a_n, then $a_{m+1} = 0$, so

$$\gcd(a_0, a_1) = \gcd(a_m, 0) = a_m. \qquad \square$$

In §1.3, to establish the incommensurability of the diagonal and side of a square, we used the variant of the Euclidean Algorithm used by Euclid himself to prove his Proposition X.2.

In the notation of Theorem 31, two consecutive lines of computations as in Figure 3.5 can be written as

$$\begin{aligned} a_n &= a_{n+1} \cdot q_n + a_{n+2}, \\ a_{n+1} &= a_{n+2} \cdot q_{n+1} + a_{n+3}; \end{aligned}$$

but we can rewrite these as

$$\begin{aligned} \frac{a_n}{a_{n+1}} &= q_n + \frac{a_{n+2}}{a_{n+1}}, \\ \frac{a_{n+1}}{a_{n+2}} &= q_{n+1} + \frac{a_{n+3}}{a_{n+2}}. \end{aligned}$$

With the notation ξ_n for a_{n+1}/a_n, we now have

$$0 \leqslant \xi_n < 1, \qquad \frac{1}{\xi_n} = q_n + \xi_{n+1}$$

(assuming $\xi_{n+1} \neq 0$), so

$$q_n = \left[\frac{1}{\xi_n}\right], \qquad \xi_{n+1} = \frac{1}{\xi_n} - q_n. \tag{††}$$

Then we have

$$\frac{1}{\xi_1} = q_1 + \xi_2 = q_1 + \frac{1}{q_2 + \xi_3} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \xi_4}} = \dots$$

For example, if we rewrite the computations of Figure 3.5 as above, we get

$$\frac{63}{23} = 2 + \frac{17}{23}, \qquad \frac{23}{17} = 1 + \frac{6}{17}, \qquad \frac{17}{6} = 2 + \frac{5}{6}, \qquad \frac{6}{5} = 1 + \frac{1}{5},$$

and therefore

$$\frac{63}{23} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5}}}}.$$

But the definition (††) can be applied to any real number chosen as ξ_1. If ξ_n is never 0 for any n, or equivalently if $(q_1, q_2, \dots)$ never ends, then by Euclid's Proposition X.2, the number ξ_1 must be irrational.

In §1.3, we worked out the example where $\xi_1 = 1/\sqrt{2}$. Indeed, let d and s be the diagonal and side of a square, respectively, as in Figure 3.6. Since $d^2 - s^2 = s^2$,

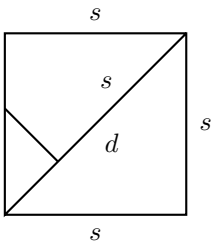


Figure 3.6. Diagonal and side

we have

$$\frac{d - s}{s} = \frac{s}{d + s}.$$

From this equation, since $s < d+s$, we have $d-s < s$. Letting $\xi_1 = s/d$, we have

$$\frac{1}{\xi_1} = \frac{d}{s}, \qquad q_1 = 1, \qquad \xi_2 = \frac{d-s}{s},$$
$$\frac{1}{\xi_2} = \frac{s}{d-s} = \frac{d+s}{s}, \qquad q_2 = 2, \qquad \xi_3 = \frac{d-s}{s},$$

so the sequence of q_n is $(1, 2, 2, \dots)$.

3.6. The Hundred Fowls Problem

Problem 3.38 in the *Mathematical Classic of Zhang Qiujian*[7] reads thus:

> Now one cock is worth 5 *qian,* one hen 3 *qian,* and 3 chicks 1 *qian.* It is required to buy 100 fowls with 100 *qian.* In each case, find the number of cocks, hens, and chicks bought. Answer says: 4 cocks worth 20 *qian,* 18 hens worth 54 *qian,* 78 chicks worth 26 *qian.* Another answer: 8 cocks worth 40 *qian,* 11 hens worth 33 *qian,* 81 chicks worth 27 *qian.* Another answer: 12 cocks worth 60 *qian,* 4 hens worth 12 *qian,* 84 chicks worth 28 *qian.*
>
> Method says: Add 4 to the number of cocks, subtract 7 from the number of hens and add 3 to the number of chicks to obtain the answer.

The given 'answers' are correct; and according to the 'method', the given answers are the only ones possible (assuming at least one cock, one hen, and one chick must be bought). But why is the method correct? Let

$$x = \#\text{ cocks}, \qquad y = \#\text{ hens}, \qquad z = \#\text{ chicks}.$$

The problem is to solve

$$x + y + z = 100,$$
$$5x + 3y + \frac{1}{3}z = 100.$$

Multiplying the second equation by 3 and subtracting the first equation yields $14x + 8y = 200$ and then

$$7x + 4y = 100.$$

Since $4 \mid 100$, one solution is $(0, 25)$, that is, $x = 0$ and $y = 25$, and then $z = 75$. Moreover, since 7 and 4 are co-prime, any increase in x must be a multiple of 4, and then y must decrease by the same multiple of 7, so z must increase by the

[7] Burton [7, pp. 36–7] discusses the problem, but my source for the text is the anthology edited by Katz [24, pp. 302–8], where it is said that the *Classic* was probably compiled between the years 466 and 485.

same multiple of 3 (according to the first equation). So we get the three solutions given, and no others (assuming at least one cock must be bought):

x	y	z
4	18	78
8	11	81
12	4	84

Joseph W. Dauben [24, p.308] writes of the Hundred Fowls Problem:

> Outside China, versions of the problem appear in the works of, among others, Alcuin of York in the eighth century, Mahavira in the ninth century, Abu Kamil in the tenth century, Bhaskara in the twelfth century, Leonardo of Pisa in the thirteenth century, and al-Kashi in the fifteenth century.

4. Prime numbers

4.1. The Fundamental Theorem of Arithmetic

In the 11th definition in Book VII of the *Elements,* Euclid defines a **prime number** (πρῶτος ἀριθμός) as a number 'that is measured by a unit alone.' But a *number* (ἀριθμός) here is 'a multitude composed of units.' A multitude is more than one. Thus a unit is *not* a number for Euclid; it is just a unit, out of which numbers can be created.

If, according to Euclid, a prime number is measured—or we might say *divided*—only by a unit, then it seems that no number measures *itself.* However, in Proposition 2 (mentioned above on page 47 in §3.3), Euclid mentions that a number *does* measure itself. So there seems to be some confusion in Euclid's text as we have it today.

Our formulation of Euclid's definition is that a positive integer is prime if it has exactly one *proper* positive divisor, which must then be 1. Having *no* proper divisors, 1 is not prime; but 2 is prime. More generally, b is prime if and only if $b > 1$ and

$$a > 0 \ \& \ a \mid b \implies a \in \{1, b\}.$$

By Theorem 18, an alternative formulation of this last condition is

$$1 < a < b \implies a \nmid b.$$

Throughout this book, p and q will always stand for primes. Then

$$\gcd(a, p) \in \{1, p\},$$

so either a and p are co-prime, or else $p \mid a$.

Theorem 32. *Every integer greater than* 1 *has a prime divisor.*

Proof. If $n > 1$, then the least of the divisors of n that are greater than 1 must be prime by Theorem 18. □

A positive integer with a proper divisor that is greater than 1 is **composite.** So 1 is neither prime nor composite, but every integer that is greater than 1 is prime or composite, but not both.

Theorem 33 (Euclid, VII.30)**.** *If $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. If $p \nmid a$, then $\gcd(a, p) = 1$, so $p \mid b$ by Theorem 28. □

Corollary. *If $p \mid a_1 \cdots a_n$, where $n \geqslant 1$, then $p \mid a_k$ for some k.*

Proof. Use induction. The claim is trivially true when $n = 1$. Suppose it is true when $n = m$. Say $p \mid a_1 \cdots a_{m+1}$. By the theorem, we have that $p \mid a_1 \cdots a_m$ or $p \mid a_{m+1}$. In the former situation, by the inductive hypothesis, $p \mid a_k$ for some k. So the claim holds when $n = m + 1$, assuming it holds when $n = m$. Therefore the claim does indeed hold for all n. □

The following appears in Gauss's *Disquisitiones Arithmeticae* as ¶16; Hardy and Wright [21, p. 10] judge that to be the first explicit statement of the theorem.

Theorem 34 (Fundamental Theorem of Arithmetic)**.** *Every positive integer is uniquely a product*

$$p_1 \cdots p_n$$

of primes, where

$$p_1 \leqslant \cdots \leqslant p_n.$$

Proof. Trivially, $1 = p_1 \cdots p_n$, where $n = 0$. Suppose $m > 1$, and let p_1 be its least prime divisor (which exists by Theorem 32). If $m = p_1$, we are done; otherwise, the least divisor of m/p_1 that is greater than 1 is a prime, p_2. If $m = p_1 p_2$, we are done; otherwise, the least divisor of $m/p_1 p_2$ that is greater than 1 is a prime p_3. Continuing thus, we get an increasing sequence $p_1, p_2, p_3, \ldots$ of primes, where $p_1 \cdots p_k \mid m$. Since

$$m > \frac{m}{p_1} > \frac{m}{p_1 p_2} > \cdots,$$

the sequence of primes must terminate by the Well Ordering Principle, and for some n we have $m = p_1 \cdots p_n$.

For uniqueness, suppose also $m = q_1 \cdots q_\ell$. Then $q_1 \mid m$, so $q_1 \mid p_i$ for some i by the corollary to Theorem 33, and therefore $q_1 = p_i$. Hence

$$p_1 \leqslant p_i = q_1.$$

By the symmetry of the argument, $q_1 \leqslant p_1$, so $p_1 = q_1$. Similarly, $p_2 = q_2$, &c., and $n = \ell$. □

Alternatively, every positive integer is uniquely a product

$${p_1}^{a_1} \cdots {p_n}^{a_n},$$

that is,

$$\prod_{k=1}^{n} {p_k}^{a_k},$$

where $p_1 < \cdots < p_n$ and the exponents a_k are all positive integers. Here of course the p_k (as well as the a_k) depend on the integer. To incorporate this dependence

into the notation, we may say that, for every positive integer a, there is a unique function $p \mapsto a(p)$ on the set of primes such that $a(p) \geqslant 0$ for all p, and $a(p) = 0$ for all but finitely many p, and

$$a = \prod_p p^{a(p)}. \qquad (*)$$

Now the Fundamental Theorem of Arithmetic allows alternative proofs of theorems like 25 and 30, since we have

$$\gcd(a, b) = \prod_p p^{c(p)}, \qquad \operatorname{lcm}(a, b) = \prod_p p^{d(p)},$$

or simply $\gcd(a, b) = c$ and $\operatorname{lcm}(a, b) = d$, where

$$c(p) = \min(a(p), b(p)), \qquad d(p) = \max(a(p), b(p)).$$

4.2. Irreducibility

What is there about $\mathbb{N}$ that makes the Fundamental Theorem of Arithmetic possible?

In an arbitrary commutative ring, the elements analogous to the prime numbers are called *irreducible*, and the elements that respect the analogue of Theorem 33 are called *prime*. To be precise, a nonzero element of an arbitrary commutative ring is a **unit** if it has a multiplicative inverse. A nonzero element a of the ring is **irreducible** if a is not a unit, but whenever $a = bc$, one of b and c must be a unit. In this sense, the prime integers are just the *positive* irreducibles in $\mathbb{Z}$. In an arbitrary commutative ring, a nonzero nonunit π is called **prime** if

$$\pi \mid ab \;\;\&\;\; \pi \nmid a \implies \pi \mid b.$$

In an arbitrary commutative ring, irreducibles need not be prime. For example, let

$$\mathbb{Z}[\sqrt{10}] = \{x + y\sqrt{10} \colon x, y \in \mathbb{Z}\},$$

which is a sub-ring of $\mathbb{R}$. In this sub-ring, we have

$$(4 + \sqrt{10})(4 - \sqrt{10}) = 6 = 2 \cdot 3.$$

In particular,

$$4 + \sqrt{10} \mid 2 \cdot 3.$$

Also, $4 + \sqrt{10}$ is irreducible, but it divides neither 2 nor 3. To show this, we use the operation σ on $\mathbb{Z}[\sqrt{10}]$ given by

$$\sigma(a + b\sqrt{10}) = a - b\sqrt{10}.$$

(Compare this with complex conjugation.) Since

$$(a \pm b\sqrt{10})(c \pm d\sqrt{10}) = ac + 10bd \pm (ad + bc)\sqrt{10},$$

we have $\sigma(xy) = \sigma(x) \cdot \sigma(y)$. Now define

$$N(x) = x \cdot \sigma(x),$$

so that $N(a + b\sqrt{10}) = a^2 - 10b^2$, which is always an integer. Then

$$N(xy) = N(x) \cdot N(y).$$

The units of $\mathbb{Z}[\sqrt{10}]$ are just those elements x such that $N(x) = \pm 1$. Indeed, if x is a unit, then $xy = 1$ for some y, and then $N(x) \cdot N(y) = N(xy) = 1$, so $N(x) = \pm 1$; conversely, if $N(x) = \pm 1$, this means $x \cdot (\pm\sigma(x)) = 1$, so x is a unit. For example, $3 + \sqrt{10}$ is a unit; but $4 + \sqrt{10}$ is not a unit, since $N(4 + \sqrt{10}) = 6$.

We always have that $N(x)$ is congruent to a square *modulo* 10; so it is conjugate to one of 0, ± 1, ± 4, and 5. If $xy = 4 + \sqrt{10}$, then $N(x) \cdot N(y) = 6$, but $N(x)$ cannot be ± 2 or ± 3, so one of $N(x)$ and $N(y)$ must be ± 1. Thus $4 + \sqrt{10}$ is irreducible.

Finally, since 6 divides neither 4 nor 9, that is, $N(4 + \sqrt{10})$ divides neither $N(2)$ nor $N(3)$, we have that $4 + \sqrt{10}$ divides neither 2 nor 3.

4.3. The Sieve of Eratosthenes

According to Nicomachus [36, pp. 100–3], who appears to be our earliest source on the matter, the following method of finding prime numbers was referred to by Eratosthenes as a **sieve** (κόσκινον).[1]

Perhaps everybody knows this method. We know 2 is prime, but the other positive even numbers are composite. We list the positive odd integers, starting with 3, continuing as far as we like. We note 3 as prime, but strike out its proper multiples from the list. The next unstricken number is 5. We note this as prime, but strike out its proper multiples, and so on, as in Table 4.1. Those numbers not stricken are prime.

At each step, once a number k is noted as prime, then only k^2 and greater multiples of k need be stricken; lesser multiples of k have already been stricken.

Hence, if it is the odd numbers less than n^2 that are listed, and the proper multiples of the primes that are less than n are stricken, then the remaining

[1] Eratosthenes of Cyrene (276–194 BCE) also measured the circumference of the earth, by measuring the shadows cast by posts a certain distance apart in Egypt. Measuring *this* distance must have needed teams of surveyors and a government to fund them. Christopher Columbus was not in a position to make the measurement again, so he had to rely on ancient measurements [32].

$\boxed{3}$ 5 7 $\not{9}$ 11 13 $\not{15}$ 17 19 $\not{21}$ 23 25 $\not{27}$ 29 31 $\not{33}$ 35 37 $\not{39}$ 41 43 $\not{45}$ 47 49 $\not{51}$ 53 55 $\not{57}$ 59 61 $\not{63}$
65 67 $\not{69}$ 71 73 $\not{75}$ 77 79 $\not{81}$ 83 85 $\not{87}$ 89 91 $\not{93}$ 95 97 $\not{99}$ 101 103 $\not{105}$ 107 109 $\not{111}$ 113 115 $\not{117}$ 119

$\boxed{3}\boxed{5}$ 7 $\not{9}$ 11 13 $\not{15}$ 17 19 $\not{21}$ 23 $\not{25}$ $\not{27}$ 29 31 $\not{33}$ $\not{35}$ 37 $\not{39}$ 41 43 $\not{45}$ 47 49 $\not{51}$ 53 $\not{55}$ $\not{57}$ 59 61 $\not{63}$
$\not{65}$ 67 $\not{69}$ 71 73 $\not{75}$ 77 79 $\not{81}$ 83 $\not{85}$ $\not{87}$ 89 91 $\not{93}$ $\not{95}$ 97 $\not{99}$ 101 103 $\not{105}$ 107 109 $\not{111}$ 113 $\not{115}$ $\not{117}$ 119

$\boxed{3}\boxed{5}\boxed{7}$ $\not{9}$ 11 13 $\not{15}$ 17 19 $\not{21}$ 23 $\not{25}$ $\not{27}$ 29 31 $\not{33}$ $\not{35}$ 37 $\not{39}$ 41 43 $\not{45}$ 47 $\not{49}$ $\not{51}$ 53 $\not{55}$ $\not{57}$ 59 61 $\not{63}$
$\not{65}$ 67 $\not{69}$ 71 73 $\not{75}$ $\not{77}$ 79 $\not{81}$ 83 $\not{85}$ $\not{87}$ 89 $\not{91}$ $\not{93}$ $\not{95}$ 97 $\not{99}$ 101 103 $\not{105}$ 107 109 $\not{111}$ 113 $\not{115}$ $\not{117}$ 119

$\boxed{3}\boxed{5}\boxed{7}\not{9}\boxed{11}\boxed{13}\not{15}\boxed{17}\boxed{19}\not{21}\boxed{23}\not{25}\not{27}\boxed{29}\boxed{31}\not{33}\not{35}\boxed{37}\not{39}\boxed{41}\boxed{43}\not{45}\boxed{47}\not{49}\not{51}\boxed{53}\not{55}\not{57}\boxed{59}\boxed{61}\not{63}$
$\not{65}\boxed{67}\not{69}\boxed{71}\boxed{73}\not{75}\not{77}\boxed{79}\not{81}\boxed{83}\not{85}\not{87}\boxed{89}\not{91}\not{93}\not{95}\boxed{97}\not{99}\boxed{101}\boxed{103}\not{105}\boxed{107}\boxed{109}\not{111}\boxed{113}\not{115}\not{117}\boxed{119}$

Table 4.1. The Sieve of Eratosthenes

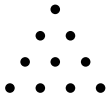
numbers are prime. In Table 4.1, as it is the odd numbers less than 11^2 that are listed, so, once the proper multiples of 3, 5, and 7 are stricken, the remaining numbers are all prime.

Formulating this as a test for individual primes, we have the following.

Theorem 35. *If $1 < m < n^2$, and $p \nmid m$ whenever $p < n$, then m must be prime.*

Proof. Suppose $1 < m < n^2$, but m is not prime. Then $m = ab$ for some a and b, where $1 < a \leqslant b < m$, so $a^2 \leqslant ab = m < n^2$ and hence $a < n$. But then a has a prime factor p by Theorem 32, so $p < n$ and $p \mid m$. □

We normally write numbers in decimal notation, which means for example that 365 is a code for the sum $5 + 6t + 3t^2$, where t is the fourth triangular number,



—called *decem* in Latin, but in English *ten.* There is no obvious reason, other than our having ten fingers, why t should be ten and not be some other number. Nonetheless, given the decimal system, we have some standard tests for divisibility by small primes:

Theorem 36. *Let $t = 2 \cdot 5$. Every positive integer $a_0 + a_1 t + \cdots + a_n t^n$ is congruent,* modulo

a) 2 *and* 5*, to a_0,*

b) 3 *(and* 9*), to $a_0 + a_1 + \cdots + a_n$,*

c) 7*, to $a_0 + 3a_1 + \cdots + 3^n a_n$,*

d) 11*, to $a_0 - a_1 + \cdots + (-1)^n a_n$,*

e) 13*, to $a_0 - 3a_1 + \cdots + (-3)^n a_n$.*

Every positive integer $b_0 + b_1 t^3 + \cdots + b_n t^{3n}$ is congruent, modulo 1001 *(that is, $1 + t^3$, or $7 \cdot 11 \cdot 13$), to $b_0 - b_1 + \cdots + (-1)^n b_n$.*

Suppose n is a composite number less than 37^2 (that is, 1369). Then n is divisible by one of the eleven primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

We can easily check for divisibility by 2, 3, and 5. If $n = a + 10b + 100c + 1000d$, we can consider $n - 1001d$, that is, $a + 10b + 100c - d$: this is divisible by 7, 11, or 13 if and only if n is. If a prime factor of n has not been detected so far, then $n \geqslant 17^2$, and n is divisible by one of 17, 19, 23, 29, and 31. In particular, n is one of the numbers listed in Table 4.2.[2]

[2]To create this table, I used a table of Burton [7, Table 2, pp. 394–403], which lists all odd

$289 = 17 \cdot 17$	$779 = 19 \cdot 41$	$1121 = 19 \cdot 59$
$323 = 17 \cdot 19$	$799 = 17 \cdot 47$	$1139 = 17 \cdot 67$
$361 = 19 \cdot 19$	$817 = 19 \cdot 43$	$1147 = 31 \cdot 37$
$391 = 17 \cdot 23$	$841 = 29 \cdot 29$	$1159 = 19 \cdot 61$
$437 = 19 \cdot 23$	$851 = 23 \cdot 37$	$1189 = 29 \cdot 41$
$493 = 17 \cdot 29$	$893 = 19 \cdot 47$	$1207 = 17 \cdot 71$
$527 = 17 \cdot 31$	$899 = 29 \cdot 31$	$1219 = 23 \cdot 53$
$529 = 23 \cdot 23$	$901 = 17 \cdot 53$	$1241 = 17 \cdot 73$
$551 = 19 \cdot 29$	$943 = 23 \cdot 41$	$1247 = 29 \cdot 43$
$589 = 19 \cdot 31$	$961 = 31 \cdot 31$	$1271 = 31 \cdot 41$
$629 = 17 \cdot 37$	$989 = 23 \cdot 43$	$1273 = 19 \cdot 67$
$667 = 23 \cdot 29$	$1003 = 17 \cdot 59$	$1333 = 31 \cdot 43$
$697 = 17 \cdot 41$	$1007 = 19 \cdot 53$	$1343 = 17 \cdot 79$
$703 = 19 \cdot 37$	$1037 = 17 \cdot 61$	$1349 = 19 \cdot 71$
$713 = 23 \cdot 31$	$1073 = 29 \cdot 37$	$1357 = 23 \cdot 59$
$731 = 17 \cdot 43$	$1081 = 23 \cdot 47$	$1363 = 29 \cdot 47$

Table 4.2. Composite numbers less than 1369 with least prime factor 17 or more

4.4. The infinity of primes

The following has been known for well over two thousand years.

Theorem 37 (Euclid, IX.20)**.** *There are more than any number of primes.*

Proof. Suppose we have n primes, say $p_1, \ldots, p_n$. Then $p_1 \cdots p_n + 1$ has a prime factor by Theorem 32, and this factor is not one of the p_k. □

There are many proofs of this ancient theorem. A recent proof by Filip Saidak [33] is as follows.[3] Define $a_0 = 2$ and $a_{n+1} = a_n(1 + a_n)$. Suppose $k < n$.

positive integers that are less than 5000 and are indivisible by 5, along with their least prime factors. As a check, I noted that my table should contain 48 numbers, namely

- 17 times one of 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79;
- 19 times one of 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71;
- 23 times one of 23, 29, 31, 37, 41, 43, 47, 53, 59;
- 29 times one of 29, 31, 37, 41, 43, 47;
- 31 times one of 31, 37, 41, 43.

Having copied what should be these products from Burton's table, along with their smaller prime factors, I used a pocket calculator to find the other factors and thus verify the numbers.

[3] I learned of the proof from *Matematik Dünyası* (2007-II [no. 73], p. 69). I write this book for myself and my students; but it is on the web. A colleague of Dr Saidak's found it and informed Dr Saidak, who kindly sent me a copy of his original paper.

Then $a_k \mid a_{k+1}$, and $a_{k+1} \mid a_{k+2}$, and so on, up to $a_{n-1} \mid a_n$, so $a_k \mid a_n$. Similarly, since $1 + a_k \mid a_{k+1}$, we have $1 + a_k \mid a_n$. Therefore $\gcd(1 + a_k, 1 + a_n) = 1$. Thus any two elements of the infinite set $\{1 + a_n : n \in \mathbb{N}\}$ are co-prime.

For yet another proof, using the full Fundamental Theorem of Arithmetic (Theorem 34), we consider the product

$$\prod_p \frac{1}{1 - 1/p},$$

which is certainly well defined if there are only finitely many primes. Each factor in the product is the sum of a **geometric series:**

$$\frac{1}{1 - 1/p} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots = \sum_{k=0}^{\infty} \frac{1}{p^k}.$$

We have now

$$\prod_p \frac{1}{1 - 1/p} = \prod_p \sum_{k=0}^{\infty} \frac{1}{p^k},$$

a product of sums (of infinitely many addends). By distributivity of multiplication over addition, this product of sums is also a sum of (infinitely many) products, and each of these products has, as a factor, an addend from each of the original sums. Such a product then is of the form

$$\prod_p \frac{1}{p^{k(p)}}, \tag{$\dagger$}$$

where $k(p) \geqslant 0$. This product is $1/k$ for some positive integer k. Moreover, by the Fundamental Theorem of Arithmetic as expressed in $(*)$, for each positive integer k, the reciprocal $1/k$ arises as a product as in $(\dagger)$ in exactly one way. Therefore, under the assumption that there are finitely many primes, we have

$$\prod_p \frac{1}{1 - 1/p} = \sum_{n=1}^{\infty} \frac{1}{n}. \tag{$\ddagger$}$$

But this is the **harmonic series,** which diverges:

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{1}{n} &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots \\
&\geqslant 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots \\
&= 1 + \frac{1}{2} \quad + \quad \frac{1}{2} \quad + \quad \frac{1}{2} \quad + \quad \cdots
\end{aligned}$$

Therefore there are infinitely many primes.

The same computations that give (‡) yield also

$$\prod_p \frac{1}{1-1/p^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}. \qquad (\S)$$

The sum converges, when $s > 1$, to the value denoted by $\zeta(s)$; this is the **Riemann zeta function** of s. Then the product also converges, in the sense that

$$\lim_{n\to\infty} \prod_{p\leqslant n} \frac{1}{1-1/p^s} = \zeta(s).$$

Hardy and Wright [21, p. 246] describe (§) as 'an analytical expression of the fundamental theorem of arithmetic.'

4.5. Bertrand's Postulate

We shall prove one result on the distribution of primes, namely the so-called Bertrand's Conjecture, Theorem 39 below. The proof does use a bit of analysis, though this could be eliminated.[4] given an arbitrary positive real number x, we define

$$\vartheta(x) = \sum_{p\leqslant x} \log p.$$

Here of course $\log x$ is the **natural logarithm** of x, that is,

$$\log x = \int_1^x \frac{\mathrm{d}t}{t}.$$

So $\vartheta(x) = \log \prod_{p\leqslant x} p$. For example, $\vartheta(\pi) = \vartheta(3) = \log 2 + \log 3 = \log 6$. If $x < 2$, then $\vartheta(x) = 0$. We could work with $\mathrm{e}^{\vartheta(x)}$ instead, which is an integer if x is; this is the only case we need consider; but there is no harm in giving a more general treatment.

Lemma. *For all positive real numbers x,*

$$\vartheta(x) < 2x \log 2.$$

[4] The proof here is based on that of Hardy and Wright [21, §22.3], who attribute it to Paul Erdős [11]. Note that Erdős's paper appeared in 1932, and Erdős was born in 1913. An earlier proof, from 1919, is due to Srinivasa Ramanujan [30]; this proof is very short (2 pages), but makes use of the Gamma function (defined in §2.4) and the so-called *Stirling's approximation* to it. Hardy and Wright attribute the earliest proof of Bertrand's Postulate to Tchebyshef in 1850.

Proof. It is enough to prove the claim when x is a positive integer n. We shall use strong induction. We have

$$\vartheta(2m) = \vartheta(2m-1),$$

so the claim holds when n is an *even* positive integer, provided it holds for lesser positive integers n.

We now show that the claim holds when n is an *odd* positive integer, provided it holds for lesser positive integers n. We have

$$\begin{aligned}\vartheta(2m+1) &= \vartheta(2m+1) - \vartheta(m+1) + \vartheta(m+1)\\ &= \sum_{m+1<p\leqslant 2m+1} \log p + \vartheta(m+1).\end{aligned}$$

Now, each p such that $m+1 < p \leqslant 2m+1$ is a factor of $(2m+1)!$ that is not also a factor of $(m+1)!$. We also have

$$\frac{(2m+1)!}{(m+1)!\cdot m!} = \binom{2m+1}{m+1},$$

which is an integer, and each p such that $m+1 < p \leqslant 2m+1$ must be a factor of *this* too. Therefore

$$\vartheta(2m+1) \leqslant \log\binom{2m+1}{m+1} + \vartheta(m+1).$$

Now, we have also

$$\binom{2m+1}{m+1} = \binom{2m+1}{m},$$

and these are terms in the expansion of $(1+1)^{2m+1}$; so

$$2\binom{2m+1}{m+1} \leqslant 2^{2m+1}.$$

Therefore

$$\begin{aligned}\vartheta(2m+1) &\leqslant \log(2^{2m}) + \vartheta(m+1)\\ &= 2m\log 2 + \vartheta(m+1).\end{aligned}$$

In particular, if $\vartheta(m+1) < 2(m+1)\log 2$, then $\vartheta(2m+1) < 2(2m+1)\log 2$. Thus the claim holds when n is odd if it holds for lesser n. □

We should also observe:[5]

[5] Erdős attributes the result to Legendre. For another proof, see Exercise 33.

Theorem 38. *For all positive integers n,*

$$\log n! = \sum_{p \leqslant n} \log p \sum_{j=1}^{\infty} \Big[\frac{n}{p^j}\Big],$$

that is, the number of times that p divides $n!$ (that is, the greatest k such that $p^k \mid n!$) is $\sum_{j=1}^{\infty}[n/p^j]$.

Proof. The number of times that p divides $n!$ is the sum of:

- the number of multiples ℓp such that $\ell p \leqslant n$,
- the number of multiples ℓp^2 such that $\ell p^2 \leqslant n$,
- and so on.

That is, it is the sum over all j of those ℓp^j such that $\ell p^j \leqslant n$; but the number of such multiples ℓp^j is $[n/p^j]$. In other words, p divides $n!$ once for each entry in each of the lists

$$p, 2p, \ldots, \Big[\frac{n}{p}\Big]p; \qquad p^2, 2p^2, \ldots, \Big[\frac{n}{p^2}\Big]p^2; \qquad \ldots \qquad \square$$

Theorem 39 (Bertrand's Postulate)**.** *For every positive integer n there is a prime p such that*

$$n < p \leqslant 2n.$$

Proof. Note that the claim is equivalent to the claim that the sequence 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631 of primes, where each successive term is less than twice the previous term, can be continued indefinitely. Suppose the claim fails for some n. Then we must have $n \geqslant 631$: in particular, $n \geqslant 2^9$. There are exponents $k(p)$ such that

$$\binom{2n}{n} = \prod_{p \leqslant n} p^{k(p)}.$$

By the last theorem, since $\log \binom{2n}{n} = \log\big((2n)!\big) - 2\log(n!)$, we have

$$k(p) = \sum_{j=1}^{\infty} \Big(\Big[\frac{2n}{p^j}\Big] - 2\Big[\frac{n}{p^j}\Big] \Big). \qquad (\P)$$

Suppose $2n/3 < p \leqslant n$. Then $2p \leqslant 2n < 3p$, so that $[2n/p] = 2$. Also

$$p^2 > \frac{4n^2}{9} = \frac{2n}{9} \cdot 2n > 2n$$

and hence $[2n/p^2] = 0$. Therefore $k(p) = 0$. We have now

$$\binom{2n}{n} = \prod_{p \leqslant 2n/3} p^{k(p)}.$$

Also, by the earlier lemma,

$$\sum_{p|\binom{2n}{n}} \log p \leqslant \sum_{p\leqslant 2n/3} \log p = \vartheta(2n/3) \leqslant \frac{4n}{3}\log 2.$$

In the series expansion (¶) for $k(p)$, each term $[2n/p^j] - 2[n/p^j]$ is 0 if $[2n/p^j]$ is even, and 1 if $[2n/p^j]$ is odd. Also the term is 0 if $p^j > 2n$, that is, $j > \log(2n)/\log p$. This then is a bound for $k(p)$, that is,

$$k(p) \leqslant \frac{\log(2n)}{\log p}. \qquad (\|)$$

Therefore, if $k(p) \geqslant 2$, then

$$2\log p \leqslant k(p)\log p \leqslant \log(2n),$$

so in particular $p \leqslant \sqrt{(2n)}$. That is, $\sqrt{(2n)}$ is a bound on the number of p such that $k(p) \geqslant 2$. By the bound $(\|)$ on $k(p)$ itself, we have now

$$\sum_{k(p)\geqslant 2} k(p)\log p \leqslant \sum_{k(p)\geqslant 2} \log(2n) \leqslant \sqrt{(2n)}\log(2n).$$

Therefore

$$\begin{aligned}\log\binom{2n}{n} &= \sum_{k(p)=1} \log p + \sum_{k(p)\geqslant 2} k(p)\log p \\ &\leqslant \sum_{p|\binom{2n}{n}} \log p + \sqrt{(2n)}\log(2n) \\ &\leqslant \frac{4n}{3}\log 2 + \sqrt{(2n)}\log(2n).\end{aligned}$$

Also,

$$2^{2n} = \sum_{j=0}^{2n}\binom{2n}{j} = 2 + \sum_{j=1}^{2n-1}\binom{2n}{j} \leqslant 2n\binom{2n}{n}.$$

Taking logarithms yields

$$\begin{aligned}2n\log 2 &\leqslant \log(2n) + \log\binom{2n}{n} \\ &\leqslant \log(2n) + \frac{4n}{3}\log 2 + \sqrt{(2n)}\log(2n),\end{aligned}$$

which gives

$$\frac{2n}{3}\log 2 \leqslant \big(1 + \sqrt{(2n)}\big)\log(2n). \qquad (**)$$

Now, $\log x$ grows more slowly than any power of x; so the last inequality should fail if n is large enough. We complete the proof by showing that the inequality fails when, as we have assumed, $n \geqslant 2^9$. To this end, we define

$$\zeta = \frac{\log n - \log 2^9}{\log 2^{10}} = \frac{\log n - 9\log 2}{10\log 2},$$

so that $1 + \zeta = \log(2n)/10\log 2$ and $2n = 2^{10(1+\zeta)}$. From the inequality $(**)$, we have now

$$\begin{aligned} 2n\log 2 &\leqslant 3\bigl(1+\sqrt{(2n)}\bigr)\log(2n), \\ 2^{10(1+\zeta)}\log 2 &\leqslant 3(1+2^{5(1+\zeta)})\cdot 10(1+\zeta)\log 2, \\ 2^{10(1+\zeta)} &\leqslant 30(1+2^{5(1+\zeta)})(1+\zeta), \\ 2^{5(1+\zeta)} &\leqslant 30(2^{-5(1+\zeta)}+1)(1+\zeta). \end{aligned}$$

Since $\zeta > 0$, we have

$$\begin{aligned} 2^{5\zeta} &\leqslant \frac{2^5-2}{2^5}(2^{-5(1+\zeta)}+1)(1+\zeta) \\ &\leqslant (1-2^{-4})(1+2^{-5})(1+\zeta) \\ &\leqslant 1+\zeta. \end{aligned}$$

But this cannot be, since

$$2^{5\zeta} = \mathrm{e}^{5\zeta\log 2} \geqslant 1 + 5\zeta\log 2 > 1+\zeta$$

because of the series expansion $\mathrm{e}^x = \sum_{j=0}^{\infty} x^j/j!$. □

Some further theorems about the distribution of primes are stated without their proofs in Appendix B.

