Elementary Number Theory

David Pierce

September 29, 2010

Mathematics Department
Middle East Technical University
Ankara 06531 Turkey
http://metu.edu.tr/~dpierce/
dpierce@metu.edu.tr

Preface

This book is for the course Elementary Number Theory (Math 365), given at METU in 2010/11. The book is based on my lectures in the same course, 2007/8. The lectures were based—and hence this book is based—mainly on Burton's text, *Elementary Number Theory* [2]. I have made a few additions. Also, where it makes sense, I try to display the mathematics in pictures or tables, as for example in Chapter 1 and in the account of the Chinese Remainder Theorem given in § 9.1.

Math 365 has this catalogue description:

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

I ask students in addition to know something of the logical foundations of number theory. Appendix A contains an account of these foundations, namely a derivation of basic arithmetic from the so-called Peano Axioms.

Appendix B contains the exercises made available to the 2007/8 class; Appendix C, the examinations given to that class, along with my solutions. 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 exercise should be done; and yet there are no such hints on examinations. Whereas the exercises in this book were originally found in 11 separate documents, issued roughly once a week, here the exercises are strung together in one numbered sequence. I have not changed the order of the exercises.

In the 2007/8 class, I defined the set $\mathbb{N}$ of natural numbers as $\{0, 1, 2, 3, \dots\}$; in the present book, I have decided to define it as $\{1, 2, 3, \dots\}$. I have tried to make the appropriate changes, except in Appendix C, but I may have missed something. I have not changed the examinations.

Full names and dates of mathematicians given in the text are taken from the MacTutor History of Mathematics archive, `http://www-gap.dcs.st-and.ac.uk/~history/index.html`. However, I have not tried to trace the origin of all of the mathematics in these notes.

Contents

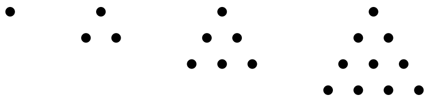
1. Proving and seeing

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. The numbers have an appearance, a **look:**



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

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

The triangular numbers can also be given in various **closed forms:**

$$t_n = \sum_{k=1}^{n} k = \binom{n+1}{2} = \frac{n(n+1)}{2}. \tag{$*$}$$

Indeed, we can prove this 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

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

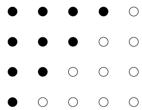
so the claim is true when $n = k + 1$.

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

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

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

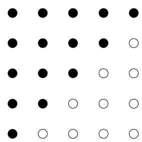
Two copies of t_n do indeed fit together to make an $n \times (n+1)$ array of dots:



Similarly, $t_{n+1} + t_n = (n+1)^2$, since

$$t_{n+1} + t_n = \frac{(n+1)(n+2)}{2} + \frac{n(n+1)}{2} = \frac{n+1}{2}(n+2+n) = (n+1)^2;$$

but this can be seen in a picture:



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, that is,

$$\sum_{k=1}^{n} (2k-1) = n^2. \tag{†}$$

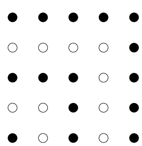
We can prove this by induction:

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. A picture shows why:



Finally, observe:

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

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

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

and prove it. (The theorem was apparently known to Nicomachus of Gerasa [10, II.20.5, p. 263], almost 2000 years ago.)

1.2. Patterns that fail

This is from Arnol′d's talk 'On the teaching of mathematics' [1]. Write the odd numbers as sums of odd numbers of summands:

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

and so on. Then we have

n	# sums for n
1	1
3	2
5	4
7	8
9	16
11	29

Thus the pattern $2^0, 2^1, 2^2, \dots$ breaks down. Is there a formula for the sequence of numbers of sums?

1.3. Incommensurability

Theorem 1. *No numbers solve the equation*

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

Proof. Suppose $a^2 = 2b^2$. 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

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

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 numbers. Therefore no a and b exist such that $a^2 = 2b^2$. □

The proof here is said to be by the method of **infinite descent.** Geometrically, the theorem is that the side and diagonal of a square are **incommensurable:** there is no line segment that evenly divides each of them. We can see this as follows [4, v. I, p. 19]. In Fig. 1.1, there is a square, $ABCD$. On the diagonal BD, the distance BE is marked equal to AB. The perpendicular at E meets AD at F. The straight line BF is drawn. Then triangles ABF and EBF are congruent, so $EF = AF$. Also, triangle DEF is similar to DAB, so $DE = EF$. Suppose a straight line d measures both AB and BD. Then it measures ED and DF, since

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

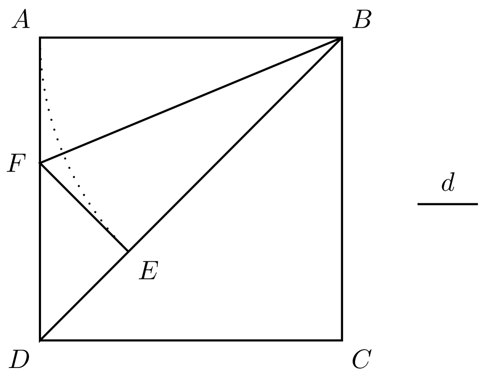


Figure 1.1. Incommensurability of diagonal and side

The same construction can be performed with triangle DEF in place of DAB. Since $2ED < AB$, there will eventually be segments that are shorter than d, but are measured by it, which is absurd. So such d 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 $a_3 = a_1 - 2a_2$, and continue recursively by defining

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

Then by induction

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

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

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

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

$$\frac{b_{n+2}}{b_{n+1}} = 2 + \frac{b_n}{b_{n+1}} = 2 + \cfrac{1}{\cfrac{b_{n+1}}{b_n}} = 2 + \cfrac{1}{2 + \cfrac{b_n}{b_{n-1}}} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{b_{n-1}}{b_{n-2}}}} = \cdots$$

If we just let $b_1 = 1$ and $b_2 = 2$, then by (‡) we get the sequence

$$1, 2, 5, 12, 27, 66, \ldots$$

Then the sequence

$$\frac{2}{1}, \frac{5}{2}, \frac{12}{5}, \frac{27}{12}, \frac{66}{27}, \ldots$$

of fractions converges to $\sqrt{2} + 1$ (though we haven't proved this). One writes

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

2. Numbers

2.1. The natural numbers

The *numbers* heretofore mentioned, namely 1, 2, 3, and so on, are more precisely the **natural numbers.** They compose the set $\mathbb{N}$. Everything about $\mathbb{N}$ follows from the following five conditions.