5. Computations with congruences

5.1. Exponentiation

Computing powers with respect to a modulus can be achieved by successively squaring and taking residues. This is justified by Theorem 23 on page 40. For example, with respect to the modulus 43, to compute 35^{14}, we can first note $35 \equiv -8$, so

$$35^{14} \equiv (-8)^{14} \equiv (-1)^{14} \cdot 8^{14} \equiv 8^{14}.$$

Also, $14 = 8 + 4 + 2 = 2^3 + 2^2 + 2^1$, so $8^{14} = 8^8 \cdot 8^4 \cdot 8^2$; and

$$8^2 = 64 \equiv 21, \qquad 21^2 = 441 \equiv 11, \qquad 11^2 = 121 \equiv -8,$$

so that

$$35^{14} \equiv -8 \cdot 11 \cdot 21 \equiv -88 \cdot 21 \equiv -2 \cdot 21 \equiv -44 \equiv 1.$$

5.2. Inversion

A special case of Theorem 23 is the implication

$$a \equiv b \pmod{n} \implies ac \equiv bc \pmod{n}. \qquad (*)$$

The converse fails, because, for example, possibly $c \equiv 0\ (n)$. Even if this case is excluded, the converse still fails:

$$1 \cdot 4 \equiv 10 \cdot 4 \pmod{6}, \qquad 1 \not\equiv 10 \pmod{6}. \qquad (\dagger)$$

The reason why we cannot cancel 4 here is that 4 and 6 have a nontrivial common divisor, in this case 2. The converse of $(*)$ does hold if c and n are co-prime:

Theorem 40. *If* $\gcd(c, n) = 1$*, then*

$$ac \equiv bc \bmod n \implies a \equiv b \bmod n.$$

Proof. The claim is a restatement of Theorem 28 on page 43. □

Hence, considering $(\dagger)$ again, since $1 \cdot 4 \equiv 10 \cdot 4\ (3)$, we have

$$1 \equiv 10 \pmod{3}.$$

The general result is the following:

Theorem 41. *For all positive moduli n, for all integers a, b, and c,*

$$ac \equiv bc \bmod n \iff a \equiv b \bmod \frac{n}{\gcd(c,n)}.$$

Proof. Let $d = \gcd(c,n)$. Then $\gcd(c/d, n/d) = 1$ by Theorem 26. Hence

$$\begin{aligned} ac \equiv bc \bmod n &\implies \frac{ac}{d} \equiv \frac{bc}{d} \bmod \frac{n}{d} \\ &\implies a \equiv b \bmod \frac{n}{d} \end{aligned}$$

by the last theorem. Conversely,

$$\begin{aligned} a \equiv b \bmod \frac{n}{d} &\implies \frac{n}{d} \mid b - a \\ &\implies \frac{cn}{d} \mid bc - ac \\ &\implies n \mid bc - ac \\ &\implies ac \equiv bc \bmod n. \end{aligned}$$

□

For example, $6x \equiv 6 \ (9) \iff x \equiv 1 \ (3)$.
A longer problem is to solve

$$70x \equiv 18 \pmod{134}.$$

This reduces to

$$35x \equiv 9 \pmod{67}, \tag{‡}$$

and solutions of this correspond to solutions to the Diophantine equation

$$35x + 67y = 9. \tag{§}$$

By Bézout's Lemma (the corollary to Theorem 25 on page 42), this is soluble if and only if $\gcd(35, 67) \mid 9$. We find $\gcd(35, 67)$ by the Euclidean algorithm:

$$\begin{aligned} 67 &= 35 \cdot 1 + 32, \\ 35 &= 32 \cdot 1 + 3, \\ 32 &= 3 \cdot 10 + 2, \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

so $\gcd(35, 67) = 1$. To find the solutions to (§), or rather to $35x + 67y = 1$, we rearrange the computations, getting

$$\begin{aligned} 32 &= 67 - 35, \\ 3 &= 35 - 32 = 35 - (67 - 35) = 35 \cdot 2 - 67, \\ 2 &= 32 - 3 \cdot 10 = 67 - 35 - (35 \cdot 2 - 67) \cdot 10 = 67 \cdot 11 - 35 \cdot 21, \\ 1 &= 3 - 2 = 35 \cdot 2 - 67 - 67 \cdot 11 + 35 \cdot 21 = 35 \cdot 23 - 67 \cdot 12. \end{aligned}$$

In particular,

$$35 \cdot 23 \equiv 1 \pmod{67}, \tag{¶}$$

so $\gcd(23, 67) = 1$, and (‡) is equivalent to

$$x \equiv 23 \cdot 9 \equiv 207 \equiv 6 \pmod{67},$$
$$x \equiv 6, 73 \pmod{134}.$$

A way to read (¶) is that 23 is an **inverse** of 35 with respect to the modulus 67. We can express this by

$$23 \equiv \frac{1}{35} \pmod{67}.$$

In particular, 35 is invertible as an element of $\mathbb{Z}_{67}$. We have in general

Theorem 42. *With respect to a modulus, a number is invertible if and only if it is prime to the modulus.*

Proof. The following are equivalent by Bézout's Lemma (the corollary to Theorem 25):

a) a is invertible *modulo* n,
b) the congruence $ax \equiv 1 \pmod{n}$ is soluble,
c) the diophantine equation $ax + ny = 1$ is soluble,
d) $\gcd(a, n) = 1$. □

5.3. Chinese remainder problems

The first known example of a so-called **Chinese remainder problem** is 3.26 in the *Sunzi suan jing* (*Mathematical Classic of Master Sun*), which is 'most probably a work of the fourth or early fifth century CE' [24, p. 295]. The problem and its supplied 'solution' read thus:

> Now there are an unknown number of things. If we count by threes, there is a remainder 2; if we count by fives, there is a remainder 3; if we count by sevens, there is a remainder 2. Find the number of things. Answer: 23.
>
> Method: If we count by threes and there is a remainder 2, put down 140. If we count by fives and there is a remainder 3, put down 63. If we count by sevens and there is a remainder 2, put down 30. Add them to obtain 233 and subtract 210 to get the answer. If we count by threes and there is a remainder 1, put down 70. If we count by fives and there is a remainder 1, put down 21. If we count by sevens and there is a remainder 1, put down 15. When [a number] exceeds 106, the result is obtained by subtracting 105. [24, p. 299]

In our terms, the problem is to solve three congruences simultaneously:

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 7.$$

Note that $3 \cdot 5 \cdot 7 = 105$. The given solution is

$$x \equiv 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 \pmod{105}.$$

This *is* a solution, because

$$\begin{aligned} &70 \equiv 1 \pmod 3, \quad &&21 \equiv 0 \pmod 3, \quad &&15 \equiv 0 \pmod 3, \\ &70 \equiv 0 \pmod 5, \quad &&21 \equiv 1 \pmod 5, \quad &&15 \equiv 0 \pmod 5, \\ &70 \equiv 0 \pmod 7, \quad &&21 \equiv 0 \pmod 7, \quad &&15 \equiv 1 \pmod 7. \end{aligned}$$

This is the *only* solution, by the corollary to Theorem 30 on page 45. The key to the solution is finding the numbers 70, 21, and 15. Note that

$$70 = (5 \cdot 7) \cdot 2, \qquad 21 = (3 \cdot 7) \cdot 1, \qquad 15 = (3 \cdot 5) \cdot 1.$$

So the real problem is to find the coefficients 2, 1, and 1, which are, respectively, inverses of $5 \cdot 7$, $3 \cdot 7$, and $3 \cdot 5$, with respect to 3, 5, and 7. When they exist, such inverses can be found by means of the Euclidean algorithm, as in the previous section.

The general problem is now solved as follows:

Theorem 43. *If moduli $n_1, \ldots, n_k$ are given, each being prime to the rest, then every system of congruences*

$$x \equiv a_1 \bmod n_1, \qquad x \equiv a_2 \bmod n_2, \qquad \ldots, \qquad x \equiv a_k \bmod n_k, \quad (\|)$$

has a solution, which is unique modulo *the product N of the moduli. This solution is given by*

$$x \equiv a_1 \cdot \frac{N}{n_1} \cdot m_1 + \cdots + a_k \cdot \frac{N}{n_k} \cdot m_k \pmod N,$$

where m_i is an inverse of N/n_i with respect to n_i.

This theorem will be discussed more theoretically in §9.1. Meanwhile, we have given the theorem in a 'self-proving' formulation: the proposed solution is easily seen to be a solution, and as noted above, there can be no others.[1]

It may be useful to consider the case of two congruences,

$$x \equiv a \pmod n, \qquad x \equiv b \pmod m, \qquad (**)$$

[1] The notion of a *self-proving theorem* is introduced and discussed by Barry Mazur [27].

where $\gcd(n, m) = 1$. For some r and s, we have

$$nr \equiv 1 \pmod{m}, \qquad ms \equiv 1 \pmod{n}, \tag{††}$$

so that the solution to (∗∗) is

$$x \equiv ams + bnr \pmod{nm}.$$

In finding this solution, we *could* choose r and s by means of the Euclidean algorithm, so that

$$nr + ms = 1;$$

but all we really need is (††). Moreover, we need not actually calculate both r and s. Indeed, the solutions of (∗∗) are just those sums $a + nt$ in which t is such that $m \mid a - b + nt$, that is,

$$b - a \equiv nt \pmod{m}; \tag{‡‡}$$

so $t \equiv r(b-a) \pmod{m}$. We need not even calculate r; we can just hunt through a complete set of residues with respect to m for a value of t as in (‡‡).

For example, the following problem is attributed to Brahmagupta:[2]

> An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

If x is that number, then

$$x \equiv 1 \pmod{2, 3, 4, 5, 6}, \qquad x \equiv 0 \pmod{7}.$$

Since $\operatorname{lcm}(2, 3, 4, 5, 6) = 60$, the problem is to find the least positive solution to

$$x \equiv 1 \pmod{60}, \qquad x \equiv 0 \pmod{7}.$$

so $x = 1 + 60t$, where t is least such that $7 \mid 1 + 60t$, that is,

$$-1 \equiv 60t \equiv 4t \pmod{7}.$$

By trial, $t = 5$, and therefore $x = 301$.

[2] My source for the problem is `http://www.chinapage.com/math/crt.html` (accessed December 14, 2010), where the problem is prefaced with the remark, 'Oystein Ore mentions another puzzle with a dramatic element from Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD)'. The page also gives the problem of Sunzi [Master Sun] quoted on page 66 above. The Brahmagupta problem is the basis of an exercise in Burton [7, Prob. 4.4.8–9, p. 83]. But the problem is not among the works of Brahmagupta given in the Katz volume [24].

6. Powers of two

6.1. Perfect numbers

Of the 13 books of Euclid's *Elements,* Books VII, VIII and IX concern numbers. The last proposition in these books is about **perfect** numbers, namely those numbers that are the sums of their (positive) proper divisors. For example, 6 and 28 are perfect since

$$6 = 1 + 2 + 3, \qquad 28 = 1 + 2 + 4 + 7 + 14.$$

Euclid gives a sufficient condition for being perfect. The proof uses that

$$1 + 2 + 4 + \cdots + 2^{k-1} = 2^k - 1.$$

Theorem 44 (Euclid, IX.36)**.** *If* $2^k - 1$ *is prime, then* $2^{k-1} \cdot (2^k - 1)$ *is perfect.*

Proof. If $2^k - 1$ is prime, then the positive divisors of $2^{k-1} \cdot (2^k - 1)$ are the divisors of 2^{k-1}, perhaps multiplied by $2^k - 1$; namely, they are:

$$\begin{array}{llll} 1, & 2, & 4, & \ldots, \quad 2^{k-1}, \\ 2^k - 1, & 2 \cdot (2^k - 1), & 4 \cdot (2^k - 1), & \ldots, \quad 2^{k-1} \cdot (2^k - 1). \end{array}$$

The sum of these is $(1 + 2 + 4 + \cdots + 2^{k-1}) \cdot 2^k$, which is $(2^k - 1) \cdot 2^k$. Subtracting the improper divisor $2^{k-1} \cdot (2^k - 1)$ leaves the same. □

Theorem 28 has a partial converse:[1]

Theorem 45. *Every* even *perfect number is* $2^{k-1} \cdot (2^k - 1)$ *for some* k *such that* $2^k - 1$ *is prime.*

Proof. Let us write $\sigma(n)$ for the sum of the positive divisors of n. Suppose n is an even perfect number. Then $n = 2^{k-1}m$ for some k and m, where $k > 1$ and m is odd. Every factor of n is uniquely the product of a factor of 2^{k-1} and a factor of m, so

$$\sigma(n) = \sigma(2^{k-1}) \cdot \sigma(m) = (1 + 2 + \cdots + 2^{k-1}) \cdot \sigma(m) = (2^k - 1) \cdot \sigma(m).$$

Since we assume $\sigma(n) = 2n$, we have now

$$2^k m = (2^k - 1) \cdot \sigma(m).$$

[1] According to Dickson [10, p. 19], Euler's proof of this was published posthumously in 1849.

In particular, $2^k \mid \sigma(m)$, so $\sigma(m) = 2^k \cdot \ell$ for some ℓ. Then

$$m = (2^k - 1) \cdot \ell = \sigma(m) - \ell, \qquad \sigma(m) = m + \ell.$$

Since m and ℓ are two distinct factors of m, they must be the *only* positive factors. In particular, $\ell = 1$, and m is prime, so n is as desired.[2] □

In his excellent textbook *Elementary Number Theory* [25] (first published in German in 1927), Edmund Landau (1877–1938) writes, before proving the foregoing theorems:

> This old-fashioned concept of perfect number, and the questions associated with it, are not especially important; we consider them only because, in so doing, we will encounter two questions that remain unanswered to this day: Are there infinitely many perfect numbers? Is there an odd perfect number? Modern mathematics has solved many (apparently) difficult problems, even in number theory; but we stand powerless in the face of such (apparently) simple problems as these. Of course, the fact that they have never been solved is irrelevant to the rest of this work. We will leave no gaps; when we come to a bypath which leads to an insurmountable barrier, we will turn around, rather than—as is so often done—continue on beyond the barrier.

The questions that Landau cites are still unanswered. It is also the aim of the present book to leave no gaps (except for the unproved theorems in Appendix B, which however we shall never use).

6.2. Mersenne primes

The number $2^n - 1$ is called a **Mersenne number,** after Marin Mersenne, 1588–1648; if the number is prime, it is a **Mersenne prime.** Since we do not know whether there are infinitely many even perfect numbers, we do not know whether there are infinitely many Mersenne primes. However, we do have the following necessary condition for being a Mersenne prime:[3]

Theorem 46. *if $2^n - 1$ is prime, then so must n be.*

Proof. We have $2^k - 1 \mid 2^{k\ell} - 1$ from the identity

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1).$$ □

So every Mersenne prime is $2^p - 1$ for some p; but the converse fails,[4] as shown in Table 6.1.[5] For every p in the table such that $2^p - 1$ is not prime, we have

[2] Exercise 43 asks how we have used that n is even.

[3] Stated by Fermat in a letter of 1640 to Mersenne, according to Dickson [10, p. 12].

[4] The counterexample $2^{11} = 2047 = 23 \cdot 89$ was apparently known to Ulrich Regius in 1536 [10, pp. III & 7]. However, see Theorem 49 on page 76.

[5] I have not personally verified that $2^p - 1$ is prime when p is 13, 17, or 19; nor have I verified that 178481 is prime.

p	$2^p - 1$	factorization	$2^{p-1}(2^p - 1)$
2	3	–	6
3	7	–	28
5	31	–	496
7	127	–	8128
11	2047	$23 \cdot 89$	
13	8191	–	33550336
17	131071	–	8589869056
19	524287	–	137438691328
23	8388607	$47 \cdot 178481$	

Table 6.1. Mersenne primes and perfect numbers

$2p + 1$ is prime, and $2p + 1 \cong \pm 1$ (8). A odd prime p such that $2p + 1$ is also prime is called a **Germain prime.**[6] Later, with Theorem 91 on page 127, we shall have that if $2p + 1$ is a prime q, and $q \cong \pm 1$ (8), then $2^p - 1$ is not prime, because q is a factor, that is,

$$2^p \equiv 1 \pmod{q}.$$

[6] Named for Sophie Germain, 1776–1831.

7. Prime moduli

7.1. Fermat's Theorem

On October 10, 1640, Pierre de Fermat (1601–65) wrote the following in a letter to Bernard Frénicle de Bessy (1605–1675):[1]

> Every prime number is always a factor of one of the powers of any [geometric] progression minus 1, and the exponent of this power is a divisor of the prime number minus 1. After one has found the first power that satisfies the proposition, all those powers of which the exponents are multiples of the exponent of the first power also satisfy the proposition.
>
> *Example:* Let the given progression be
>
> | 1 | 2 | 3 | 4 | 5 | 6 | |
> |---|---|---|---|---|---|---|
> | 3 | 9 | 27 | 81 | 243 | 729 | etc. |
>
> with its exponents written on top.
>
> Now take, for instance, the prime number 13. It is a factor of the third power minus 1, of which 3 is the exponent and a divisor of 12, which is one less than the number 13, and because the exponent of 729, which is 6, is a multiple of the first exponent, which is 3, it follows that 13 is also a factor of this power 729 minus 1.
>
> And this proposition is generally true for all progressions and for all prime numbers, of which I would send you the proof if I were not afraid to be too long.

More symbolically, the claim is:

1. For all p, for all a [such that $p \nmid a$—Fermat does not appear to make this condition explicit], there is some positive n such that $p \mid a^n - 1$.
2. If k is the least such n, then $k \mid p - 1$.
3. In this case, if $k \mid m$, then $p \mid a^m - 1$.

A consequence of the claim is that, if $p \nmid a$, then $p \mid a^{p-1} - 1$. This is called *Fermat's Theorem*.[2]

[1] The letter was in French; I take this selection, in translation, from Struik's anthology [34, p. 28]. The translator of Gauss assigns to what must be the same letter the date of October 18, 1640 [16, p. 32, n. 1].

[2] The theorem is sometimes called Fermat's *Little* Theorem, as opposed to the so-called Fermat's *Last* Theorem (see page 20, note 6).

A proof of this theorem was found among the writings of Leibniz (1646–1716) [10, p. 59]. The first *published* proof was by Euler, in 1736.[3] This proof uses the following:

Lemma. *If* $0 < k < p$*, then*

$$p \mid \binom{p}{k}.$$

Proof. If $0 < k < p$, then p divides $p!$, but not $k!$ or $(p-k)!$. Since

$$p! = \binom{p}{k} \cdot k!(p-k)!,$$

the claim follows from Theorem 33 on page 51. □

Theorem 47 (Fermat)**.** *For all* a*,*

$$a^p \equiv a \pmod{p}. \tag{$*$}$$

Consequently, for all positive m *and* n*,*

$$m \equiv n \bmod (p-1) \implies a^m \equiv a^n \bmod p.$$

If $p \nmid a$*, that is,* $\gcd(p, a) = 1$*, then*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{$\dagger$}$$

Proof (Euler). We use induction. The claim $(*)$ holds trivially when $a = 1$. If it holds when $a = b$, then by the lemma,

$$(b+1)^p \equiv b^p + 1^p \equiv b + 1 \pmod{p},$$

so the claim holds when $a = b+1$. Therefore $(*)$ holds for all a. We now have $(\dagger)$ by Theorem 40 on page 64. □

Induction normally proves something true for all *positive* integers. But $(*)$ holds for *all* integers a, and Euler's proof establishes this, since every integer is congruent *modulo* p to a positive integer, and if $a \equiv b\ (p)$, then $a^p \equiv b^p\ (p)$ by Theorem 23. Alternatively, we can understand the proof as establishing $a^p = a$ for all a in $\mathbb{Z}_p$. Induction still works here; it just takes us around in a circle, from 1, to 2, to 3, and so on up to p, and then back to 1. (See Figure 7.1.) In particular, $\mathbb{Z}_p$ is one of the sets mentioned after the Axiom in §2.1, in which only part of the Axiom is satisfied. Indeed, $\mathbb{Z}_p$ allows induction, but here 1 is the successor of p.

[3] This is stated by Gauss in the *Disquisitiones Arithmeticae* [16, ¶50] and confirmed by Dickson [10, p. 60] and Struik [34, p. 35, n. 2].

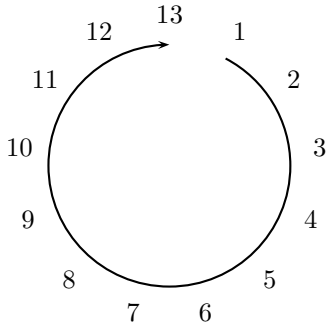


Figure 7.1. The integers *modulo* 13, or $\mathbb{Z}_{13}$

Euler later proved the more general claims of Fermat in the quotation above.[4] In particular, he showed that, if $p \nmid a$, then there is some λ such that $\lambda > 1$ and $p \mid a^\lambda - 1$. The *least* such λ is what we shall call the *order* of a *modulo* p in §10.1. If λ is this order, then Euler showed $\lambda \mid p-1$, and then $p \mid a^{p-1} - 1$. He later generalized this result, establishing what is called Euler's Theorem (Theorem 66 on page 95).[5]

There is yet another proof of Fermat's Theorem, published by James Ivory in 1806 [23].[6] Perhaps it is the best. If $\gcd(a, p) = 1$, then the products a, $2a$, ..., $(p-1)a$ are all incongruent *modulo* p, since

$$ia \equiv ja \bmod p \implies i \equiv j \bmod p$$

by Theorem 40. But 1, 2, ..., $p-1$ are also incongruent. By Theorem 22, there are only $p-1$ numbers that are incongruent with each other and 0 *modulo* p; so the numbers a, $2a$, ..., $(p-1)a$ are congruent respectively to 1, 2, ..., $p-1$ in some order. Now multiply the numbers on each side together:

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod p.$$

Since $(p-1)!$ and p are co-prime, we can conclude (†). This implies (∗) in case $p \nmid a$; but if $p \mid a$, then (∗) is obvious.

With Fermat's Theorem, we can compute residues of large powers easily. For example,

$$6^{58} \equiv 6^{48+10} \equiv (6^{16})^3 \cdot 6^{10} \equiv 6^{10} \pmod{17}.$$

[4] Euler's treatment can be read in Struik [34, pp. 31–5].

[5] An account of this is in Dickson [10, p. 61].

[6] According to Dickson [10, p. 65], this proof was later rediscovered and published by Dirichlet in 1828. Landau [25, p. 50] uses the proof. Hardy and Wright [21, p. 63] also use it, but the historical information that they supply about Fermat's and Euler's theorems does not address this proof.

We can continue the computation as in §5.1, by analyzing the exponent 10 as a sum of powers of 2. Since $10 = 8 + 2$, we have $6^{10} = 6^8 \cdot 6^2$; but $6^2 \equiv 36 \equiv 2$ (17), so $6^8 \equiv (6^2)^4 \equiv 2^4 \equiv 16 \equiv -1$ (17), and hence

$$6^{58} \equiv -2 \pmod{17}.$$

A contrapositive formulation of Fermat's Theorem is that, if $a^n \not\equiv a \pmod{n}$, then n must not be prime. For example, to see whether 133 is prime, we may note that $133 = 128 + 4 + 1 = 2^7 + 2^2 + 1$, so $2^{133} = 2^{2^7} \cdot 2^{2^2} \cdot 2$. Also,

$$\begin{aligned}
2^{2^2} &= 4; \\
2^{2^2} &= 4^2 = 16; \\
2^{2^3} &= 16^2 = 256 \equiv 123 \equiv -10 \pmod{133}; \\
2^{2^4} &\equiv (-10)^2 = 100 \equiv -33; \\
2^{2^5} &\equiv (-33)^2 = 1089 \equiv 25; \\
2^{2^6} &\equiv 25^2 = 625 \equiv -40; \\
2^{2^7} &\equiv (-40)^2 = 1600 \equiv 4. \qquad (\ddagger)
\end{aligned}$$

Therefore $2^{133} \equiv 4 \cdot 16 \cdot 2 \equiv -5 \pmod{133}$, so 133 must not be prime. Note an alternative computation after (‡): We have $2^{128} = 2^{2^7} \equiv 4 \equiv 2^2$, so $2^{126} \equiv 1$, hence $2^{133} = 2^{126+7} \equiv 2^7 = 128 \equiv -5$.

Now, if we just want to know whether 133 is prime, it is probably easier to use the theorems in §4.3. Indeed, $[\sqrt{133}] = 11$, so it is enough to test for divisibility by 2, 3, 5, 7, and 11. We find then $133 = 7 \cdot 19$.

Still, we may raise the theoretical question: Does Fermat's Theorem give us an *infallible* method for testing for primes? Can *every* composite number be detected by means of the theorem? The answer turns out to be no.

7.2. Carmichael numbers

The converse of Fermat's Theorem fails. It may be that $a^n \equiv a \pmod{n}$ for all a, although n is not prime. To see this, we first define n to be a **pseudo-prime** if n is composite, but

$$2^n \equiv 2 \pmod{n}.$$

To establish an example, we shall use:

Theorem 48. *If $p \neq q$, and $a^p \equiv a$ (q) and $a^q \equiv a$ (p), then $a^{pq} \equiv a$ (pq).*

Proof. Under the hypothesis, we have

$$a^{pq} = (a^p)^q \equiv a^q \equiv a \pmod{q},$$
$$a^{pq} = (a^q)^p \equiv a^p \equiv a \pmod{p},$$

and hence $a^{pq} \equiv a \pmod{\operatorname{lcm}(p,q)}$ by Theorem 30 and corollary. □

Then 341 is a pseudo-prime, since $341 = 11 \cdot 31$, and

$$2^{11} = 2048 = 31 \cdot 66 + 2 \equiv 2 \pmod{31},$$
$$2^{31} = (2^{10})^3 \cdot 2 \equiv 2 \pmod{11}.$$

We can now state and prove what resembles a converse to Theorem 46:

Theorem 49. *If n is a pseudo-prime, then so is $2^n - 1$.*

Proof. If n is a pseudo-prime, then it is not prime, so by Theorem 46, neither is $2^n - 1$. We also have $2^n \equiv 2 \pmod{n}$ by Fermat's Theorem; say $2^n - 2 = kn$. Then

$$2^{2^n-1} - 2 = 2 \cdot (2^{2^n-2} - 1) = 2 \cdot (2^{kn} - 1),$$

which has the factor $2^n - 1$; so $2^{2^n-1} \equiv 2 \pmod{2^n - 1}$. □

Pseudo-primes as we defined them can be called more precisely *pseudo-primes of base* 2. Then a pseudo-prime of base a is a composite number n such that $a^n \equiv a \pmod{n}$. A composite number that is a pseudo-prime of *every* base can be called an **absolute pseudo-prime.** It is also called a **Carmichael number** after Robert Daniel Carmichael (1879–1967), who published the first examples of such numbers in 1910 [8]. If n is a Carmichael number, then

$$a^{n-1} \equiv 1 \pmod{n}$$

whenever $\gcd(a, n) = 1$. We shall establish the converse of this in Theorem 80 on page 116.

Meanwhile, 561 is a Carmichael number. To see this, we first factorize 561 as $3 \cdot 11 \cdot 17$ and note

$$3 - 1 \mid 561 - 1, \qquad 11 - 1 \mid 561 - 1, \qquad 17 - 1 \mid 561 - 1,$$

that is, $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$. We now make the following observations.

a) If $3 \nmid a$, then $a^2 \equiv 1 \pmod{3}$, so $a^{560} \equiv 1 \pmod{3}$.

b) If $11 \nmid a$, then $a^{10} \equiv 1 \pmod{3}$, so $a^{560} \equiv 1 \pmod{11}$.

c) If $17 \nmid a$, then $a^{16} \equiv 1 \pmod{3}$, so $a^{560} \equiv 1 \pmod{17}$.

Hence if one of 3, 11, and 17 fails to divide a, then we have $a^{560} \equiv 1 \pmod{561}$ and therefore

$$a^{561} \equiv a \pmod{561}. \qquad (\S)$$

But if each of 3, 11, and 17 divides a, then $561 \mid a$, so again we have (§).

A positive integer is **squarefree** if it has no divisor p^2. The proof that 561 is an absolute pseudo-prime generalizes to establish the following:[7]

Theorem 50. *A number n greater than 1 is a prime or absolute pseudo-prime if it is squarefree and $p-1 \mid n-1$ whenever $p \mid n$.*

The sufficient condition given by the theorem for being an absolute pseudo-prime is **Korselt's Criterion,** so called after Alwin Reinhold Korselt (1864–1947), who proved its sufficiency and necessity in 1899, apparently without actually finding any absolute pseudo-primes. The term *Korselt's Criterion* is used by Alford *et al.* in their 1994 paper [1], where they prove that there are infinitely many absolute pseudo-primes.

We can prove the necessity of *part* of Korselt's Criterion now; the rest will have to wait until Theorem 75 (p. 109), when we have *primitive roots* of primes.

Theorem 51. *Every absolute pseudo-prime is squarefree.*

Proof. Suppose n is an absolute pseudo-prime. If $p^2 \mid n$, then

$$p^n \equiv p \pmod{p^2}.$$

But $n > 1$ (since it is composite), so $p^n \equiv 0 \pmod{p^2}$, and therefore $p \equiv 0 \pmod{p^2}$, which is absurd. □

7.3. Wilson's Theorem

Evidently $(p-1)! \not\equiv 0 \pmod{p}$. By the next theorem, the congruence

$$(p-1)! \equiv x \pmod{p} \qquad (\P)$$

has the same solution for all p, namely -1. This was known to Abu Ali al-Hasan ibn al-Haytham (965–1040)[8] and probably also to Leibniz. The theorem was published by Edward Waring (c. 1736–98) in 1770 and attributed to his student John Wilson (1741–93), so it is called Wilson's Theorem. However, the first published *proof* was by Joseph-Louis Lagrange (1736–1813) in 1773.[9]

Lagrange's proof makes use of a result that arises from considering successive differences of powers as in Table 7.1 below. (However, Lagrange's proof is not

[7] The proof is Exercise 49.

[8] According to `http://www-history.mcs.st-andrews.ac.uk/Biographies/Al-Haytham.html` (accessed December 19, 2010).

[9] The bare facts are in Dickson [10, p. 62].

$$
\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & & & & & & & \\

corresponding entry of row m of the array whose top row consists of powers of m. By inductive hypothesis, every entry of this row m is $m!$. This completes the induction.

This result gives us the $(p-1)!$ in Wilson's Theorem; the -1 that solves (¶) comes from a more general expression for successive differences:[10]

Lemma. *For all non-negative integers n, for all x in $\mathbb{R}$,*

$$n! = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} (x+k)^n.$$

Proof. Given a function f on $\mathbb{R}$, we define the function Δf by

$$\Delta f(x) = f(x+1) - f(x).$$

Then by recursion we define

$$\Delta^0 f = f, \qquad \Delta^{n+1} f = \Delta^n \Delta f.$$

By induction,

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k).$$

Indeed, the claim holds easily when $n = 0$, and if it holds when $n = m$, then by the computations in Table 7.2 (page 83), it holds when $n = m+1$.

Now we consider the special case when $f(x) = x^m$. We shall be done if we show that, if $0 \leqslant m \leqslant n$, then

$$\Delta^n(x^m) = \begin{cases} 0, & \text{if } m < n, \\ n!, & \text{if } m = n. \end{cases}$$

(Here of course $\Delta^n(x^m)$ stands for $\Delta^n f(x)$, where f is $x \mapsto x^m$.) The claim is easily true when $n = 0$. Suppose it is true when $n = s$. If $m \leqslant s$, then $\Delta^s(x^m)$ is a constant function of x, so $\Delta^{s+1}(x^m) = 0$. Considering the case $m = s+1$, we have

$$\begin{aligned} \Delta^{s+1}(x^{s+1}) &= \Delta^s\big((x+1)^{s+1} - x^{s+1}\big) \\ &= \Delta^s \sum_{k=0}^{s} \binom{s+1}{k} x^k \\ &= \sum_{k=0}^{s} \binom{s+1}{k} \Delta^s x^k \\ &= (s+1) \cdot s! \\ &= (s+1)!. \end{aligned}$$

[10] The lemma appears to be due to Euler [10, p. 63].

So the claim is true when $n = s + 1$. □

Theorem 52 (Wilson)**.** *Suppose $n > 1$. Then $(n-1)! \equiv -1 \pmod{n}$ if and only if*[11] *n is prime.*

Proof (Lagrange). Suppose n is not prime, so that $n = ab$, where $1 < a < n$. Then $a \leqslant n - 1$, so $a \mid (n-1)!$, so $a \nmid (n-1)! + 1$, so $n \nmid (n-1)! + 1$.

For the converse, from the lemma in case $n = p - 1$ and $x = 0$ we have

$$(p-1)! = \sum_{k=0}^{p-1} (-1)^{p-1-k} \binom{p-1}{k} k^{p-1}.$$

By Fermat's Theorem then,

$$\begin{aligned}(p-1)! &\equiv \sum_{k=1}^{p-1} (-1)^{p-1-k} \binom{p-1}{k} \\ &\equiv \sum_{k=0}^{p-1} (-1)^{p-1-k} \binom{p-1}{k} - 1 \\ &\equiv (1-1)^{p-1} - 1 \\ &\equiv -1 \pmod{p}.\end{aligned}$$

□

Wilson's Theorem gives a theoretical test for primality, though not a practical one.

For an alternative proof of the hard direction of Wilson's Theorem, we may note that, by Theorem 42, each number on the list $1, 2, 3, \ldots, p-1$ has an inverse *modulo* p. Also, $x^2 \equiv 1 \pmod{p}$ has only the solutions ± 1, that is, 1 and $p - 1$, since if $p \mid x^2 - 1$, then $p \mid x \pm 1$. So each number on the list $2, 3, \ldots, p-2$ has an inverse that is also on the list and is distinct from itself. Also the inverse of the inverse is the original number. Therefore the product of the numbers on the list is 1 *modulo* p. Consequently

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}.$$

For example, *modulo* 11, we have

$$1 \equiv 2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8,$$

and therefore

$$10! \equiv (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10 \equiv 10 \equiv -1.$$

[11] The *necessity* that n be prime was apparently not part of the original statement of Wilson's Theorem. Lagrange proved it [10, p. 63].

Since the modulus was small, the inverses here could be found by trial. With a larger modulus, the Euclidean Algorithm can be used as in §5.2.

We may also note that 2 has the following powers with respect to the modulus 11:

k	1	2	3	4	5	6	7	8	9	10	
2^k	2	4	8	5	10	9	7	3	6	1	mod 11

So every number that is prime to 11 is congruent to a power of 2. In particular, the invertible integers *modulo* 11 compose a multiplicative group generated by 2; we express this by saying 2 is a *primitive root* of 11. We shall investigate primitive roots in Chapter 10. Meanwhile, if in the last table, we write the residues that are least in absolute value, we get

k	1	2	3	4	5	6	7	8	9	10	
2^k	2	4	-3	5	-1	-2	-4	3	-5	1	mod 11

In particular,

$$-1 \equiv 2^5 \pmod{11}.$$

Then the congruence $-1 \equiv x^2$ (11) is insoluble. Indeed, any solution would be congruent to a power 2^k, and then $2^5 \equiv 2^{2k}$, so $2^{2k-5} \equiv 1$; but this is impossible, since all residues of $2k-5$ with respect to 10 are odd, and powers of 2 with odd exponents 1, 3, 5, 7, or 9 are never 1. We say therefore that -1 is a *quadratic nonresidue* of 11.

By contrast, from the table

k	1	2	3	4	5	6	7	8	9	10	11	12	
2^k	2	4	-5	3	6	-1	-2	-4	5	-3	-6	1	(mod 13)

we have

$$-1 \equiv 2^6 \equiv (\pm 5)^2 \pmod{13},$$

so -1 is a *quadratic residue* of 13.

In general, if p is an odd prime not dividing a, then a is a **quadratic residue** of p if the congruence $a \equiv x^2$ (p) is soluble; otherwise, a is a **quadratic nonresidue** of p. We shall develop the theory of quadratic residues and nonresidues in Chapter 11. Meanwhile, a preliminary result follows from Wilson's Theorem. For convenience in stating and proving it, we use the notation[12]

$$\varpi = \varpi(p) = \frac{p-1}{2}, \qquad (\|)$$

where p is an odd prime.

[12]The symbol ϖ is a variant of π; in using it here I follow Hardy and Wright [21, p. 87].

Theorem 53. *Suppose p is an odd prime. Then*

$$(\varpi!)^2 \equiv (-1)^{\varpi-1} \pmod{p}, \qquad (**)$$

and the following are equivalent.

1. $p \equiv 1 \pmod 4$.
2. $(\varpi!)^2 \equiv -1 \pmod p$.
3. -1 *is a quadratic residue of* p.

Proof. By Wilson's Theorem, *modulo* p,

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdots \varpi \cdot (\varpi+1) \cdots (p-1) \\ &\equiv 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots \varpi \cdot (\varpi+1) \\ &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \varpi \cdot (-\varpi) \\ &\equiv (-1)^{\varpi} (\varpi!)^2, \end{aligned}$$

that is,

$$-1 \equiv \prod_{k=1}^{\varpi} k \cdot \prod_{k=\varpi+1}^{p-1} k \equiv \prod_{k=1}^{\varpi} \big(k \cdot (p-k)\big) \equiv (-1)^{\varpi} \cdot \prod_{k=1}^{\varpi} (k^2) \equiv (-1)^{\varpi} \cdot (\varpi!)^2,$$

which yields $(**)$. If $p \equiv 1 \pmod 4$, then ϖ is even, so $(\varpi!)^2 \equiv -1$, and therefore -1 is a quadratic residue of p.

Conversely, if $a^2 \equiv -1 \pmod p$, then by Fermat's Theorem,

$$1 \equiv a^{p-1} \equiv (a^2)^{\varpi} \equiv (-1)^{\varpi} \pmod{p},$$

so ϖ must be even, and therefore $p \equiv 1 \pmod 4$. □

A related argument using quadratic residues in §11.2 will provide yet another proof of Wilson's Theorem.

$$
\begin{aligned}
&\Delta^{m+1} f(x) \\
&= \Delta^m \Delta f(x) \\
&= \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \Delta f(x+k) \\
&= \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} \big(f(x+k+1) - f(x+k)\big) \\
&= \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} f(x+k+1) - \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} f(x+k) \\
&= f(x+m+1) + \sum_{k=0}^{m-1} (-1)^{m-k} \binom{m}{k} f(x+k+1) \\
&\qquad\qquad - \sum_{k=1}^{m} (-1)^{m-k} \binom{m}{k} f(x+k) - (-1)^m f(x) \\
&= f(x+m+1) + \sum_{k=1}^{m} (-1)^{m+1-k} \binom{m}{k-1} f(x+k) \\
&\qquad\qquad + \sum_{k=1}^{m} (-1)^{m+1-k} \binom{m}{k} f(x+k) + (-1)^{m+1} f(x) \\
&= f(x+m+1) + \sum_{k=1}^{m} (-1)^{m+1-k} \binom{m+1}{k} f(x+k) + (-1)^{m+1} f(x) \\
&= \sum_{k=0}^{m+1} (-1)^{m+1-k} \binom{m+1}{k} f(x+k),
\end{aligned}
$$

Table 7.2. The inductive step for $\Delta^n f(x)$ (see page 79)

8. Arithmetic functions

8.1. Multiplicative functions

We work now with positive integers—natural numbers—only. A function on $\mathbb{N}$ is an **arithmetic function.** One such function is σ as defined in the proof of Theorem 45, so that $\sigma(n)$ is the sum of the (positive) divisors of n. For the *number* of positive divisors of n, we write $\tau(n)$. For example,

$$\begin{aligned}\tau(12) &= 1+2+3+4+6+12 = 28,\\ \sigma(12) &= 1+1+1+1+1+\ 1\ =\ 6.\end{aligned}$$

Indeed, $12 = 2^2 \cdot 3$, so the divisors of 12 are

$$\begin{array}{lll} 2^0\cdot 3^0, & 2^1\cdot 3^0, & 2^2\cdot 3^0,\\ 2^0\cdot 3^1, & 2^1\cdot 3^1, & 2^2\cdot 3^1. \end{array}$$

Then the factors of 12 are determined by a choice from $\{0,1,2\}$ for the exponent of 2, and from $\{0,1\}$ for the exponent of 3. Hence

$$\tau(12) = (2+1)\cdot(1+1).$$

Similarly, each factor of 12 itself has two factors: one from $\{1,2,4\}$, and the other from $\{1,3\}$; so

$$\begin{aligned}\sigma(12) &= (1+2+4)\cdot(1+3)\\ &= (1+2+2^2)\cdot(1+3)\\ &= \frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}.\end{aligned}$$

These ideas work in general. Here we use the notation introduced in §4.1:

Theorem 54. *If* $n = \prod_p p^{n(p)}$, *then*

$$\tau(n) = \prod_p (n(p)+1), \qquad \sigma(n) = \prod_p \frac{p^{n(p)+1}-1}{p-1}.$$

We can abbreviate the definitions of σ and τ as follows:

$$\sigma(n) = \sum_{d|n} d, \qquad \tau(n) = \sum_{d|n} 1. \tag{$*$}$$

Implicitly here, d ranges over the *positive* divisors of n. In the theorem, the indices p range over all primes; but they need only range over the primes dividing n (since $n(p) = 0$ when $p \nmid n$). That is, we can write n as $\prod_{p|n} p^{n(p)}$, and then

$$\tau(n) = \prod_{p|n} (n(p) + 1), \qquad \sigma(n) = \prod_{p|n} \frac{p^{n(p)+1} - 1}{p - 1}.$$

In short, each of $\sigma(n)$ and $\tau(n)$ is of the form $\prod_{p|n} f(p)$ for some function f on the set of primes.

Theorem 55. *If* $\gcd(m, n) = 1$*, then for any function* f *on the set of primes,*

$$\prod_{p|mn} f(p) = \prod_{p|m} f(p) \cdot \prod_{q|n} f(q).$$

Proof. If $\gcd(m, n) = 1$ and $p \mid mn$, then by Theorem 33, $p \mid m \iff p \nmid n$. □

Consequently, if $\gcd(m, n) = 1$, then

$$\sigma(mn) = \sigma(m) \cdot \sigma(n), \qquad \tau(mn) = \tau(m) \cdot \tau(n).$$

We say therefore that σ and τ are *multiplicative*. in general, an arithmetic function f is **multiplicative** if

$$f(nm) = f(n) \cdot f(m)$$

whenever n and m are co-prime. We do not require the identity to hold for arbitrary m and n. For example,

$$\sigma(2 \cdot 2) = \sigma(4) = 1 + 2 + 4 = 7, \qquad \sigma(2) \cdot \sigma(2) = (1 + 2) \cdot (1 + 2) = 9.$$

The identify function $n \mapsto n$ and the constant function $n \mapsto 1$ are multiplicative. We can denote these functions by

$$\mathrm{id}, \qquad 1,$$

respectively. Since $\sigma(n) = \sum_{d|n} d = \sum_{d|n} \mathrm{id}(d)$ and $\tau(n) = \sum_{d|n} 1 = \sum_{d|n} 1(d)$, the multiplicativity of σ and τ is also a special case of the following.

Theorem 56. *If* f *is multiplicative, and* F *is given by*

$$F(n) = \sum_{d|n} f(d), \tag{†}$$

then F *is multiplicative.*

Before working out a formal proof, we can see why the theorem ought to be true from an example. Note first that, if f is multiplicative and *non-trivial,* so that $f(n) \neq 0$ for some n, then

$$0 \neq f(n) = f(n \cdot 1) = f(n) \cdot f(1),$$

so $f(1) = 1$. If also f and F are related by (†), then

$$\begin{aligned}
&F(36)\\
&= F(2^2 \cdot 3^2)\\
&= f(1) + f(2) + f(4) + f(3) + f(6) + f(12) + f(9) + f(18) + f(36)\\
&= \quad f(1) \cdot f(1) + f(2) \cdot f(1) + f(4) \cdot f(1) +\\
&\quad + f(1) \cdot f(3) + f(2) \cdot f(3) + f(4) \cdot f(3) +\\
&\quad + f(1) \cdot f(9) + f(2) \cdot f(9) + f(4) \cdot f(9)\\
&= (f(1) + f(2) + f(4)) \cdot (f(1) + f(3) + f(9))\\
&= F(4) \cdot F(9).
\end{aligned}$$

Proof of theorem. Assuming $\gcd(m, n) = 1$, we show first

$$F(mn) = \sum_{c \mid mn} f(c) = \sum_{d \mid m} \sum_{e \mid n} f(de). \tag{‡}$$

Suppose $c \mid mn$. Then every prime power that divides c divides exactly one of m and n. Hence c and $\gcd(c, m)\gcd(c, n)$ have the same prime power divisors, so they are equal. Moreover, if $c = de$, where $d \mid m$ and $e \mid n$, then $c \mid mn$, $d = \gcd(c, m)$, and $e = \gcd(c, n)$. So we have (‡). Continuing, we have

$$\begin{aligned}
F(mn) &= \sum_{d \mid m} \sum_{e \mid n} f(de)\\
&= \sum_{d \mid m} \sum_{e \mid n} f(d) \cdot f(e)\\
&= \sum_{d \mid m} f(d) \cdot \sum_{e \mid n} f(e) \qquad (\S)\\
&= F(m) \cdot F(n). \qquad \square
\end{aligned}$$

In the proof, note that the expression in (§) should be understood first as $\sum_{d \mid m} \big(f(d) \cdot \sum_{e \mid n} f(e) \big)$, and second as its equal, $\big(\sum_{d \mid m} f(d) \big) \cdot \sum_{e \mid n} f(e)$.

8.2. The Möbius function

Suppose again F is defined from f as in (†), so that

$$\begin{aligned}
F(1) &= f(1)\\
F(2) &= f(1) + f(2)\\
F(3) &= f(1) + f(3)\\
F(4) &= f(1) + f(2) + f(4)\\
F(6) &= f(1) + f(2) + f(3) + f(6)\\
F(8) &= f(1) + f(2) + f(4) + f(8)\\
F(9) &= f(1) + f(3) + f(9)\\
F(12) &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12)\\
F(18) &= f(1) + f(2) + f(3) + f(6) + f(9) + f(18)\\
F(24) &= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)
\end{aligned}$$

Then we can solve successively for $f(1)$, $f(2)$, and so on:

$$\begin{aligned}
f(1) &= F(1)\\
f(2) &= -F(1) + F(2)\\
f(3) &= -F(1) + F(3)\\
f(4) &= -F(2) + F(4)\\
f(6) &= F(1) - F(2) - F(3) + F(6)\\
f(8) &= -F(4) + F(8)\\
f(9) &= -F(3) + F(9)\\
f(12) &= F(2) - F(4) - F(6) + F(12)\\
f(18) &= F(3) - F(6) - F(9) + F(18)\\
f(24) &= F(4) - F(8) - F(12) + F(24)
\end{aligned}$$

There is some function ξ, taking integral values, such that

$$f(n) = \sum_{d|n} F(d) \cdot \xi(n, d).$$

A candidate for ξ that works in our examples is $(n, d) \mapsto \mu(n/d)$, where μ is given by

$$\mu(n) = \begin{cases} 0, & \text{if } p^2 \mid n \text{ for some prime } p;\\ (-1)^r, & \text{if } n = p_1 \cdots p_r, \text{ where } p_1 < \cdots < p_r. \end{cases}$$

In particular, $\mu(1) = 1$. The function μ is called the **Möbius function** (after August Ferdinand Möbius, 1790–1868). In an alternative (but equivalent) definition, $\mu(n) = 0$ unless n is squarefree, but in this case

$$\mu(n) = \prod_{p|n} -1. \qquad (\P)$$

Theorem 57. *The Möbius function* μ *is multiplicative.*

Proof. Suppose $\gcd(m,n) = 1$. If $p^2 \mid mn$, then we may assume $p^2 \mid m$, so $\mu(mn) = 0 = \mu(m) = \mu(m) \cdot \mu(n)$. If mn is squarefree, then (¶) and the proof of Theorem 55 show $\mu(mn) = \mu(m) \cdot \mu(n)$. □

It will be useful to define the **unit function,** namely the function ε given by

$$\varepsilon(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}$$

This is easily a multiplicative function. Both the statement and the proof of the following theorem are important.

Theorem 58. *For all* n*,*

$$\sum_{d|n} \mu(d) = \varepsilon(n).$$

Proof. Both sides of the desired equation are multiplicative functions of n. *Therefore it is sufficient to prove the equation when* n *is a prime power.* This is easy:

$$\begin{aligned} \sum_{d|p^s} \mu(d) &= \sum_{k=0}^{s} \mu(p^k) \\ &= \mu(1) + \mu(p) + \cdots + \mu(p^s) \\ &= \begin{cases} \mu(1), & \text{if } s = 0, \\ \mu(1) + \mu(p), & \text{if } s > 0 \end{cases} \\ &= \begin{cases} 1, & \text{if } s = 0, \\ 1 - 1, & \text{if } s > 0 \end{cases} \\ &= \varepsilon(p^s). \end{aligned}$$

□

Another important, albeit easy, observation is:

Theorem 59. *For all arithmetic functions* f*,*

$$\sum_{d|n} f(d) \cdot \varepsilon\Big(\frac{n}{d}\Big) = f(n).$$

Now we can prove that the function ξ above is indeed $(n,d) \mapsto \mu(n/d)$:

Theorem 6o (Möbius Inversion)**.** *If* f *determines* F *by the rule* (†)*, namely*

$$F(n) = \sum_{d|n} f(d),$$

then F determines f by the rule

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot F(d),$$

and conversely.

Proof. We just start calculating:

$$\begin{aligned}\sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot F(d) &= \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot \sum_{e|d} f(e) \\ &= \sum_{d|n} \sum_{e|d} \mu\Big(\frac{n}{d}\Big) \cdot f(e).\end{aligned}$$

Now we want to rearrange indices. For all factors d and e of n, we have

$$e \mid d \iff \frac{n}{d} \mid \frac{n}{e}$$

by Theorem 29. So there is a bijection between $\{(d,e)\colon d \mid n \ \ \& \ \ e \mid d\}$ and $\{(e,c)\colon e \mid n \ \ \& \ \ c \mid n/e\}$, namely $(d,e) \mapsto (e, n/d)$; the inverse is $(e,c) \mapsto (n/c, e)$. Therefore

$$\begin{aligned}\sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot F(d) &= \sum_{e|n} \sum_{c|(n/e)} \mu(c) \cdot f(e) \\ &= \sum_{e|n} f(e) \cdot \sum_{c|(n/e)} \mu(c) \\ &= \sum_{e|n} f(e) \cdot \varepsilon\Big(\frac{n}{e}\Big) \\ &= f(n)\end{aligned}$$

by the last two theorems. The converse is similar.[1] □

8.3. Convolution

We can streamline some of the foregoing results. If f and g are arithmetic functions, their **convolution** is the function $f * g$, given by

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g\Big(\frac{n}{d}\Big).$$

Now, we have the following general principle:

[1] This is Exercise 66.

Theorem 61. *For every arithmetic function f,*

$$\sum_{d|n} f(d) = \sum_{d|n} f\Big(\frac{n}{d}\Big).$$

We shall use this below for an alternative proof of Theorem 68 (p. 97) and for Theorem 70 (p. 100). Meanwhile, we have

$$(f * g)(n) = \sum_{d|n} f\Big(\frac{n}{d}\Big) \cdot g(d),$$

or more simply

$$f * g = g * f. \tag{‖}$$

The definition $(*)$ of σ and τ can be written as

$$\sigma = \mathrm{id} * 1, \qquad\qquad \tau = 1 * 1.$$

Theorem 56 is that if f is multiplicative and $F = f * 1$, then F is multiplicative. The proof can be adapted to show that, if f and g are multiplicative, then so is $f * g$. Theorems 58 and 59 are

$$\mu * 1 = \varepsilon, \qquad\qquad f * \varepsilon = f. \tag{$**$}$$

Then Theorem 60, Möbius Inversion, is

$$F = f * 1 \iff f = F * \mu.$$

We proved this by manipulating indices of summation. Using such manipulations, we can show instead

$$f * (g * h) = (f * g) * h.$$

By this and (‖), Theorem 60 is equivalent to

$$f * 1 * \mu = f;$$

but we can now understand this as an *immediate* consequence of Theorems 58 and 59, as expressed in $(**)$.

By repeated convolution, we have the following equations:

$$\begin{aligned} \mu * 1 &= \varepsilon, & \varepsilon * \mu &= \mu, \\ \varepsilon * 1 &= 1, & 1 * \mu &= \varepsilon, \\ 1 * 1 &= \tau, & \tau * \mu &= 1. \end{aligned}$$

You can read down the first column, and up the second; each row is an instance of Möbius inversion. In short, we have a sequence

$$\ldots, \mu, \varepsilon, 1, \tau, \ldots$$

where passage to the right is by convolving with 1; and to the left, μ. Since $\mathrm{id} * 1 = \sigma$, the corresponding sequence with σ is

$$\ldots, \mathrm{id}, \sigma, \ldots$$

We now define the entry to the left of id as φ. That is,

$$\varphi = \mathrm{id} * \mu. \tag{††}$$

Then φ is multiplicative, and

$$\varphi(p^s) = \begin{cases} 1, & \text{if } s = 0, \\ p^s - p^{s-1}, & \text{if } s > 0. \end{cases}$$

This is precisely the size of the set $\{x\colon 0 \leqslant x < n \ \ \& \ \ \gcd(x, n) = 1\}$ when $n = p^s$. In general, this set can be understood as the set of invertible congruence-classes *modulo* n. Recall from §3.2 that the set of *all* congruence-classes *modulo* n can be denoted by $\mathbb{Z}_n$. Then the set of invertible elements is denoted by

$$\mathbb{Z}_n{}^{\times}.$$

So in case $n = p^s$, we have

$$\varphi(n) = |\mathbb{Z}_n{}^{\times}|.$$

We shall show in the next chapter that this holds generally.

Meanwhile, it may be of interest to note that convolution is called in particular *Dirichlet convolution* (after Johann Peter Gustav Lejeune Dirichlet,[2] 1805–1859), because analogous operations, also called convolutions, arise in other contexts. For example, the reader may be in a position to recall that in analysis one defines

$$(f * g)(t) = \int_0^t f(x)g(t - x)\,\mathrm{d}\,x.$$

This is related to the *Laplace transform*, which converts a suitable function f into the function $\mathcal{L}\{f\}$, namely

$$s \mapsto \int_0^\infty \mathrm{e}^{-st} f(t)\,\mathrm{d}\,t.$$

[2] The pronunciation is *dirikle*, not *dirişle*.

Then

$$\mathcal{L}\{f * g\} = \mathcal{L}\{f\} \cdot \mathcal{L}\{g\}.$$

Also, the transform is linear, and

$$\begin{aligned}\mathcal{L}\{f'\} &= \mathrm{id} \cdot \mathcal{L}\{f\} - f(0),\\ \mathcal{L}\{f''\} &= \mathrm{id}^2 \cdot \mathcal{L}\{f\} - \mathrm{id} \cdot f(0) - f'(0),\end{aligned}$$

so that, if

$$f'' + af' + bf = g,$$

then

$$\begin{aligned}\mathcal{L}\{f\} &= \frac{f(0) \cdot \mathrm{id} + af(0) + f'(0)}{\mathrm{id}^2 + a \cdot \mathrm{id} + b} + \frac{\mathcal{L}\{g\}}{\mathrm{id}^2 + a \cdot \mathrm{id} + b}\\ &= \mathcal{L}\{\varphi\} + \mathcal{L}\{g\} \cdot \mathcal{L}\{h\}\\ &= \mathcal{L}\{\varphi\} + \mathcal{L}\{g * h\}\end{aligned}$$

for some φ and h that are independent of g.

9. Arbitrary moduli

9.1. The Chinese Remainder Theorem

The possibility of solving Chinese remainder problems can be understood through tables. Since $\gcd(4, 9) = 1$, for every choice of a and b, Theorem 43 (p. 67) gives us a solution to

$$x \equiv a \pmod 4, \qquad\qquad x \equiv b \pmod 9, \qquad\qquad (*)$$

and the solution is unique *modulo* 36. We can find this solution by first filling out a table diagonally as follows:

	0	1	2	3	4	5	6	7	8
0	0				4				8
1		1				5			
2			2				6		
3				3				7	

	0	1	2	3	4	5	6	7	8
0	0			12	4			16	8
1	9	1			13	5			17
2		10	2			14	6		
3			11	3			15	7	

	0	1	2	3	4	5	6	7	8
0	0		20	12	4		24	16	8
1	9	1		21	13	5		25	17
2	18	10	2		22	14	6		26
3		19	11	3		23	15	7	

	0	1	2	3	4	5	6	7	8
0	0	28	20	12	4	32	24	16	8
1	9	1	29	21	13	5	33	25	17
2	18	10	2	30	22	14	6	34	26
3	27	19	11	3	31	23	15	7	35

The solution to $(*)$ is the entry in row a, column b. For example, 14 solves the congruences $x \equiv 2$ (4) and $x \equiv 5$ (9). Making such a table is not always practical. Still, the general procedure has the following theoretical formulation.

Theorem 62 (Chinese Remainder Theorem)**.** *If* $\gcd(m,n)=1$*, then the function* $x \mapsto (x,x)$ *is a well-defined bijection from* $\mathbb{Z}_{mn}$ *to* $\mathbb{Z}_m \times \mathbb{Z}_n$*.*

Proof. The given function is well defined, since if $a \equiv b \ (mn)$, then $a \equiv b$ *modulo* m and n. The converse of this holds too, by the corollary to Theorem 30, since $mn = \operatorname{lcm}(m,n)$; so the function is injective. Since the domain and codomain are finite sets of the same size (namely mn), the function is a bijection. □

For all m and n, we have

$$\gcd(x,mn)=1 \iff \gcd(x,m)=1 \ \ \& \ \ \gcd(x,n)=1. \qquad (\dagger)$$

This means, in the table above, if we delete row i and column j whenever $\gcd(4,i) \neq 1$ and $\gcd(9,j) \neq 1$, then the remaining numbers are precisely those that are prime to 36:

	0	1	2	3	4	5	6	7	8
0									
1		1	29		13	5		25	17
2									
3		19	11		31	23		7	35

Recall that on page 91 we defined $\mathbb{Z}_n{}^\times$ as the set of invertible elements of $\mathbb{Z}_n$. Then we have the following general result.

Theorem 63. *If* $\gcd(m,n)=1$*, then the function* $x \mapsto (x,x)$ *is a well-defined bijection from* $\mathbb{Z}_{mn}{}^\times$ *to* $\mathbb{Z}_m{}^\times \times \mathbb{Z}_n{}^\times$*.*

Proof. By (†), for all m and n, the function $x \mapsto (x,x)$ maps $\mathbb{Z}_{mn}{}^\times$ into $\mathbb{Z}_m{}^\times \times \mathbb{Z}_n{}^\times$. If $\gcd(m,n)=1$, then by the Chinese Remainder Theorem, every element of $\mathbb{Z}_m{}^\times \times \mathbb{Z}_n{}^\times$ is (x,x) for some x, which must be in $\mathbb{Z}_{mn}{}^\times$. □

Recall that φ was defined as $\mathrm{id} * \mu$ in (††) in §8.3 (p. 91). As promised, we now have:

Theorem 64. *For all* n*,*

$$\varphi(n) = |\mathbb{Z}_n{}^\times|.$$

Proof. We follow the principle used in proving Theorem 58. Being the convolution of multiplicative functions, φ is multiplicative. By the last theorem, the function $n \mapsto |\mathbb{Z}_n{}^\times|$ is multiplicative. Finally, the given equation holds when n is a prime power, as shown in §8.3. □

This will enable us to establish a generalization of Fermat's Theorem.

9.2. Euler's Theorem

Since $\varphi(p) = p - 1$, Fermat's Theorem is that, if n is prime, and $\gcd(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

We shall show that this holds for all n.

The multiplicative function φ is called the **Euler phi-function** after Leonhard Euler, 1707–1783. Euler's original definition apparently corresponds to Theorem 64: $\varphi(n)$ is the number of x such that $0 \leqslant x < n$ and x is prime to n. For calculating this, we now have[1]

Theorem 65. *For all n,*

$$\varphi(n) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big).$$

Proof. If $n = \prod_{p|n} p^{n(p)}$, then

$$\begin{aligned} \varphi(n) = \prod_{p|n} \varphi(p^{n(p)}) &= \prod_{p|n} (p^{n(p)} - p^{n(p)-1}) \\ &= \prod_{p|n} p^{n(p)} \prod_{p|n} \Big(1 - \frac{1}{p}\Big) = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big). \end{aligned}$$

□

For example,

$$\varphi(30) = 30 \cdot \Big(1 - \frac{1}{2}\Big) \cdot \Big(1 - \frac{1}{3}\Big) \cdot \Big(1 - \frac{1}{5}\Big) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$$

Since 180 has the same prime divisors as 30, we have

$$\frac{\varphi(180)}{\varphi(30)} = \frac{180}{30} = 6,$$

so $\varphi(180) = 6\varphi(30) = 48$. But 15 and 30 do not have the same prime divisors, and we cannot expect $\varphi(15)/\varphi(30)$ to be 15/30, or 1/2; indeed, $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8 = \varphi(30)$.

Theorem 66 (Euler)**.** *If* $\gcd(a, n) = 1$*, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

[1] Gauss proves the theorem in the *Disquisitiones Arithmeticae* [16, ¶38], attributing it to Euler in 1760–1.

Proof. Assume $\gcd(a, n) = 1$. Then the function $x \mapsto ax$ is a bijection from ${\mathbb{Z}_n}^\times$ to itself. Hence

$$\prod_{x \in {\mathbb{Z}_n}^\times} x \equiv \prod_{x \in {\mathbb{Z}_n}^\times} (ax) \equiv a^{\varphi(n)} \prod_{x \in {\mathbb{Z}_n}^\times} x \pmod{n}.$$

Since the product $\prod_{x \in {\mathbb{Z}_n}^\times} x$ is invertible (since its factors are), we obtain the result. □

Again, Fermat's Theorem is the special case when $n = p$. But we do *not* generally have $a^{\varphi(n)+1} \equiv a \pmod{n}$ for arbitrary a. For example, $\varphi(12) = 4$, but $2^5 = 32 \equiv 8 \pmod{12}$.

Euler's Theorem gives us a procedure for solving certain congruences. For example, to solve

$$369^{19587} x \equiv 1 \pmod{1000},$$

we compute

$$\varphi(1000) = \varphi(10^3) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = 4 \cdot 100 = 400.$$

Now reduce the exponent:

$$\frac{19587}{400} = 48 + \frac{387}{400}.$$

So we want to solve

$$\begin{aligned} 369^{387} x &\equiv 1 \pmod{1000}, \\ x &\equiv 369^{13} \pmod{1000}. \end{aligned}$$

Now proceed, using that $13 = 8 + 4 + 1 = 2^3 + 2^2 + 1$. Multiplication *modulo* 1000 requires only three columns, so the computations of Table 9.1 give us the solution $\boxed{x \equiv 609 \pmod{1000}.}$

Euler's Theorem gives a neat theoretical solution to Chinese remainder problems:

Theorem 67. *Suppose the positive integers $n_1, \ldots, n_s$ are pairwise co-prime, and the integers $a_1, \ldots, a_s$ are arbitrary. Define*

$$n = n_1 \cdots n_s, \qquad N_i = \frac{n}{n_i}.$$

Then we have

$$x \equiv a_1 \pmod{n_1}, \qquad \ldots, \qquad x \equiv a_s \pmod{n_s}$$

if and only if

$$x \equiv a_1 \cdot {N_1}^{\varphi(n_1)} + \cdots + a_s \cdot {N_s}^{\varphi(n_s)} \pmod{n}.$$

Proof. If $i \neq j$, then $n_j \mid N_i$, so ${N_i}^{\varphi(n_i)} \equiv 0 \pmod{n_j}$. □

$$\begin{array}{r}3\,6\,9\\ 3\,6\,9\\ \hline 3\,2\,1\\ 1\,4\\ 7\\ \hline 1\,6\,1\end{array}\quad\text{so } 369^2 \equiv 161 \pmod{1000};\qquad \begin{array}{r}1\,6\,1\\ 1\,6\,1\\ \hline 1\,6\,1\\ 6\,6\\ 1\\ \hline 9\,2\,1\end{array}\quad\text{so } 369^4 \equiv 161^2 \equiv 921 \pmod{1000};$$

$$\begin{array}{r}9\,2\,1\\ 9\,2\,1\\ \hline 9\,2\,1\\ 4\,2\\ 9\\ \hline 2\,4\,1\end{array}\quad\text{so } 369^8 \equiv 921^2 \equiv 241 \pmod{1000};$$

$$369^{13} \equiv 369^8 \cdot 369^4 \cdot 369 \equiv 241 \cdot 921 \cdot 369 \pmod{1000};$$

$$\begin{array}{r}2\,4\,1\\ 9\,2\,1\\ \hline 2\,4\,1\\ 8\,2\\ 9\\ \hline 9\,6\,1\end{array}\qquad \begin{array}{r}9\,6\,1\\ 3\,6\,9\\ \hline 6\,4\,9\\ 6\,6\\ 3\\ \hline 6\,0\,9\end{array}\quad\text{so } 369^{13} \equiv 609 \pmod{1000}.$$

Table 9.1. Exponentiation *modulo* 1000

9.3. Gauss's Theorem

Given the theoretical developments of the previous chapter, we can immediately prove:[2]

Theorem 68 (Gauss[3])**.** *For all positive integers n,*

$$\sum_{d|n} \varphi(d) = n. \qquad (\ddagger)$$

[2]The three theorems of the present section are versions of the three theorems in Burton's section, 'Some properties of the phi-function' [7, §7.4, pp. 141–5]. I have tried to suggest a connection between the first two theorems. In Burton, the last theorem is just what we have expressed as $\varphi = \mu * \mathrm{id}$; but this is also derivable from Gauss's Theorem. Hence I have named the section for Gauss.

[3]Gauss proves this in the *Disquisitiones Arithmeticae* [16, ¶39], but he does not have all of our theory at his disposal.

Proof. The claim is $\varphi * 1 = \mathrm{id}$, which is the result of applying Möbius Inversion (in reverse) to the original definition of φ. □

Without relying on Möbius inversion, we can prove Gauss's theorem by the technique of Theorems 58 and 64. Both sides of the equation are multiplicative functions of n, and

$$\sum_{d|p^s} \varphi(d) = \sum_{k=0}^{s} \varphi(p^k) = 1 + \sum_{k=1}^{s} (p^k - p^{k-1})$$
$$= 1 + (p-1) + (p^2 - p) + \cdots + (p^s - p^{s-1}) = p^s.$$

Yet another proof[4] of Gauss's theorem makes use of the principle of Theorem 61. Partition the set $\{0, 1, \ldots, n-1\}$ according to greatest common divisor with n. For example, suppose $n = 12$. We can construct a table as follows, where the rows are labelled with the divisors of 12. Each number x from 0 to 11 inclusive is assigned to row d, if $\gcd(x, 12) = d$.

	0	1	2	3	4	5	6	7	8	9	10	11
12	0											
6							6					
4					4				8			
3				3						9		
2			2								10	
1		1				5		7				11

But when $d \mid 12$, we have

$$0 \leqslant x < 12 \;\;\&\;\; \gcd(x, 12) = d$$

if and only if we have

$$d \mid x \;\;\&\;\; \gcd\Big(\frac{x}{d}, \frac{12}{d}\Big) = 1 \;\;\&\;\; 0 \leqslant \frac{x}{d} < \frac{12}{d}.$$

So the number of entries in row d of the table is just $\varphi(12/d)$. The number of entries in all rows together is 12, so

$$12 = \sum_{d|12} \varphi\Big(\frac{12}{d}\Big);$$

but this is just $\sum_{d|12} \varphi(d)$, by Theorem 61. This argument is not specific to 12; it can be generalized to establish Gauss's theorem. Is there anything noticeable about the table for $n = 12$? Try some other values of n, as in Table 9.2.[5]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	0															
8									8							
4					4								12			
2			2				6				10				14	
1		1		3		5		7		9		11		13		15

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	0																	
9										9								
6							6						12					
3				3											15			
2			2		4				8		10				14		16	
1		1				5		7				11		13				17

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	0																				
7								7							14						
3				3			6			9			12			15			18		
1			2		4	5			8		10	11		13			16	17		19	20

Table 9.2. Numbers according to gcd with 16, 18, and 21

The entries are symmetric about a vertical axis, except for 0. More precisely, if d is a *proper* divisor of n, then the function $x \mapsto n - x$ is a permutation of $\{0 \leqslant x < n\colon \gcd(x, n) = d\}$. In other words, the average value of an element x of $\{1, \ldots, n-1\}$ such that $\gcd(x, n) = d$ is $n/2$. We can write out the case where $d = 1$ as follows.

Theorem 69. *For all n, if we understand*

$$\mathbb{Z}_n{}^{\times} = \{k\colon 0 < k < n \ \ \&\ \ \gcd(k, n) = 1\}$$

then

$$\varphi(n) = \frac{2}{n} \sum_{k \in \mathbb{Z}_n{}^{\times}} k.$$

Proof. Since the function $x \mapsto n - x$ permutes the indices of the given summation, and $|\mathbb{Z}_n{}^{\times}| = \varphi(n)$, we have

$$\sum_{k \in \mathbb{Z}_n{}^{\times}} k = \sum_{k \in \mathbb{Z}_n{}^{\times}} (n - k) = \varphi(n) \cdot n - \sum_{k \in \mathbb{Z}_n{}^{\times}} k,$$

which yields the claim. □

The following relates a function of *all* of the divisors of n with a function of its prime divisors.

Theorem 70. *For all n,*

$$\sum_{d \mid n} \frac{\mu(d)}{d} = \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big).$$

Proof. From the original definition (††) of φ as $\mathrm{id} * \mu$, or by applying Möbius Inversion to Gauss's Theorem, and then by Theorem 61, as well as by Theorem 65, we have

$$\sum_{d \mid n} \frac{n}{d} \cdot \mu(d) = \varphi(n) = n \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big).$$

Now divide by n. □

[4] This is basically Gauss's proof.

[5] Information as in this table will be of use in the next section, §10.1.

For example,

$$\begin{aligned}\sum_{d|12}\frac{\mu(d)}{d} &= \frac{\mu(1)}{1}+\frac{\mu(2)}{2}+\frac{\mu(3)}{3}+\frac{\mu(4)}{4}+\frac{\mu(6)}{6}+\frac{\mu(12)}{12}\\ &= 1-\frac{1}{2}-\frac{1}{3}+\frac{1}{6}\\ &= 1-\frac{1}{2}-\frac{1}{3}+\frac{1}{2\cdot 3}\\ &= \Big(1-\frac{1}{2}\Big)\Big(1-\frac{1}{3}\Big)=\prod_{p|12}\Big(1-\frac{1}{p}\Big).\end{aligned}$$

This may suggest a proof of the last theorem by direct computation. Indeed, suppose the distinct prime factors of n are $p_1, \ldots, p_r$. Then

$$\prod_{p|n}\Big(1-\frac{1}{p}\Big)=\sum_{j=0}^{r}\sum_{1\leqslant k(1)<\cdots<k(j)\leqslant r}\frac{(-1)^j}{p_{k(1)}\cdots p_{k(j)}}=\sum_{d|n}\frac{\mu(d)}{d}.$$

10. Primitive roots

10.1. Order

Euler's Theorem can be improved in some cases. For example, $255 = 3 \cdot 5 \cdot 17$, so $\varphi(255) = \varphi(3) \cdot \varphi(5) \cdot \varphi(17) = 2 \cdot 4 \cdot 16 = 128$, and hence, by Euler's Theorem,

$$\gcd(a, 255) = 1 \implies a^{128} \equiv 1 \pmod{255}.$$

But by Fermat's Theorem,

$$\begin{aligned} 3 \nmid a &\implies a^2 \equiv 1 \pmod 3 \implies a^{16} \equiv 1 \pmod 3; \\ 5 \nmid a &\implies a^4 \equiv 1 \pmod 5 \implies a^{16} \equiv 1 \pmod 5; \\ 17 \nmid a &\implies a^{16} \equiv 1 \pmod{17}. \end{aligned}$$

Therefore $\gcd(a, 255) = 1 \implies a^{16} \equiv 1 \pmod{3, 5, 17}$, that is,

$$\gcd(a, 255) = 1 \implies a^{16} \equiv 1 \pmod{255}.$$

If it exists, the **order** of a *modulo* n is the least positive k such that

$$a^k \equiv 1 \pmod n.$$

Theorem 71. *A number a has an order* modulo n *if and only if*

$$\gcd(a, n) = 1.$$

Proof. If a has the order k *modulo* n, then $a^k - 1 = n \cdot \ell$ for some ℓ, so

$$a \cdot a^{k-1} - n \cdot \ell = 1,$$

and therefore $\gcd(a, n) = 1$. Conversely, if $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod n$, so a has an order *modulo* n. □

Assuming $\gcd(a, n) = 1$, let us denote the order of a *modulo* n by

$$\operatorname{ord}_n(a).$$

For example, what is $\operatorname{ord}_{17}(2)$? Just compute powers of 2 *modulo* 17:

k	1	2	3	4	5	6	7	8
$2^k \pmod{17}$	2	4	8	-1	-2	-4	-8	1

Then $\operatorname{ord}_{17}(2) = 8$. Likewise, $\operatorname{ord}_{17}(3) = 16$:

k	1	2	3	4	5	6	7	8
$3^k \pmod{17}$	3	-8	-7	-4	5	-2	-6	-1
k	9	10	11	12	13	14	15	16
$3^k \pmod{17}$	-3	8	7	4	-5	2	6	1

Note how, in each computation, halfway through, we just change signs. From the last table, taking every other entry, we can extract

k	1	2	3	4	5	6	7	8
$(-8)^k \pmod{17}$	-8	-4	-2	-1	8	4	2	1

which means $\operatorname{ord}_{17}(-8) = 8$. Likewise, $\operatorname{ord}_{17}(-4) = 4$, and $\operatorname{ord}_{17}(-1) = 2$. So we have

a	1	2	3	4	5	6	7	8
$\operatorname{ord}_{17}(a)$	1		16					
$\operatorname{ord}_{17}(-a)$	2			4				8

How can we complete the table? For example, what is $\operatorname{ord}_{17}(-7)$? Since $-7 \equiv 3^3 \pmod{17}$, and $\gcd(3, 16) = 1$, we shall be able to conclude $\operatorname{ord}_{17}(-7) = 16$. Likewise, $\operatorname{ord}_{17}(5) = 16$. But $\operatorname{ord}_{17}(-2) = 16/\gcd(6, 16) = 8$, since $-2 \equiv 3^6 \pmod{17}$. This is by a general theorem to be proved presently. We complete the last table thus:

a	1	2	3	4	5	6	7	8
$\operatorname{ord}_{17}(a)$	1	8	16	4	16	16	16	8
$\operatorname{ord}_{17}(-a)$	2	8	16	4	16	16	16	8

Theorem 72. *Suppose* $\gcd(a, n) = 1$. *Then*

a) $a^k \equiv 1 \pmod{n}$ *if and only if* $\operatorname{ord}_n(a) \mid k$;

b) $\operatorname{ord}_n(a^s) = \operatorname{ord}_n(a)/\gcd(s, \operatorname{ord}_n(a))$;

c) $a^k \equiv a^\ell$ *if and only if* $k \equiv \ell \pmod{\operatorname{ord}_n(a)}$.

Proof. For (a), the reverse direction is easy. For the forward direction, suppose $a^k \equiv 1 \pmod{n}$. Now use division:

$$k = \operatorname{ord}_n(a) \cdot s + r$$

for some s and r, where $0 \leqslant r < \operatorname{ord}_n(a)$. Then

$$1 \equiv a^k \equiv a^{\operatorname{ord}_n(a)\cdot s + r} \equiv (a^{\operatorname{ord}_n(a)})^s \cdot a^r \equiv a^r \pmod{n}.$$

By minimality of $\operatorname{ord}_n(a)$ as an integer k such that $a^k \equiv 1 \pmod{n}$, we conclude $r = 0$. This means $\operatorname{ord}_n(a) \mid k$.

To prove (b), by (a) we have, *modulo* n,

$$(a^s)^k \equiv 1 \iff a^{sk} \equiv 1 \iff \operatorname{ord}_n(a) \mid sk \iff \frac{\operatorname{ord}_n(a)}{\gcd(s, \operatorname{ord}_n(a))} \mid k,$$

but also $(a^s)^k \equiv 1 \iff \operatorname{ord}_n(a^s) \mid k$, hence

$$\frac{\operatorname{ord}_n(a)}{\gcd(s, \operatorname{ord}_n(a))} \mid k \iff \operatorname{ord}_n(a^s) \mid k.$$

This is true for all k. Since orders are positive, we conclude (b).

Finally, (c) follows from (a), since

$$\begin{aligned} a^k \equiv a^\ell \pmod{n} &\iff a^{k-\ell} \equiv 1 \pmod{n} \\ &\iff \operatorname{ord}_n(a) \mid k - \ell \\ &\iff k \equiv \ell \pmod{\operatorname{ord}_n(a)}. \end{aligned}$$

(We have used that $\gcd(a, n) = 1$, so that $a^{-\ell}$ exists.) □

Hence, from

k	1	2	3	4	5	6	7	8	9
$2^k \pmod{19}$	2	4	8	−3	−6	7	−5	9	−1
$2^{k+9} \pmod{19}$	−2	−4	−8	3	6	−7	5	−9	1

we obtain

a	1	2	3	4	5	6	7	8	9
$\operatorname{ord}_{19}(a)$	1	18	18	9	9	9	3	6	9
$\operatorname{ord}_{19}(-a)$	2	9	9	18	18	18	6	3	18

by the computations in Table 10.1 (which make use of information in Table 9.2 on page 99 above). If $d \mid 18$, let $\psi_{19}(d)$ be the number[1] of incongruent residues *modulo* 19 that have order d. Then we have

d	$\psi_{19}(d)$
18	6
9	6
6	2
3	2
2	1
1	1

[1] In the *Disquisitiones Arithmeticae* [16, ¶52], Gauss introduces the notation ψd for this number.

$$\begin{aligned}
\operatorname{ord}_{19}(2^k) = 18 &\iff \gcd(k,18) = 1\\
&\iff k \equiv 1,5,7,11,13,17 \pmod{18}\\
&\iff 2^k \equiv 2,-6,-5,-4,3,-9 \pmod{19};\\
\operatorname{ord}_{19}(2^k) = 9 &\iff \gcd(k,18) = 2\\
&\iff k \equiv 2,4,8,10,14,16 \pmod{18}\\
&\iff 2^k \equiv 4,-3,9,-2,6,5 \pmod{19},\\
\operatorname{ord}_{19}(2^k) = 6 &\iff \gcd(k,18) = 3\\
&\iff k \equiv 3,15 \pmod{18}\\
&\iff 2^k \equiv 8,-7 \pmod{19},\\
\operatorname{ord}_{19}(2^k) = 3 &\iff \gcd(k,18) = 6\\
&\iff k \equiv 6,12 \pmod{18}\\
&\iff 2^k \equiv 7,-8 \pmod{19},\\
\operatorname{ord}_{19}(2^k) = 2 &\iff \gcd(k,18) = 9\\
&\iff k \equiv 9 \pmod{18}\\
&\iff 2^k \equiv -1 \pmod{19}.
\end{aligned}$$

Table 10.1. Orders *modulo* 19

Note that $\psi_{19}(d) = \varphi(d)$ here. This is no accident. Indeed, if $d \mid 18$, so $18 = d\ell$ for some ℓ, we have

$$\begin{aligned}
\operatorname{ord}_{19}(2^k) = d &\iff \gcd(k,18) = \ell\\
&\iff \ell \mid k \ \ \&\ \ \gcd\Big(\frac{k}{\ell}, d\Big) = 1.
\end{aligned}$$

Thus, *modulo* 18, the number of k such that $\operatorname{ord}_{19}(2^k) = d$ is just $\varphi(d)$. But every number that is prime to 19 is congruent *modulo* 19 to 2^k for some such k. Therefore $\psi_{19}(d) = \varphi(d)$.

If $\gcd(a,n) = 1$, and $\operatorname{ord}_n(a) = \varphi(n)$, then a is called a **primitive root** of n. So we have shown that 3, but not 2, is a primitive root of 17.

Also, 2 is a primitive root of 19, and we have used this to show $\psi_{19}(d) = \varphi(d)$ if $d \mid 18$. The same argument shows $\psi_n(d) = \varphi(d)$, if n has a primitive root. We shall show that every p has a primitive root; but this will be a *corollary* to Theorem 74, that $\psi_p(d) = \varphi(d)$.

There will be no formula for determining primitive roots: we just have to look

for them. But once we know that 2 is a primitive root of 19, then we know that 2^5, 2^7, 2^{11}, 2^{13}, and 2^{17} are primitive roots—or rather, -6, -5, -4, 3, and -9 are primitive roots. In particular, the number of primitive roots of 19 is $\varphi(18)$.

10.2. Groups

We can understand what we are doing algebraically as follows. On the set $\mathbb{Z}_n$ of congruence-classes *modulo* n, addition and multiplication are well-defined by Theorem 23, and so the set, considered with these operations, is a **ring.** The multiplicatively invertible elements of this ring compose the set ${\mathbb{Z}_n}^\times$. This set is closed under multiplication and inversion: it is a (multiplicative) **group.** Suppose $k \in {\mathbb{Z}_n}^\times$. (More precisely one might write the element as $k + (n)$ or $\bar{k}$. On the other hand, we are free to treat ${\mathbb{Z}_n}^\times$ as being literally a subset of $\mathbb{Z}$: we did this in Theorem 69. In this case, one must just remember that multiplication and addition are not the usual operations on $\mathbb{Z}$.) Then we have the function

$$x \mapsto k^x$$

from $\mathbb{Z}$ to ${\mathbb{Z}_n}^\times$. Since $k^{x+y} = k^x \cdot k^y$, this function is a **homomorphism** from the additive group $\mathbb{Z}$ to the multiplicative group ${\mathbb{Z}_n}^\times$.