1. There is a **first** natural number, **one** or 1.
2. Each n in $\mathbb{N}$ has a **successor,** $\mathrm{s}(n)$.
3. The number 1 is not a successor.
4. Distinct numbers have distinct successors: if $n \neq m$, then $\mathrm{s}(n) \neq \mathrm{s}(m)$.
5. **proof by induction** is possible: a subset A of $\mathbb{N}$ is the whole set, provided
    a) $1 \in A$, and
    b) whenever $n \in A$, then also $\mathrm{s}(n) \in A$.

Theorem 2 (Recursion)**.** *Suppose A is a set with 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 $\mathbb{N}$.*

For the proof, see Appendix A. We now define addition by defining $x \mapsto m+x$ recursively:

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

Now the function g in the Recursion Theorem is such that

$$g(1) = b, \qquad\qquad g(n + 1) = f(g(n)).$$

We can then define multiplication by

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

Also the ordering of $\mathbb{N}$ is defined recursively by the requirements

$$x \nless 1, \qquad\qquad x < m + 1 \iff x \leqslant m.$$

Really we have defined the function $m \mapsto \{x\colon x < m\}$ recursively. Here $\{x\colon x < m\}$ is the set of **predecessors** of m. Then the usual properties can be proved, usually by induction (exercise; see Appendix A).

Some books suggest wrongly that everything about $\mathbb{N}$ is a consequence of:

Theorem 3 (Well Ordering Principle). *Every non-empty subset of* $\mathbb{N}$ *has a least element.*

Here the **least** element of a set A of natural numbers is some k such that
a) $k \in A$;
b) if $m \in A$, then $k \leqslant m$.

Let's try to prove the WOP (the Well Ordering Principle). Suppose $A \subseteq \mathbb{N}$, and A has no least element. We want to show that A is empty, that is, $\mathbb{N} \smallsetminus A = \mathbb{N}$. Try induction. For the base step, we cannot have $1 \in A$, since then 1 would be the least element of A. So $1 \notin A$.

For the inductive step, suppose $n \notin A$. This is not enough to establish $n+1 \notin A$, since maybe $n-1 \in A$, so $n+1$ can be in A without being least. We need to use the following.

Theorem 4 (Strong Induction). *Suppose* $A \subseteq \mathbb{N}$, *and for all* n *in* $\mathbb{N}$, *if all predecessors of* n *belong to* A, *then* $n \in A$. *Then* $A = \mathbb{N}$.

For the proof, see Appendix A. Now we can prove well-ordering: If A has no least element, and no member of the set $\{x \in \mathbb{N}\colon x < n\}$ belongs to A, then A must not belong either. Therefore, by strong induction, $A = \varnothing$.

2.2. The integers

The **integers** compose the set

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

denoted by $\mathbb{Z}$. Then we extend addition and multiplication to $\mathbb{Z}$, and we define additive inversion on $\mathbb{Z}$, so that

$$\begin{aligned} a + (b + c) &= (a + b) + c & a \cdot (b \cdot c) &= (a \cdot b) \cdot c, \\ b + a &= a + b, & b \cdot a &= a \cdot b, \\ a + 0 &= a, & a \cdot 1 &= a, \\ a + (-a) &= 0, \end{aligned}$$

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Then $\mathbb{Z}$ is a **commutative ring.** We also extend the ordering to $<$ so that

$$a < b \Rightarrow a + c < b + c,$$
$$0 < a \mathbin{\&} 0 < b \Rightarrow 0 < a \cdot b.$$

Then $\mathbb{Z}$ is an **ordered** commutative ring. An integer a is **positive** if $a > 0$; **negative,** if $a < 0$.

2.3. Other numbers

Given integers a and b, where $b \neq 0$, we can form the **rational number**

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

or a/b. The properties of rational numbers follow from the rule

$$\frac{a}{b} = \frac{x}{y} \iff ay = bx.$$

The set of rational numbers is denoted by $\mathbb{Q}$ and is an **ordered field,** of which $\mathbb{Z}$ is an ordered sub-ring. Then $\mathbb{Q}$ has a **completion,** the set $\mathbb{R}$ of **real numbers;** this is a complete ordered field. The (unordered) field $\mathbb{C}$ of **complex numbers** consists of the formal sums $x + y\mathrm{i}$, where x and y are in $\mathbb{R}$ and $\mathrm{i}^2 = -1$.

Every equation $a + bx = 0$, where a and b are integers, and $b \neq 0$, has a solution in $\mathbb{Q}$, namely $-a/b$. In particular, there is a solution when $b = 1$; but then the solution is just $-a$, an integer. More generally, if a_0, …, a_{n-1} are integers, a solution in $\mathbb{C}$ to an equation

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

is called an **algebraic integer.** The algebraic integers are the subject of **algebraic number theory.** 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.** That part of number theory that makes use of analysis is **analytic number theory.** One may observe for example that the function given by

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

satisfies $\Gamma(n+1) = n\Gamma(n)$, and $\Gamma(1) = 1$, so that $G(n+1) = n!$.

Our subject is **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.

3. Divisibility

3.1. Division and congruence

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

$$(a).$$

Then $b \in (a)$ if and only if a **divides** b, or a is a **divisor** of b; this situation is denoted by

$$a \mid b.$$

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

$$b \equiv c \pmod{a},$$

saying b and c are **congruent** with respect to the **modulus** a, or b and c are congruent ***modulo*** a; also c is a **residue** of b *modulo* a.

(This terminology and notation appear to be due to Johann Carl Friedrich Gauss, 1777–1855; they and many results in this book are set forth in Gauss's *Disquisitiones Arithmeticae* [7].) If the modulus a is understood, we might write simply

$$b \equiv c.$$

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

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

If $a = 0$, then congruence *modulo* a is equality. Otherwise, there are $|a|$ congruence-classes *modulo* a, namely the classes of 0, 1, ..., $|a| - 1$. This is by the Division Theorem below.