We have shown that the function $x \mapsto 2^x$ is surjective onto ${\mathbb{Z}_{19}}^\times$, and its kernel is (18). Call this function f_2. Then (by the First Isomorphism Theorem for Groups) f_2 is an **isomorphism** from $\mathbb{Z}_{18}$ onto ${\mathbb{Z}_{19}}^\times$:

$$\mathbb{Z}_{18} \cong {\mathbb{Z}_{19}}^\times,$$
$$(\{0, 1, 2, \ldots, 17\}, +) \cong (\{1, 2, 3, \ldots, 18\}, \cdot\,).$$

From analysis, we have the exponential function $x \mapsto \mathrm{e}^x$ or exp from $\mathbb{R}$ to $\mathbb{R}^\times$, where $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ (the set of multiplicatively invertible real numbers). We have

$$\exp(x + y) = \exp(x) \cdot \exp(y).$$

The range of exp is the interval $(0, \infty)$, which is closed under multiplication and inversion. Also exp is injective. So exp is an isomorphism from $(\mathbb{R}, +)$ onto $((0, \infty), \cdot\,)$.

We are looking at a similar isomorphism in discrete mathematics. If a is a primitive root of n, then $x \mapsto a^x$ is an isomorphism from $\mathbb{Z}_{\varphi(n)}$ to ${\mathbb{Z}_n}^\times$. In particular, ${\mathbb{Z}_n}^\times$ is cyclic. Conversely, if ${\mathbb{Z}_n}^\times$ is cyclic, then a generator is a primitive root of n. For example:

a) ${\mathbb{Z}_2}^\times = \{1\}$, so 1 is a primitive root of 2.
b) ${\mathbb{Z}_3}^\times = \{1, 2\}$, and $2^2 \equiv 1 \pmod 3$, so 2 is a primitive root of 3.
c) ${\mathbb{Z}_4}^\times = \{1, 3\}$, and $3^2 \equiv 1 \pmod 4$, so 3 is a primitive root of 4.

d) $\mathbb{Z}_5{}^\times = \{1,2,3,4\}$, and $2^2 \equiv 4$, $2^3 \equiv 3$, and $2^4 \equiv 1 \pmod 5$, so 2 is a primitive root of 5.
e) $\mathbb{Z}_6{}^\times = \{1,5\}$, and $5^2 \equiv 1 \pmod 6$, so 5 is a primitive root of 6.
f) $\mathbb{Z}_7{}^\times = \{1,2,3,4,5,6\}$, and we have

k	1	2	3	4	5	6
2^k	2	4	1			
3^k	3	2	6	4	5	1

so 3 (but not 2) is a primitive root of 7.
g) $\mathbb{Z}_8{}^\times = \{1,3,5,7\}$, but $3^2 \equiv 1$, $5^2 \equiv 1$, and $7^2 \equiv 1 \pmod 8$, so 8 has no primitive root.

We shall show in §10.5 that the following numbers, and only these, have primitive roots:

a) powers of odd primes;
b) 2 and 4;
c) doubles of powers of odd primes.

10.3. Primitive roots of primes

To prove generally that the number of primitive roots of p is $\varphi(p-1)$, we shall need the following (attributed to Joseph-Louis Lagrange, 1736–1813.)

Theorem 73 (Lagrange[2]). *Every congruence of the form*

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod p$$

*has n solutions or fewer (*modulo p*).*

Proof. Use induction. The claim is easily true when $n = 1$. Suppose it is true when $n = k$. Say the congruence

$$x^{k+1} + a_1 x^k + \cdots + a_k x + a_{k+1} \equiv 0 \pmod p \qquad (*)$$

has a solution b. Then we can factorize the left member, and rewrite the congruence as

$$(x-b)\cdot(x^k + c_1 x^{k-1} + \cdots + c_{k-1}x + c_k) \equiv 0 \pmod p.$$

Any solution to this that is different from b is a solution of

$$x^k + c_1 x^{k-1} + \cdots + c_{k-1}x + c_k \equiv 0 \pmod p.$$

But by inductive hypothesis, there are at most k such solutions. Therefore $(*)$ has at most $k+1$ solutions. This completes the induction and the proof. □

[2] In the *Disquisitiones Arithmeticae* [16, ¶¶43–4], Gauss proves this theorem and traces its original proof to Lagrange in 1768, while mentioning also later proofs by Legendre and Euler. He says Euler had proved an (unspecified) special case in 1754–5.

How did we use that p is prime? We needed to know that, if $f(x)$ and $g(x)$ are polynomials, and $f(a) \cdot g(a) \equiv 0 \pmod{p}$, then either $f(a) \equiv 0 \pmod{p}$, or else $g(a) \equiv 0 \pmod{p}$. That is, if $mn \equiv 0 \pmod{p}$, then either $m \equiv 0 \pmod{p}$ or $n \equiv 0 \pmod{p}$. That is, if $p \mid mn$, then $p \mid m$ or $p \mid n$. This fails if p is replaced by a composite number.

Indeed, the congruence $x^2 - 1 \equiv 0$ (8) has the solutions 1, 3, 5, and 7 (as shown in §10.2). Also $x^2 - 5x \equiv 0$ (6) has solutions 0 and 5, but also 2 and 3, since $x^2 - 5x \equiv x^2 - 5x + 6 \equiv (x-2)(x-3)$.

Theorem 74. *If $d \mid p-1$, let $\psi_p(d)$ be the number of incongruent residues* modulo p *that have order d. Then*

$$\psi_p(d) = \varphi(d).$$

Proof. Every number prime to p has an order *modulo* p, and this order divides $\varphi(p)$, which is $p-1$; so

$$\sum_{d \mid p-1} \psi_p(d) = p - 1.$$

By Gauss's Theorem (Theorem 68, p. 97), we have $\sum_{d \mid p-1} \varphi(d) = p-1$; therefore

$$\sum_{d \mid p-1} \psi_p(d) = \sum_{d \mid p-1} \varphi(d). \qquad (\dagger)$$

Hence, to establish $\psi_p(d) = \varphi(d)$, it is enough to show that $\psi_p(d) \leqslant \varphi(d)$ whenever $d \mid p-1$. Indeed, if we show this, but $\psi_p(e) < \varphi(e)$ for some divisor e of $p-1$, then

$$\sum_{d \mid p-1} \psi_p(d) = \sum_{\substack{d \mid p-1 \\ d \neq e}} \psi_p(d) + \psi_p(e) < \sum_{\substack{d \mid p-1 \\ d \neq e}} \varphi(d) + \varphi(e) = \sum_{d \mid p-1} \varphi(d),$$

contradicting (†).

If $\psi_p(d) = 0$, then certainly $\psi_p(d) \leqslant \varphi(d)$. So suppose $\psi_p(d) \neq 0$. Then $\operatorname{ord}_p(a) = d$ for some a. In particular, a is a solution of the congruence

$$x^d - 1 \equiv 0 \pmod{p}. \qquad (\ddagger)$$

But then every power of a is a solution, since $(a^d)^n = (a^n)^d$. Moreover, if $0 < k < \ell \leqslant d$, then

$$a^k \not\equiv a^\ell \pmod{p}$$

by Theorem 72. Hence the numbers a, a^2, …, a^d are incongruent solutions to the congruence (‡). Moreover, by Lagrange's Theorem, 73, every solution is congruent to one of these solutions. Among these solutions, those that have order

d modulo p are just those powers a^k such that $\gcd(k, d) = 1$, again by Theorem 72. The number of such powers is just $\varphi(d)$. Therefore[3] $\psi_p(d) = \varphi(d)$, under the assumption $\psi_p(d) > 0$; in any case, $\psi_p(d) \leqslant \varphi(d)$. □

Corollary. *Every prime number has a primitive root.*

Proof. $\psi_p(p-1) = \varphi(p-1) \geqslant 1$. □

Now we can prove the necessity of (all of) Korselt's Criterion for being a Carmichael number (p. 77):

Theorem 75. *If n is a Carmichael number, and $p \mid n$, then $p - 1 \mid n - 1$.*

Proof. Given that n is a Carmichael number and $p \mid n$, we let a be a primitive root of p. Since $a^n \equiv a \ (n)$, we have $a^n \equiv a \ (p)$, and therefore $a^{n-1} \equiv 1 \ (p)$. But $\operatorname{ord}_p(a) = p - 1$, so $p - 1 \mid n - 1$. □

So now we know that the Carmichael numbers are *precisely* those squarefree composite numbers n such that $p \mid n \implies p - 1 \mid n - 1$. We shall be able to give another characterization in §10.5, once we know that squares of primes have primitive roots.

10.4. Discrete logarithms

The inverse of the function exp from $\mathbb{R}$ onto $(0, \infty)$ is the logarithm function[4] log, where as noted in §4.5, $\log x = \int_1^x (\mathrm{d}t/t)$.

We can use similar terminology for the inverse of an isomorphism $x \mapsto b^x$ from $\mathbb{Z}_{p-1}$ to $\mathbb{Z}_p{}^\times$. Here b must be a primitive root of p, and if $b^x \equiv y \ (p)$, we can write

$$x \equiv \log_b y \pmod{(p-1)}.$$

For example, *modulo* 17, we have Table 10.2. If $3^k = \ell$, then we can denote k by $\log_3 \ell$. But we can think of these numbers as congruence classes:

$$3^k \equiv \ell \pmod{17} \iff k \equiv \log_3 \ell \pmod{16}.$$

The usual properties hold:

$$\log_3(xy) \equiv \log_3 x + \log_3 y \pmod{16}; \qquad \log_3 x^n \equiv n \log_3 x \pmod{16}.$$

For example,

$$\log_3(11 \cdot 14) \equiv \log_3 11 + \log_3 14 \equiv 7 + 9 \equiv 16 \equiv 0 \pmod{16},$$

[3] Gauss gives just this proof in the *Disquisitiones Arithmeticae* [16, ¶¶53–4].

[4] This function can be denoted by ln, for **logarithmus naturalis,** in case one happens to want to use log to denote the inverse of the function $x \mapsto 10^x$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	(mod 16)
3^k	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	(mod 17)

Rearranged:

3^k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	(mod 17)
k	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8	(mod 16)

Table 10.2. Powers of 3 *modulo* 17

and therefore $11 \cdot 14 \equiv 3^0 \equiv 1 \pmod{17}$.

We can define logarithms for any modulus that has a primitive root; then the base of the logarithms will be a primitive root. If b is a primitive root of a modulus n, and $\gcd(a, n) = 1$, then there is some s such that

$$b^s \equiv a \pmod{n}.$$

Then s is unique *modulo* $\varphi(n)$. Indeed, by Theorem 72,

$$b^x \equiv b^y \pmod{n} \iff x \equiv y \pmod{\varphi(n)}.$$

Then $\log_b a$ can be defined as the least non-negative such s.

Another application of logarithms, besides multiplication problems, is congruences of the form

$$x^d \equiv a \pmod{n},$$

again where n has a primitive root b. The last congruence is then equivalent to

$$\log_b(x^d) \equiv \log_b a \pmod{\varphi(n)},$$
$$d \log_b x \equiv \log_b a \pmod{\varphi(n)}.$$

If this is to have a solution, then we must have

$$\gcd(d, \varphi(n)) \mid \log_b a.$$

For example, let's work *modulo* 7:

k	0	1	2	3	4	5
3^k	1	3	2	6	4	5

ℓ	1	2	3	4	5	6
$\log_3 \ell$	0	2	1	4	5	3

Then we have, for example,

$$x^3 \equiv 2 \pmod{7} \iff 3 \log_3 x \equiv 2 \pmod{6},$$

so there is no solution, since $\gcd(3, 6) = 3$, and $3 \nmid 2$. But we also have

$$\begin{aligned} x^3 \equiv 6 \pmod{7} &\iff 3 \log_3 x \equiv 3 \pmod{6} \\ &\iff \log_3 x \equiv 1 \pmod{2} \\ &\iff \log_3 x \equiv 1, 3, 5 \pmod{6} \\ &\iff x \equiv 3^1, 3^3, 3^5 \pmod{7} \\ &\iff x \equiv 3, 6, 5 \pmod{7}. \end{aligned}$$

We expect no more than 3 solutions, by Lagrange's Theorem. Is there an alternative to using logarithms? As $6 \equiv 3^3 \pmod{7}$, we have

$$x^3 \equiv 6 \pmod{7} \iff x^3 \equiv 3^3 \pmod{7};$$

but we cannot conclude from this $x \equiv 3 \pmod 7$.

For congruences *modulo* 11, we can use the following table:

k	0	1	2	3	4	5	6	7	8	9	$\log_2 \ell \pmod{10}$
$2^k \pmod{11}$	1	2	4	-3	5	-1	-2	-4	3	-5	ℓ

We have then

$$\begin{aligned}
4x^{15} \equiv 7 \pmod{11} &\iff 4x^5 \equiv 7 \pmod{11} \\
&\iff \log_2(4x^5) \equiv \log_2 7 \pmod{10} \\
&\iff \log_2 4 + 5\log_2 x \equiv \log_2 7 \pmod{10} \\
&\iff 2 + 5\log_2 x \equiv 7 \pmod{10} \\
&\iff 5\log_2 x \equiv 5 \pmod{10} \\
&\iff \log_2 x \equiv 1 \pmod 2 \\
&\iff \log_2 x \equiv 1, 3, 5, 7, 9 \pmod{10} \\
&\iff x \equiv 2^1, 2^3, 2^5, 2^7, 2^9 \pmod{11} \\
&\iff x \equiv 2, 8, 10, 7, 6 \pmod{11}.
\end{aligned}$$

Why are there five solutions?

Theorem 76. *Suppose n has a primitive root, $\gcd(a, n) = 1$, and*

$$d = \gcd(k, \varphi(n)).$$

The following are equivalent:

a) *The congruence*

$$x^k \equiv a \pmod n \qquad (\S)$$

is soluble.

b) *The congruence (§) has d solutions.*

c) $a^{\varphi(n)/d} \equiv 1 \pmod n$.

Proof. The following are equivalent:

$$\begin{gathered}
x^k \equiv a \text{ is soluble} \pmod n; \\
k \log x \equiv \log a \text{ is soluble} \pmod{\varphi(n)}; \\
d \mid \log a; \\
\varphi(n) \mid \frac{\varphi(n)}{d} \cdot \log a;
\end{gathered}$$

$$\frac{\varphi(n)}{d} \cdot \log a \equiv 0 \pmod{\varphi(n)};$$
$$\log(a^{\varphi(n)/d}) \equiv 0 \pmod{\varphi(n)};$$
$$a^{\varphi(n)/d} \equiv 1 \pmod{n}.$$

Thus (a)⇔(c). Trivially, (b)⇒(a). Finally, assume (a), so that $d \mid \log a$, as above. Letting r be the base of the logarithms, we have

$$\begin{aligned}
x^k \equiv a \pmod{n} &\iff k \log x \equiv \log a \pmod{\varphi(n)} \\
&\iff \frac{k}{d} \cdot \log x \equiv \frac{\log a}{d} \pmod{\frac{\varphi(n)}{d}} \\
&\iff \log x \equiv \frac{\log a}{k} \pmod{\frac{\varphi(n)}{d}} \\
&\iff \log x \equiv \frac{\log a}{k} + \frac{\varphi(n)}{d} \cdot j \pmod{\varphi(n)}, \\
&\qquad \text{where } j \in \{0, 1, \ldots, d-1\} \\
&\iff x \equiv r^{(\log a)/k} \cdot (r^{\varphi(n)/d})^j \pmod{n}, \\
&\qquad \text{where } j \in \{0, 1, \ldots, d-1\}.
\end{aligned}$$

Finally, these d solutions are incongruent. Indeed, since $\mathrm{ord}_n(r) = \varphi(n)$, the powers $(r^{\varphi(n)/d})^j$ are incongruent; and $r^{(\log a)/k}$ is invertible. □

10.5. Composite numbers with primitive roots

We know that all primes have primitive roots. Now we show that the numbers with primitive roots are precisely:

$$2, \qquad 4, \qquad p^s, \qquad 2 \cdot p^s,$$

where p is an odd prime, and $s \geqslant 1$. We shall first show that the numbers *not* on this list do *not* have primitive roots:

Lemma. *If $k > 2$, then $2 \mid \varphi(k)$.*

Proof. Suppose $k > 2$. Then either $k = 2^s$, where $s > 1$, or else $k = p^s \cdot m$ for some odd prime p, where $s > 0$ and $\gcd(p, m) = 1$. In the first case, $\varphi(k) = 2^s - 2^{s-1} = 2^{s-1}$, which is even. In the second case, $\varphi(k) = \varphi(p^s) \cdot \varphi(m)$, which is even, since $\varphi(p^s) = p^s - p^{s-1}$, the difference of two odd numbers. □

Theorem 77. *If m and n are co-prime, both greater than 2, then mn has no primitive root.*

Proof. Suppose $\gcd(a, mn) = 1$. (This is the only possibility for a primitive root.) Then a is prime to m and n, so

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \qquad a^{\varphi(n)} \equiv 1 \pmod{n},$$

Therefore $a^{\operatorname{lcm}(\varphi(m),\varphi(n))} \equiv 1$ *modulo* m and n, and hence *modulo* $\operatorname{lcm}(m, n)$, which is mn. By the lemma, 2 divides both $\varphi(m)$ and $\varphi(n)$, so

$$\operatorname{lcm}(\varphi(m), \varphi(n)) \mid \frac{\varphi(m)\varphi(n)}{2},$$

that is, $\operatorname{lcm}(\varphi(m), \varphi(n)) \mid \varphi(mn)/2$. Therefore

$$\operatorname{ord}_{mn}(a) \leqslant \frac{\varphi(mn)}{2},$$

so a is not a primitive root of mn. □

Theorem 78. *If $k \geqslant 1$, then 2^{2+k} has no primitive root.*

Proof. Any primitive root of 2^{2+k} must be odd. Let a be odd. We shall show by induction that

$$a^{\varphi(2^{2+k})/2} \equiv 1 \pmod{2^{2+k}}.$$

Since $\varphi(2^{2+k}) = 2^{2+k} - 2^{1+k} = 2^{1+k}$, it is enough to show

$$a^{2^k} \equiv 1 \pmod{2^{2+k}}.$$

The claim is true when $k = 1$, since $a^2 \equiv 1 \pmod 8$ for all odd numbers a. Suppose the claim is true when k is *some* positive integer ℓ, that is,

$$a^{2^\ell} \equiv 1 \pmod{2^{2+\ell}}.$$

This means

$$a^{2^\ell} = 1 + 2^{2+\ell} \cdot m$$

for some m. Now square:

$$\begin{aligned} a^{2^{1+\ell}} = (a^{2^\ell})^2 = (1 + 2^{2+\ell} \cdot m)^2 &= 1 + 2^{3+\ell} \cdot m + 2^{4+2\ell} \cdot m^2 \\ &= 1 + 2^{3+\ell} \cdot m \cdot (1 + 2^{1+\ell} \cdot m). \end{aligned}$$

Hence $a^{2^{1+\ell}} \equiv 1 \pmod{2^{3+\ell}}$, so our claim is true when $k = \ell + 1$. □

Now for the positive results. These will use the following.

Lemma. *Let r be a primitive root of p, and $k > 0$. Then*

$$\operatorname{ord}_{p^k}(r) = (p-1)p^\ell$$

for some ℓ, where $0 \leqslant \ell < k$.

Proof. Let $\operatorname{ord}_{p^k}(r) = n$. Then $n \mid \varphi(p^k)$. But $\varphi(p^k) = p^k - p^{k-1} = (p-1)\cdot p^{k-1}$. Thus,

$$n \mid (p-1)\cdot p^{k-1}.$$

Also, $r^n \equiv 1 \pmod{p^k}$, so $r^n \equiv 1 \pmod{p}$, which means $\operatorname{ord}_p(r) \mid n$. But r is a primitive root of p, so $\operatorname{ord}_p(r) = \varphi(p) = p-1$. Therefore

$$p-1 \mid n.$$

The claim now follows. □

Theorem 79. *p^2 has a primitive root. In fact, if r is a primitive root of p, then either r or $r+p$ is a primitive root of p^2.*

Proof. Let r be a primitive root of p. If r is a primitive root of p^2, then we are done. Suppose r is not a primitive root of p^2. Then $\operatorname{ord}_{p^2}(r) = p-1$, by the last lemma. Hence, *modulo* p^2, we have

$$\begin{aligned}(r+p)^{p-1} &\equiv r^{p-1} + (p-1)\cdot r^{p-2}\cdot p + \binom{p-1}{2}\cdot r^{p-3}\cdot p^2 + \cdots \\ &\equiv r^{p-1} + (p-1)\cdot r^{p-2}\cdot p \\ &\equiv 1 + (p-1)\cdot r^{p-2}\cdot p \\ &\equiv 1 - r^{p-2}\cdot p \\ &\not\equiv 1,\end{aligned}$$

since $p \nmid r$. (Note that this argument holds even if $p = 2$.) Hence $\operatorname{ord}_{p^2}(r+p) \neq p-1$, so by the lemma, the order must be $(p-1)\cdot p$, that is, $\varphi(p^2)$. This means r is a primitive root of p^2. □

Alternatively, if r is a primitive root of p, then either r or $r+rp$ is a primitive root of p^2. For, $\operatorname{ord}_{p^2}(1+p) = p$, simply because the order is not 1, but

$$(1+p)^p = \sum_{j=0}^{p}\binom{p}{j}p^j = 1 + p^2 + \sum_{j=2}^{p}\binom{p}{j}p^j \equiv 1 \pmod{p^2}.$$

Then r and $1+p$ have orders $p-1$ and p respectively, *modulo* p^2, so their product must have order $p(p-1)$ (see Exercise 97).

Now we can give another characterization of Carmichael numbers (which were defined on page 76 as those composite numbers n such that $a^n \equiv a \ (n)$ for all a):

Theorem 80. *A composite number n is a Carmichael number if and only if, whenever* $\gcd(a, n) = 1$*, we have*

$$a^{n-1} \equiv 1 \pmod{n}. \tag{¶}$$

Proof. Suppose n is a Carmichael number and $\gcd(a, n) = 1$. If $p \mid n$, then $a^n \equiv a \pmod{p}$, so $a^{n-1} \equiv 1 \ (p)$. Since n is squarefree by Theorem 51 (p. 77), we have that n is the least common multiple of its prime divisors, and therefore (¶) holds.

Conversely, suppose (¶) holds whenever $\gcd(a, n) = 1$. The proof of Theorem 75 (p. 109) still works to show $p \mid n \implies p - 1 \mid n - 1$. Also, n is squarefree. Indeed, suppose $p^2 \mid n$. But p^2 has a primitive root a, and by the Chinese Remainder Theorem, we may assume $\gcd(a, n) = 1$. Then $a^{n-1} \equiv 1$ *modulo* n and therefore *modulo* p^2, so $\varphi(p^2) \mid n - 1$. But $p \mid \varphi(p^2)$, so $p \mid n - 1$, which is absurd. Therefore n must be squarefree, so by Theorem 50, it is a Carmichael number. □

Theorem 81. *All odd prime powers (that is, all powers of odd primes) have primitive roots. In fact, a primitive root of p^2 is a primitive root of every power p^{1+k}, where p is odd.*

Proof. Assume p is an odd prime. We know p and p^2 have primitive roots. Let r be a primitive root of p^2. We prove by induction that r is a primitive root of p^{1+k}. The claim is trivially true when $k = 1$. Suppose it is true when k is some positive integer ℓ. This means

$$\operatorname{ord}_{p^{1+\ell}}(r) = (p - 1) \cdot p^{\ell}.$$

In particular,

$$r^{(p-1)\cdot p^{\ell-1}} \not\equiv 1 \pmod{p^{1+\ell}}.$$

However, since $\varphi(p^{\ell}) = (p - 1) \cdot p^{\ell-1}$, we have

$$r^{(p-1)\cdot p^{\ell-1}} \equiv 1 \pmod{p^{\ell}}.$$

We can now conclude

$$r^{(p-1)\cdot p^{\ell-1}} = 1 + p^{\ell} \cdot m$$

for some m that is indivisible by p. Now raise both sides of this equation to the power p:

$$r^{(p-1)\cdot p^{\ell}} = 1 + p^{1+\ell} \cdot m + \binom{p}{2} \cdot p^{2\ell} \cdot m^2 + \binom{p}{3} \cdot p^{3\ell} \cdot m^3 + \cdots$$

Since $p > 2$ and $\ell \geqslant 1$, so that $p \mid \binom{p}{2}$ and $2\ell \geqslant 1 + \ell$, we have

$$r^{(p-1)\cdot p^{\ell}} \equiv 1 + p^{1+\ell} \cdot m \not\equiv 1 \pmod{p^{2+\ell}}.$$

Therefore we must have

$$\operatorname{ord}_{p^{2+\ell}}(r) = (p-1)\cdot p^{1+\ell} = \varphi(p^{2+\ell}),$$

which means r is a primitive root of $p^{2+\ell}$. □

For example, 3 has the primitive root 2, since $2 \not\equiv 1 \pmod 3$, but $2^2 \equiv 1 \pmod 3$. Hence, either 2 or 5 is a primitive root of 9, by Theorem 79. In fact, both are. Using $5 \equiv -4 \pmod 9$, we have:

k	2	3
$2^k \pmod 9$	4	-1
$(-4)^k \pmod 9$	-2	-1

so the order of 2 and -4 is not 2 or 3 *modulo* 9; hence it must be 6, since this is $\varphi(9)$. By Theorem 81 then, 27 has 6 non-congruent primitive roots, each congruent *modulo* 9 to one of 2 and -4; those roots then are -13, -7, -4, 2, 5, and 11. Indeed, $\varphi(27) = 18$ and we have

k	2	3	4	5	6	7	8	9
$(-13)^k \pmod{27}$	7	-10	-5	11	-8	-4	-2	-1
$(-4)^k \pmod{27}$	-11	-10	13	2	-8	5	7	-1
$5^k \pmod{27}$	-2	-10	4	-7	-8	-13	-11	-1
$(-7)^k \pmod{27}$	-5	8	-2	13	10	-11	4	-1
$2^k \pmod{27}$	4	8	-11	5	10	-7	13	-1
$11^k \pmod{27}$	13	8	7	-4	10	2	-5	-1

But does 18 have a primitive root? The numbers 2 and -4 cannot be primitive roots of 18, since they are not prime to it; but $\varphi(18) = 6$ and we have

k	2	3
$(-7)^k \pmod{18}$	-5	-1
$5^k \pmod{18}$	7	-1

so -7 and 5 are primitive roots of 18.

Theorem 82. *If p is an odd prime, and r is a primitive root of p^s, then either r or $r + p^s$ is a primitive root of $2p^s$—whichever one is odd.*

Proof. Let r be an odd primitive root of p^s. Then $\gcd(r, 2p^s) = 1$, so r has an order *modulo* $2p^s$. Since also $\operatorname{ord}_{p^s}(r) = \varphi(p^s)$, we have

$$\varphi(p^s) \mid \operatorname{ord}_{2p^s}(r).$$

But also $\operatorname{ord}_{2p^s}(r) \mid \varphi(2p^s)$; and $\varphi(p^s) = \varphi(2p^s)$. Hence $\operatorname{ord}_{2p^s}(r) = \varphi(2p^s)$. □

11. Quadratic reciprocity

11.1. Quadratic equations

If $p \nmid a$, then the linear congruence

$$ax + b \equiv 0 \pmod{p}$$

is always soluble. The next step is to consider quadratic congruences,

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{$*$}$$

where still $p \nmid a$. For example, let us try to solve

$$2x^2 - 8x + 9 \equiv 0 \pmod{11}. \tag{$\dagger$}$$

We cannot factorize the polynomial $2x^2 - 8x + 9$ over $\mathbb{Z}$ (or even $\mathbb{R}$), since $8^2 - 4 \cdot 2 \cdot 9 = -8$, which is not a square (or even positive). However, after replacing coefficients with residues *modulo* 11, we may be able to factorize. Still, a better method of solution is **completing the square.** We have, *modulo* 11,

$$\begin{aligned} 2x^2 - 8x + 9 \equiv 0 &\iff x^2 - 4x \equiv -\frac{9}{2} \\ &\iff x^2 - 4x + 4 \equiv 4 - \frac{9}{2} \\ &\iff (x-2)^2 \equiv -\frac{1}{2} \equiv \frac{10}{2} \equiv 5. \end{aligned}$$

(We did not need to compute the inverse of 2 *modulo* 11, although we may see easily enough that it is 6.) If 5 is a square *modulo* 11, then ($\dagger$) has a solution; if not, not. One way to settle the question is by hunting: we have $5 \equiv 16 \equiv 4^2$, so

$$\begin{aligned} 2x^2 - 8x + 9 \equiv 0 &\iff (x-2)^2 \equiv 4^2 \\ &\iff x - 2 \equiv \pm 4 \\ &\iff x \equiv 2 \pm 4 \equiv 6 \text{ or } 9. \end{aligned}$$

Note that we have used Lagrange's Theorem (Theorem 73) to conclude that the congruence has exactly two solutions. We now know

$$2x^2 - 8x + 9 \equiv 2(x-6)(x+2) \equiv 2(x-6)(x-9).$$

Possibly, with some cleverness, we might have been able to see this from the beginning. But suppose we want to solve

$$x^2 - 4x - 3 \equiv 0 \pmod{11}. \qquad (\ddagger)$$

We find

$$x^2 - 4x - 3 \equiv 0 \iff x^2 - 4x + 4 \equiv 7 \iff (x-2)^2 \equiv 7.$$

Now, if $7 \equiv k^2$, then we may assume $-5 \leqslant k < 5$. The positive integers that are congruent to 7 and are less than or equal to 5^2 are 7 and 18, and neither of them is a square. Therefore the congruence (‡) is insoluble. In particular, the polynomial $x^2 - 4x - 3$ has no factorization over $\mathbb{Z}_{11}$; so it would have been futile to hunt for a factorization. Completing the square is the way to go.

Another way to see that 7 has no square root *modulo* 11 is to note first that 2 is a primitive root of 11. Since $11 \nmid 7$, but $7 \equiv -4$, the following table shows that 7 is not a square *modulo* 11, because -4 does not appear as an even power of 2 (that is, a power of 2 with even exponent):

k	0	1	2	3	4	mod 5
2^{2k}	1	4	5	-2	3	mod 11

Indeed, $2^m \equiv 2^n \ (11)$ if and only if $m \equiv n \ (10)$, by Theorem 72. Since 10 is even, the only numbers prime to 11 that are squares *modulo* 11 are the even powers of 2.

Considering the general quadratic congruence $(*)$, and assuming p is odd (so that 2 is invertible *modulo* p), we have

$$\begin{aligned} ax^2 + bx + c \equiv 0 &\iff x^2 + \frac{b}{a}x \equiv -\frac{c}{a} \\ &\iff x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} \equiv \frac{b^2}{4a^2} - \frac{c}{a} \\ &\iff \left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2 - 4ac}{(2a)^2}, \end{aligned}$$

just as when one derives the usual quadratic formula. Working over $\mathbb{R}$, one knows that the equation $ax^2 + bx + c = 0$ (where $a \neq 0$) is soluble if and only if $b^2 - 4ac \geqslant 0$. Another way to express this condition is that the discriminant $b^2 - 4ac$ must be a *square* in $\mathbb{R}$. It is the same *modulo* p: the congruence $(*)$ is soluble if and only if $b^2 - 4ac$ is a square *modulo* p. In the terminology introduced in §7.3, this condition is that $b^2 - 4ac$ either is divisible by p or is a **quadratic residue** of p.

As we have just observed, assuming $p \nmid b^2 - 4ac$, one way to tell whether $b^2 - 4ac$ is a quadratic residue is first to find its least positive residue, say m, and then

to check whether any of the residues $m + kp$ is a square, where $0 \leqslant k$ and also $m + kp \leqslant ((p-1)/2)^2$, that is,

$$m + kp \leqslant \varpi^2,$$

in the notation of (‖) in §7.3 (p. 81). So it is sufficient to check when $0 \leqslant k < \varpi/2$. This could still be a lot of work if p is large.

We shall develop a way to test for quadratic residues that is more practical as well as theoretically interesting.

11.2. Quadratic residues

We have just seen that the quadratic residues of 11 are the even powers of 2, namely 1, 4, 5, −2, and 3, or rather 1, 4, 5, 9, and 3. The **quadratic non-residues** are the odd powers: 2, −3, −1, −4, and −5, that is, 2, 8, 10, 7, and 6. So there are five residues, and five non-residues. (The general formulation of this equality will be Theorem 87.)

Theorem 83 (Euler's Criterion)**.** *Let p be an odd prime, and $\gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if*

$$a^{(p-1)/2} \equiv a^{\varpi} \equiv 1 \pmod{p}, \tag{§}$$

and a is a quadratic non-residue of p if and only if

$$a^{\varpi} \equiv -1 \pmod{p}. \tag{¶}$$

Proof. Let r be a primitive root of p. Any solution of $x^2 \equiv a \pmod{p}$ is r^k for some k, and then

$$a^{\varpi} \equiv (r^{2k})^{\varpi} \equiv (r^k)^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Theorem (Theorem 47).

In any case, $a \equiv r^{\ell} \pmod{p}$ for some ℓ. Suppose $a^{\varpi} \equiv 1 \pmod{p}$. Then

$$1 \equiv (r^{\ell})^{\varpi} \equiv r^{\ell \cdot \varpi} \pmod{p},$$

so $\operatorname{ord}_p(r) \mid \ell \cdot \varpi$, that is,

$$p - 1 \mid \ell \cdot \varpi.$$

Therefore $\ell/2$ is an integer, that is, ℓ is even. Say $\ell = 2m$. Then $a \equiv r^{2m} \equiv (r^m)^2 \pmod{p}$.

Since $a^{p-1} \equiv 1 \pmod{p}$, by Fermat's Theorem, we have $a^{\varpi} \equiv \pm 1 \pmod{p}$, so the second part of the claim follows. □

Another way to prove the theorem arises from the following considerations, which also lead to the alternative proof of Wilson's Theorem promised at the end of §7.3 (p. 82). Suppose a is a quadratic non-residue of p. If $b \in \{1, \dots, p-1\}$, then the congruence

$$bx \equiv a \pmod{p}$$

has a unique solution in $\{1, \dots, p-1\}$, and we denote the solution by a/b. Then $b \neq a/b$, since a is not a quadratic residue of p. Now we define a sequence $(b_1, \dots, b_\varpi)$ recursively. If b_k has been chosen when $k < \ell < \varpi$, then let b_ℓ be the least element of $\{1, \dots, p-1\} \smallsetminus \{b_1, a/b_1, \dots, b_{\ell-1}, a/b_{\ell-1}\}$. Note then that a/b_ℓ must be in this set too, since otherwise $a/b_\ell = b_k$ for some k such that $k < \ell$, and then $b_\ell = a/b_k$. We now have

$$\left\{b_1, \frac{a}{b_1}, \dots, b_\varpi, \frac{a}{b_\varpi}\right\} = \{1, \dots, p-1\}.$$

Now multiply everything together:

$$a^\varpi \equiv (p-1)! \pmod{p}. \qquad (\|)$$

If we have Wilson's Theorem (Theorem 52, p. 80), we can conclude (¶). Conversely, this and (‖) give us Wilson's Theorem.

Now suppose a is a quadratic residue of p. We choose the b_k as before, except this time let b_1 be the least positive solution of $x^2 \equiv a \pmod{p}$, and replace a/b_1 with the next least positive solution, which is $p - b_1$. We have then

$$\left\{b_1, p-b_1, b_2, \frac{a}{b_2}, \dots, b_\varpi, \frac{a}{b_\varpi}\right\} = \{1, \dots, p-1\},$$

and multiplication now gives us

$$-a^\varpi \equiv (p-1)! \pmod{p}.$$

Now (§) is equivalent to Wilson's Theorem. Since we do have (§) when $a = 1$, Wilson's Theorem holds.[1]

11.3. The Legendre symbol

Again, p is an odd prime, and $p \nmid a$. Euler's Criterion can be abbreviated by

$$a^\varpi \equiv \left(\frac{a}{p}\right) \pmod{p}, \qquad (**)$$

[1] This is the first proof of Wilson's Theorem given by Hardy and Wright [21, p. 68].

where (a/p) is called the **Legendre symbol.**[2] More precisely, we have

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p; \\ -1, & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

Theorem 84. *If p is an odd prime not dividing a or b, then:*

$$\left(\frac{a \pm kp}{p}\right) = \left(\frac{a}{p}\right),$$
$$\left(\frac{a^2}{p}\right) = 1,$$
$$\left(\frac{1}{p}\right) = 1,$$
$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4, \end{cases} \qquad (\dagger\dagger)$$
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. The first three equations follow immediately from the definitions; the others, from Euler's Criterion as summarized by $(**)$. (Also $(\dagger\dagger)$ is equivalent to Theorem 53 on page 82.) □

With these properties, we can calculate many Legendre symbols. For example,

$$\left(\frac{50}{19}\right) = \left(\frac{12}{19}\right) = \left(\frac{2}{19}\right)^2\left(\frac{3}{19}\right) = \left(\frac{3}{19}\right),$$
$$3^{\varpi} \equiv 3^9 \equiv 3^8 \cdot 3 \equiv 9^4 \cdot 3 \equiv 81^2 \cdot 3 \equiv 5^2 \cdot 3 \equiv 6 \cdot 3 \equiv 18 \equiv -1 \mod 19,$$

so $(50/19) = -1$, which means the congruence $x^2 \equiv 50 \pmod{19}$ has no solution.

We may ask whether $(\dagger\dagger)$ has a simpler form, owing to the existence of only finitely many p satisfying one of the cases. This possibility fails.

Theorem 85. *There are infinitely many primes p such that $p \equiv 3 \pmod 4$.*

Proof. Suppose $(q_1, q_2, \ldots, q_n)$ is a list of primes. We shall prove that there is a prime p, not on this list, such that $p \equiv 3 \pmod 4$. Let

$$s = 4q_1 \cdot q_2 \cdots q_n - 1.$$

Then $s \equiv 3 \pmod 4$. Then s must have a prime factor p such that $p \equiv 3 \pmod 4$. Indeed, if all prime factors of s are congruent to 1, then so must s be. But p is not any of the q_k. □

[2] Named for Adrien-Marie Legendre, 1752–1833.

A similar argument *fails* to show that there are infinitely many primes p such that $p \equiv 1\ (4)$. For, even though $4q_1 \cdot q_2 \cdots q_n - 3 \equiv 1\ (4)$, possibly all prime factors of $4q_1 \cdot q_2 \cdots q_n - 3$ are congruent to 3. (This is the case when $n = 1$ and $q_1 = 3$, for example.) Nonetheless, we still have:

Theorem 86. *There are infinitely many primes p such that $p \equiv 1 \pmod 4$.*

Proof. Suppose $(q_1, q_2, \ldots, q_n)$ is a list of primes. We shall prove that there is a prime p, not on this list, such that $p \equiv 1 \pmod 4$. Let

$$s = 2q_1 \cdot q_2 \cdots q_n.$$

Then $s^2 + 1$ is odd, so it is divisible by some odd prime p, which is distinct from each of the q_k. This means $s^2 + 1 \equiv 0 \pmod p$, so s is a solution of the congruence $x^2 \equiv -1 \pmod p$. Then $(-1/p) = 1$, so $p \equiv 1 \pmod 4$, by (††) above. □

From the rules so far, we obtain the following table:

a	1	2	3	4	5	6	7	8	9	10	11	12
$(a/13)$	1		1	1					1	1		1

Indeed, under the squares 1, 4, and 9, we put 1. Also $4^2 = 16 \equiv 3$, so $(3/13) = 1$. Finally, by (††), we have $(-1/13) = 1$; or we can just compute this: $(-1)^{\varpi} = (-1)^6 = 1$. Hence the table will be symmetric; that is, $(13 - a/13) = (-a/13) = (-1/13) \cdot (a/13) = (a/13)$. In particular, $(10/13) = 1$ and $(12/13) = 1$. So half of the slots have been filled with 1. The other half must take -1, by the following.

Theorem 87. *For all odd primes p,*

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0.$$

Proof. Let r be a primitive root of p. Then

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{r^k}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{r}{p}\right)^k.$$

But $(r/p) = -1$, because r is a primitive root and therefore $r^{\varpi} \equiv -1 \pmod p$. Hence

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0.$$ □

So now we can complete the table above:

a	1	2	3	4	5	6	7	8	9	10	11	12
$(a/13)$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1

11.4. Gauss's Lemma

Again, p is an odd prime. Given an integer k, we have

$$\left[\frac{k}{p}\right] \leqslant \frac{k}{p} < \left[\frac{k}{p}\right] + 1,$$
$$p \cdot \left[\frac{k}{p}\right] \leqslant k < p \cdot \left[\frac{k}{p}\right] + p,$$
$$0 \leqslant k - p \cdot \left[\frac{k}{p}\right] < p.$$

Thus the least positive residue of k *modulo* p is $k - p \cdot [k/p]$. For use in some proofs, let us define

$$|k|_p = \begin{cases} k - p \cdot [k/p], & \text{if this is less than } p/2, \\ p - (k - p \cdot [k/p]), & \text{otherwise.} \end{cases} \qquad (\ddagger\ddagger)$$

Then $0 \leqslant |k|_p < p/2$, and $|k|_p$ is the least distance between k and a multiple of p.

Theorem 88 (Gauss's Lemma)**.** *Let p be an odd prime, and* $\gcd(a, p) = 1$. *Then*

$$\left(\frac{a}{p}\right) = (-1)^n,$$

where n is the number of elements k of the set

$$\{a, 2a, 3a, \ldots, \varpi a\}$$

whose least positive residues exceed $p/2$.

Proof. If $|ka|_p = |\ell a|_p$, then $ka \equiv \pm \ell a \ (p)$, so $k = \pm \ell \ (p)$. Therefore

$$\{1, 2, \ldots, \varpi\} = \{|a|_p, |2a|_p, \ldots, |\varpi a|_p\},$$

so

$$\prod_{k=1}^{\varpi} k = \prod_{k=1}^{\varpi} |ka|_p.$$

Also $|ka|_p \equiv \pm ka \ (p)$, and $|ka|_p \equiv -ka \ (p)$ if and only if ka has least positive residue exceeding $p/2$. Therefore, with n as in the statement, we have

$$\varpi! \cdot a^{\varpi} \equiv \prod_{k=1}^{\varpi} (ka) \equiv (-1)^n \cdot \prod_{k=1}^{\varpi} |ka|_p \equiv (-1)^n \cdot \prod_{k=1}^{\varpi} k \equiv (-1)^n \cdot \varpi! \mod p,$$

which yields the claim by Euler's Criterion. □

For example, to find $(3/19)$, we can look at

$$3, \quad 6, \quad 9, \quad 12, \quad 15, \quad 18, \quad 21, \quad 24, \quad 27,$$

whose remainders on division by 19 are, respectively,

$$3, \quad 6, \quad 9, \quad 12, \quad 15, \quad 18, \quad 2, \quad 5, \quad 8.$$

Of these, only 12, 15, and 18 exceed $19/2$, and they are three; so

$$\left(\frac{3}{19}\right) = (-1)^3 = -1.$$

We shall use Gauss's Lemma to prove the Law of Quadratic Reciprocity, by which we shall be able to relate (p/q) and (q/p) when both p and q are odd primes. Meanwhile, besides the direct application of Gauss's Lemma to computing Legendre symbols, we have the following, which we shall also need in order to take full advantage of the Law of Quadratic Reciprocity:

Theorem 89. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8; \\ -1, & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Proof. To apply Gauss's Lemma, we look at the numbers $2 \cdot 1$, $2 \cdot 2$, …, $2 \cdot \varpi$. Each is its own remainder on division by p. Hence $(2/p) = (-1)^n$, where n is the number of integers k such that

$$\frac{p}{2} < 2k \leqslant p - 1,$$

or rather $p/4 < k \leqslant \varpi$. This means

$$n = \varpi - \left[\frac{p}{4}\right].$$

Now consider the possibilities:

$$\begin{aligned} p = 8k+1 &\implies n = 4k - \left[2k + \frac{1}{4}\right] = 2k, \\ p = 8k+3 &\implies n = 4k+1 - \left[2k + \frac{3}{4}\right] = 2k+1, \\ p = 8k+5 &\implies n = 4k+2 - \left[2k + \frac{5}{4}\right] = 4k+1, \\ p = 8k+7 &\implies n = 4k+3 - \left[2k + \frac{7}{4}\right] = 4k+2. \end{aligned}$$

In each case then, $(2/p)$ is as claimed. ∎

As $13 \equiv -3 \pmod 8$, we have $(2/13) = -1$, which we found by other methods above. An alternative formulation of the theorem is

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

since

$$\begin{aligned} p \equiv \pm 1 \pmod 8 &\implies p \equiv \pm 1, \pm 7 \pmod{16} \implies p^2 \equiv 1 \pmod{16}, \\ p \equiv \pm 3 \pmod 8 &\implies p \equiv \pm 3, \pm 5 \pmod{16} \implies p^2 \equiv 9 \pmod{16}. \end{aligned}$$

We can also use the theorem to find some primitive roots. Given a prime q and an integer a that q does not divide, we know that a is a primitive root of q, provided that

$$a^d \not\equiv 1 \pmod q$$

whenever d is a *proper* divisor of $q-1$. Verifying this condition is easier, the fewer proper divisors q has. If q is odd, then $q-1$ has the fewest possible divisors when it is $2p$ for some p. Recall from page 71 that in this case p is called a **Germain prime,** assuming p itself is odd. That is, an odd prime p is a Germain prime if and only if $2p+1$ is also prime.

Theorem 90. *Suppose p is a Germain prime, and let $\varpi = (p-1)/2$. Then $2p+1$ has the primitive root $(-1)^{\varpi} \cdot 2$, which is 2 if $p \equiv 1 \pmod 4$, and is otherwise -2.*

Proof. Let $r = (-1)^{\varpi} \cdot 2$, and denote $2p+1$ by q. We want to show $\operatorname{ord}_q(r)$ is not 1, 2, or p. But $p \geqslant 3$, so $q \geqslant 7$, and hence $r^1, r^2 \not\equiv 1 \pmod q$. Hence $\operatorname{ord}_q(r)$ is not 1 or 2. Also, from Euler's Criterion,

$$r^p \equiv r^{(q-1)/2} \equiv \left(\frac{r}{q}\right) \pmod q.$$

So it is enough to show $(r/q) = -1$. We consider two cases.

1. If $p \equiv 1 \pmod 4$, then $r = 2$, but also $q \equiv 3 \pmod 8$, so

$$\left(\frac{r}{q}\right) = \left(\frac{2}{q}\right) = -1$$

by the last theorem.

2. If $p \equiv 3 \pmod 4$, then $r = -2$, but also $q \equiv 7 \pmod 8$, and

$$\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2} = (-1)^p = -1,$$

so $(r/q) = (-2/q) = (-1/q)(2/q) = -1$. □

Hence, for example, we have the following Germain primes and their primitive roots:

p	3	5	11	23	29	41	53	83	89	113	131	173	179
$2p+1$	7	11	23	47	59	83	107	167	179	227	263	347	359
p.r. of $2p+1$	-2	2	-2	-2	2	2	2	-2	2	2	-2	2	-2

It is not known whether there infinitely many Germain primes. However, some of them give examples of Mersenne numbers that are not primes, as noted on page 71:

Theorem 91. *If p is a Germain prime, and $2p+1 \equiv \pm 1 \pmod 8$, then $2^p - 1$ is not prime, because*

$$2^p \equiv 1 \pmod{2p+1}.$$

Proof. Let $q = 2p+1$. Under the given conditions, we have $(2/q) = 1$ by Theorem 89, so $2^q \equiv 1 \ (q)$ by Euler's Criterion. □

Another consequence of Theorem 89 is:

Theorem 92. *There are infinitely many primes congruent to -1 modulo 8.*

Proof. Let $q_1, \ldots, q_n$ be a finite list of primes. We show that there is p not on the list such that $p \equiv -1 \pmod 8$. Let

$$M = (4q_1 \cdots q_n)^2 - 2.$$

Then $M \equiv -2 \pmod{16}$, so M is not a power of 2; in particular, M has odd prime divisors. Also, for every odd prime divisor p of M, we have

$$(4q_1 \cdots q_n)^2 \equiv 2 \pmod p,$$

so $(2/p) = 1$, and therefore $p \equiv \pm 1 \pmod 8$. Since $M/2 \equiv -1 \pmod 8$, we conclude that not every odd prime divisor of M can be congruent to 1 *modulo* 8. □

11.5. The Law of Quadratic Reciprocity

We now aim to establish the Law of Quadratic Reciprocity, Theorem 93 below. To prove the Law, we shall use the following consequence of Gauss's Lemma (Theorem 88):

Lemma. *If p is an odd prime, $p \nmid a$, and a is odd, then*

$$\left(\frac{a}{p}\right) = (-1)^m,$$

where

$$m = \sum_{k=1}^{\varpi} \left[\frac{ka}{p} \right].$$

Proof. With n as in Gauss's Lemma, we need only show $m \equiv n \ (2)$. As in the proof of Gauss's Lemma, we have

$$\{1, 2, \ldots, \varpi\} = \{|a|_p, |2a|_p, \ldots, |\varpi a|_p\}.$$

We now work with modulus 2, so that $-1 \equiv 1$, and $a + 1 \equiv 0$. Then

$$0 \equiv (a+1) \cdot \sum_{k=1}^{\varpi} k \equiv \sum_{k=1}^{\varpi} (ka - k) \equiv \sum_{k=1}^{\varpi} (ka + |ka|_p).$$

From the original definition (‡‡) of $|k|_p$ on page 124, and because $-1 \equiv 1$, we have

$$ka + |ka|_p \equiv \begin{cases} p \cdot [ka/p], & \text{if (residue of } ka \textit{ modulo } p) < p/2, \\ p \cdot [ka/p] + p, & \text{otherwise.} \end{cases}$$

Therefore

$$0 \equiv \sum_{k=1}^{\varpi} p \cdot \left[\frac{ka}{p} \right] + np \equiv m + n. \qquad \square$$

The following was:

- conjectured by Euler, 1783;
- imperfectly proved by Legendre, 1785, 1798;
- discovered and proved independently by Gauss, 1795, at age 18.

The following proof is due to Gauss's student Eisenstein. We have so far denoted $(p-1)/2$ by ϖ; but now, going back to the original definition (‖) on page 81, we must use $\varpi(p)$:

Theorem 93 (Law of Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\varpi(p) \cdot \varpi(q)}.$$

Proof. By the lemma, it is enough to show

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \varpi(p) \cdot \varpi(q) = \sum_{k=1}^{\varpi(p)} \left[\frac{kq}{p} \right] + \sum_{\ell=1}^{\varpi(q)} \left[\frac{\ell p}{q} \right].$$

We do this by considering a rectangle $ABCD$ in the Cartesian plane as in Figure 11.1. The number of points in the interior of $ABCD$ with integral coordinates

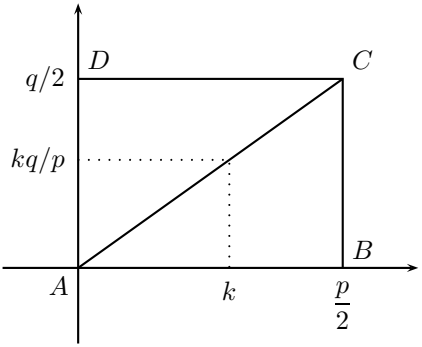


Figure 11.1. Two ways of counting, for the Law of Quadratic Reciprocity

is $[p/2] \cdot [q/2]$, that is, $\varpi(p) \cdot \varpi(q)$. None of these points lie on the diagonal AC. The number of points in the interior of triangle ABC with first coordinate k and second coordinate integral is $[kp/q]$. Therefore the number of points in the interior of ABC with integral coordinates is $\sum_{k=1}^{\varpi(p)} [kq/p]$. A similar consideration of triangle ACD yields the claim. □

For example, suppose $p = 13$ and $q = 7$. The points that we count in the proof are shown in Figure 11.2. Counted in columns, the number of points inside ABC

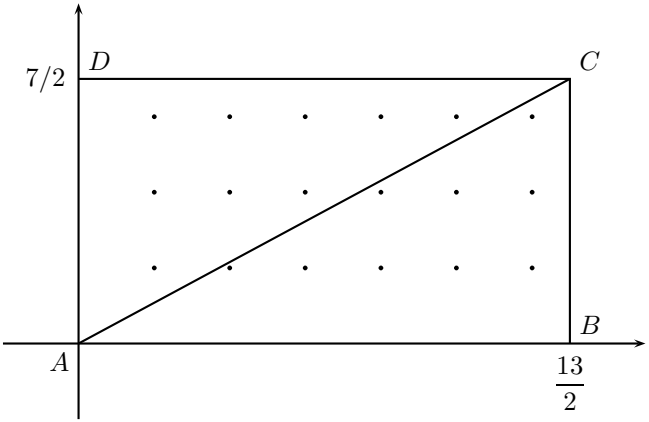


Figure 11.2. Example of the proof of quadratic reciprocity

is $0 + 1 + 1 + 2 + 2 + 3$, which is

$$\left[\frac{7}{13}\right] + \left[\frac{14}{13}\right] + \left[\frac{21}{13}\right] + \left[\frac{28}{13}\right] + \left[\frac{35}{13}\right] + \left[\frac{42}{13}\right].$$

Counted in rows, the number of points inside ACD is $1+3+5$, which is

$$\left[\frac{13}{7}\right]+\left[\frac{26}{7}\right]+\left[\frac{39}{7}\right].$$

The more useful form of the Law of Quadratic Reciprocity is:

$$\left(\frac{q}{p}\right)=\begin{cases}(p/q), & \text{if } p\equiv 1 \text{ or } q\equiv 1 \pmod 4;\\ -(p/q), & \text{if } q\equiv 3\equiv p \pmod 4.\end{cases}$$

It is important to remember here that both p and q are *odd primes.* We have not defined the symbol (a/n) except when n is an odd prime not dividing a. In this case, we can reduce the computation to computation of symbols (p/q) by means of Theorems 84 and 89. For example, we can compute one Legendre symbol as

$$\begin{aligned}
\left(\frac{365}{941}\right) &= \left(\frac{5}{941}\right)\left(\frac{73}{941}\right) && \text{[factorizing]}\\
&= \left(\frac{941}{5}\right)\left(\frac{941}{73}\right) && [5, 73\equiv 1 \pmod 4]\\
&= \left(\frac{1}{5}\right)\left(\frac{65}{73}\right) && \text{[dividing]}\\
&= \left(\frac{5}{73}\right)\left(\frac{13}{73}\right) && \text{[factorizing]}\\
&= \left(\frac{73}{5}\right)\left(\frac{73}{13}\right) && [5, 13\equiv 1 \pmod 4]\\
&= \left(\frac{3}{5}\right)\left(\frac{8}{13}\right) && \text{[dividing]}\\
&= \left(\frac{5}{3}\right)\left(\frac{2}{13}\right)^3 && [5\equiv 1 \pmod 4;\ \text{factorizing}]\\
&= \left(\frac{2}{3}\right)\left(\frac{2}{13}\right) && [(p/q)^2=1]\\
&= (-1)(-1)=1 && [3\equiv 3 \ \&\ 13\equiv -3 \pmod 8].
\end{aligned}$$

Table 11.1. Computation of (365/941)

in Table 11.1. Similarly, we have

$$\left(\frac{47}{199}\right)=-\left(\frac{199}{47}\right)=-\left(\frac{11}{47}\right)=\left(\frac{47}{11}\right)=\left(\frac{3}{11}\right)=-\left(\frac{11}{3}\right)=-\left(\frac{2}{3}\right)=1.$$

Thus we can compute any Legendre symbol (a/p), as long as we can recognize which numbers less than p are prime.

The value of $(2/p)$ cannot be computed by the Law of Quadratic Reciprocity; we need Theorem 89. We *can* use the Law to compute $(3/p)$ when we need it; but we can also compute it once for all as follows.

Theorem 94. *For all primes greater than* 3*,*

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1, & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Proof. We have

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & \text{if } p \equiv 1 \pmod{4}, \\ -\left(\frac{p}{3}\right), & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{3}, \\ -1, & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

It is a Chinese remainder problem to compute

$$\left\{\begin{matrix} p \equiv 1 & (4) \\ p \equiv 1 & (3) \end{matrix}\right\} \iff p \equiv 1 \quad (12),$$

$$\left\{\begin{matrix} p \equiv 1 & (4) \\ p \equiv 2 & (3) \end{matrix}\right\} \iff p \equiv 5 \quad (12),$$

$$\left\{\begin{matrix} p \equiv 3 & (4) \\ p \equiv 1 & (3) \end{matrix}\right\} \iff p \equiv 7 \quad (12),$$

$$\left\{\begin{matrix} p \equiv 3 & (4) \\ p \equiv 2 & (3) \end{matrix}\right\} \iff p \equiv 11 \quad (12).$$

□

One could find a similar rule for (q/p) for any fixed q.

11.6. Composite moduli

Assuming $\gcd(a, n) = 1$, we know when the congruence $x^2 \equiv a \pmod{n}$ has solutions, provided n is an odd prime; but what about the other cases? When $n = 2$, then the congruence always has the solution 1. If $\gcd(m, n) = 1$, and $\gcd(a, mn) = 1$, then the congruence $x^2 \equiv a \pmod{mn}$ is soluble if and only if the system

$$x^2 \equiv a \pmod{m}, \qquad x^2 \equiv a \pmod{n}$$

is soluble. By the Chinese Remainder Theorem, the system is soluble if and only if the individual congruences are separately soluble. Indeed, suppose $b^2 \equiv a \pmod{m}$, and $c^2 \equiv a \pmod{n}$. By the Chinese Remainder Theorem, there is some d such that $d \equiv b \pmod{m}$ and $d \equiv c \pmod{n}$. Then $d^2 \equiv b^2 \equiv a \pmod{m}$, and $d^2 \equiv c^2 \equiv a \pmod{n}$, so $d^2 \equiv a \pmod{mn}$.

For example, suppose we want to solve

$$x^2 \equiv 365 \pmod{667}.$$

Factorize 667 as $23 \cdot 29$. Then we first want to solve

$$x^2 \equiv 365 \pmod{23}, \qquad x^2 \equiv 365 \pmod{29}.$$

But we have $(365/23) = (20/23) = (5/23) = (23/5) = (3/5) = -1$ by the formula for $(3/p)$, so the first of the two congruences is insoluble, and therefore the original congruence is insoluble. It doesn't matter whether the second of the two congruences is insoluble.

Contrast with the following: $(2/11) = -1$, and $(7/11) = -(11/7) = -(4/7) = -1$; so the congruences

$$x^2 \equiv 2 \pmod{11}, \qquad x^2 \equiv 7 \pmod{11}$$

are insoluble; but $x^2 \equiv 14 \pmod{11}$ is soluble.

Now consider

$$x^2 \equiv 361 \pmod{667}.$$

One may notice that this has the solutions $x \equiv \pm 19$; but there are others, and we can find them as follows. We first solve

$$x^2 \equiv 16 \pmod{23}, \qquad x^2 \equiv 13 \pmod{29}.$$

The first of these is solved by $x \equiv \pm 4 \pmod{23}$ (and nothing else, since 23 is prime). For the second, note $13 \equiv 42, 71, 100 \pmod{29}$, so $x \equiv \pm 10 \pmod{29}$. So the solutions of the original congruence are the solutions of one of the following systems:

$$\left\{\begin{aligned} x &\equiv 4 \pmod{23}, \\ x &\equiv 10 \pmod{29} \end{aligned}\right\}, \qquad \left\{\begin{aligned} x &\equiv 4 \pmod{23}, \\ x &\equiv -10 \pmod{29} \end{aligned}\right\},$$
$$\left\{\begin{aligned} x &\equiv -4 \pmod{23}, \\ x &\equiv 10 \pmod{29} \end{aligned}\right\}, \qquad \left\{\begin{aligned} x &\equiv -4 \pmod{23}, \\ x &\equiv -10 \pmod{29} \end{aligned}\right\}.$$

One finds $x \equiv \pm 19, \pm 280 \pmod{667}$, or alternatively

$$x \equiv 648, 280, 387, 19 \pmod{667}.$$

So now $x^2 \equiv a \pmod{n}$ is soluble if and only if the congruences

$$x^2 \equiv a \pmod{p^{n(p)}}$$

are soluble, where $n = \prod_{p|n} p^{n(p)}$.

Theorem 95. *If p is odd, $p \nmid a$, and $(a/p) = 1$, then the congruence*

$$x^2 \equiv a \pmod{p^k} \qquad (*)$$

has two solutions for each positive k.

Proof. The set $\{x^2 : x \in \mathbb{Z}_{p^k}{}^\times\}$ consists of those a in $\mathbb{Z}_{p^k}{}^\times$ such that $(*)$ is soluble. For such a, we have $(a/p) = 1$. Thus

$$\{x^2 : x \in \mathbb{Z}_{p^k}{}^\times\} \subseteq \{a \in \mathbb{Z}_{p^k}{}^\times : (a/p) = 1\}.$$

But we have also

$$|\{a \in \mathbb{Z}_{p^k}{}^\times : (a/p) = 1\}| = \frac{\varphi(p^k)}{2}.$$

Indeed, this formula is correct when $k = 1$, by Theorem 87 on page 123. Moreover, for every element a of $\mathbb{Z}_p$, exactly p^{k-1} elements of $\mathbb{Z}_{p^k}{}^\times$ have the residue a *modulo* p: those elements are a, $a+p$, $a+2p$, $\ldots$, $a+(p^{k-1}-1)\cdot p$. This yields the claim for arbitrary positive k, since the value of (a/p) depends only on the residue of a *modulo* p.

Each congruence $(*)$ has at most 2 solutions, and therefore

$$|\{x^2 : x \in \mathbb{Z}_{p^k}{}^\times\}| \geqslant \frac{\varphi(p^k)}{2}.$$

For, if $x^2 = y^2 \pmod{p^k}$, then $p \mid (x+y)(x-y)$, but if p divides both $x+y$ and $x-y$, then p divides $2x$ and therefore x, and similarly $p \mid y$. Assuming we have neither of these conclusions, we have $p^k \mid x \pm y$, that is, $x \equiv \pm y \ (p^k)$.

Combining what we have so far yields

$$|\{x^2 : x \in \mathbb{Z}_{p^k}{}^\times\}| = |\{a \in \mathbb{Z}_{p^k}{}^\times : (a/p) = 1\}| = \frac{\varphi(p^k)}{2}.$$

But we have also shown that the function $x \mapsto x^2$ from $\mathbb{Z}_{p^k}{}^\times$ to itself sends at most two elements to the same element. Since $\mathbb{Z}_{p^k}{}^\times$ has just $\varphi(p^k)$ elements, the squaring function must send *exactly* two elements to the same element. This just means $(*)$ has exactly two solutions when $(a/p) = 1$. □

In this proof, we have used a kind of pigeonhole principle: If the $\varphi(p^k)$-many elements of $\mathbb{Z}_{p^k}{}^\times$ are pigeons, and the squares of those elements are pigeon-holes,

then there are at most two pigeons for each hole, so there are at least $\varphi(p^k)/2$-many holes; but there are at most $\varphi(p^k)/2$-many holes, therefore there are exactly that many, and there are two pigeons for each hole.

An alternative argument that $(*)$ is soluble is by induction. Suppose $b^2 \equiv a \ (p^k)$ for some positive k. This means

$$b^2 = a + c \cdot p^k$$

for some c. Then

$$\begin{aligned}(b + p^k \cdot y)^2 &= b^2 + 2bp^k \cdot y + p^{2k} \cdot y^2 \\ &= a + (c + 2by)p^k + p^{2k} \cdot y^2\end{aligned}$$

Therefore $(b+p^k \cdot y)^2 \equiv a \pmod{p^{k+1}} \iff c+2by \equiv 0 \pmod{p}$. But the latter congruence is soluble, since p is odd.

We must finally consider powers of 2.

Theorem 96. *Suppose a is odd.*

a) $x^2 \equiv a \pmod 2$ *is soluble.*

b) $x^2 \equiv a \pmod 4$ *is soluble if and only if* $a \equiv 1 \pmod 4$.

c) *The following are equivalent:*

(i) $x^2 \equiv a \pmod{2^{2+k}}$ *is soluble for all positive k;*

(ii) $x^2 \equiv a \pmod{2^{2+k}}$ *is soluble for some positive k;*

(iii) $x^2 \equiv a \pmod 8$ *is soluble;*

(iv) $a \equiv 1 \pmod 8$.

Proof. The only hard part is to show that, if $a \equiv 1 \ (8)$, then for all positive k, the congruence $x^2 \equiv a \ (2^{2+k})$ is soluble. We prove this by induction. It is easily true when $k = 1$. Suppose it is true when $k = \ell$, and in fact $b^2 \equiv a \pmod{2^{2+\ell}}$. Then $b^2 = a + 2^{2+\ell} \cdot c$ for some c. Hence

$$\begin{aligned}(b + 2^{1+\ell} \cdot y)^2 &= b^2 + 2^{2+\ell} \cdot by + 2^{2+2\ell} \cdot y^2 \\ &= a + 2^{2+\ell} \cdot c + 2^{2+\ell} \cdot by + 2^{2+2\ell} \cdot y^2 \\ &= a + 2^{2+\ell} \cdot (c + by) + 2^{2+2\ell} \cdot y^2,\end{aligned}$$

and this is congruent to a *modulo* $2^{3+\ell}$ if and only if $c + by \equiv 0 \pmod 2$. But this congruence is soluble, since b is odd (since a is odd). □

12. Sums of squares

Now we shall show that, if n is a natural number, then the Diophantine equation

$$x^2 + y^2 + z^2 + w^2 = n \qquad (*)$$

is soluble. This is easy when n is 1 or 2, since

$$1^2 + 0^2 + 0^2 + 0^2 = 1, \qquad 1^2 + 1^2 + 0^2 + 0^2 = 2.$$

We continue by showing:

1) for each odd prime p, $(*)$ is soluble when $n = mp$ for some m where $m < p$;
2) for each odd prime p, $(*)$ is soluble when $n = p$;
3) the set of n for which $(*)$ is soluble is closed under multiplication.

For the first step, the following lemma is more than enough. Note that the lemma is nothing new when p is odd and $(a/p) = 1$.

Lemma. *For every odd prime p, for every integer a, the congruence*

$$x^2 + y^2 \equiv a \pmod{p}$$

is soluble.

Proof. If $0 \leqslant s \leqslant t \leqslant \varpi$, then $0 \leqslant s + t < p$. If also $s^2 \equiv t^2\ (p)$, then $p \mid (t + s)(t - s)$ and hence $p \mid t - s$, so $s = t$. This shows that no two distinct elements of the set

$$\{x^2 \colon 0 \leqslant x \leqslant \varpi\}$$

are congruent to one another *modulo* p; and the same is true for the set

$$\{a - y^2 \colon 0 \leqslant y \leqslant \varpi\}.$$

But each of these sets has $(p+1)/2$ elements, so one element from one of the sets must be congruent to an element of the other, by the pigeonhole principle. □

Another way to express the lemma is that, for all odd primes p, there are a, b, and m such that

$$a^2 + b^2 + 1^2 + 0^2 = a^2 + b^2 + 1 = mp.$$

We may assume $|a|$ and $|b|$ are less than $p/2$, so $a^2 + b^2 < p^2/2$, and hence $m < p$.

Theorem 97 (Euler)**.** *The product of two sums of four squares is the sum of four squares, and indeed*

$$(a^2+b^2+c^2+d^2)(x^2+y^2+u^2+v^2) = \left\{ \begin{array}{c} (ax+by+cu+dv)^2 \\ +(ay-bx+cv-du)^2 \\ +(au-bv-cx+dy)^2 \\ +(av+bu-cy-dx)^2. \end{array} \right\} \qquad (\dagger)$$

One can prove this by multiplying out either side; but there is a neater way to proceed. In $\mathbb{C}$, if $z = x + y\mathrm{i}$, we define

$$\bar{z} = x - y\mathrm{i};$$

this is the **conjugate** of z. If we think of z as the matrix in (§) on page 34 in §2.4, then $\bar{z}$ is its transpose. Then $z \cdot \bar{z} = x^2 + y^2$, an element of $\mathbb{R}$. More generally, $\overline{z \cdot w} = \bar{w} \cdot \bar{z} = \bar{z} \cdot \bar{w}$.

Now we define the set $\mathbb{H}$ of **quaternions** as the set of matrices

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}, \qquad (\ddagger)$$

where z and w range over $\mathbb{C}$. Then $\mathbb{H}$ is still a ring, albeit not commutative. Indeed, we identify $\mathbb{C}$ with its image in $\mathbb{H}$ under the map

$$z \mapsto \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix},$$

and we define

$$\mathrm{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then every element of $\mathbb{H}$ is uniquely $z + w\mathrm{j}$ for some z and w in $\mathbb{C}$; moreover, $\mathrm{j}^2 = -1$. But $\mathrm{j} \cdot \mathrm{i} = -\mathrm{i} \cdot \mathrm{j}$, by the computation

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} = \begin{pmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix} = - \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We may write k for $\mathrm{i} \cdot \mathrm{j}$; then every element of $\mathbb{H}$ is uniquely $x + y\mathrm{i} + u\mathrm{j} + v\mathrm{k}$ for some x, y, u, and v in $\mathbb{R}$. If the matrix in (‡) is α, then we define

$$\bar{\alpha} = \begin{pmatrix} \bar{z} & -w \\ \bar{w} & z \end{pmatrix},$$

which is the transpose of the matrix resulting from taking the conjugate of every entry. Hence if also $\beta \in \mathbb{H}$, then $\overline{\beta \cdot \alpha} = \bar{\alpha} \cdot \bar{\beta}$. Moreover,

$$\alpha \cdot \bar{\alpha} = z \cdot \bar{z} + w \cdot \bar{w};$$

this is an element of $\mathbb{R}$, so it commutes with all quaternions. If $\alpha = x+y\mathrm{i}+u\mathrm{j}+v\mathrm{k}$, then $\alpha \cdot \bar{\alpha} = x^2 + y^2 + z^2 + w^2$. We have also

$$\beta \cdot \alpha \cdot \overline{\beta \cdot \alpha} = \beta \cdot \alpha \cdot \bar{\alpha} \cdot \bar{\beta} = \beta \cdot \bar{\beta} \cdot \alpha \cdot \bar{\alpha},$$

which is just Euler's Theorem. Indeed, if $\beta = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$, then

$$\begin{aligned}
\beta \cdot \alpha &= \big((a+b\mathrm{i}) + (c+d\mathrm{i})\mathrm{j}\big) \cdot \big((x+y\mathrm{i}) + (u+v\mathrm{i})\mathrm{j}\big) \\
&= \left\{ \begin{array}{c} (a+b\mathrm{i}) \cdot (x+y\mathrm{i}) - (c+d\mathrm{i}) \cdot (u-v\mathrm{i}) \\ + \big((a+b\mathrm{i}) \cdot (u+v\mathrm{i}) + (c+d\mathrm{i}) \cdot (x-y\mathrm{i})\big)\mathrm{j} \end{array} \right\} \\
&= \left\{ \begin{array}{c} ax - by - cu - dv \\ + (ay + bx + cv - du)\mathrm{i} \\ + (au - bv + cx + dy)\mathrm{j} \\ + (av + bu - cy + dx)\mathrm{k}, \end{array} \right\}
\end{aligned}$$

and therefore

$$(a^2+b^2+c^2+d^2) \cdot (x^2+y^2+u^2+v^2) = \left\{ \begin{array}{c} (ax-by-cu-dv)^2 \\ + (ay+bx+cv-du)^2 \\ + (au-bv+cx+dy)^2 \\ + (av+bu-cy+dx)^2. \end{array} \right\};$$

this yields (†) when β is replaced with $\bar{\beta}$.

Theorem 98 (Lagrange)**.** *Every positive integer is the sum of four squares.*

Proof. By the lemma and Euler's Theorem (Theorem 97), it is now enough to show the following. Let p be a prime. Suppose m is a positive integer less than p such that

$$a^2 + b^2 + c^2 + d^2 = mp \qquad (\S)$$

for some a, b, c, and d. We shall show that the same is true for some smaller positive m, unless m is already 1.

First we show that, if m is even, then we can replace it with $m/2$. Indeed, if $a^2 + b^2 = n$, then

$$\Big(\frac{a+b}{2}\Big)^2 + \Big(\frac{a-b}{2}\Big)^2 = \frac{n}{2},$$

and if n is even, then so are $(a \pm b)/2$. In (§) then, if m is even, then we may assume that $a^2 + b^2$ and $c^2 + d^2$ are both even, so

$$\Big(\frac{a+b}{2}\Big)^2 + \Big(\frac{a-b}{2}\Big)^2 + \Big(\frac{c+d}{2}\Big)^2 + \Big(\frac{c-d}{2}\Big)^2 = \frac{m}{2} \cdot p.$$

Henceforth we may assume m is odd. Then there are x, y, u, and v *strictly* between $-m/2$ and $m/2$ such that, *modulo* m,

$$x \equiv a, \qquad y \equiv b, \qquad u \equiv c, \qquad v \equiv d.$$

Then

$$x^2 + y^2 + u^2 + v^2 \equiv 0 \pmod{m},$$

but also $x^2 + y^2 + u^2 + v^2 < m^2$, so

$$x^2 + y^2 + u^2 + v^2 = km$$

for some positive k less than m. We now have

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + u^2 + v^2) = km^2 p.$$

By Euler's Theorem, we know the left-hand side as a sum of four squares; moreover, each of the squared numbers in that sum is divisible by m:

$$\begin{aligned} ax + by + cu + dv &\equiv x^2 + y^2 + u^2 + v^2 \equiv 0 \pmod{m}, \\ ay - bx + cv - du &\equiv xy - yx + uv - vu = 0, \\ au - bv - cx + dy &\equiv xu - yv - ux + vy = 0, \\ av + bu - cy - dx &\equiv xv + yu - uy - vx = 0. \end{aligned}$$

Therefore we obtain kp as a sum of four squares. This yields the claim, as discussed above. □

A. Foundations

A.1. Construction of the natural numbers

In §2.1 it is *assumed* that the set $\mathbb{N}$ of natural numbers exists with certain properties. We can *prove* this assertion by *constructing* $\mathbb{N}$. The following is the most direct formulation of the construction that I can come up with. The construction is basically John von Neumann's [39] of 1923.

Of course we shall still have to assume *something*. We start with the undefined notion of a **class.** A class is a sort of thing that has **members** or **elements.** Let us denote classes by boldface capital letters. If a class $\boldsymbol{C}$ has a member a, we write

$$a \in \boldsymbol{C}.$$

The members determine the class, in the sense that two classes with the same members are identical. A class $\boldsymbol{D}$ **includes** a class $\boldsymbol{C}$, so that $\boldsymbol{C}$ is a **subclass** of $\boldsymbol{D}$, if every member of $\boldsymbol{C}$ is a member of $\boldsymbol{D}$. In this case, we write

$$\boldsymbol{C} \subseteq \boldsymbol{D}.$$

If $\boldsymbol{C}$ is a **proper** subclass of $\boldsymbol{D}$,—a subclass that is not the whole class itself—, we write

$$\boldsymbol{C} \subset \boldsymbol{D}.$$

In ordinary language, one tends to confuse the notions of membership and inclusion; but here we must keep them distinct. For our purposes, a **set** is a class with two special properties:

a) it is a member of other classes;

b) its own members are sets.[1]

Some classes are not sets; for example, the class of all sets that are not members of themselves is not a set. This is the **Russell Paradox** [31].[2] We may denote sets by plainface minuscule letters.

Let us restrict our attention to classes whose *only* members are sets. A class in this sense is called **transitive** when it confuses the notions of membership and inclusion to the point that it includes each of its members. Symbolically, a class $\boldsymbol{C}$ is transitive if and only if

$$x \in y \ \ \& \ \ y \in \boldsymbol{C} \implies x \in \boldsymbol{C}.$$

[1] This means our sets are *hereditary* sets; but we need not consider any other kind of set.

[2] The Burali-Forti Paradox, Theorem 99 below, was discovered earlier. The *resolution* of the paradoxes, by distinguishing sets from classes, took some time.

A *set* is called an **ordinal number,** or just an **ordinal,** if it is transitive and well-ordered by membership. The class of ordinals is denoted by

$$\mathbf{ON}.$$

The Greek letters α, β, γ, ..., will denote ordinals. A well-ordering is to be understood in particular as a *strict* ordering, so that $\alpha \notin \alpha$.

Lemma. ON *is transitive, that is, every element of an ordinal is an ordinal. Also every ordinal* properly *includes its elements.*

Proof. Suppose $\alpha \in \mathbf{ON}$ and $b \in \alpha$. Then $b \subseteq \alpha$ by transitivity of α, so b, like α, is well-ordered by membership. Suppose $c \in b$ and $d \in c$. Then $c \in \alpha$, so $c \subseteq \alpha$, and hence $d \in \alpha$. Since $d \in c$ and $c \in b$, and all are elements of α, where membership is a transitive relation, we have $d \in b$. Thus b is transitive. Now we know b is an ordinal. Therefore $\alpha \subseteq \mathbf{ON}$. So **ON** is transitive. Finally, $b \subset \alpha$ simply because membership is a strict ordering of α. □

Lemma. *Every ordinal contains every ordinal that it properly includes.*

Proof. Suppose $\beta \subset \alpha$. Then $\alpha \setminus \beta$ contains some γ. Then $\beta \subseteq \gamma$; indeed, if $\delta \in \beta$, then, since $\gamma \notin \beta$, we have $\gamma \notin \delta$ and $\gamma \neq \delta$, so $\delta \in \gamma$. We show that, if γ is the *least* member of $\alpha \setminus \beta$, then $\gamma = \beta$. Suppose $\beta \subset \gamma$. Then $\gamma \setminus \beta$ contains some δ. In particular, $\delta \in \alpha \setminus \beta$. By the last lemma, $\delta \subset \gamma$, so $\gamma \notin \delta$. In particular, γ was not the least element of $\alpha \setminus \beta$. □

Theorem 99 (Burali-Forti Paradox [6])**. ON** *is transitive and well-ordered by membership; so it is not a set.*

Proof. By the next-to-last lemma, **ON** is transitive. Now let α and β be two ordinals such that $\beta \notin \alpha$. We prove $\alpha \subseteq \beta$, so that either $\alpha = \beta$ or $\alpha \in \beta$ by the last lemma. If not, then $\alpha \setminus \beta$ has a least element, γ. This means every element of γ is an element of β; that is, $\gamma \subseteq \beta$. But $\gamma \neq \beta$ (since $\beta \notin \alpha$), so $\gamma \in \beta$ by the lemma, contrary to assumption.