Lemma. *If $0 < a < b$, then $b < na$ for some n in $\mathbb{N}$.*

Proof. Suppose if possible $na \leqslant b$ for all n in $\mathbb{N}$. By the Well Ordering Principle, we may assume b is the *least* integer with this property. Then $na = b$ for some n in $\mathbb{N}$ (by minimality of b), so $(n+1)a > na = b$, which contradicts the original assumption. □

The property of $\mathbb{N}$ given by the lemma is that it is **archimedean.**

Theorem 5 (Division)**.** *If a and b are integers, and $a \neq 0$, then the system*

$$b = ax + y, \qquad\qquad 0 \leqslant y < |a|$$

has a unique solution.

Proof. The set $\{z \in \mathbb{N} \colon z = b - ax \text{ for some } x \text{ in } \mathbb{Z}\}$ is non-empty (why?). Let r be its least element (which exists by the Well Ordering Principle), and let q be such that $r = b - aq$. Then $b = aq + r$ and $0 \leqslant r < |a|$. □

In the notation of the proof, q is the number times that a *goes into* b, and r is the **remainder.**

Every square has the form $3n$ or $3n+1$. Indeed, every number is $3k$ or $3k+1$ or $3k+2$, and

$$\begin{aligned}(3k)^2 &= 9k^2 = 3(3k^2),\\ (3k+1)^2 &= 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1,\\ (3k+2)^2 &= 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1.\end{aligned}$$

An alternative argument can make use of the following:

Theorem 6. *If $a \equiv b$ and $c \equiv d$, then*

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

Proof. If $n \mid b - a$ and $n \mid d - c$, then $n \mid b - a + d - c$, that is,

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

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

$$n \mid bd - ac.$$

□

In particular, congruent numbers have congruent squares. Since

$$0^2 = 0, \qquad 1^2 = 1, \qquad 2^2 = 4 \equiv 1 \pmod 3,$$

again we conclude that every square is $3n$ or $3n+1$ for some n.

As suggested above, with respect to a positive modulus n, every integer is congruent to exactly one of the integers $0, 1, \dots, n-1$. Therefore these integers are said to compose a **complete set of residues** *modulo* n. Another complete set of residues *modulo* n is the set of a such that

$$-\frac{n}{2} < a \leqslant \frac{n}{2}.$$

Hence for example every cube is $7n$ or $7n \pm 1$, since

$$0^3 \equiv 0, \quad (\pm 1)^3 \equiv \pm 1, \quad (\pm 2)^3 \equiv \pm 8 \equiv \pm 1, \quad (\pm 3)^3 \equiv \pm 27 \equiv \mp 1 \pmod{7}.$$

Some properties of divisibility are:

$$\begin{gathered}
a \mid 0; \\
0 \mid a \iff a = 0; \\
1 \mid a \;\&\; a \mid a; \\
a \mid b \;\&\; b \neq 0 \Rightarrow |a| \leqslant |b|; \\
a \mid b \;\&\; b \mid c \Rightarrow a \mid c \\
a \mid b \;\&\; c \mid d \Rightarrow ac \mid bd; \\
a \mid b \Rightarrow a \mid bx; \qquad (*) \\
a \mid b \;\&\; a \mid c \Rightarrow a \mid b + c. \qquad (\dagger)
\end{gathered}$$

3.2. Greatest common divisors

By the last two implications, $(*)$ and $(\dagger)$, 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

$$(a, b).$$

Then $(0, 0) = (0)$. Otherwise, assuming one of a and b is not 0, let k be the least positive element of (a, b). Then k divides a and b. Indeed, $a = kq + r$ 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 $k \mid a$. Similarly, $k \mid b$. Thus k is a common divisor of a and b. Indeed, k is the **greatest**

common divisor of a and b, that is, if $d \mid a$ and $d \mid b$, then $d \mid k$. This is so, since k is a linear combination of a and b. We write then

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

We have also

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

we can conclude then that $\mathbb{Z}$ is a **principal ideal domain.** Indeed, immediately, $(k) \subseteq (a, b)$. Also, as k divides a and b, it divides every element of (a, b), so $(a, b) \subseteq (k)$.

If $\gcd(a, b) = 1$, then a and b are **relatively prime** or **co-prime.** So this is the case if and only if the equation

$$ax + by = 1$$

has a solution. In general, if $\gcd(a, b) = k$, then

$$\gcd\left(\frac{a}{k}, \frac{b}{k}\right) = 1,$$

since both $ax + by = k$ and $(a/k)x + (b/k)y = 1$ have solutions.

Suppose a and b are co-prime, and each divides c; then so does ab. Indeed, the following have solutions:

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

where $c = bs = ar$. Euclid proves the following in Proposition VII.30 of the *Elements* [4, 5], though his *statement* of the theorem assumes a is *prime* (see p. 26).

Theorem 7 (Euclid, VII.30)**.** *If* $a \mid bc$ *and* $\gcd(a, b) = 1$*, then* $a \mid c$*.*

Proof. Again, the following have solutions:

$$\begin{aligned} ax + by &= 1, \\ acx + bcy &= c. \end{aligned}$$

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

3.3. Least common multiples

The positive divisors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60. These twelve numbers can be arranged in a so-called **Hasse diagram** with respect to divisibility; see Fig. 3.1. Here a line is drawn from a number a up to a number b