If a is a set of ordinals with an element β, then the least element of a is the least element of $a \cap \beta$, if this set is nonempty; otherwise it is β. Thus **ON** is well-ordered by membership. In particular, it cannot contain itself; so it must not be a set. □

Since, on **ON** and hence on every ordinal, the relations of membership and proper inclusion are the same, they can both be denoted by $<$. However, we have not yet established that there *are* any ordinals, or even any sets at all.

We take it for granted that there is an **empty set,** which is generally denoted by $\varnothing$, but which, in the present context, we denote by

$$0.$$

We also assume that if x and y are sets, then so is the class whose members are just y and the members of x; this is the class—now a *set*—denoted by

$$x \cup \{y\}.$$

We are interested mainly in the set $x \cup \{x\}$, which we denote by

$$x'.$$

The following is easy to show.

Theorem 100. ON *contains* 0 *and is closed under the operation* $x \mapsto x'$.

An ordinal is called a **limit** if it is neither 0 nor α' for any α. The class of ordinals that neither *are* limits nor *contain* limits[3] is denoted by

$$\omega.$$

Theorem 101 (Dedekind[4])**.** *The class* ω *satisfies the Peano Axioms when* 0 *is considered as the* first *element of* ω*, and* α' *is the* successor *of* α.

Proof. We must show three things.

1. Since $\alpha \in \alpha'$, we have $0 \neq \alpha'$.

2. If α and β are distinct ordinals, then we may assume $\alpha \in \beta$, so that $\beta \notin \alpha$ and $\beta \neq \alpha$, and therefore $\beta \notin \alpha'$; but $\beta \in \beta'$, so $\alpha' \neq \beta'$.

3. Suppose $\boldsymbol{C} \subseteq \omega$. Then $\omega \setminus \boldsymbol{C}$ has a least element α. Either $\alpha = 0$ or else $\alpha = \beta'$ for some β, which must be in $\boldsymbol{C}$. Hence $\boldsymbol{C}$ either does not contain 0 or else is not closed under succession. □

[3]The following is a remark on English grammar. One could say, 'The class of ordinals that neither *are* nor *contain* limits is denoted by ω'; but this would violate the principles laid down by Fowler in his *Modern English Usage* [15, Cases] of 1926 and reaffirmed by Gowers in the second edition [14] of 1982. In the original sentence, namely 'The class of ordinals that neither *are* limits nor *contain* limits is denoted by ω', the second instance of *limits* is the direct object of *contain,* so it is notionally in the 'objective case'; but the first instance of *limits* is is not an object of *are* (which does not take objects), but is in the 'subjective case', like the subject, *that,* of the relative clause. On similar grounds, the common expression 'x is less than or equal to y' is objectionable, unless *than,* like *to,* is construed as a preposition. However, allowing *than* to be used as a preposition can cause ambiguity: does 'She likes tea better than me' mean 'She likes tea better than she likes me', or 'She likes tea better than I do'? Therefore it is recommended in [15, Than 6] and (less strongly) in [14] that *than* not be used as a preposition. On these grounds, '$x \leqslant y$' should be read as 'x is less than y or [x is] equal to y.' But I don't believe anybody does so, and this itself is grounds for rethinking Fowler's grammatical distinctions.

[4]Dedekind recognized that the natural numbers have the properties given by this theorem, and that all structures with these properties are isomorphic [9, II: §§ 71, 132].

We have so far not assumed that ω is a set. If it *is* a set, then it is in **ON**; if it is *not* a set, then it must *be* **ON**. As far as number theory is concerned, there does not appear to be any need to make a decision one way or other; but it seems to be customary to consider ω and its subclasses as sets. If ω is a set, it is the least of the **transfinite** ordinals.

We denote $\{0\}$ by 1. Then $\omega \setminus \{0\}$ also satisfies the Peano Axioms, when 1 is considered as the first element. You just have to decide whether to begin the natural numbers with 0 or 1; but if you start with 0, you should adjust the definitions of addition, multiplication, exponentiation, and factorial accordingly, so that

$$m + 0 = m, \qquad m \cdot 0 = 0, \qquad m^0 = 1, \qquad 0! = 1;$$

also one should note that the ordering of ω satisfies

$$m \leqslant n \iff \exists x\, m + x = n.$$

A.2. Why it matters

Some teachers and texts give the impression that the properties of the natural numbers can be derived from a single principle, such as the so-called Well-Ordering Principle. My excellent high school teacher Mr Brown did this. Burton does this, writing for example, 'With the Well-Ordering Principle available, it is an easy matter to derive the First Principle of Finite Induction' [7, p. 2]. The principle of induction here is that a set containing the first natural number, and containing the successor of each natural number that it contains, contains all of the natural numbers. One needs *more* than well-ordering to prove this, since *every* ordinal number is well-ordered, but the ordinals like ω' that are greater than ω do not admit induction in the sense referred to. Indeed, ω is distinguished among all of the transfinite ordinals as the one that admits induction in the present sense.

Burton is saved from true inconsistency by having written on the previous page,

> We shall make no attempt to construct the integers axiomatically, assuming instead that they are already given and that any reader of this book is familiar with many elementary facts about them.

Burton's proof of induction relies on some of these unspecified 'elementary facts'. On the other hand, the needed 'facts' are so simple that it seems dishonest not to name them. Burton could have axiomatized the set of natural numbers by the requirements:

1) it is well ordered,
2) there is no greatest element,

3) every element after the first is a successor.

Like the Peano Axioms, these conditions determine the set up to isomorphism.

By referring, in the passage quoted above, to an 'attempt to construct the integers axiomatically', Burton confuses two approaches to the natural numbers:

1) *assuming* they exist so as to satisfy the Peano Axioms, as we did in §2.1;

2) constructing them as ω, as we did in the last section.

The construction of ω is perhaps too specialized for a number theory course. However, I will suggest that every mathematician should know the Peano Axioms and know that they determine the natural numbers up to isomorphism. It might prevent certain infelicities and mistakes, such as can be found, for example, in Burton.

Before proving induction as Theorem 1.2, Burton proves the 'Archimedean property' as Theorem 1.1. Before stating this theorem, he says,

> Because this principle [of well-ordering] plays a crucial role in the proofs here and in subsequent chapters, let us use it to show that the set of positive integers has what is known as the Archimedean property.

This comment does not clarify why the Archimedean property should be proved. Will it be needed later, or is is just a warming-up example of the use of well-ordering?

Burton's 'Second Principle of Finite Induction' is that a set S contains all positive integers if

a) S contains 1, and

b) S contains $k+1$ when it contains $1, \ldots, k$.

This statement may be useful for the writer in a hurry. Such a writer may attempt a proof by the 'First Principle' of induction, only to find that the weaker inductive hypothesis there, namely $k \in S$, is not enough. Then the writer can just assume that $1, \ldots, k$ are all in S. But it would be better to go back and erase the proof that $1 \in S$, then prove $k \in S$ on the assumption that $1, \ldots, k-1$ are in S, using what I have called 'Strong Induction' (Theorem 14). In case $k = 1$, one has proved $1 \in S$; this need not be treated separately.

Burton says presently, 'Mathematical induction is often used as a method of definition as well as a method of proof.' This is a misconception that Peanso shared, but that Landau identified in his *Foundations of Analysis* [26]. Definition by induction should be called something else, like definition by recursion, because it is logically stronger than proof by induction, as noted in §2.1.

B. Some theorems without their proofs

I state some theorems, without giving proofs; some of them are recent and reflect ongoing research:

Theorem 102 (Dirichlet)**.** *If* $\gcd(a, b) = 1$*, and* $b > 0$*, then* $\{a + bn \colon n \in \mathbb{N}\}$ *contains infinitely many primes.*

That is in an arithmetic progression whose initial term is prime to the common difference, there are infinitely many primes. It is moreover possible to find arbitrary long arithmetic progressions consisting entirely of primes:[1]

Theorem 103 (Ben Green and Terence Tao, 2004 [20])**.** *For every* n*, there are* a *and* b *such that each of the numbers* $a, a + b, a + 2b, \ldots, a + nb$ *is prime (and* $b > 0$*).*

Is it possible that each of the numbers

$$a, a + b, a + 2b, a + 3b, \ldots$$

is prime? Yes, if $b = 0$. What if $b > 0$? Then No, since $a \mid a + ab$. But what if $a = 1$? Then replace a with $a + b$.

Two primes p and q are **twin primes** if $|p - q| = 2$. The list of all primes begins:

$$2, \underbrace{3, 5}, 7, \underbrace{11, 13}, \underbrace{17, 19}, 23, \underbrace{29, 31}, 37, \underbrace{41, 43}, 47, \ldots$$

and there are several twins. Are there infinitely many? People think so, but cannot prove it. We do have:

Theorem 104 (Goldston, Pintz, Yıldırım, 2005 [17])**.** *For every positive real number* ε*, there are primes* p *and* q *such that* $0 < q - p < \varepsilon \cdot \log p$*.*

The logarithm function also appears in the much older

Theorem 105 (Prime Number Theorem)**.** *Let* $\pi(n)$ *be the number of primes* p *such that* $p \leqslant n$*. Then*

$$\lim_{n \to \infty} \frac{\pi(n)}{n / \log n} = 1.$$

[1] This theorem is not mentioned in Burton [7].

C. Exercises

In the following exercises, if a *statement* is given that is not a definition, then the exercise is to prove the statement. Minuscule letters range over $\mathbb{Z}$, or sometimes just over $\mathbb{N}$; letters p, p_i, and q range over the prime numbers.

Many of these exercises are inspired by exercises in [7, Ch. 2].

Exercise 1. Prove the unproved propositions in Chapter 2.

Exercise 2. An integer n is a triangular number if and only if $8n + 1$ is a square number. *Solution:* If n is triangular, then $x = k(k + 1)/2$ for some k, and then $8n + 1 = 4k^2 + 4k + 1 = (2k + 1)^2$. Conversely, if $8n + 1$ is square, then, since this number is also odd, the square is $(2k + 1)^2$ for some k, and then $n = \big((2k + 1)^2 - 1)\big)/8 = k(k + 1)/2$, a triangular number.

Exercise 3.

a) If n is triangular, then so is $9n + 1$.

b) Find infinitely many pairs (k, ℓ) such that, if n is triangular, then so is $kn + \ell$.

Exercise 4. If $a = n(n + 3)/2$, then $t_a + t_{n+1} = t_{a+1}$.

Exercise 5. The **pentagonal numbers** are 1, 5, 12, ...: call these p_1, p_2, &c.

a) Give a recursive definition of these numbers.

b) Find a closed expression for p_n (that is, an expression not involving p_{n-1}, p_{n-2}, &c.).

c) Find such an expression involving triangular numbers and square numbers.

Exercise 6. Given a positive modulus n and an integer a, find a formula for the unique residue in $\{a, \ldots, a + n - 1\}$ of an arbitrary integer x. (Gauss does this in the *Disquisitiones Arithmeticae*.)

Exercise 7. Show that every cube is congruent to 0 or ± 1 *modulo* 7.

Exercise 8.

a) $7 \mid 2^{3n} + 6$.

b) Given a in $\mathbb{Z}$ and k in $\mathbb{N}$, find integers b and c such that $b \mid a^{kn} + c$ for all n in $\mathbb{N}$.

Exercise 9. $\gcd(a, a + 1) = 1$.

Exercise 10. $(k!)^n \mid (kn)!$ for all k and n in $\mathbb{N}$.

Exercise 11. If a and b are co-prime, and a and c are co-prime, then a and bc are co-prime.

Exercise 12. Let $\gcd(204, 391) = n$.
a) Compute n.
b) Find a solution of $204x + 391y = n$.

Exercise 13. Let $\gcd(a, b) = n$.
a) If $k \mid \ell$ and $\ell \mid 2k$, then $|\ell| \in \{|k|, |2k|\}$.
b) Show $\gcd(a + b, a - b) \in \{n, 2n\}$.
c) Find an example for each possibility.
d) $\gcd(2a + 3b, 3a + 4b) = n$.
e) Solve $\gcd(ax + by, az + bw) = n$.

Exercise 14. $\gcd(a, b) \mid \operatorname{lcm}(a, b)$.

Exercise 15. When are $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ the same?

Exercise 16. The binary operation $(x, y) \mapsto \gcd(x, y)$ on $\mathbb{N}$ is commutative and associative.

Exercise 17. The co-prime relation on $\mathbb{N}$, namely

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} \colon \gcd(x, y) = 1\}$$

—is it reflexive? irreflexive? symmetric? anti-symmetric? transitive?

Exercise 18. Give complete solutions, or show that they do not exist, for:
a) $14x - 56y = 34$;
b) $10x + 11y = 12$.

Exercise 19. I have some 1-TL pieces and some 50- and 25-Kr pieces: 16 coins in all. They make 6 TL. How many coins of each denomination have I got?

Exercise 20. $p \equiv \pm 1 \pmod 6$ if $p > 3$. (This exercise is used in Exercise 45.)

Exercise 21. If $p \equiv 1 \pmod 3$ then $p \equiv 1 \pmod 6$.

Exercise 22. If $n \equiv 2 \pmod 3$, then n has a factor p such that $p \equiv 2 \pmod 3$.

Exercise 23. Find all primes of the form $n^3 - 1$.

Exercise 24. Find all p such that $3p + 1$ is square.

Exercise 25. Find all p such that $p^2 + 2$ is prime.

Exercise 26. $n^4 + 4$ is composite unless $n = \pm 1$.

Exercise 27. If n is positive, then $8^n + 1$ is composite.

Exercise 28. Find all integers n such that the equation

$$x^2 = ny^2$$

has only the zero solution. Prove your findings.

Exercise 29. If $p_1 < \cdots < p_n$, prove that the sum

$$\frac{1}{p_1} + \cdots + \frac{1}{p_n}$$

is not an integer.

Exercise 30. Prove that the following are equivalent:
a) Every even integer greater than 2 is the sum of two primes.
b) Every integer greater than 5 is the sum of three primes.

Exercise 31. Infinitely many primes are congruent to -1 *modulo* 6.

Exercise 32. With $\vartheta(x) = \sum_{p \leqslant x} \log p$ as in §4.5, and defining

$$\psi(x) = \sum_{k=1}^{\infty} \vartheta(\sqrt[k]{x}),$$

show

$$\log[x]! = \sum_{j=1}^{\infty} \psi\Big(\frac{x}{j}\Big).$$

Exercise 33. Define the **Mangoldt function,** Λ, by

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^m \text{ for some positive } m; \\ 0, & \text{otherwise.} \end{cases}$$

a) $\log k = \sum_{d|k} \Lambda(d)$ (as in Exercise 67).
b) $\log(n!) = \sum_{j=1}^{n} \Lambda(j)[n/j]$.
c) Now give another proof of Theorem 38, that

$$\log(n!) = \sum_{p \leqslant n} \log p \sum_{j=1}^{\infty} \Big[\frac{n}{p^j}\Big].$$

Exercise 34. Prove that $\sum_p 1/p$ diverges.

Exercise 35. Find all n such that

a) $n!$ is square;
b) $n! + (n+1)! + (n+2)!$ is square.

Exercise 36. Determine whether $a^2 \equiv b^2 \pmod{n} \implies a \equiv b \pmod{n}$.

Exercise 37. Compute $\sum_{k=1}^{1001} k^{365} \pmod 5$.

Exercise 38. $39 \mid 53^{103} + 103^{53}$.

Exercise 39. Solve $6^{n+2} + 7^{2n+1} \equiv x \pmod{43}$.

Exercise 40. Determine whether $a \equiv b \pmod{n} \implies c^a \equiv c^b \pmod{n}$.

Exercise 41. Solve the system

$$\begin{cases} x \equiv 1 \pmod{17}, \\ x \equiv 8 \pmod{19}, \\ x \equiv 16 \pmod{21}. \end{cases}$$

Exercise 42. The system

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

has a solution if and only if $\gcd(n, m) \mid b - a$.

Exercise 43. In the proof of Theorem 45 (p. 69), how do we use that n is even?

Exercise 44. Show that every even perfect number is a triangular number.

Exercise 45.

a) If $a \equiv b \pmod 6$, show $2^a \equiv 2^b \pmod 9$.

b) Show that $n \equiv 1 \pmod 9$ for every even perfect number n other than 6. (See Exercise 20.)

Exercise 46. Find every positive integer that is equal to the product of its proper divisors. (See Exercise 59.)

Exercise 47. Compute 16200 *modulo* 19.

Exercise 48. If $p \neq q$, and $\gcd(a, pq) = 1$, and $n = \operatorname{lcm}(p-1, q-1)$, show

$$a^n \equiv 1 \pmod{pq}.$$

Exercise 49. Prove Theorem 50 (p. 77).

Exercise 50. Show $a^{13} \equiv a \pmod{70}$.

Exercise 51. Assuming $\gcd(a, p) = 1$, and $0 \leqslant n < p$, solve the congruence

$$a^n x \equiv b \pmod{p}.$$

Exercise 52. Solve $2^{14}x \equiv 3 \pmod{23}$.

Exercise 53. Show $\displaystyle\sum_{k=1}^{p-1} k^p \equiv 0 \pmod{p}$.

Exercise 54. We can write the congruence $2^p \equiv 2 \pmod{p}$ as

$$2^p - 1 \equiv 1 \pmod{p}.$$

Show that, if $n \mid 2^p - 1$, then $n \equiv 1 \pmod{p}$. (*Suggestion:* Do this first if n is a prime q. Then $2^{q-1} \equiv 1 \pmod{q}$. If $q \not\equiv 1 \pmod{p}$, then $\gcd(p, q-1) = 1$, so $pa + (q-1)b = 1$ for some a and b. Now look at $2^{pa} \cdot 2^{(q-1)b}$ *modulo* n.)

Exercise 55. Let $F_n = 2^{2^n} + 1$. (Then $F_0, \ldots, F_4$ are primes.) Show

$$2^{F_n} \equiv 2 \pmod{F_n}.$$

Exercise 56. Show that 1105, 2821, and 15841 are Carmichael numbers.[1] *Solution:* First, factorize: $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$, and $15841 = 7 \cdot 31 \cdot 73$.

Exercise 57. Assuming p is an *odd* prime:

a) $(p-1)! \equiv p - 1 \pmod{1 + 2 + \cdots + (p-1)}$;
b) $1 \cdot 3 \cdots (p-2) \equiv (-1)^{(p-1)/2} \cdot (p-1) \cdot (p-3) \cdots 2 \pmod{p}$;
c) $1 \cdot 3 \cdots (p-2) \equiv (-1)^{(p-1)/2} \cdot 2 \cdot 4 \cdots (p-1) \pmod{p}$;
d) $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

Exercise 58. $\tau(n) \leqslant 2\sqrt{n}$.

Exercise 59. $\prod_{d|n} = n^{\tau(n)/2}$. (See Exercise 46.)

Exercise 60. $\tau(n)$ is odd if and only if n is square.

Exercise 61. Assuming n is odd: $\sigma(n)$ is odd if and only if n is square.

Exercise 62. $\displaystyle\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$.

Exercise 63. $\{n \colon \tau(n) = k\}$ is infinite (when $k > 1$), but $\{n \colon \sigma(n) = k\}$ is finite.

[1] Carmichael did this in 1910 [8].

Exercise 64. Let $m \in \mathbb{Z}$. The number-theoretic function $n \mapsto n^m$ is multiplicative.

Exercise 65. Let $\omega(n)$ be the number of *distinct* prime divisors of n, and let m be a non-zero integer. Then $n \mapsto m^{\omega(n)}$ is multiplicative.

Exercise 66. Prove the other half of the Möbius Inversion Theorem (Theorem 60 on page 88): if F and f are arithmetic functions such that

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot F(d),$$

then

$$F(n) = \sum_{d|n} f(d).$$

Exercise 67. Let Λ be the Mangoldt function defined in Exercise 33.

a) $\log n = \sum_{d|n} \Lambda(d)$.

b) $\Lambda(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \log d$.

c) $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.

Exercise 68. $\prod_{p|n}(1-p) = \sum_{d|n} \mu(d) \cdot d$.

Exercise 69. If f is multiplicative and non-zero, then

$$\sum_{d|n} \mu(d) \cdot f(d) = \prod_{p|n}(1 - f(p)).$$

Exercise 70. If ω is as in Exercise 65, then $\sum_{d|n} \mu(d) \cdot \tau(d) = (-1)^{\omega(n)}$.

Exercise 71. $f(568) = f(638)$ when $f \in \{\tau, \sigma, \varphi\}$.

Exercise 72. Solve:

a) $n = 2\varphi(n)$.

b) $\varphi(n) = \varphi(2n)$.

c) $\varphi(n) = 12$. (Do this without a table. There are 6 solutions.)

Exercise 73. Find a sequence $(a_n : n \in \mathbb{N})$ of positive integers such that

$$\lim_{n\to\infty} \frac{\varphi(a_n)}{a_n} = 0.$$

(If you assume that there *is* an answer to this problem, then it is not hard to see what the answer must be. To actually *prove* that the answer is correct, recall that, formally,

$$\sum_n \frac{1}{n} = \prod_p \frac{1}{1-\frac{1}{p}},$$

so $\lim_{n\to\infty} \prod_{k=1}^{n} \frac{1}{1-\frac{1}{p_k}} = \infty$ if $(p_k : k \in \mathbb{N})$ is the list of primes.)

Exercise 74. Prove $\sum_{d|n} \mu(d)\varphi(d) = \prod_{p|n}(2-p)$. (This is a special case of Exercise 69.)

Exercise 75. If n is squarefree, and $k \geqslant 0$, show

$$\sum_{d|n} \sigma(d^k)\varphi(d) = n^{k+1}.$$

Exercise 76. $\sum_{d|n} \sigma(d)\varphi\left(\frac{n}{d}\right) = n\tau(n)$.

Exercise 77. $\sum_{d|n} \tau(d)\varphi\left(\frac{n}{d}\right) = \sigma(n)$.

Exercise 78. a) Show $a^{100} \equiv 1 \pmod{1000}$ if $\gcd(a, 1000) = 1$.
b) Find n such that $n^{101} \not\equiv n \pmod{1000}$.

Exercise 79. a) Show $a^{24} \equiv 1 \pmod{35}$ if $\gcd(a, 35) = 1$.
b) Show $a^{13} \equiv a \pmod{35}$ for all a.
c) Is there n such that $n^{25} \not\equiv n \pmod{35}$?

Exercise 80. If $\gcd(m, n) = 1$, show $m^{\varphi(n)} \equiv n^{\varphi(m)} \pmod{mn}$.

Exercise 81. If n is odd, and is not a prime power, and if $\gcd(a, n) = 1$, show $a^{\varphi(n)/2} \equiv 1 \pmod{n}$. (This generalizes Exercise 79(b).)

Exercise 82. Solve $5^{10000}x \equiv 1 \pmod{153}$.

Exercise 83. We have $(\pm 3)^2 \equiv 2 \pmod{7}$. Compute the orders of 2, 3, and -3, *modulo* 7.

Exercise 84. Suppose $\mathrm{ord}_n(a) = k$, and $b^2 \equiv a \pmod{n}$.
a) Show that $\mathrm{ord}_n(b) \in \{k, 2k\}$.
b) Find an example for each possibility of $\mathrm{ord}_n(b)$.
c) Find a condition on k such that $\mathrm{ord}_n(b) = 2k$.

Exercise 85. This is about 23:
a) Find a primitive root of least absolute value.
b) How many primitive roots are there?
c) Find these primitive roots as powers of the root found in (a).
d) Find these primitive roots as elements of $[-11, 11]$.

Exercise 86. Assuming $\mathrm{ord}_p(a) = 3$, show:
a) $a^2 + a + 1 \equiv 0 \pmod 3$;
b) $(a+1)^2 \equiv a \pmod 3$;
c) $\mathrm{ord}_p(a+1) = 6$.

Exercise 87. Find all elements of $[-30, 30]$ having order 4 *modulo* 61.

Exercise 88. $f(x) \equiv 0 \pmod n$ may have more than $\deg(f)$ solutions:
a) Find four solutions to $x^2 - 1 \equiv 0 \pmod{35}$.
b) Find conditions on a such that the congruence $x^2 - a^2 \equiv 0 \pmod{35}$ has four distinct solutions, and find these solutions.
c) If p and q are odd primes, find conditions on a such that the congruence $x^2 - a^2 \equiv 0 \pmod{pq}$ has four distinct solutions, and find these solutions.

Exercise 89. If $\mathrm{ord}_n(a) = n - 1$, then n is prime.

Exercise 90. If $a > 1$, show $n \mid \varphi(a^n - 1)$.

Exercise 91. If $2 \nmid p$ and $p \mid n^2 + 1$, show $p \equiv 1 \pmod 4$.

Exercise 92.
a) Find conditions on p such that, if r is a primitive root of p, then so is $-r$.
b) If p does not meet these conditions, then what is $\mathrm{ord}_p(-r)$?

Exercise 93. For $(\mathbb{Z}/(17))^\times$:
a) construct a table of logarithms using 5 as the base;
b) using this (or some other table, with a different base), solve:
(i) $x^{15} \equiv 14 \pmod{17}$;
(ii) $x^{4095} \equiv 14 \pmod{17}$;
(iii) $x^4 \equiv 4 \pmod{17}$;
(iv) $11x^4 \equiv 7 \pmod{17}$.

Exercise 94. If n has primitive roots r and s, and $\gcd(a, n) = 1$, prove

$$\log_s a \equiv \frac{\log_r a}{\log_r s} \pmod{\varphi(n)}.$$

Exercise 95. In $(\mathbb{Z}/(337))^\times$, for any base, show

$$\log(-a) \equiv \log a + 168 \pmod{336}.$$

Exercise 96. Solve $4^x \equiv 13 \pmod{17}$.

Exercise 97. a) If $\mathrm{ord}_r(a)$ and $\mathrm{ord}_r(b)$ are relatively prime, show

$$\mathrm{ord}_r(ab) = \mathrm{lcm}(\mathrm{ord}_r(a), \mathrm{ord}_r(b)).$$

b) Show that this may fail if $\mathrm{ord}_r(a)$ and $\mathrm{ord}_r(b)$ are not relatively prime.

Exercise 98. How many primitive roots has 22? Find them.

Exercise 99. Find a primitive root of 1250.

Exercise 100. Define the function λ by the rules

$$\lambda(2^k) = \begin{cases} \varphi(2^k), & \text{if } 0 < k < 3; \\ \varphi(2^k)/2, & \text{if } k \geqslant 3; \end{cases}$$

$$\lambda(2^k \cdot {p_1}^{\ell(1)} \cdots {p_m}^{\ell(m)}) = \mathrm{lcm}(\lambda(2^k), \varphi({p_1}^{\ell(1)}), \ldots, \varphi({p_m}^{\ell(m)})).$$

where the p_i are distinct odd primes.[2]

a) Prove that, if $\gcd(a, n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$.

b) Using this, show that, if n is not 2 or 4 or an odd prime power or twice an odd prime power, then n has no primitive root.

Exercise 101. Solve the following quadratic congruences.

a) $8x^2 + 3x + 12 \equiv 0 \pmod{17}$;

b) $14x^2 + x - 7 \equiv 0 \pmod{29}$;

c) $x^2 - x - 17 \equiv 0 \pmod{23}$;

d) $x^2 - x + 17 \equiv 0 \pmod{23}$.

Exercise 102. The Law of Quadratic Reciprocity makes it easy to compute many Legendre symbols, but this law is not always needed. Compute $(n/17)$ and $(m/19)$ for as many n in $\{1, 2, \ldots, 16\}$ and m in $\{1, 2, \ldots, 18\}$ as you can, using only that, whenever p is an odd prime, and a and b are prime to p, then:

- $a \equiv b \pmod{p} \implies (a/p) = (b/p)$;
- $(1/p) = 1$;
- $(-1/p) = (-1)^{(p-1)/2}$;
- $(a^2/p) = 1$;
- $(2/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$

[2] Carmichael defined this function in 1910 [8].

Exercise 103. Compute all of the Legendre symbols $(n/17)$ and $(m/19)$ by means of Gauss's Lemma.

Exercise 104. Find all primes of the form $5 \cdot 2^n + 1$ that have 2 as a primitive root.

Exercise 105. For every prime p, show that there is an integer n such that

$$p \mid (3 - n^2)(7 - n^2)(21 - n^2).$$

Exercise 106.

a) If $a^n - 1$ is prime, show that $a = 2$ and n is prime.
b) Primes of the form $2^p - 1$ are called **Mersenne primes.** Examples are 3, 7, and 31. Show that, if $p \equiv 3 \pmod 4$, and $2p + 1$ is a prime q, then $q \mid 2^p - 1$, and therefore $2^p - 1$ is not prime. (*Hint:* Compute $(2/q)$.)

Exercise 107. Assuming p is an odd prime, and $2p + 1$ is a prime q, show that -4 is a primitive root of q. (*Hint:* Show $\operatorname{ord}_q(-4) \notin \{1, 2, p\}$.)

Exercise 108. Compute the Legendre symbols $(91/167)$ and $(111/941)$.

Exercise 109. Find $(5/p)$ in terms of the class of p *modulo* 5.

Exercise 110. Find $(7/p)$ in terms of the class of p *modulo* 28.

Exercise 111. The nth **Fermat number,** or F_n, is $2^{2^n} + 1$. A **Fermat prime** is a Fermat number that is prime.

a) Show that every prime number of the form $2^m + 1$ is a Fermat prime.
b) Show $4^k \equiv 4 \pmod{12}$ for all positive k.
c) If p is a Fermat prime, show $(3/p) = -1$.
d) Show that 3 is a primitive root of every Fermat prime.
e) Find a prime p less than 100 such that $(3/p) = -1$, but 3 is not a primitive root of p.

Exercise 112. Solve the congruence $x^2 \equiv 11 \pmod{35}$.

Exercise 113. We have so far defined the Legendre symbol (a/p) only when $p \nmid a$; but if $p \mid a$, then we can define $(a/p) = 0$. We can now define (a/n) for arbitrary a and arbitrary *odd* n: the result is the **Jacobi symbol,** and the definition is

$$\left(\frac{a}{n}\right) = \prod_p \left(\frac{a}{p}\right)^{k(p)}, \quad \text{where} \quad n = \prod_p p^{k(p)}.$$

a) Prove that the function $x \mapsto (x/n)$ on $\mathbb{Z}$ is **completely multiplicative** in the sense that $(ab/n) = (a/n) \cdot (b/n)$ for all a and b (not necessarily co-prime).

b) If $\gcd(a, n) = 1$, and the congruence $x^2 \equiv a \pmod{n}$ is soluble, show $(a/n) = 1$.

c) Find an example where $(a/n) = 1$, and $\gcd(a, n) = 1$, but $x^2 \equiv a \pmod{n}$ is insoluble.

d) If m and n are co-prime, show

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^k, \quad \text{where} \quad k = \frac{m-1}{2} \cdot \frac{n-1}{2}.$$

D. 2007–8 examinations

In the following examinations, the set of natural numbers is $\{0, 1, 2, \dots\}$ or ω, while (as usual) $\mathbb{N} = \omega \setminus \{0\} = \{1, 2, 3, \dots\}$.

D.1. In-term examination

The exam lasts 90 minutes. All answers must be justified to the reader.

Problem 1.1. *For all natural numbers k and integers n, prove*

$$k! \mid n \cdot (n+1) \cdots (n+k-1).$$

Solution.

$$\frac{n \cdot (n+1) \cdots (n+k-1)}{k!} = \begin{cases} \binom{n+k-1}{k}, & \text{if } n > 0; \\ 0, & \text{if } n \leqslant 0 < n+k; \\ (-1)^k \cdot \binom{-n}{k}, & \text{if } n+k \leqslant 0. \end{cases}$$

Remark. Every binomial coefficient $\binom{j}{i}$ is an integer for the reason implied by its name: it is one of the coefficients in the expansion of $(x+y)^j$. (It is pretty obvious that those coefficients in this expansion must be integers, but one can prove it by induction on j.)

Remark. In the set $\{n, n+1, \dots, n+k-1\}$, one of the elements is divisible by k, one by $k-1$, one by $k-2$, and so forth. This observation is not enough to solve the problem, since for example, in the set $\{3, 4, 5\}$, one of the elements is divisible by 4, one by 3, and one by 2, but $4! \nmid 3 \cdot 4 \cdot 5$.

Remark. For similar reasons, proving the claim by induction is difficult. It is therefore not recommended. However, one way to proceed is as follows. The claim is trivially true (for all n) when $k = 0$, since $0! = 1$, which divides everything. (When $k = 0$, then the product $n \cdot (n+1) \cdots (n+k-1)$ is the 'empty product', so it should be understood as the neutral element for multiplication, namely 1.) As a first inductive hypothesis, we suppose the claim is true (for all n) when $k = \ell$. We want to show

$$(\ell+1)! \mid n \cdot (n+1) \cdots (n+\ell) \qquad (*)$$

for all n. We first prove it when $n \geqslant -\ell$ by entering a second induction. The relation $(*)$ is true when $n = -\ell$, since then $n \cdot (n+1) \cdots (n+\ell) = 0$. As a second inductive hypothesis, we suppose the relation is true when $n = m$, so that

$$(\ell + 1)! \mid m \cdot (m+1) \cdots (m+\ell). \tag{$\dagger$}$$

By the first inductive hypothesis, we have

$$\ell! \mid (m+1) \cdots (m+\ell).$$

Since also $\ell + 1 \mid m + \ell + 1 - m$, we have

$$(\ell + 1)! \mid (m+1) \cdots (m+\ell)(m+\ell+1-m).$$

Distributing, we have

$$(\ell + 1)! \mid (m+1) \cdots (m+\ell)(m+\ell+1) - m \cdot (m+1) \cdots (m+\ell).$$

By the second inductive hypothesis, $(\dagger)$, we conclude

$$(\ell + 1)! \mid (m+1) \cdots (m+\ell)(m+\ell+1).$$

So the second induction is complete, and $(*)$ holds when $n \geqslant -\ell$. It therefore holds for all n, since

$$n \cdot (n+1) \cdots (n+\ell) = (-1)^{\ell+1}(-n-\ell) \cdot (-n-\ell+1) \cdots (-n).$$

Hence the *first* induction is now complete.

Problem 1.2. *Find the least natural number x such that*

$$\begin{cases} x \equiv 1 \pmod 5, \\ x \equiv 3 \pmod 6, \\ x \equiv 5 \pmod 7. \end{cases}$$

Solution. We have

$$\begin{aligned} 6 \cdot 7 &\equiv 1 \cdot 2 \equiv 2 \pmod 5, & 2 \cdot 3 &\equiv 1 \pmod 5; \\ 5 \cdot 7 &\equiv -1 \cdot 1 \equiv -1 \pmod 5, & -1 \cdot 5 &\equiv 1 \pmod 6; \\ 5 \cdot 6 &\equiv -1 \cdot (-2) \equiv 2 \pmod 7, & 2 \cdot 4 &\equiv 1 \pmod 7. \end{aligned}$$

Therefore, *modulo* $5 \cdot 6 \cdot 7$ (which is 210), we conclude

$$\begin{aligned} x &\equiv 1 \cdot 6 \cdot 7 \cdot 3 + 3 \cdot 5 \cdot 7 \cdot 5 + 5 \cdot 5 \cdot 6 \cdot 4 \\ &\equiv 126 + 525 + 600 \\ &\equiv 1251 \\ &\equiv 201. \end{aligned}$$

Therefore $\boxed{x = 201}$ (since $0 \leqslant 201 < 210$).

Remark. Instead of solving the equations

$$\begin{aligned} 2x_1 &\equiv 1 \pmod 5, \\ -1x_2 &\equiv 1 \pmod 6, \\ 2x_3 &\equiv 1 \pmod 7, \end{aligned}$$

(getting $(x_1, x_2, x_3) = (3, 5, 4)$ as above,) one may solve

$$\begin{aligned} 2y_1 &\equiv 1 \pmod 5, \\ -1y_2 &\equiv 3 \pmod 6, \\ 2y_3 &\equiv 5 \pmod 7, \end{aligned}$$

getting $(y_1, y_2, y_3) = (3, 3, 6)$. But then

$$x \equiv 6 \cdot 7 \cdot 3 + 5 \cdot 7 \cdot 3 + 5 \cdot 6 \cdot 6$$

(that is, one doesn't use as coefficients the numbers 1, 3, and 5 respectively, because they are already incorporated in the y_i).

Remark. Some people noticed, in effect, that the original system is equivalent to

$$\begin{cases} x + 9 \equiv 10 \equiv 0 \pmod 5, \\ x + 9 \equiv 12 \equiv 0 \pmod 6, \\ x + 9 \equiv 14 \equiv 0 \pmod 7, \end{cases}$$

which in turn means $x + 9 \equiv 0 \pmod{210}$ and so yields the minimal positive solution $x = 201$. But not every such problem will be so easy.

Problem 1.3. *Find all integers n such that $n^4 + 4$ is prime.*

Solution. We can factorize as follows:

$$\begin{aligned} n^4 + 4 &= n^4 + 4n^2 + 4 - 4n^2 \\ &= (n^2 + 2)^2 - (2n)^2 \\ &= (n^2 + 2 + 2n) \cdot (n^2 + 2 - 2n) \\ &= ((n + 1)^2 + 1) \cdot ((n - 1)^2 + 1). \end{aligned}$$

Both factors are positive. Moreover, one of the factors is 1 if and only if $n = \pm 1$. So $n^4 + 4$ is prime *only* if $n = \pm 1$. Moreover, if $n = \pm 1$, then $n^4 + 4 = 5$, which is prime. So the answer is, $\boxed{n = \pm 1.}$

Problem 1.4. a) *Find a solution to the equation* $151x + 71y = 1$.

b) *Find integers s and t such that*

$$\gcd(a,b)=1 \implies \gcd(151a+71b, sa+tb)=1.$$

Solution. (a) We compute

$$\begin{aligned} 151 &= 71\cdot 2+9,\\ 71 &= 9\cdot 7+8,\\ 9 &= 8\cdot 1+1, \end{aligned}$$

and hence

$$\begin{aligned} 9 &= 151-71\cdot 2,\\ 8 &= 71-(151-71\cdot 2)\cdot 7 = -151\cdot 7+71\cdot 15,\\ 1 &= 151-71\cdot 2-(-151\cdot 7+71\cdot 15) = 151\cdot 8-71\cdot 17. \end{aligned}$$

Thus, $\boxed{(8,-17)}$ is a solution to $151x+71y=1$.