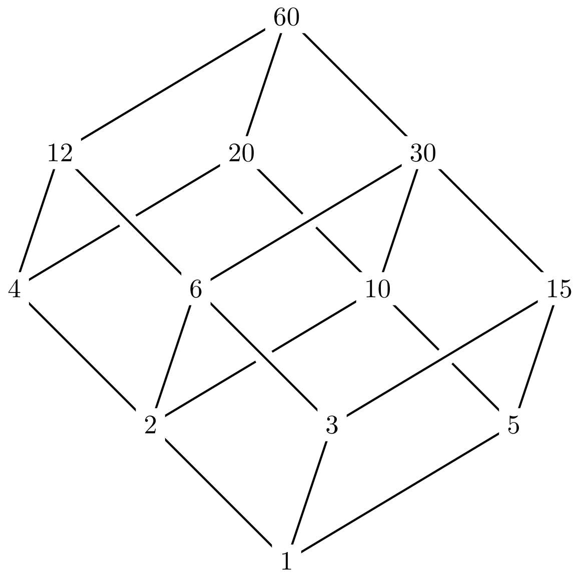


Figure 3.1. Divisors of 60

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 there is a path upwards from a to b. Then greatest common divisors can be read off the diagram; for example, $\gcd(12, 15) = 3$. By the symmetry of the diagram, it follows that the *least common multiple* of $60/12$ and $60/15$ is $60/3$; that is,

$$\operatorname{lcm}(5, 4) = 20.$$

Recall that $(a, b) = \{\text{linear combinations of } a \text{ and } b\}$; its least positive element (if one of a and b is not 0) is $\gcd(a, b)$. Let this be k. We showed

$$(a, b) = (k). \tag{‡}$$

The set $(a) \cap (b)$ consists of the common multiples of a and b; so its least positive

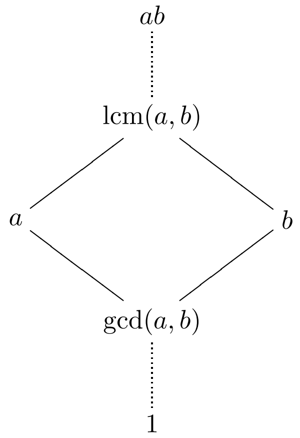


Figure 3.2. gcd and lcm

element is the **least common multiple** of a and b, or

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

Suppose this is m. As we showed (‡), so we can show

$$(a) \cap (b) = (m).$$

Indeed, suppose n is a common multiple of (a) and (b), that is, $n \in (a) \cap (b)$. Then $n = mq + r$ and $0 \leqslant r < m$ for some q and r. In particular, $r \in (a) \cap (b)$, so $r = 0$ by minimality of m. Thus $m \mid n$. We have a Hasse diagram as in Fig. 3.2.

Theorem 8. $\gcd(a, b) \operatorname{lcm}(a, b) = |ab|$.

Proof. If an integer n is a common divisor of a and b, then

$$\frac{ab}{n} = \frac{a}{n} \cdot b = a \cdot \frac{b}{n},$$

so $n \mid ab$ and ab/n is a common multiple of ab. The least common multiple of a and b divides ab since this is a common multiple. Therefore $\operatorname{lcm}(a, b) = ab/n$ for some n; in particular, n is a common divisor of a and b. The claim now follows, since among common divisors m and n of a and b,

$$m \mid n \iff \frac{ab}{n} \mid \frac{ab}{m}. \qquad \square$$

3.4. The Euclidean algorithm

How can we find solutions to an equation like the following?

$$63x + 7 = 23y.$$

Rewrite as

$$63x - 23y = -7.$$

For a solution, we must have

$$\gcd(63, 23) \mid 7.$$

We can find this gcd by the algorithm demonstrated by Euclid in Propositions VII.1 and 2 of the *Elements*. Indeed,

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

so 63 and 23 are co-prime by Euclid's VII.1. But $\gcd(9, 12) = 3$ by VII.2, since

$$\begin{gathered} 12 = 9 \cdot 1 + 3, \\ 3 \mid 9. \end{gathered}$$

In general, suppose $a_0 > a_1 \geqslant 0$. By *strong* recursion (and the Division Theorem), we obtain a sequence $a_0, a_1, a_2, \ldots$ by defining

$$a_n = a_{n+1}q + a_{n+2} \;\&\; 0 \leqslant a_{n+2} < a_{n+1} \tag{§}$$

(for some q) if $a_{n+1} \neq 0$; but if $a_{n+1} = 0$, we let $a_{n+2} = 0$. Then the descending sequence

$$a_0 > a_1 > a_2 > \cdots$$

must stop. That is, let a_m be the least element of $\{a_n \colon a_n > 0\}$, so that $a_{m+1} = 0$. Then

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

For, if $a_{n+1} \neq 0$, then $\gcd(a_n, a_{n+1}) = \gcd(a_{n+1}, a_{n+2})$ by (§); so, by induction,

$$\gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_m, a_{m+1}) = \gcd(a_m, 0) = a_m.$$

This method of finding a gcd is called the **Euclidean algorithm.**

In obtaining (§) in § 1.3, we used the Euclidean Algorithm (in particular, we used the algorithm given by Euclid in his Proposition X.2). As in Fig. 3.3, let d

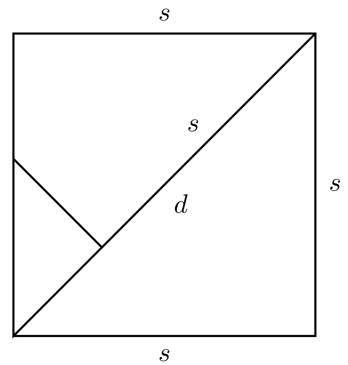


Figure 3.3. Diagonal and side.

and s be the diagonal and side of a square. Since $d^2 - s^2 = s^2$, we have

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

Since $s < d + s$, so $d - s < s$. Because also $d + s = s \cdot 2 + d - s$, we have that s goes into $d + s$ twice, with remainder $d - s$. Then the Euclidean process is endless:

$$\begin{aligned} d + s &= s \cdot 2 + d - s, \\ s &= (d - s) \cdot 2 + \cdots, \\ d - s &= \cdots 2 + \cdots, \end{aligned}$$

and so on. As before, we may write

$$\frac{d+s}{s} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}.$$

Compare with an ordinary application of the Algorithm. For $\gcd(134, 35)$, we have

$$\begin{aligned} 134 &= 35 \cdot 3 + 29, \\ 35 &= 29 \cdot 1 + 6, \\ 29 &= 6 \cdot 4 + 5, \\ 6 &= 5 \cdot 1 + 1, \\ 5 &= 1 \cdot 5, \end{aligned}$$

so $\gcd(134, 35) = 1$; but what is the significance of the numbers 3, 1, 4, 1, 5? They appear in the continued fraction:

$$\begin{aligned} \frac{134}{35} = 3 + \frac{29}{35} = 3 + \cfrac{1}{\cfrac{35}{29}} = 3 + \cfrac{1}{1 + \cfrac{6}{29}} = 3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{29}{6}}} \\ = 3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{5}{6}}} = 3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\cfrac{6}{5}}}} = 3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{5}}}} \end{aligned}$$

3.5. A linear system

A cock costs 5 L; a hen, 3 L; 3 chicks, 1 L. Can we buy 100 birds with 100 L? Let

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

We want to solve

$$\begin{aligned} x + y + z &= 100, \\ 5x + 3y + \frac{1}{3}z &= 100. \end{aligned} \tag{¶}$$

Eliminate z and proceed:

$$\begin{aligned} z &= 100 - x - y, \\ 15x + 9y + z &= 300, \\ 15x + 9y + 100 - x - y &= 300, \\ 14x + 8y &= 200, \\ 7x + 4y &= 100. \end{aligned} \tag{$\|$}$$

Since $4 \mid 100$, one solution is $(0, 25)$, that is, $x = 0$ and $y = 25$. Then $y = 75$. So the answer to the original question is Yes. But can we include at least one cock? What are all the solutions?

Think of linear algebra. If (x_0, y_0) and (x_1, y_1) are two solutions to ($\|$), then

$$\begin{aligned} 7x_0 + 4y_0 &= 100, \\ 7x_1 + 4y_1 &= 100, \\ 7(x_1 - x_0) + 4(y_1 - y_0) &= 0. \end{aligned}$$

So we want to solve

$$7x + 4y = 0.$$

Since $\gcd(7, 4) = 0$, the solutions are $(4t, -7t)$. (Here is a difference with the usual linear algebra.) So the original system (¶) has the general solution

$$(x, y, z) = (4t, 25 - 7t, 75 + 3t).$$

If we want all entries to be positive, this means

$$\begin{gathered} 4t > 0, \quad 25 - 7t > 0, \quad 75 + 3t > 0; \\ t > 0, \quad 7t < 25, \quad 3t > -75; \\ 0 < t < \frac{25}{7}; \\ 0 < t \leqslant 3. \end{gathered}$$

So there are three solutions:

x	y	z
4	18	78
8	11	81
12	4	88

4. Prime numbers

4.1. The fundamental theorem

A positive integer is **prime** if it has exactly two distinct positive divisors. So, 1 is not prime, but 2 is. More generally, b is prime if and only if $b > 1$ and for all positive integers a,

$$a \mid b \Rightarrow a \in \{1, b\}.$$

Throughout these notes, 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 9 (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 7. □

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

Proof. Use induction. Indeed, the claim is 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. □

Theorem 10 (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 $m > 1$. If a is a divisor of m that is greater than 1, but is not prime, then a has a divisor b such that $1 < b < a$; but also then b is a divisor of m. Consequently, the *least* divisor of m that is greater than 1 is a prime, p_1. 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_1p_2 that is greater than 1 is a prime p_3. Continuing thus, we get a decreasing sequence $p_1, p_2, p_3, \dots$ of primes, where $p_1 \cdots p_k \mid m$. Since

$$m > \frac{m}{p_1} > \frac{m}{p_1p_2} > \cdots,$$

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 9, 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

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

where $p_1 < \cdots < p_n$ and the exponents a_k are all positive integers.

An integer greater than 1 that is not prime is called **composite,** since it can be written as a product ab, where both factors are greater than 1.

4.2. Irreducibility

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 if $a = bc$, then one of b and c is a unit. Thus the prime numbers are just the positive irreducibles in the ring of integers.

In an arbitrary commutative ring, the analogue of Theorem 9 may fail. For example, let $\mathbb{Z}[\sqrt{10}]$ be the ring of numbers $a + b\sqrt{10}$. Here,

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

but the factors $4 \pm \sqrt{10}$, 2, and 3 are irreducible. To show this, we use the function σ from $\mathbb{Z}[\sqrt{10}]$ to itself given by

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

Compare this with complex conjugation. Since

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

we have

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

Now define $N(x) = x \cdot \sigma(x)$, so that

$$N(a + b\sqrt{10}) = a^2 - 10b^2,$$

an integer. Then

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

If a is a unit of $\mathbb{Z}[\sqrt{10}]$, then $ab = 1$ for some b in $\mathbb{Z}[\sqrt{10}]$, so $N(ab) = N(1)$, that is, $N(a) \cdot N(b) = 1$, so $N(a) = \pm 1$. Conversely, if $N(a) = \pm 1$, then $a \cdot (\pm\sigma(a)) = 1$, so a is a unit. Finally, $N(c)$ is always a square *modulo* 10. We have

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9 \equiv -1, \quad 4^2 = 16 \equiv -4, \quad 5^2 = 25 \equiv 5,$$

so $N(c)$ is congruent to 0, ± 1, ± 4 or 5, *modulo* 10. Now 2 is irreducible, since if $2 = ab$, then $N(2) = N(ab)$, that is, $4 = N(a) \cdot N(b)$, so $N(a) \in \{\pm 1, \pm 2, \pm 4\}$ and therefore $N(a) \in \{\pm 1, \pm 4\}$; so one of $N(a)$ or $N(b)$ is ± 1, so it is a unit. Likewise for the other factors.

4.3. Eratosthenes

One can find primes with the **Sieve of Eratosthenes** (assumed known to the reader). Eratosthenes of Cyrene (276–194 B.C.E.) 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. Columbus was not in a position to make the measurement again, so he had to rely on ancient measurements [12].