(b) We want s and t such that, if a and b are co-prime, then so are $151a+71b$ and $sa+tb$. It is enough if we can obtain a and b as linear combinations of $151a+71b$ and $sa+tb$. That is, it is enough if we can solve

$$(151a+71b)x+(sa+tb)y=a$$

and (independently) $(151a+71b)x+(sa+tb)y=b$. The first equation can be rearranged as

$$(151x+sy)a+(71x+ty)b=a,$$

which is soluble if and only if the linear system

$$\begin{cases} 151x+sy=1,\\ 71x+ty=0 \end{cases}$$

is soluble. Similarly, we want to be able to solve

$$\begin{cases} 151x+sy=0,\\ 71x+ty=1. \end{cases}$$

It is enough if the coefficient matrix $\begin{pmatrix} 151 & s\\ 71 & t\end{pmatrix}$ is invertible *over the integers;* this means

$$\pm 1=\det\begin{pmatrix} 151 & s\\ 71 & t\end{pmatrix}=151t-71s$$

(since ± 1 are the only invertible integers). A solution to this equation is $\boxed{(17,8).}$

Remark. Another method for (a) is to solve

$$\begin{aligned} 151x &\equiv 1 \pmod{71}, \\ 9x &\equiv 1 \pmod{71}, \\ x &\equiv 8 \pmod{71}, \end{aligned}$$

and then solve

$$\begin{aligned} 151 \cdot 8 + 71y &= 1, \\ y &= \frac{-1207}{71} = -17. \end{aligned}$$

But finding inverses may not always be so easy as finding the inverse of 9 *modulo* 71.

Problem 1.5. *Find the least positive x such that*

$$19^{365}x \equiv 2007 \pmod{17}.$$

Solution. By applying the elementary-school division algorithm as necessary [computations omitted here], we find

$$\begin{aligned} 19 &\equiv 2 \pmod{17}, \\ 365 &\equiv 13 \pmod{16}, \\ 2007 &\equiv 1 \pmod{17}, \end{aligned}$$

which means our problem is equivalent to solving

$$\begin{aligned} 2^{13}x &\equiv 1 \pmod{17}, \\ x &\equiv 2^3 \pmod{17}, \\ x &\equiv 8 \pmod{17}; \end{aligned}$$

so $\boxed{x = 8}$ (since $0 < 8 \leqslant 17$).

Remark. Some people failed to use that $2^{16} \equiv 1 \pmod{17}$ by Fermat's Theorem. Of these, some happened to notice an alternative simplification: $2^4 \equiv -1 \pmod{17}$; but a simplification along these lines, unlike the Fermat Theorem, may not always be available.

Problem 1.6. *Prove $a^{13} \equiv a \pmod{210}$ for all a.*

Solution. We have the prime factorization $210 = 2 \cdot 3 \cdot 5 \cdot 7$, along with the following implications:

- If $2 \nmid a$, then $a \equiv 1 \pmod 2$, and hence $a^{12} \equiv 1 \pmod 2$;
- if $3 \nmid a$, then $a^2 \equiv 1 \pmod 3$, and hence $a^{12} \equiv 1 \pmod 3$;
- if $5 \nmid a$, then $a^4 \equiv 1 \pmod 2$, and hence $a^{12} \equiv 1 \pmod 5$;
- if $7 \nmid a$, then $a^6 \equiv 1 \pmod 2$, and hence $a^{12} \equiv 1 \pmod 7$.

This means that, for all a, we have

$$\begin{aligned} a^{13} &\equiv a \pmod 2, \\ a^{13} &\equiv a \pmod 3, \\ a^{13} &\equiv a \pmod 5, \\ a^{13} &\equiv a \pmod 7. \end{aligned}$$

Therefore $a^{13} \equiv a \pmod{210}$ for all a, since $210 = \operatorname{lcm}(2, 3, 5, 7)$.

Remark. One should be clear about the restrictions on a, if any. The argument here assumes that the reader is familiar with the equivalence between the two forms of Fermat's Theorem:
a) $a^{p-1} \equiv 1 \pmod p$ when $p \nmid a$;
b) $a^p \equiv p \pmod p$ for all a.

Problem 1.7. *On ω, we define the binary relation $\leqslant$ so that $a \leqslant b$ if and only if the equation $a + x = b$ is soluble. Prove the following for all natural numbers a, b, and c. You may use the 'Peano Axioms' and the standard facts about addition and multiplication that follow from them.*
a) $0 \leqslant a$.
b) $a \leqslant b \iff a + c \leqslant b + c$.
c) $a \leqslant b \iff a \cdot (c + 1) \leqslant b \cdot (c + 1)$.

Solution. (a) $0 + a = a$.

(b) By the definition of $\leqslant$, and the standard cancellation properties for addition, we have

$$\begin{aligned} a \leqslant b &\iff a + d = b \text{ for some } d \\ &\iff a + c + d = b + c \text{ for some } d \\ &\iff a + c \leqslant b + c. \end{aligned}$$

(c) We use induction on a. By part (a), the claim is trivial when $a = 0$. Suppose it is true when $a = d$; we shall prove it is true when $a = d + 1$. Note that, if $d + 1 \leqslant b$, then $d + e + 1 = b$ for some e, so b is a successor: $b = e + 1$ for

some e; in particular, $b \neq 0$. Similarly, if $(d+1)\cdot(c+1) \leqslant b\cdot(c+1)$, then $b \neq 0$, so b is a successor. So it is enough now to observe:

$$\begin{aligned} d+1 \leqslant e+1 &\iff d \leqslant e && \text{[by (b)]}\\ &\iff d\cdot(c+1) \leqslant e\cdot(c+1) && \text{[by I.H.]}\\ &\iff d\cdot(c+1)+c+1 \leqslant e\cdot(c+1)+c+1 && \text{[by (b)]}\\ &\iff (d+1)\cdot(c+1) \leqslant (e+1)\cdot(c+1). \end{aligned}$$

This completes the induction.

Remark. In (c), one may proceed as in (b):

$$\begin{aligned} a \leqslant b &\implies a+d=b \text{ for some } d\\ &\implies a\cdot(c+1)+d\cdot(c+1)=b\cdot(c+1)\\ &\implies a\cdot(c+1) \leqslant b\cdot(c+1). \end{aligned}$$

Conversely, if $a\cdot(c+1) \leqslant b\cdot(c+1)$, then $a\cdot(c+1)+d=b\cdot(c+1)$ for some d; but then d must be a multiple of $c+1$ (although this is not proved in my notes on 'Foundations of number-theory', which are the source of this problem). So we have

$$\begin{gathered} a\cdot(c+1)+e\cdot(c+1)=b\cdot(c+1),\\ (a+e)\cdot(c+1)=b\cdot(c+1),\\ a+e=b,\\ a \leqslant b \end{gathered}$$

by the standard cancellation properties of multiplication.

D.2. In-term examination

The exam lasts 90 minutes. Answers must be justified. Solutions should follow a reasonably efficient procedure.

Problem 2.1. *We define exponentiation on* ω *recursively by* $n^0=1$ *and* $n^{m+1}=n^m\cdot n$. *Prove that* $n^{m+k}=n^m\cdot n^k$ *for all* n, m, *and* k *in* ω.

Solution. Use induction on k. For the base step, that is, $k=0$, we have

$$n^{m+0}=n^m=n^m\cdot 1=n^m\cdot n^0.$$

So the claim holds when $k=0$. For the inductive step, suppose, as an inductive hypothesis, that the claim holds when $k=\ell$, so that

$$n^{m+\ell}=n^m\cdot n^\ell.$$

Then

$$\begin{aligned} n^{m+(\ell+1)} &= n^{(m+\ell)+1} \\ &= n^{m+\ell} \cdot n && \text{[by def'n of exponentiation]} \\ &= (n^m \cdot n^\ell) \cdot n && \text{[by inductive hypothesis]} \\ &= n^m \cdot (n^\ell \cdot n) \\ &= n^m \cdot n^{\ell+1} && \text{[by def'n of exponentiation].} \end{aligned}$$

Thus the claim holds when $k = \ell + 1$. This completes the induction and the proof.

Remark. Some people apparently forgot that, by the convention of this course, the first element of ω is 0, so that the induction here must start with the case $k = 0$. This convention can be inferred from the statement of the problem, since the given recursive definition of exponentiation starts with n^0, not n^1.

Remark. The formal recursive definition of exponentiation is intended to be make precise the informal definition

$$n^m = \underbrace{n \cdot n \cdots n}_{m}.$$

Likewise, mathematical induction makes precise the informal proof

$$n^{m+k} = \underbrace{n \cdot n \cdots n}_{m+k} = \underbrace{n \cdot n \cdots n}_{m} \cdot \underbrace{n \cdot n \cdots n}_{k} = n^m \cdot n^k.$$

Everybody knows $n^{m+k} = n^m \cdot n^k$; the point of the problem is to prove it precisely, so the informal proof is not enough.

Problem 2.2. *Find some n such that $35 \cdot \varphi(n) \leqslant 8n$.*

Solution. We want $\dfrac{\varphi(n)}{n} \leqslant \dfrac{8}{35}$. We have

$$\frac{\varphi(n)}{n} = \prod_{p|n} \frac{p-1}{p}.$$

If we take enough primes, this product should get down to $8/35$. As $35 = 5 \cdot 7$, we might try the primes up to 7. Indeed,

$$\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = \frac{2 \cdot 4}{5 \cdot 7} = \frac{8}{35};$$

so we may let $\boxed{n = 2 \cdot 3 \cdot 5 \cdot 7 = 210.}$

Problem 2.3. *Suppose f and g are multiplicative functions on $\mathbb{N}$. Define h and H by $h(n) = f(n) \cdot g(n)$ and $H(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right)$. Prove that these are multiplicative.*

Solution. Suppose $\gcd(m, n) = 1$. Then

$$\begin{aligned} h(mn) &= f(mn) \cdot g(mn) \\ &= f(m) \cdot f(n) \cdot g(m) \cdot g(n) \qquad \text{[by multiplicativity of } f \text{ and } g\text{]} \\ &= f(m) \cdot g(m) \cdot f(n) \cdot g(n) \\ &= h(m) \cdot h(n), \end{aligned}$$

so h is multiplicative. Also, since every divisor of mn can be factorized *uniquely* as $d \cdot e$, where $d \mid m$ and $e \mid n$, we have

$$\begin{aligned} H(mn) &= \sum_{d|mn} f(d) \cdot g\left(\frac{mn}{d}\right) \\ &= \sum_{d|m} \sum_{e|n} f(de) \cdot g\left(\frac{mn}{de}\right) \\ &= \sum_{d|m} \sum_{e|n} f(d) \cdot f(e) \cdot g\left(\frac{m}{d}\right) \cdot g\left(\frac{n}{e}\right) \qquad \text{[mult. of } f, g\text{]} \\ &= \sum_{d|m} f(d) \cdot \left(\frac{m}{d}\right) \cdot \sum_{e|n} f(e) \cdot g\left(\frac{m}{d}\right) \cdot g\left(\frac{n}{e}\right) \qquad \text{[distributivity]} \\ &= \left(\sum_{d|m} f(d) \cdot \left(\frac{m}{d}\right)\right) \cdot \sum_{e|n} f(e) \cdot g\left(\frac{m}{d}\right) \cdot g\left(\frac{n}{e}\right) \qquad \text{[distributivity]} \\ &= H(m) \cdot H(n), \end{aligned}$$

so H is multiplicative.

Remark. The assumption that $\gcd(m, n) = 1$ is essential here, because otherwise we could not conclude, for example, $f(mn) = f(m) \cdot f(n)$; neither could we do the trick with the divisors of mn.

Remark. Since f is multiplicative, we know for example that $\sum_{d|n} f(d)$ is a multiplicative function of n. Hence $\sum_{d|n} f(n/d)$ is also multiplicative, since it is the same function. Likewise, once we know that fg is multiplicative, then we know that $\sum_{d|n} f(d)g(d)$ is multiplicative. But we *cannot* conclude so easily that $\sum_{d|n} f(d)g(n/d)$ is multiplicative. It does not make sense to say $g(n/d)$ is multiplicative, since it has two variables. We do not have $g(mn/d) = g(m/d) \cdot g(n/d)$; neither do we have $g(n/de) = g(n/d) \cdot g(n/e)$. What we have is $g(mn/de) = g(m/d)g(n/e)$, if $d \mid m$ and $e \mid n$; but it takes some work to make use of this.

Problem 2.4. *Concerning* 13*:*

a) *Show that* 2 *is a primitive root.*

b) *Find all primitive roots as powers of* 2*.*

c) *Find all primitive roots as elements of* $[1, 12]$.

d) *Find all elements of* $[1, 12]$ *that have order* 4 modulo 13*.*

Solution. (a) *Modulo* 13, we have

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2	4	8	3	6	12	11	9	5	10	7	1

(b) 2^k, where $\gcd(k, 12) = 1$; so $\boxed{2,\ 2^5,\ 2^7,\ 2^{11}.}$

(c) From the table, $\boxed{2,\ 6,\ 11,\ 7.}$

(d) 2^k, where $4 = 12/\gcd(k, 12)$, that is, $\gcd(k, 12) = 3$, so k is 3 or 9; so, again from the table, $\boxed{8,\ 5.}$

Problem 2.5 (4 points)**.** *Prove* $\displaystyle\sum_{d|n} \mu(d) \cdot \sigma(d) = \prod_{p|n} (-p)$.

Solution. Each side of the equation is a multiplicative function of n, so it is enough to check the claim when n is a prime power. Accordingly, we have

$$\sum_{d|p^s} \mu(d) \cdot \sigma(d) = \sum_{k=0}^{s} \mu(p^k) \cdot \sigma(p^k) =$$

$$= \mu(1) \cdot \sigma(1) + \mu(p) \cdot \sigma(p) = 1 - (1 + p) = -p = \prod_{q|p^s} (-q).$$

This establishes the claim when n is a prime power, hence for all n.

Remark. It should be understood in the product $\prod_{p|n}(-p)$ that p is prime. This product is a multiplicative function of n, because if $\gcd(m, n) = 1$, and $p \mid mn$, then $p \mid m$ or $p \mid n$, but not both, so that $\prod_{p|mn}(-p) = \prod_{p|m}(-p) \cdot \prod_{p|n}(-p)$.

Remark. Using multiplicativity of functions to prove their equality is a powerful technique. It works like magic. It is possible here to prove the desired equation directly, for arbitrary n; but the proof is long and complicated. It is not enough to write out part of the summation, detect a pattern, and claim (as some people did) that everything cancels but what is wanted: one must *prove* this claim precisely. One way is as follows. Every positive integer n can be written as $\prod_{p \in A} p^{s(p)}$, where A is a (finite) set of prime numbers, and each exponent $s(p)$ is at least 1. (Note the streamlined method of writing a product.) Then the only divisors d of

n for which $\mu(d) \neq 0$ are those divisors of the form $\prod_{p\in B} p$ for some subset B of A. Moreover, each such number *is* a divisor of n. Hence

$$\begin{aligned}
\sum_{d|n} \mu(d)\cdot\sigma(d) &= \sum_{X\subseteq A} \mu\Big(\prod_{p\in X} p\Big)\cdot\sigma\Big(\prod_{p\in X} p\Big)\\
&= \sum_{X\subseteq A} (-1)^{|X|}\cdot\prod_{p\in X}(1+p)\\
&= \sum_{X\subseteq A} (-1)^{|X|}\cdot\sum_{Y\subseteq X}\prod_{p\in Y} p\\
&= \sum_{Y\subseteq A}\prod_{p\in Y} p\cdot\sum_{Y\subseteq X\subseteq A}(-1)^{|X|}\\
&= \sum_{Y\subseteq A}\prod_{p\in Y} p\cdot(-1)^{|Y|}\cdot\sum_{Z\subseteq A\smallsetminus Y}(-1)^{|Z|}\\
&= \sum_{Y\subseteq A}\prod_{p\in Y} p\cdot(-1)^{|Y|}\cdot\sum_{j=0}^{|A\smallsetminus Y|}\binom{|A\smallsetminus Y|}{j}(-1)^j\\
&= \sum_{Y\subseteq A}\prod_{p\in Y} p\cdot(-1)^{|Y|}\cdot(1+(-1))^{|A\smallsetminus Y|}\\
&= \prod_{p\in A} p\cdot(-1)^{|A|}\\
&= \prod_{p\in A}(-p).
\end{aligned}$$

This proves the desired equation; but it is probably easier just to use the multiplicativity of each side, as above.

Problem 2.6. *Solve* $6^{3164}x \equiv 2 \pmod{365}$.

Solution. $365 = 5\cdot 73$, so $\varphi(365) = \varphi(5)\cdot\varphi(73) = 4\cdot 72 = 288$. And 288 goes into 3164 ten times, with remainder 284. Therefore, *modulo* 365, we have

$$\begin{aligned}
6^{3164}x \equiv 2 &\iff 6^{284}x \equiv 2\\
&\iff x \equiv 2\cdot 6^4\\
&\qquad\equiv 2\cdot 36^2\\
&\qquad\equiv 2\cdot 1296\\
&\qquad\equiv 2\cdot 201\\
&\qquad\equiv 402\\
&\qquad\equiv 37.
\end{aligned}$$

Remark. One may note that, since $4 \mid 72$, we have that $a^{72} \equiv 1 \pmod{365}$ whenever $\gcd(a, 365) = 1$. Such an observation might make computations easier in some problems, though perhaps not in this one.

Problem 2.7. *Show that the least positive primitive root of* 41 *is* 6. *(Try to compute as few powers as possible.)*

Solution. $\varphi(41) = 40 = 2^3 \cdot 5 = 8 \cdot 5$, so the proper divisors of $\varphi(41)$ are divisors of 8 or 20. So we want to show, *modulo* 41,

a) when $\ell \in \{2, 3, 4, 5\}$, then either ℓ^8 or ℓ^{20} is congruent to 1;
b) neither 6^8 nor 6^{20} is congruent to 1.

To establish that $\ell^{2k} \equiv 1$, it is enough to show $\ell^k \equiv \pm 1$. To establish that $\ell^{2k} \not\equiv 1$, it is enough to show $\ell^k \not\equiv \pm 1$. So we proceed:

a) $2^2 \equiv 4$; $2^4 \equiv 4^2 \equiv 16$; $2^8 \equiv 16^2 \equiv 256 \equiv 10$; $2^{10} \equiv 2^8 \cdot 2^2 \equiv 10 \cdot 4 \equiv 40 \equiv -1$.
b) $3^2 \equiv 9$; $3^4 \equiv 9^2 \equiv 81 \equiv -1$.
c) $4^5 \equiv 2^{10} \equiv -1$.
d) $5^2 \equiv 25 \equiv -16$; $5^4 \equiv 16^2 \equiv 256 \equiv 10 \equiv 2^8 \equiv 4^4$; hence $5^{20} \equiv 4^{20} \equiv 1$;
e) $6^2 \equiv 36 \equiv -5$; $6^4 \equiv 25 \equiv -16$; $6^8 \equiv 256 \equiv 10$; $6^{10} \equiv 10 \cdot (-5) \equiv -50 \equiv -9$; $6^{20} \equiv 81 \equiv -1$.

Remark. Another possible method is first to write out all of the powers of 6 (*modulo* 41), thus showing that 6 is a primitive root, and then to select from among these the other primitive roots of 41, write them as positive numbers, and note that 6 is the least. That is, one can start with

k	1	2	3	4	5	6	7	8	9	10
6^k	6	−5	11	−16	−14	−2	−12	10	19	−9
k	11	12	13	14	15	16	17	18	19	20
6^k	−13	4	−17	−20	3	18	−15	−8	−7	−1
k	21	22	23	24	25	26	27	28	29	30
6^k	−6	5	−11	16	14	2	12	−10	−19	9
k	31	32	33	34	35	36	37	38	39	40
6^k	13	−4	17	20	−3	−18	15	8	7	1

Then 6 is indeed a primitive root of 41, so every primitive root of 41 takes the form 6^k, where $\gcd(k, 40) = 1$. So the incongruent primitive roots are 2^k, where

$$k \in \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$$

(that is, k is an odd positive integer less than 40 and indivisible by 5). From the table, if we convert these powers to congruent positive integers less than 41, we get the list

$$6, 11, 29, 19, 28, 24, 26, 34, 35, 30, 12, 22, 13, 17, 15, 7$$

The least number on the list is 6.

Remark. Some people noted that 6 is the least element of the set $\{6^k\colon 0 < k \leqslant 40 \ \&\ \gcd(k, 40) = 1\}$. This is true, but it does not establish the claim that 6 is the least positive primitive root of 41, since some of the powers in the set may be congruent *modulo* 41 to lesser positive numbers, which numbers will still be primitive roots.

D.3. In-term examination

The exam lasts 90 minutes. Several connected problems involve the prime number 23. As usual, answers must be reasonably justified to the reader.

Bracketed numbers (as [108]) refer to related homework exercises.

Problem 3.1. *Compute the Legendre symbol* $\left(\frac{63}{271}\right)$. [108]

Solution. $\left(\frac{63}{271}\right) = \left(\frac{7\cdot 3^2}{271}\right) = \left(\frac{7}{271}\right) = -\left(\frac{271}{7}\right) = -\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1) = 1$.

Remark. The computation uses the following features of the Legendre symbol:

a) the complete multiplicativity of $x \mapsto (x/p)$;
b) that $(a/p) = \pm 1$;
c) the Law of Quadratic Reciprocity;
d) the dependence of (a/p) only on the class of a *modulo* p;
e) the rule for $(2/p)$.

If $(p/q) = -(q/p)$ by the Law of Quadratic Reciprocity, then also $-(q/p) = (-1/p)(q/p) = (-q/p)$, since $p \equiv 3 \pmod 4$. So one could also argue $(63/271) = (7\cdot 3^2/271) = (7/271) = -(271/7) = (-271/7) = (2/7) = 1$.

However, the equation $(63/271) = -(271/63)$ is not available without explanation and proof. Because 63 is not prime, $(271/63)$ is not a Legendre symbol. It is a Jacobi symbol, but these were defined only in [113].

Problem 3.2 (3 points)**.** *Find the Legendre symbol* $(a/29)$*, given that* [103]

$$\left\{ka - 29\cdot\left[\frac{ka}{29}\right] : 1 \leqslant k \leqslant 14\right\} = \{1,2,5,6,7,10,11,12,15,16,20,21,25,26\}.$$

Solution. The given set has 6 elements greater than $29/2$. Since $ka - 29\cdot[ka/29]$ is the remainder of ka after division by 29, by Gauss's Lemma we have $(a/29) = (-a)^6 = 1$.

Problem 3.3 (3 points)**.** *The numbers* 1499 *and* 2999 *are prime. Find a primitive root of* 2999. [107]

Solution. Since $2999 = 2 \cdot 1499 + 1$, it has the primitive root $(-1)^{(1499-1)/2} \cdot 2$, that is, -2.

Remark. The number 1499 is a Germain prime. If p is a Germain prime, so that $2p + 1$ is a prime q, then the number of (congruence classes of) primitive roots of q is $\varphi(\varphi(q))$, which is $p - 1$ or $(q - 3)/2$. So *almost* half the numbers that are prime to q are primitive roots of q. We showed $(-1)^{(p-1)/2} \cdot 2$ is a primitive root; the cited homework exercise shows -4 is a primitive root. By the same method of proof, if $q \nmid r$, then the following are equivalent:

a) r is a primitive root of q;
b) $\operatorname{ord}_q(r) \notin \{1, 2, p\}$;
c) $r \not\equiv \pm 1 \pmod q$ and $(r/q) = 1$.

In particular, to show r is a primitive root of q, it is not enough to show $(r/q) = 1$. (One must also show $r^2 \neq 1 \pmod q$; and again, this is enough only in case $(q - 1)/2$ is prime.)

Problem 3.4 (4 points)**.** *Fill out the following table of logarithms. (It should be clear what method you used.)* [93(a)]

k	1	2	3	4	5	6	7	8	9	10	11	$\pmod{23}$
$\log_5 k$												$\pmod{22}$
$\log_5(-k)$												$\pmod{22}$

Solution. First compute powers of 5, then rearrange:

ℓ	0	1	2	3	4	5	6	7	8	9	10	$\pmod{22}$
5^ℓ	1	5	2	10	4	-3	8	-6	-7	11	9	$\pmod{23}$
$5^{\ell+11}$	-1	-5	-2	-10	-4	3	-8	6	7	-11	-9	$\pmod{23}$

k	1	2	3	4	5	6	7	8	9	10	11	$\pmod{23}$
$\log_5 k$	0	2	16	4	1	18	19	6	10	3	9	$\pmod{22}$
$\log_5(-k)$	11	13	5	15	12	7	8	17	21	14	20	$\pmod{22}$

Remark. Implicitly, 5 must be a primitive root of 23, which implies $5^{11} \equiv -1 \pmod{23}$. Hence $\log_5(-1) \equiv 11 \pmod{22}$, and more generally $\log_5(-k) \equiv \log_5 k \pm 11 \pmod{22}$. Thus the second row of the table can be obtained easily from the first.

Problem 3.5 (3 points)**.** *Fill out the following table of Legendre symbols. (Again, your method should be clear.)*

a	1	2	3	4	5	6	7	8	9	10	11
$\left(\frac{a}{23}\right)$											
$\left(\frac{-a}{23}\right)$											

Solution. The quadratic residues of 23 are just the even powers of a primitive root, such as 5. Those even powers are just the numbers whose logarithms are even. So, in the logarithm table in Problem 3.4, we can replace even numbers with 1, and odd numbers with -1, obtaining

a	1	2	3	4	5	6	7	8	9	10	11
$\left(\frac{a}{23}\right)$	1	1	1	1	-1	1	-1	1	1	-1	-1
$\left(\frac{-a}{23}\right)$	-1	-1	-1	-1	1	-1	1	-1	-1	1	1

Remark. One can find the Legendre symbols by means of Euler's Criterion and the properties in the remark on Problem 3.1 (as in [102]), or by Gauss's Lemma (as in [103]); but really, all of the necessary work has already been done in Problem 3.4.

Problem 3.6 (7 points)**.** *Solve the following congruences* modulo 23. [93(b)]

a) $x^2 \equiv 8$ b) $x^{369} \equiv 7$

Solution. (a) From the solution to Problem 3.4, we have $8 \equiv 5^6 \equiv (5^3)^2 \equiv 10^2$, so

$$x^2 \equiv 8 \iff \boxed{x \equiv \pm 10 \equiv 10, 13}.$$

(b) From the computation at the right, as well as Problem 3.4, we have

$$\begin{aligned} x^{369} \equiv 7 \pmod{23} &\iff x^{17} \equiv 7 \pmod{23} \\ &\iff 17 \log_5 x \equiv 19 \pmod{22} \\ &\iff \log_5 x \equiv \frac{19}{17} \equiv \frac{-3}{-5} \equiv \frac{3}{5} \pmod{22} \\ &\iff \log_5 x \equiv 3 \cdot 9 \equiv 27 \equiv 5 \pmod{22} \\ &\iff x \equiv 5^5 \equiv -3 \pmod{23} \\ &\iff \boxed{x \equiv 20} \pmod{23} \end{aligned}$$

$$\begin{array}{r} 16 \\ 22 \overline{)\,369} \\ \underline{22} \\ 149 \\ \underline{132} \\ 17 \end{array}$$

Remark. Some people seemed to overlook the information available from Problem 3.4. In part (a), one may note from Problem 3.5 that there must be a solution, since $(8/23) = 1$; but there is no need to do this, if one actually *finds* the solutions.

Problem 3.7 (3 points)**.** *Solve the congruence* $x^2 - x + 5 \equiv 0 \pmod{23}$. [101]

Solution. Complete the square:

$$\begin{aligned} x^2 - x + 5 \equiv 0 &\iff x^2 - x + \frac{1}{4} \equiv \frac{1}{4} - 5 \equiv \frac{-19}{4} \equiv 1 \\ &\iff \left(x - \frac{1}{2}\right)^2 \equiv 1 \\ &\iff x - \frac{1}{2} \equiv \pm 1 \\ &\iff x \equiv \frac{1}{2} \pm 1 \equiv 12 \pm 1 \equiv \boxed{11, 13} \pmod{23}. \end{aligned}$$

Remark. Although fractions with denominators prime to 23 are permissible here, one may avoid them thus:

$$\begin{aligned} x^2 - x + 5 \equiv 0 &\iff x^2 + 22x + 5 \equiv 0 \\ &\iff x^2 + 22x + 121 \equiv 121 - 5 \equiv 116 \equiv 1 \\ &\iff (x + 11)^2 \equiv 1 \\ &\iff x + 11 \equiv \pm 1. \end{aligned}$$

Alternatively, one may apply the identity

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac),$$

finding in the present case

$$\begin{aligned} x^2 - x + 5 \equiv 0 &\iff 4x^2 - 4x + 20 \equiv 0 \\ &\iff (2x - 1)^2 \equiv 1 - 20 \equiv -19 \equiv 4. \end{aligned}$$

All approaches used to far can be used on any quadratic congruence (with odd prime modulus). Nonetheless, many people chose to look for a factorization. Here

are some that were found:

$$x^2 - x + 5 \equiv x^2 - x - 110 \equiv (x - 11)(x + 10);$$
$$x^2 - x + 5 \equiv x^2 - x + 143 \equiv (x - 11)(x - 13);$$

$$\begin{aligned} x^2 - x + 5 &\equiv 0 \\ &\iff -22x^2 + 22x - 18 \equiv 0 \\ &\iff -11x^2 + 11x - 9 \equiv 0 \\ &\iff 12x^2 - 12x + 14 \equiv 0 \\ &\iff 6x^2 - 6x + 7 \equiv 0 \\ &\iff 6x^2 + 17x + 7 \equiv 0 \\ &\iff (3x + 7)(2x + 1) \equiv 0; \end{aligned}$$

$$\begin{aligned} x^2 - x + 5 &\equiv 0 \\ &\iff -22x^2 + 22x - 18 \equiv 0 \\ &\iff -11x^2 + 11x - 9 \equiv 0 \\ &\iff 12x^2 + 11x - 9 \equiv 0 \\ &\iff 12x^2 - 12x - 9 \equiv 0 \\ &\iff 4x^2 - 4x - 3 \equiv 0 \\ &\iff (2x - 3)(2x + 1) \equiv 0; \end{aligned}$$

$$\begin{aligned} x^2 - x + 5 &\equiv 0 \\ &\iff 24x^2 + 22x + 28 \equiv 0 \\ &\iff 12x^2 + 11x + 14 \equiv 0 \\ &\iff 12x^2 + 34x + 14 \equiv 0 \\ &\iff (4x + 2)(3x + 7) \equiv 0; \end{aligned}$$

$$\begin{aligned} x^2 - x + 5 &\equiv 0 \\ &\iff 24x^2 + 22x + 5 \equiv 0 \\ &\iff (12x + 5)(2x + 1) \equiv 0. \end{aligned}$$

But for such problems, it does not seem advisable to rely on one's ingenuity to find factorizations. How would one best solve a congruence like $x^2 - 2987 + 2243 \equiv 0 \pmod{2999}$?

Problem 3.8 (4 points)**.** *Explain briefly why exactly one element n of the set $\{2661, 2662\}$ has a primitive root. Give two numbers such that at least one of them is a primitive root of n.* [99]

Solution. The numbers with primitive roots are just 2, 4, odd prime powers, and doubles of odd prime powers. Since $2661 = 3 \cdot 887$, and $3 \nmid 887$, the number 2661 has no primitive root. However, $2662 = 2 \cdot 1331 = 3 \cdot 11 \cdot 121 = 2 \cdot 11^3$, so this has a primitive root.

By the computation

k	1	2	3	4	5	$\pmod{10}$
2^k	2	4	-3	-6	-1	$\pmod{11}$

we have that 2 is a primitive root of 11. Therefore 2 or $2 + 11$ is a primitive root of 121. Therefore $2 + 121$ or $2 + 11$ is a primitive root of 121, hence of 1331, hence of 2662.

Remark. This problem relies on the following propositions about odd primes p:

a) if r is a primitive root of p, then r or $r + p$ is a primitive root of p^2;
b) every primitive root of p^2 is a primitive root of every higher power p^{2+k};
c) every *odd* primitive root of p^ℓ is a primitive root of $2 \cdot p^\ell$.

One must also observe that being a primitive root is a property of the *congruence class* of a number, so if $r \equiv s \pmod{n}$, and r is a primitive root of p, then so is s.

D.4. Final Examination

You may take 120 minutes. Several connected problems involve the Fermat prime 257. As usual, answers must be reasonably justified.

A table of powers of 3 *modulo* 257 was provided for use in several problems [see Table D.1].

Problem 4.1. *For positive integers n, let $\omega(n) = |\{p\colon p \mid n\}|$, the number of primes dividing n.*

a) *Show that the function $n \mapsto 2^{\omega(n)}$ is multiplicative.*
b) *Define the Möbius function μ in terms of ω.*
c) *Show $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$ for all positive integers n.*

Powers of 3 *modulo* 257:

Solution. a) If $\gcd(m, n) = 1$, then $\omega(mn) = \omega(m) + \omega(n)$, so

$$2^{\omega(mn)} = 2^{\omega(m)+\omega(n)} = 2^{\omega(m)} \cdot 2^{\omega(n)}.$$

b) $\mu(n) = \begin{cases} 0, & \text{if } p^2 \mid n \text{ for some } p; \\ (-1)^{\omega(n)}, & \text{otherwise.} \end{cases}$

c) As μ is multiplicative, so are $|\mu|$ and $n \mapsto \sum_{d|n} |\mu(d)|$. Hence it is enough to establish the equation when n is a prime power. We have

$$\sum_{d|p^s} |\mu(d)| = \sum_{k=0}^{s} |\mu(p^k)| = |\mu(1)| + |\mu(p)| = 1 + 1 = 2 = 2^1 = 2^{\omega(p^s)}.$$

Problem 4.2. *Fill out the following table of Legendre symbols:*

a	1	2	3	5	7	11	13	17	19
$\left(\frac{a}{257}\right)$									

Solution. By the table of powers, 3 must be a primitive root of 257. Hence $(a/257) = 1$ if and only if a is an even power of 3 *modulo* 257. In particular,

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k	3	9	27	81	−14	−42	−126	−121	−106	−61	74	−35	−105	−58	83	−8
3^{16+k}	−24	−72	41	123	112	79	−20	−60	77	−26	−78	23	69	−50	107	64
3^{32+k}	−65	62	−71	44	−125	−118	−97	−34	−102	−49	110	73	−38	−114	−85	2
3^{48+k}	6	18	54	−95	−28	−84	5	15	45	−122	−109	−70	47	−116	−91	−16
3^{64+k}	−48	113	82	−11	−33	−99	−40	−120	−103	−52	101	46	−119	−100	−43	128
3^{80+k}	127	124	115	88	7	21	63	−68	53	−98	−37	−111	−76	29	87	4
3^{96+k}	12	36	108	67	−56	89	10	30	90	13	39	117	94	25	75	−32
3^{112+k}	−96	−31	−93	−22	−66	59	−80	17	51	−104	−55	92	19	57	−86	−1

Table D.1. Powers of 3 *modulo* 257

$(-1/257) = 1$, so $(a/257) = (-a/257)$. So the table of powers yields the answers:

a	1	2	3	5	7	11	13	17	19
$\left(\frac{a}{257}\right)$	1	1	-1	-1	-1	1	1	1	-1

Remark. Many people preferred to find these Legendre symbols by means of the Law of Quadratic Reciprocity. Possibly this method is faster than hunting for numbers in the table of powers; but it may also provide more opportunity for error.

Problem 4.3. *In the following table, in the box below each number a, write the least positive integer n such that* $\operatorname{ord}_{257}(n) = a$.

1	2	4	8	16	32	64	128	256

Solution. If r is a primitive root of 257, then $\operatorname{ord}_{257}(r^{256/a}) = a$. The primitive roots of 257 are 3^s, where s is odd. So below a we want the least n such that $n \equiv 3^{(256/a)\cdot s}$ for some odd s. (In searching the table of powers, since $3^{k+128} \equiv -3^k$, we can ignore signs, except when $a \leqslant 2$. For example, when $a = 4$, then $3^{(256/a)\cdot s} = 3^{64s}$, so n can only be $|3^{64}|$. When $a = 32$, then $3^{(256/a)\cdot s} = 3^{8s}$, so n will be the absolute value of an entry in the column of powers that is headed by 8.)

1	2	4	8	16	32	64	128	256
1	256	16	4	2	15	11	9	3

Remark. Another way to approach the problem is to note that

$$\operatorname{ord}_{257}(3^k) = \frac{256}{\gcd(256, k)}.$$

Then one must look among those powers 3^k such that $\gcd(256, k) = 256/a$. *Some* explanation is necessary, though it need not be so elaborate as what I gave above.

Some people apparently misread the problem as asking for the orders of the given numbers. Others provided numbers that had the desired orders; but they weren't the *least positive* such numbers.

Problem 4.4. *Solve* $x^2 + 36x + 229 \equiv 0 \pmod{257}$.

Solution. Complete the square: $(36/2)^2 = (2\cdot 9)^2 = 4\cdot 81 = 324$, and $324 - 229 = 95$, so (using the table of powers)

$$\begin{aligned} x^2 + 36x + 229 \equiv 0 &\iff (x+18)^2 \equiv 95 \equiv 3^{128+52} \equiv 3^{180} \equiv (3^{90})^2 \\ &\iff x + 18 \equiv \pm 3^{90} \equiv \mp 98 \\ &\iff x \equiv -116, 80 \\ &\iff x \equiv 141, 80 \pmod{257}. \end{aligned}$$

Remark. There were a few unsuccessful attempts to factorize the polynomial directly. See my remark on Problem 7 of Exam 3.

Problem 4.5. *Solve* $197^x \equiv 137 \pmod{257}$.

Solution. From the table of powers of 3, we can obtain logarithms:

$$\begin{aligned} 197^x \equiv 137 \pmod{257} &\iff (-60)^x \equiv -120 \pmod{257} \\ &\iff x \log_3(-60) \equiv \log_3(-120) \pmod{256} \\ &\iff x \cdot 24 \equiv 72 \pmod{256} \\ &\iff x \cdot 8 \equiv 24 \pmod{256} \\ &\iff x \equiv 3 \pmod{32} \\ &\iff x \equiv 3, 35, 67, 99, 131, 163, 195, 227 \pmod{256}. \end{aligned}$$

Remark. A number of people overlooked the change of modulus when passing from $x \cdot 8 \equiv 24$ to $x \equiv 3$. One need not use logarithms explicitly; one can observe instead $197 \equiv -60 \equiv 3^{24}$ and $137 \equiv -120 \equiv 3^{72} \pmod{256}$, so that

$$\begin{aligned} 197^x \equiv 137 \pmod{257} &\iff 3^{24x} \equiv 3^{72} \pmod{257} \\ &\iff 24x \equiv 72 \pmod{256}, \end{aligned}$$

and then proceed as above.

Problem 4.6. *Solve* $127x + 55y = 4$.

Solution. Use the Euclidean algorithm:

$$\begin{aligned} 127 &= 55 \cdot 2 + 17, & 17 &= 127 - 55 \cdot 2, \\ 55 &= 17 \cdot 3 + 4, & 4 &= 55 - (127 - 55 \cdot 2) \cdot 3 = 55 \cdot 7 - 127 \cdot 3, \\ 17 &= 4 \cdot 4 + 1, & 1 &= 17 - 4 \cdot 4 = 127 - 55 \cdot 2 - (55 \cdot 7 - 127 \cdot 3) \cdot 4 \\ & & &= 127 \cdot 13 - 55 \cdot 30. \end{aligned}$$

Hence $4 = 127 \cdot 52 - 55 \cdot 120$, and $\gcd(127, 55) = 1$, so the original equation has the general solution

$$(52, -120) + (55, -127) \cdot t.$$

Remark. Some people omitted to find the general solution. In carrying out the Euclidean algorithm here, one can save a step, as some people did, by noting that, once we find $4 = 55 \cdot 7 - 127 \cdot 3$, we need not find 1 as a linear combination of 127 and 55; we can pass immediately to the general solution $(7, -3) + (55, -127) \cdot t$.