4.4. The infinity of primes

Theorem 11 (Euclid, IX.20). *There are more than any number of primes.*

Proof. Suppose $p_1 < \cdots < p_n$, all prime. Then $p_1 \cdots p_1 + 1$ has a prime factor, distinct from the p_k. □

An alternative argument by Filip Saidak (2005) is reported in *Matematik Dünyası* (2007-II [no. 73], p. 69): Define $a_0 = 2$ and $a_{n+1} = a_n(1 + a_n)$. Suppose $k < n$. 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 another proof of the infinity of primes, using the full Fundamental Theorem of Arithmetic, consider the product

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

(recall that p ranges over the primes). If there are only finitely many primes, then this product is well defined. In any case, each factor is the sum of a **geometric series:**

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

Hence, at least formally,

$$\prod_p \frac{1}{1 - 1/p} = \prod_p \Big(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\Big).$$

Alternatively, if the primes are p_1, p_2, ..., then the product is

$$\Big(1 + \frac{1}{p_1} + \frac{1}{{p_1}^2} + \cdots\Big) \cdot \Big(1 + \frac{1}{p_2} + \frac{1}{{p_2}^2} + \cdots\Big) \cdots$$

which can be understood as the sum of terms

$$\frac{1}{{p_1}^{e(1)}{p_2}^{e(2)} \dots},$$

where $e(i) \geqslant 0$, and $e(i) = 0$ for all but finitely many indices i. But every positive integer is *uniquely* such a product ${p_1}^{e(1)}{p_2}^{e(2)} \cdots$, by the Fundamental Theorem. Therefore

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

This is the **harmonic series,** which diverges:

$$1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\geqslant 1/2} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\geqslant 1/2} + \cdots$$

Therefore there are infinitely many primes. Using similar ideas, one can show that $\sum_p 1/p$ diverges.

4.5. Some theorems

I state some theorems, without giving proofs; some of them are recent and reflect ongoing research:

Theorem 12 (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 13 (Ben Green and Terence Tao [9], 2004). *For every* n*, there are* a *and* b *such that each of the numbers* $a, a+b, a+2b, \ldots, a_n b$ *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 can't prove it. We do have:

Theorem 14 (Goldston, Pintz, Yıldırım [8], 2005). *For every positive real number* ε*, there are primes* p *and* q *such that* $0 < q - p < \varepsilon \cdot \log p$*.*

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

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

This function also appears in the much older

Theorem 15 (Prime Number Theorem). *Let* $\pi(n)$ *be the number of primes* p *such that* $p \leqslant n$*. Then*

$$\lim_{n \to \infty} \frac{\pi(n) \cdot \log n}{n} = 1.$$

[1] This theorem is not mentioned in Burton [2].

5. Computations with congruences

5.1. Exponentiation

We can compute $35^{14} \pmod{43}$ as follows: First, $35 \equiv -8 \ (43)$, so

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

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

$$\begin{aligned} 8^2 &= 64 \equiv 21, \\ 21^2 &= 441 \equiv 11, \\ 11^2 &= 121 \equiv 35 \equiv -8, \end{aligned}$$

so that

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

5.2. Inversion

If $a \equiv b \ (n)$, then $ac \equiv bc \ (n)$. But do we have the converse? We do if c is invertible (is a unit) *modulo* n. In that case, $cd \equiv 1 \ (n)$ for some d, and then

$$\begin{aligned} ac \equiv bc \pmod{n} &\implies acd \equiv bcd \pmod{n} \\ &\implies a \equiv b \pmod{n}. \end{aligned}$$

Invertibility of c *modulo* n is equivalent to solubility of $cx \equiv 1 \ (n)$, or equivalently of

$$cx + ny = 1.$$

Thus c is invertible *modulo* n if and only if c and n are co-prime.

Alternatively, if $ac \equiv bc \pmod{n}$, and c and n are co-prime, then we can argue by Theorem 9 that, since $n \mid bc - ac$, that is, $n \mid (b-a)c$, we have $n \mid b - a$, that is, $a \equiv b \pmod{n}$.

Suppose we simply have $\gcd(c, n) = d$. Then $\gcd(c, n/d) = 1$. Hence

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

Conversely,

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

In short,

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

For example, $6x \equiv 6 \pmod{9} \iff x \equiv 1 \pmod{3}$. A longer problem is to solve

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

This reduces to

$$35x \equiv 9 \pmod{67}.$$

or $35x + 67y = 9$. So there is a solution if and only if $\gcd(35, 67) \mid 9$. We check the divisibility 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 $\gcd(35, 67) = 1$. Rearranging the computations, we have

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

In particular, $35 \cdot 23 \equiv 1 \pmod{67}$, so $(*)$ is equivalent to

$$\begin{gathered} x \equiv 23 \cdot 9 \equiv 207 \equiv 6 \quad (67), \\ x \equiv 6, 73 \quad (134). \end{gathered}$$

5.3. Chinese Remainder Theorem

A puzzle from a newspaper [the *Guardian Weekly*] is mathematically the same as one attributed [2, Prob. 4.4.8–9, p. 83] to Brahmagupta (7th century C.E.): A man dreams he runs up a flight of stairs. If he takes the stairs 2, 3, 4, 5, or 6 at time, then one stair is left before the top. If he takes them 7 at a time, then he reaches the top exactly. How many stairs are there?

If x is that number, then

$$\begin{aligned} x &\equiv 1 \quad (\text{mod } 2, 3, 4, 5, 6), \\ x &\equiv 0 \quad (\text{mod } 7). \end{aligned}$$

But $\operatorname{lcm}(2, 3, 4, 5, 6) = 60$, so $x = 60n + 1$, where $7 \mid 60n + 1$. We have this when $n = 5$, hence when $n = 12, 19, \ldots$

The general problem is to solve systems

$$x \equiv a_1 \bmod n_1, \qquad x \equiv a_2 \bmod n_2, \qquad \ldots, \qquad x \equiv a_k \bmod n_k. \tag{†}$$

Let's start with two congruences:

$$x \equiv a \bmod n, \qquad\qquad x \equiv b \bmod m. \tag{‡}$$

A solution will take the form

$$x = a + nu = mv + b.$$

Then we shall have $a \equiv mv + b \ (n)$ and $a + nu \equiv b \ (m)$, that is,

$$mv \equiv a - b \pmod{n}, \qquad\qquad nu \equiv b - a \pmod{m}.$$

These can be achieved if each of m and n is invertible *modulo* the other, that is, $\gcd(n, m) = 1$. In this case we have $nr \equiv 1 \ (m)$ and $ms \equiv 1 \ (n)$ for some r and s, so that a solution to (‡) is

$$x = ams + bnr.$$

Any two solutions are congruent *modulo* m and n, hence $\operatorname{lcm}(n,m)$, which is nm since $\gcd(n,m)=1$.

We can solve (†) similarly, under the assumption

$$\gcd(n_i, n_j) = 1$$

whenever $1 \leqslant i < j \leqslant k$. We have

$$\begin{aligned} x &= a_1 m_1 n_2 \cdots n_k + a_2 n_1 m_2 n_3 \cdots n_k + \cdots + a_k n_1 \cdots n_{k-1} m_k \\ &= \sum_{k=1}^{n} a_k m_k \frac{\prod_{j=1}^{n} n_j}{n_k}, \end{aligned}$$

where the m_k are chosen so that

$$m_1 n_2 \cdots n_k \equiv 1 \quad (n_1),$$

and so forth, that is,

$$m_k \frac{\prod_{j=1}^{n} n_j}{n_k} \equiv 1 \pmod{n_k};$$

this is possible since

$$\gcd(n_1, n_2 \cdots n_k) = 1.$$

The solution is unique *modulo* $n_1 \cdots n_k$. This is the **Chinese Remainder Theorem.**

6. Mersenne

6.1. Perfect numbers

Of the 13 books of Euclid's *Elements,* VII, VIII and IX concern number-theory. The last proposition in these books is:

Theorem 16 (Euclid, IX.36)**.** *If* $1+2+4+\cdots+2^n$ *is prime, then the product*

$$2^n \cdot (1+2+\cdots+2^n)$$

is perfect.

A number is **perfect** if it is the sum of its positive proper divisors:

$$\begin{aligned} 6 &= 1+2+3, \\ 28 &= 1+2+4+7+14. \end{aligned}$$

Proof of theorem. Use the notation

$$M_{n+1} = 1+2+4+\cdots+2^n = \sum_{k=0}^{n} 2^k = 2^{n+1}-1. \tag{$*$}$$

If M_{n+1} is prime, then the positive divisors of $2^n \cdot M_{n+1}$ are the divisors of 2^n, perhaps multiplied by M_{n+1}. So they are

$$1,\ 2,\ 4,\ \ldots,\ 2^n,\ M_{n+1},\ 2 \cdot M_{n+1},\ 4 \cdot M_{n+1},\ \ldots,\ 2^n \cdot M_{n+1}.$$

The sum of these is $(1+2+4+\cdots+2^n) \cdot (1+M_{n+1})$, which is $M_{n+1} \cdot 2^{n+1}$. Subtracting $2^n \cdot M_{n+1}$ itself leaves the same. $\square$

6.2. Mersenne primes

The number $2^n - 1$, denoted by M_n as in $(*)$, is called a **Mersenne number,** after Marin Mersenne, 1588–1648); if the number is prime, it is a **Mersenne prime.** We do not know whether there are infinitely many Mersenne primes. However, if M_n is prime, then so is n, since $2^a - 1 \mid 2^{ab} - 1$, because of the identity

$$x^m - y^m = (x-y) \cdot (x^{m-1} + x^{m-2} \cdot y + x^{m-3} \cdot y^2 + \cdots + x \cdot y^{m-2} + y^{m-1}).$$

7. Fermat

7.1. Fermat's factorization method

One method of factorizing n is to get a table of primes and test whether $p \mid n$ when $p \leqslant \sqrt{n}$.

The method of Pierre de Fermat (1601–1665) is to solve

$$x^2 - y^2 = n,$$

since then $n = (x+y)(x-y)$. This method always works in principle, since

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

We may assume n is odd, so if $n = ab$, then $a \pm b$ are even.

For example, the first square greater than $2\,279$ is $2\,304$, or 48^2, and $2\,304 - 2\,279 = 25 = 5^2$, so

$$2\,279 = (48+5)(48-5) = 53 \cdot 43.$$

We can generalize the method by solving

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

If $x^2 - y^2 = mn$, then find $\gcd(x+y, n)$ and $\gcd(x-y, n)$.

7.2. Fermat's little theorem

Suppose $p \nmid a$, that is, $\gcd(p, a) = 1$. What is a^{p-1} *modulo* p? Consider a, $2a$, …, $(p-1)a$. These are all incongruent *modulo* p, since

$$ia \equiv ja \pmod{p} \implies i \equiv j \pmod{p}.$$

But 1, 2, …, $p-1$ are also incongruent. There are only $p-1$ numbers incongruent with each other and 0 *modulo* p; so the numbers a, $2a$, …, $(p-1)a$ are congruent respectively with 1, 2, …, $p-1$ in some order. Now multiply:

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

Since $(p-1)!$ and p are co-prime, we conclude:

$$\gcd(a,p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}.$$

This is **Fermat's Little Theorem.** Equivalently,

$$a^p \equiv a \pmod{p}$$

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

$$m \equiv n \pmod{(p-1)} \implies a^m \equiv a^n \pmod{p}.$$

For example,

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

Since $10 = 8+2$, we have $6^{10} = 6^8 \cdot 6^2$; but $6^2 \equiv 36 \equiv 2 \ (17)$, so $6^8 \equiv 2^4 \equiv 16 \equiv -1 \ (17)$, and hence

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

If $a^n \not\equiv a \pmod{n}$, then n must not be prime. For example, what is 2^{133} *modulo* 133? We have $133 = 128 + 4 + 1 = 2^7 + 2^2 + 1$, so $2^{133} = 2^{2^7} \cdot 2^{2^2} \cdot 2$. Also,

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

Therefore

$$2^{133} \equiv 4 \cdot 16 \cdot 2 \equiv -5 \pmod{133},$$

so 133 must not be prime. Indeed, $133 = 7 \cdot 19$.

7.3. Carmichael numbers

The converse of the Fermat 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 not prime, but

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

Then 341 is a pseudo-prime. Indeed, $341 = 11 \cdot 31$; but

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

Hence $2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$ by the following.