Problem 4.7. *Solve* $x^2 \equiv 59 \pmod{85}$.

Solution. Since $85 = 5 \cdot 17$, we first solve $x^2 \equiv 59$ *modulo* 5 and 17 separately:

$$\begin{aligned} x^2 &\equiv 59 \pmod 5 \\ &\iff x^2 \equiv 4 \pmod 5 \\ &\iff x \equiv \pm 2 \pmod 5; \end{aligned} \qquad \begin{aligned} x^2 &\equiv 59 \pmod{17} \\ &\iff x^2 \equiv 8 \pmod{17} \\ &\iff x^2 \equiv 25 \pmod{17} \\ &\iff x \equiv \pm 5 \pmod{17}. \end{aligned}$$

Now there are four systems to solve:

$$\left.\begin{aligned} x &\equiv \pm 2 \pmod 5 \\ x &\equiv \pm 5 \pmod{17} \end{aligned}\right\} \iff x \equiv \pm 22 \pmod{85},$$

$$\left.\begin{aligned} x &\equiv \pm 2 \pmod 5 \\ x &\equiv \mp 5 \pmod{17} \end{aligned}\right\} \iff x \equiv \pm 12 \pmod{85}.$$

(I solved these by trial.) So the original congruence is solved by

$$x \equiv \pm 22, \pm 12 \pmod{85},$$

or $x \equiv 12, 22, 63, 73 \pmod{85}$.

Remark. One may, as some people did, use the algorithm associated with the Chinese Remainder Theorem here. Even if we do not use the algorithm, we rely on it to know that the solution we find to each pair of congruences is the *only* solution. Some used a theoretical formation of the solution, noting for example that $\left\{\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 5 \pmod{17} \end{aligned}\right\}$ has the solution $x \equiv 2 \cdot 17^{\varphi(5)} + 5 \cdot 5^{\varphi(17)} \pmod{85}$; but this is not *useful* (the number is not between 0 and 85, or between $-85/2$ and $85/2$).

E. 2010–1 examinations

E.1. In-term examination

Problem 1.1. *Let* $\omega = \{0, 1, 2, \dots\}$. *All variables in this problem range over* ω. *Given* a *and* b *such that* $a \neq 0$, *we define*

$$\operatorname{rem}(b, a) = r,$$

if $b = ax + r$ *for some* x, *and* $r < a$.

a) *Prove* $\operatorname{rem}(a + b, n) = \operatorname{rem}(\operatorname{rem}(a, n) + \operatorname{rem}(b, n), n)$.

b) *Prove* $\operatorname{rem}(ab, n) = \operatorname{rem}(\operatorname{rem}(a, n) \cdot \operatorname{rem}(b, n), n)$.

Solution. a) For $\operatorname{rem}(c, n)$, write c'. Then for some x, y, and z in ω, we have

$$a = nx + a', \qquad b = ny + b', \qquad a' + b' = nz + (a' + b')',$$

hence $a + b = n(x + y + z) + (a' + b')'$. Since $(a' + b')' < n$, we have

$$(a + b)' = (a' + b')'$$

as desired.

b) With the same notation, for some w in ω we have

$$a' \cdot b' = nw + (a' \cdot b')',$$

so for some u in ω, we have $ab = nu + a' \cdot b' = n(w + u) + (a' \cdot b')'$, and therefore (since $(a' \cdot b')' < n$) we have

$$(ab)' = (a' \cdot b')'$$

as desired.

Remark. Books VII, VIII, and IX of Euclid's *Elements* develop some of the theory of what we would call the positive integers. If we allow also a zero, but not negative numbers, then we could define

$$a \equiv b \pmod{n} \iff \operatorname{rem}(a, n) = \operatorname{rem}(b, n).$$

This problem then could be used to establish the basic facts about congruence.

Remark. A number of students used the arrow "⇒" in their proofs. Such usage is a bad habit, albeit a common one, even among teachers. Indeed, I learned this bad habit from somebody who was otherwise one of my best teachers. Later I unlearned the habit.

In logic, the expression $A \Rightarrow B$ means

> If A is true, then B is true.

One rarely wants to say this in proofs. Rather, one wants to say things like

> A is true, and therefore B is true.

If this is what you want to say, then you should just say it in words.

In the expression "$A \Rightarrow B$", the arrow is a verb, usually read as "implies". When somebody writes the arrow in a proof, the intended meaning seems usually to be that of "*which* implies" or "*and this* implies". But the arrow should not be loaded up with these extra meanings.

One student used the arrow in place of the equals sign "=". This usage must definitely be avoided.

Another practice that should be avoided is drawing arrows to direct the reader's eye. It should be possible to read a proof left to right, top to bottom, in the usual fashion. If you need to refer to something that came before, then just say so.

It is true that, when I grade papers, I may use arrows. This is in part because, when you see your paper, I am there to explain what I meant by the arrow, if this is necessary. But what *you* write on exam should make sense without need for additional explanation by you.

If I ask you to prove a claim, I already know the claim is true. The point is not to convince me that the claim is true, or even to convince me that *you* know the claim is true. The point is to write a proof of the claim. The point is to write the sort of thing that is found in research articles and books of mathematics, often labelled with the word *Proof.*

Problem 1.2. *Find integers k and ℓ, both greater than 1, such that, for all positive integers n,*

$$k \mid 1965^{10n} + \ell.$$

Solution. Since 1965^{10n} is odd, we can let $\boxed{\ell = 3,\ k = 2.}$

Remark. This problem is based on Exercise 8. As it is stated, the problem has many solutions.

(i) The solution given here is a special case of letting k be any number such that $1965 \equiv 1 \pmod{k}$, and then letting $\ell = 2k - 1$ (or $k - 1$ if $k > 2$).

(ii) We could also let ℓ be a factor of 1965, and then let k be a factor of ℓ.

(iii) Finally, since $11 \nmid 1965$, we have by Fermat $1965^{10} \equiv 1 \pmod{11}$, so we could let $k = 11$ and $\ell = 10$.

Problem 1.3. *Find two positive integers a and b such that, for all integers m and n, the integer $am - bn$ is a solution of the congruences*

$$x \equiv m \pmod{999}, \qquad x \equiv n \pmod{1001}.$$

Solution. A solution of the congruences takes the form

$$x \equiv m \cdot 1001s + n \cdot 999t \pmod{999 \cdot 1001},$$

where $1001s \equiv 1 \pmod{999}$ and $999t \equiv 1 \pmod{1001}$. So we want

$$2s \equiv 1, \qquad s \equiv 500 \pmod{999}, \qquad -2t \equiv 1, \qquad t \equiv 500 \pmod{1001}.$$

Then the solution to the original congruences is

$$x \equiv m \cdot 1001 \cdot 500 + n \cdot 999 \cdot 500 \equiv 1001 \cdot 500m - 999 \cdot 501n \pmod{999 \cdot 1001}.$$

So we can let $\boxed{a = 1001 \cdot 500,\ b = 999 \cdot 501.}$

Remark. This is just a Chinese Remainder Theorem problem with letters instead of numbers.

Problem 1.4. *Letting $n = \sum_{j=1}^{408} j$, find an integer k such that $0 \leqslant k < 409$ and*

$$408! \equiv k \pmod{n}.$$

Solution. We have $n = 409 \cdot 408/2$; also 409 is prime, so by Wilson's Theorem $408! \equiv -1 \pmod{409}$. Then $408! \equiv 408$ *modulo* both 409 and 408, hence *modulo* any divisor of the least common multiple of these. But n is such a divisor. Thus we can let $\boxed{k = 408.}$

Remark. This problem is based on Exercise 57. A number of people argued as follows.

> Since $408! \equiv -1$ (409), we must have $k \equiv -1$ (409). Since it is required that $0 \leqslant k < 409$, it must be that $k = 408$.

But this argument does *not* prove $408! \equiv 408$ (n). Maybe I made a mistake, and there is *no* k meeting the stated conditions.

Problem 1.5. *With justification, find an integer n, greater than 1, such that, for all integers a,*

$$a^n \equiv a \pmod{1155}.$$

Solution. We have $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, and $\gcd(3-1, 5-1, 7-1, 11-1) = \gcd(2, 4, 6, 10) = 60$. Then we can let $\boxed{n = 61.}$ Indeed, by Fermat,

- If $3 \nmid a$, then $a^2 \equiv 1 \pmod 3$, so $a^{60} \equiv 1 \pmod 3$.
- If $5 \nmid a$, then $a^4 \equiv 1 \pmod 5$, so $a^{60} \equiv 1 \pmod 5$.
- If $7 \nmid a$, then $a^6 \equiv 1 \pmod 7$, so $a^{60} \equiv 1 \pmod 7$.
- If $11 \nmid a$, then $a^{10} \equiv 1 \pmod{11}$, so $a^{60} \equiv 1 \pmod{11}$.

Therefore, for all a, we have $a^{61} \equiv a$ *modulo* any of 3, 5, 7, and 11, hence *modulo* their least common multiple, which is 1155.

Remark. This problem is related to Exercise 50 and our discussion of absolute pseudoprimes.

Problem 1.6. *Let* $\mathbb{N} = \{1, 2, 3, \dots\}$. *Suppose all we know about this set is:*

(i) proofs by induction are possible;

(ii) addition can be defined on $\mathbb{N}$*, and it satisfies*

$$x + y = y + x, \qquad x + (y + z) = (x + y) + z;$$

(iii) multiplication can be defined by

$$x \cdot 1 = x, \qquad x \cdot (y + 1) = x \cdot y + x.$$

Prove

$$x \cdot y = y \cdot x.$$

Solution. We use induction on y. As the base step, we show $x \cdot 1 = 1 \cdot x$ for all x. We do *this* by induction: Trivially, $1 \cdot 1 = 1 \cdot 1$. Suppose, as an inductive hypothesis, $x \cdot 1 = 1 \cdot x$ for some x. Then

$$\begin{aligned} 1 \cdot (x + 1) &= 1 \cdot x + 1 && \text{[by definition of multiplication]} \\ &= x \cdot 1 + 1 && \text{[by inductive hypothesis]} \\ &= x + 1 && \text{[by definition of multiplication]} \\ &= (x + 1) \cdot 1. && \text{[by definition of multiplication]} \end{aligned}$$

By induction then, $x \cdot 1 = 1 \cdot x$.

Next we assume $x \cdot y = y \cdot x$ for all x, for some y, and we prove $x \cdot (y + 1) = (y + 1) \cdot x$. We do *this* by induction on x. By what we have already shown, $1 \cdot (y+1) = (y+1) \cdot 1$. Suppose, as an inductive hypothesis, $x \cdot (y+1) = (y+1) \cdot x$ for some x. Then

$$\begin{aligned} (x + 1) \cdot (y + 1) &= (x + 1) \cdot y + x + 1 && \text{[by definition of multiplication]} \\ &= y \cdot (x + 1) + x + 1 && \text{[by the first inductive hypothesis]} \\ &= y \cdot x + y + x + 1 && \text{[by definition of multiplication]} \\ &= x \cdot y + x + y + 1 && \text{[by the first inductive hypothesis]} \\ &= x \cdot (y + 1) + y + 1 && \text{[by definition of multiplication]} \\ &= (y + 1) \cdot x + y + 1 && \text{[by the second inductive hypothesis]} \\ &= (y + 1) \cdot (x + 1). && \text{[by definition of multiplication]} \end{aligned}$$

This completes the proof that $x \cdot (y+1) = (y+1) \cdot x$ for all x. *This* completes the proof that $x \cdot y = y \cdot x$ for all x and y.

Remark. This is part of Exercise 1. I tried to write out a "first generation" proof: one you might write without thinking of how to break it into parts. A proof that is easier to follow is perhaps the "second generation" proof that goes as follows (see Lemma A.3 and Theorem A.3): First show

$$x \cdot 1 = 1 \cdot x \tag{$*$}$$

by induction on x, then show

$$(y+1) \cdot x = y \cdot x + x \tag{$\dagger$}$$

by induction on x, and finally show $x \cdot y = y \cdot x$ by induction on x. In fact, almost all students just *assumed* that $(*)$ and $(\dagger)$ were known; but they were *not* among the propositions that the problem allowed you to use.

E.2. In-term examination

Problem 2.1. *Exactly one of* 1458 *and* 1536 *has a primitive root. Which one, and why? Find a primitive root of the number that has one.*

Solution. $1458 = 2 \cdot 729 = 2 \cdot 3^6$ and $1536 = 3 \cdot 512 = 3 \cdot 2^9$.

The numbers with primitive roots are just 2, 4, p^k, and $2 \cdot p^k$, where p is an *odd* prime.

Therefore 1458, but not 1536, has a primitive root.

$\phi(9) = 6$, and

k	1	2	3	4	5	6	
5^k	5	-2	-1	4	2	1	mod9

so 5 is a primitive root of 9.

Then 5 is a primitive root of 3^6.

Since 5 is odd, it is a primitive root of 1458.

Remark. 1. A number of people computed $\phi(1458)$ and $\phi(1536)$, but this is of no practical use in this problem.

2. Some people pointed out that if a is a primitive root of n, then $a^{\phi(n)} \equiv 1 \pmod{n}$. This is logically correct, but useless, since by Euler's Theorem we have $a^{\phi(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$ (not just when a is a primitive root).

3. Our sequence of theorems about primitive roots of composite numbers is the following. Throughout, p is an odd prime.

(i) If r is a primitive root of p, then r or $r + p$ is a primitive root of p^2.

(ii) If r is a primitive root of p^2, then r is a primitive root of p^s whenever $s \geqslant 2$.

(iii) If r is a primitive root of p^s (where $s \geqslant 2$), then r or $r + p^s$ (whichever is odd) is a primitive root of $2p^s$.

Some people misremembered this sequence, or wrongly combined two of its theorems. For example, some wrote 'If r is a primitive root of p, then r or $r + p^s$ (whichever is odd) is a primitive root of $2p^s$.' This assertion is false. It would be correct to say for example, 'If r is a primitive root of p^2, then r or $r + p^2$ (whichever is odd) is a primitive root of $2p^s$.' Using this, one might observe that 2 is a primitive root of 9, and therefore 11 is a primitive root of 1458.

Problem 2.2. *Remembering that p is always prime, define the arithmetic function ω by*

$$\omega(n) = \sum_{p|n} 1.$$

a) *Define μ, preferably using ω.*

b) *Prove that, if m and n are co-prime, then $\omega(mn) = \omega(m) + \omega(n)$.*

c) *Prove that*

$$\sum_{d|n} \tau(d) \cdot \mu(d) = (-1)^{\omega(n)}.$$

d) *Find a simple description of the function f given by*

$$f(n) = \sum_{d|n} \omega(d) \cdot \mu\Big(\frac{n}{d}\Big).$$

Solution. a) $\mu(n) = \begin{cases} 0, & \text{if } p^2 \mid n \text{ for some } p, \\ (-1)^{\omega(n)}, & \text{if } p^2 \mid n \text{ for no } p. \end{cases}$.

b) Assume m and n are co-prime. If $p \mid mn$, then

$$p \mid m \iff p \nmid n.$$

Therefore

$$\omega(mn) = \sum_{p|mn} 1 = \sum_{p|m} 1 + \sum_{p|n} 1 = \omega(m) + \omega(n).$$

c) Each side of the equation is multiplicative, and

$$\sum_{d|p^k} \tau(d) \cdot \mu(d) = \tau(1) \cdot \mu(1) + \tau(p) \cdot \mu(p) = 1 - 2 = (-1)^{\omega(p^k)}.$$

d) By Möbius inversion,

$$\omega(n) = \sum_{d|n} f(d).$$

Since also $\omega(n) = \sum_{p|n} 1$, we have

$$f(n) = \begin{cases} 1, & \text{if } n \text{ is prime,} \\ 0, & \text{if } n \text{ is not prime.} \end{cases}$$

Remark. 1. In my solution to part a, the condition '$p^2 \mid n$ for no p' is equivalent to '$p^2 \nmid n$ for all p'. Similarly in part d.

2. For part a, some people wrote (as part of their answer) '$\mu(n) = (-1)^s$ if $n = p_1 \cdots p_s$'. Strictly, one must specify that the p_i are all distinct. The best way that I know to do this is to say $p_1 < \cdots < p_s$.

3. As an alternative solution to part b, one can write (as some people did) that, since m and n are co-prime, we have

$$m = {p_1}^{m(1)} \cdots {p_s}^{m(s)}, \qquad n = {q_1}^{n(1)} \cdots {q_t}^{n(t)},$$

where the exponents are positive, $p_1 < \cdots < p_s$, $q_1 < \cdots < q_t$, and $p_i \neq q_j$ in each case, and therefore

$$\omega(mn) = s + t = \omega(m) + \omega(n).$$

This may be a clearer argument than the one I wrote above. I don't know a good way to make the argument just with the Σ-notation. Some people wrote

$$\text{'}\omega(mn) = \sum_{pq|mn} 1\text{'},$$

which doesn't make sense. (If it means anything, it means $\omega(mn)$ is the number of factors d that mn has, where d is the product of two primes, possibly not distinct. This is not what $\omega(mn)$ is.) Others wrote

$$\text{'}\omega(mn) = \sum_{p|m} \sum_{q|n} 1\text{'};$$

this is meaningful, but false, since it makes $\omega(mn)$ equal to the *product* $\omega(m) \cdot \omega(n)$.

4. In part c, it doesn't hurt to say *why* the two sides are multiplicative. The left-hand side is multiplicative because the product of two multiplicative functions is multiplicative (we didn't prove this, but it's fairly obvious), and if g is multiplicative, so is $n \mapsto \sum_{d|n} g(d)$ (we did prove this). The right-hand side is multiplicative by part b.

5. In notation introduced in class, the function f in part d is given by $f = \omega * \mu$, and therefore $\omega = f * 1$ by Möbius inversion. It may not be immediately obvious that f *must* be as in the solution above. But if f *is* that function, then indeed $\omega = f * 1$, and therefore $f = \omega * \mu$, as required. So f must be as given in the solution.

Problem 2.3. *Find the least positive x such that*

$$11^{5117}x \equiv 57 \pmod{600}.$$

Solution. $600 = 2^3 \cdot 3 \cdot 5^2$, so $\phi(600) = 4 \cdot 2 \cdot 20 = 160$. We compute

$$\begin{array}{r|l} & 31 \\ \hline 160 & 5117 \\ & 480 \\ \hline & 317 \\ & 160 \\ \hline & 157 \end{array}.$$

Hence

$$5117 \equiv 157 \equiv -3 \pmod{160}.$$

Therefore

$$\begin{aligned} & 11^{1557}x \equiv 5 \pmod{600} \\ \iff\ & 11^{-3}x \equiv 5 \pmod{600} \\ \iff\ & x \equiv 5 \cdot 11^3 \pmod{600}. \end{aligned}$$

But

$$\begin{aligned} 11^3 = 121 \cdot 11 = 1331 \equiv 131 \pmod{600}, \\ 5 \cdot 131 = 655 \equiv 55 \pmod{600}, \end{aligned}$$

so the least positive solution is $\boxed{55}$.

Remark. Not too many problems here. I'm guessing this is the sort of problem that the *dershane* prepares one for. According to the Wikipedia article 'Long division', my notation for long division is what used in Anglophone countries; the notation I see on papers, Francophone. But the symbolism $b\,)\,a$ (used in the former notation) for a/b is traced to Michael Stifel of the University of Jena in Germany in 1544 (see the Wikipedia article 'Division (mathematics)').

Problem 2.4. a) *Since 2 is a primitive root of 29, the function $x \mapsto \log_2 x$ from $\mathbb{Z}_{29}{}^\times$ to $\mathbb{Z}_{28}$ is defined. Considering this as a function from $\{-14, \dots, -1, 1, \dots 14\}$*

to $\{-14, \ldots, 14\}$*, fill out the table below.*

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$														
$\log_2(-m)$														

b) *With respect to the modulus* 29*, exactly one of the two congruences*

$$x^{400} \equiv 13, \qquad\qquad x^{400} \equiv -13$$

*has a solution. Find all of its solutions (*modulo 29*), and explain why the other congruence has no solutions.*

Solution. a)

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$	0	1	5	2	-6	6	12	3	10	-5	-3	7	-10	13
$\log_2(-m)$	14	-13	-9	-12	8	-8	-2	-11	-4	9	11	-7	4	-1

b) For the first congruence, we have

$$\begin{aligned} & x^{400} \equiv 13 \pmod{29} \\ \iff & 400 \log x \equiv -10 \pmod{28} \\ \iff & 200 \log x \equiv -5 \pmod{14}; \end{aligned}$$

the congruence has no solution since $\gcd(200, 14) = 2$, and $2 \nmid -5$. For the second congruence:

$$\begin{aligned} & x^{400} \equiv -13 \pmod{29} \\ \iff & 400 \log x \equiv 4 \pmod{28} \\ \iff & 100 \log x \equiv 1 \pmod{7} \\ \iff & 2 \log x \equiv 1 \pmod{7} \\ \iff & \log x \equiv 4 \pmod{7} \\ \iff & \log x \equiv 4, 11, -10, -3 \pmod{28} \\ \iff & x \equiv -13, -11, 13, 11 \pmod{29}. \end{aligned}$$

Remark. The quickest way I know to fill out the table is, keeping in mind

$$\log_2 m \equiv k \bmod 28 \iff 2^k \equiv m \bmod 29,$$

to start out as follows,

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$	0	1		2				3						
$\log_2(-m)$													4	

continuing to get

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$	0	1	5	2		6	12	3	10			7		13
$\log_2(-m)$	14				8					9	11		4	

then filling in the remaining spaces by using

$$\log m - \log(-m) \equiv \log(-1) \equiv \pm 14 \pmod{28}.$$

Some people may have done something like this, but they put the logarithms into the set $\{0, \dots, 27\}$ rather than $\{-14, \dots, 14\}$ as requested (this set could have been $\{-13, \dots, 14\}$. Other people gave negative logarithms, but they were off by 1, as if the modulus had been taken as 29 rather than 28. In solving the congruences, there were various confusions about modulus.

E.3. Final examination

Problem 3.1. *Find all solutions of the congruence*

$$x^{2821} \equiv x \pmod{2821}.$$

Solution. Every integer would be a solution if 2821 were a prime or a Carmichael number. It factorizes as $7 \cdot 403$, hence as $7 \cdot 13 \cdot 31$, which is squarefree. Also $2820 = 10 \cdot 2 \cdot 141 = 2^2 \cdot 3 \cdot 5 \cdot 47$, so it is divisible by 6, 12, and 30. Therefore 2821 is a Carmichael number, and $\boxed{\text{all integers}}$ solve the given congruence.

Problem 3.2. *Find all solutions to the congruence* $x^2 \equiv 23 \pmod{133}$.

Solution. $133 = 7 \cdot 19$, so we solve simultaneously

$$x^2 \equiv 23 \pmod{7}, \qquad x^2 \equiv 23 \pmod{19}.$$

For the first, $x^2 \equiv 2 \equiv 9$, so $x \equiv \pm 3$ (7); for the second, $x^2 \equiv 4$, so $x \equiv \pm 2$ (19). Now we have some Chinese remainder problems: First,

$$x \equiv \pm 3 \pmod{7}, \qquad x \equiv \pm 2 \pmod{19},$$

that is, $x \equiv \pm(3 \cdot 19 \cdot 3 + 2 \cdot 7 \cdot -8) \equiv \pm 59$ (133), since $19 \equiv -2$ (7) and $-2 \cdot 3 \equiv 1$ (7), while $7 \cdot -8 \equiv 1$ (19). Second,

$$x \equiv \pm 3 \pmod{7}, \qquad x \equiv \mp 2 \pmod{19},$$

that is, $x \equiv \pm(3 \cdot 19 \cdot 3 - 2 \cdot 7 \cdot -8) \equiv \pm 283 \equiv \pm 17 \pmod{133}$. The solutions to the original problem are therefore $\boxed{x \equiv \pm 59, \pm 17 \pmod{133}}$.

Problem 3.3. *Is the following congruence soluble? Explain. (It is given that* 2999 *is prime.)*

$$x^2 - 2987x + 2243 \equiv 0 \pmod{2999}.$$

Solution. By completing the square, the congruence is equivalently

$$\begin{aligned} x^2 + 12x &\equiv 756, \\ (x+6)^2 &\equiv 792. \end{aligned}$$

Also, $792 = 2^3 \cdot 3^2 \cdot 11$, so

$$\begin{aligned} \left(\frac{792}{2999}\right) &= \left(\frac{2}{2999}\right)\left(\frac{11}{2999}\right) \\ &= \left(\frac{11}{2999}\right) && \text{[since } 2999 \equiv -1 \pmod{8}\text{]} \\ &= -\left(\frac{2999}{11}\right) && \text{[since } 11 \equiv 3 \equiv 2999 \pmod{4}\text{]} \\ &= -\left(\frac{-4}{11}\right) \\ &= -\left(\frac{-1}{11}\right) \\ &= 1; && \text{[since } 11 \equiv 3 \pmod{4}\text{]} \end{aligned}$$

therefore there must be a solution.

Problem 3.4.

a) *Find an arithmetic function that is* not *multiplicative.*

b) *Prove that, for all positive integers* n*,*

$$\sum_{d|n} \sum_{e|n/d} \phi(e) = \sum_{d|n} d.$$

Solution. a) $n \mapsto 2$.

b) By a theorem of Gauss,

$$\sum_{d|n} \sum_{e|n/d} \phi(e) = \sum_{d|n} n/d = \sum_{d|n} d.$$

Remark. Various approaches are possible. One may, for example, write the desired equation as $1 * \phi * 1 = 1 * \mathrm{id}$, and this follows from Gauss's theorem, expressed as $1 * \phi = \mathrm{id}$. If one does not remember Gauss's Theorem, one may let $f(n) = \sum_{d|n} \phi(d)$, so that

$$\sum_{d|n} \sum_{e|n/d} \phi(e) = \sum_{d|n} f(n/d) = \sum_{d|n} f(d).$$

Then it is enough to prove $f(n) = n$; but each side of this equation is am multiplicative function of n, and $f(p^k) = \sum_{j=0}^{k} \phi(p^j) = 1 + \sum_{j=1}^{k} (p^j - p^{j-1}) = p^k$.

Problem 3.5. *Describe,* as well as possible, *the set of primes q such that 2 is a primitive root of q* and $q = 2^n \cdot p + 1$ *for some prime p. (In particular, first find the possibilities for n, and then p.)*

Solution. If $n = 0$, then p can only be 2, and then $q = 3$, which is in the desired set.

Now suppose q is as desired, but not 3, so $n \geqslant 1$. A primitive root cannot be a square, so we must have $(2/q) = -1$, that is, $q \equiv \pm 3 \ (8)$, and therefore $n \leqslant 2$.

If $n = 1$, then for the same reason, we must have $2p+1 \equiv 3, 5 \ (8)$, equivalently, $2p \equiv 2, 4 \ (8)$, that is, $p \equiv 1, 2 \ (4)$. If $p \equiv 2 \ (4)$, then $p = 2$, so $q = 5$; of this, 2 is a primitive root, so 5 is in the desired set.

Suppose conversely $p \equiv 1 \ (4)$, so $q \geqslant 11$ and $q \equiv 3 \ (8)$. By Euler's Criterion, $-1 = (2/q) \equiv 2^p \ (q)$, so $\mathrm{ord}_q(2) \neq p$. But this order can only be 1, 2, p or $q - 1$, and it is not 1 or 2 (since $q \geqslant 11$), so it must be $q - 1$. Therefore 2 is a primitive root of a prime number $2p + 1$ if and only if $p \equiv 1 \ (4)$.

Now suppose $n = 2$. Then $(2/q) = -1$ if and only if $4p \equiv 2, 4 \ (8)$, that is, $p \equiv 1 \ (2)$, which is always the case (since p is odd). So we have $\mathrm{ord}_q(2) \nmid 2p$. Also the order is not 4 when $p = 3$ or when $p \geqslant 5$—that is, ever. Therefore, 2 is a primitive root of every prime number $4p + 1$.

In sum, the desired set consists of:

- 3;
- primes $2p + 1$, where $p \equiv 1 \pmod 4$;
- primes $4p + 1$.

Bibliography

[1] W. R. Alford, Andrew Granville, and Carl Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3):703–722, 1994.

[2] Hippocrates G. Apostle. *Aristotle's Physics*. The Peripatetic Press, Grinnell, Iowa, 1980. Translated with Commentaries and Glossary.

[3] Archimedes. *The works of Archimedes. Vol. I*. Cambridge University Press, Cambridge, 2004. The two books on the sphere and the cylinder, Translated into English, together with Eutocius' commentaries, with commentary, and critical edition of the diagrams by Reviel Netz.

[4] V. I. Arnol′d. On the teaching of mathematics. *Russian Mathematical Surveys*, 53(1):229–234, 1998.

[5] Carl B. Boyer. *A history of mathematics*. John Wiley & Sons Inc., New York, 1968.

[6] Cesare Burali-Forti. A question on transfinite numbers (1897). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 104–12. Harvard University Press, 1976.

[7] David M. Burton. *Elementary Number Theory*. McGraw-Hill, Boston, sixth edition, 2007.

[8] R. D. Carmichael. Note on a new number theory function. *Bull. Amer. Math. Soc.*, 16(5):232–238, 1910.

[9] Richard Dedekind. *Essays on the theory of numbers. I: Continuity and irrational numbers. II: The nature and meaning of numbers*. authorized translation by Wooster Woodruff Beman. Dover Publications Inc., New York, 1963.

[10] Leonard Eugene Dickson. *History of the Theory of Numbers*, volume 1. Chelsea, New York, 1952.

[11] P. Erdős. Beweis eines Satzes von Tschebyschef (in German). *Acta Litt. Sci. Szeged*, 5:194–198, 1932. Available at `http://www.renyi.hu/~p_erdos/1932-01.pdf` (as of December 3, 2010).

[12] Euclid. *The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix*. Dover Publications Inc., New York, 1956. Translated with introduction and commentary by Thomas L. Heath, 2nd ed.

[13] Euclid. *Euclid's Elements*. Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, the Thomas L. Heath translation, edited by Dana Densmore.

[14] H. W. Fowler. *A Dictionary of Modern English Usage*. Oxford University Press, second edition, 1982. revised and edited by Ernest Gowers.

[15] H. W. Fowler. *A Dictionary of Modern English Usage*. Wordsworth Editions, Ware, Hertfordshire, UK, 1994. reprint of the original 1926 edition.

[16] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, 1986. Translated into English by Arthur A. Clarke, revised by William C. Waterhouse.

[17] D. A. Goldston, J. Pintz, and C. Y. Yıldırım. `http://arxiv.org`, 2005. arXiv:math/0508185v1 [math.NT].

[18] Timothy Gowers. *Mathematics*. Oxford University Press, Oxford, 2002. A very short introduction.

[19] Timothy Gowers, June Barrow-Green, and Imre Leader, editors. *The Princeton companion to mathematics*. Princeton University Press, Princeton, NJ, 2008.

[20] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. `http://arxiv.org`, 2004. arXiv:math/0404188v6 [math.NT].

[21] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[22] Thomas Heath. *A history of Greek mathematics. Vol. I*. Dover Publications Inc., New York, 1981. From Thales to Euclid, Corrected reprint of the 1921 original.

[23] James Ivory. Demonstration of a theorem respecting prime numbers. In Thomas Leybourn, editor, *New Series of the Mathematical Repository*, volume I, chapter II, pages 6–8. W. Glendinning, London, 1806.

[24] Victor J. Katz, editor. *The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook*. Princeton University Press, Princeton and Oxford, 2007.

[25] Edmund Landau. *Elementary number theory*. Chelsea Publishing Co., New York, N.Y., 1958. Translated by J. E. Goodman.

[26] Edmund Landau. *Foundations of Analysis. The Arithmetic of Whole, Rational, Irrational and Complex Numbers*. Chelsea Publishing Company, New York, N.Y., third edition, 1966. translated by F. Steinhardt; first edition 1951; first German publication, 1929.

[27] Barry Mazur. How did Theaetetus prove his theorem? In P. Kalkavage and E. Salem, editors, *The Envisoned Life: Essays in honor of Eva Brann*. Paul Dry Books, 2007. `http://www.math.harvard.edu/~mazur/preprints/Eva.pdf`, accessed September 20, 2012.

[28] Nicomachus of Gerasa. *Introduction to Arithmetic*, volume XVI of *University of Michigan Studies, Humanistic Series*. University of Michigan Press, Ann Arbor, 1938. First printing, 1926.

[29] Giuseppe Peano. The principles of arithmetic, presented by a new method (1889). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 83–97. Harvard University Press, 1976.

[30] Srinivasa Ramanujan. A proof of Bertrand's postulate. *Journal of the Indian Mathematical Society*, XI:181–2, 1919. Available at `http://www.imsc.res.in/~rao/ramanujan/CamUnivCpapers/Cpaper24/page1.htm` (as of December 3, 2010).

[31] Bertrand Russell. Letter to Frege (1902). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 124–5. Harvard University Press, 1976.

[32] Lucio Russo. *The forgotten revolution*. Springer-Verlag, Berlin, 2004. How science was born in 300 BC and why it had to be reborn, Translated from the 1996 Italian original by Silvio Levy.

[33] Filip Saidak. A new proof of Euclid's theorem. *The American Mathematical Monthly*, 113(10):937–8, Dec. 2006.

[34] D. J. Struik, editor. *A source book in mathematics, 1200–1800*. Princeton Paperbacks. Princeton University Press, Princeton, NJ, 1986. Reprint of the 1969 edition.

[35] Théon de Smyrne. *Exposition des connaissances mathématiques utiles pour la lecture de Platon*. Hachette, Paris, 1892. Greek text, with French translation by J. Dupuis.

[36] Ivor Thomas, editor. *Selections illustrating the history of Greek mathematics. Vol. I. From Thales to Euclid*. Harvard University Press, Cambridge, Mass., 1951. With an English translation by the editor.

[37] Ivor Thomas, editor. *Selections illustrating the history of Greek mathematics. Vol. II. From Aristarchus to Pappus*. Harvard University Press, Cambridge, Mass, 1951. With an English translation by the editor.

[38] Jean van Heijenoort. *From Frege to Gödel. A source book in mathematical logic, 1879–1931*. Harvard University Press, Cambridge, Mass., 1967.

[39] John von Neumann. On the introduction of transfinite numbers (1923). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 346–354. Harvard University Press, 1976.

Index

abelian group, 31
absolute pseudo-prime, 76
algebraic, 34
archimedean property of $\mathbb{R}$, 39
arithmetic function, 84

Bézout's Lemma, 43
base of induction, 26
Bertrand's Postulate, 61

Carmichael, — number, 76
Cauchy sequence, 24, 34
Chinese Remainder Problem, 93
Chinese remainder problem, 66
class, 139
closed form, 11
co-prime, 43
commutative ring, 31
complete, 34
complete set of residues, 40
completely multiplicative function, 154
completion, 33
composite number, 51
congruent numbers, 38
conjugate, 136
convolution, 89
countable, 34
cut, 33

dense, 33
Diophantine equation, 20
divides, divisor, 36

element, 139
Euclid, 43
—'s Theorem, 51, 57, 69
Euclidean algorithm, 47
Euler, 95, 128
— phi-function, 95
—'s Criterion, 120
—'s Theorem, 95, 136

Fermat, 20
— number, — prime, 154
—'s Theorem, 72
Fermat's Last Theorem, 20
field, 32
first natural number, 26
function
arithmetic —, 84
completely multiplicative —, 154
Euler phi-—, 95
homomorphism, 106
isomorphism, 106
Möbius function, 87
multiplicative —, 85
unit —, 88
Fundamental Theorem of Arithmetic, 52

Gamma function, 35, 59
Gauss, 38
—'s Lemma, 124
—'s Theorem, 97
geometric series, 58
Germain, — prime, 71, 126
greatest common divisor, 41
greatest integer, 39
group, 106

abelian —, 31

harmonic series, 58
Hasse diagram, 37
homomorphism, 106

ideal, 36, 42
incommensurable, 20
induction, 11, 26
inductive condition, 26
inductive hypothesis, 26
strong —, 28
infinite descent, 20
integral domain, 32
inverse, 66
irreducible, 53
isomorphism, 106

Jacobi symbol, 154

Korselt's Criterion, 77, 109

Lagrange, —'s Theorem, 107
least common multiple, 44
Legendre, 122, 128
— symbol, 122
Leibniz, 77
linear ordering, 28
logarithm, 59
look, 11

measure, 20
member, 139
Mersenne, 70
— number, 70
— prime, 70, 154
Möbius, 87
— Inversion, 88
— function, 87
modulus, *modulo*, 38
multiplicative function, 85
completely —, 154

natural logarithm, 59
natural number, 25
negative, 32
non-residue, quadratic, 120
number, *see also* prime
Carmichael —, 76
composite —, 51
congruent —s, 38
first natural —, one, 26
Mersenne —, 70
natural —, 25
one, 26
pentagonal —, 145
perfect —, 69
predecessor, 28
squarefree —, 77
successor, 26
triangular —, 11

one, 26
open subset, 33
order, 74, 102
ordered commutative ring, 32
ordered field, 32
ordering, 37
linear —, 28
well ordered, 29
ordinal number, ordinal, 140

Peano axioms, 25
pentagonal number, 145
perfect number, 69
Pigeonhole Principle, 133, 135
positive, 32
predecessor, 28
prime, 43, 53
Germain —, 71, 126
absolute pseudo-—, 76
Fermat —, 154
Mersenne —, 70, 154
pseudo-—, 75
relatively —, co-—, 43

twin —s, 144
prime number, 51
primitive root, 77, 81, 105
proof
— by induction, 26
— by infinite descent, 20
pseudo-prime, 75
absolute —, 76

quadratic
— non-residue, 120
— residue, 119
quadratic residue, nonresidue, 81
quaternion, 136

rational numbers, 32
real number, 33
recursive definition, 11
relatively prime, 43
remainder
Chinese — problem, 93
residue, 38
complete set of —s, 40
quadratic —, 119
quadratic non-—, 120
Riemann zeta function, 59
ring, 31, 106

set, 139
square root, 34
squarefree number, 77
Stirling's approximation, 59
strict linear ordering, 28
strong inductive hypothesis, 28
subclass, 139
successor, 26
supremum, 33

Theon of Smyrna, 14, 40
theorem
Euclid's Th—, 51, 57, 69
Euler's Criterion, 120
Euler's Th—, 95, 136
Fermat's Last Th—, 20
Fermat's Th—, 72
Fundamental Th— of Arithmetic, 52
Gauss's Lemma, 124
Gauss's Th—, 97
Lagrange's Th—, 107
Möbius Inversion, 88
Pigeonhole Principle, 133, 135
Wilson's Th—, 80
topology, 33
transfinite, 142
transitive class, 139
triangular number, 11
twin primes, 144

uncountable, 34
unit function, 88
unit of a ring, 53

well ordered, 29
Wilson, —'s Theorem, 80

zero, 32