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

Proof. Under the hypothesis, we have

$$\begin{aligned} a^{pq} &= (a^p)^q \equiv a^q \equiv a \pmod{q}, \\ a^{pq} &= (a^q)^p \equiv a^p \equiv a \pmod{p}, \end{aligned}$$

and hence $a^{pq} \equiv a \pmod{\operatorname{lcm}(p,q)}$; but $\operatorname{lcm}(p,q) = pq$. □

Again, we now have $2^{341} \equiv 2 \pmod{341}$, so 341 is pseudo-prime.

Theorem 17. *If n is a pseudo-prime, then so is $2^n - 1$.*

Proof. Since n factors non-trivially as ab, but $2^a - 1 \mid (2^a)^b - 1$, we have that 2^a is a non-trivial factor of $2^n - 1$. So $2^n - 1$ is not prime. We assume also $2^n \equiv 2 \pmod{n}$; 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 $2^{2^n - 1} \equiv 2 \pmod{2^n - 1}$. □

One can ask whether $3^n \equiv 3 \pmod{n}$, for example. But a number n is called an **absolute pseudo-prime** or a **Carmichael number** (named for Robert Daniel Carmichael, 1879–1967) if

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

for all a. Then 561 is a Carmichael number. Indeed,

$$561 = 3 \cdot 11 \cdot 17;$$

and

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

that is,

$$2 \mid 560, \qquad 10 \mid 560, \qquad 16 \mid 560.$$

Hence

$$\begin{aligned} 3 \nmid a &\implies a^2 \equiv 1 \pmod{3} \implies a^{560} \equiv 1 \pmod{3}; \\ 11 \nmid a &\implies a^{10} \equiv 1 \pmod{11} \implies a^{560} \equiv 1 \pmod{11}; \\ 17 \nmid a &\implies a^{17} \equiv 1 \pmod{17} \implies a^{560} \equiv 1 \pmod{17}. \end{aligned}$$

Hence $a^{561} \equiv a \pmod{3, 11, 17}$ for *all* a, so

$$a^{561} \equiv a \pmod{561}.$$

In general, if $n = p_0 \cdot p_1 \cdots p_k$, where $p_0 < p_1 < \cdots < p_k$, and $p_i - 1 \mid n - 1$ for each i, then the same argument shows that n is an absolute pseudo-prime.

For n to be a pseudo-prime, it is necessary that n have no square factor. Indeed, if $a^n \equiv a \pmod{n}$ for all a, but $m^2 \mid n$, then $m^n \equiv m \pmod{n}$, so

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

But if $n > 1$, then $m^n \equiv 0 \pmod{m^2}$, so $m \equiv 0 \pmod{m^2}$, which is absurd unless $m = \pm 1$.

7.4. Wilson's Theorem

Can we solve $(p-1)! \equiv x \pmod{p}$? The answer is certainly not 0.

Theorem 18. *Suppose* $n > 1$*. Then* $(n-1)! \equiv -1 \pmod{n}$ *if and only if* n *is prime.*

This is called **Wilson's Theorem** after John Wilson, 1741–1793, who apparently conjectured the result, but did not prove it. (It appears the result was also known to Abu Ali al-Hasan ibn al-Haytham, 965–1039.) The result gives a theoretical test for primality, though not a practical one.

Proof of theorem. One of the two directions should be easier; which one? 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 $n \nmid (n-1)! + 1$.

Now suppose n is a prime p. Each number on the list $1, 2, 3, \dots, p-1$ has an inverse *modulo* p. Also, $x^2 \equiv 1 \pmod{p}$ has only the solutions ± 1, that is, 1 and $p-1$, since it requires $p \mid x \pm 1$. So the numbers on the list $2, 3, \dots, p-2$ have inverses different from themselves. Hence we can partition these numbers into pairs $\{a, b\}$, where $ab \equiv 1 \pmod{p}$. Therefore $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. □

For example,

$$2 \cdot 4 \equiv 1, \qquad\qquad 3 \cdot 5 \equiv 1 \pmod{7},$$

so $6! = (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 6 \equiv -1 \pmod{7}$. How can one find inverses *modulo* 7, other than by trial? Take successive powers. We have

$$\begin{aligned} 2^2 &= 4, \\ 2^3 &= 8 \equiv 1 \pmod{7}, \end{aligned}$$

so not every number that is prime to 7 is a power of 2 *modulo* 7; but

$$\begin{aligned} 3^2 &= 9 \equiv 2 \pmod{7}, \\ 3^3 &\equiv 2 \cdot 3 \equiv 6 \pmod{7}, \\ 3^4 &\equiv 6 \cdot 3 \equiv 4 \pmod{7}, \\ 3^5 &\equiv 4 \cdot 3 \equiv 5 \pmod{7}, \\ 3^6 &\equiv 5 \cdot 3 \equiv 1 \pmod{7}. \end{aligned}$$

So the invertible numbers *modulo* 7 compose a multiplicative group generated by 3; we express this by saying 3 is a **primitive root** of 7. Primitive roots will be investigated later. Meanwhile, we have now

$$3 \cdot 3^5 \equiv 3^2 \cdot 3^4 \equiv 1 \pmod{7}.$$

An application of Wilson's Theorem is the following.

Theorem 19. *Let p be an odd prime. Then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

Proof. Suppose $a^2 \equiv -1 \pmod{p}$. By the Fermat Theorem,

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p},$$

so $(p-1)/2$ must be even: $4 \mid p-1$, so $p \equiv 1 \pmod{4}$.

Conversely, by Wilson's Theorem, we have

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \\ &\equiv 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \\ &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \frac{1-p}{2} \\ &\equiv (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2} \right)! \right)^2 . \end{aligned}$$

So if $p \equiv 1 \pmod{4}$, then $x^2 \equiv -1 \pmod{p}$ is solved by $((p-1)/2)!$. $\square$

For example,

$$-1 \equiv 4! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \equiv 2^2 \pmod{5},$$

while, *modulo* 13, we have

$$-1 \equiv 12! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdot 3 \cdot (-3) \cdot 4 \cdot (-4) \cdot 5 \cdot (-5) \cdot 6 \cdot (-6) \equiv (6!)^2 \quad (13).$$

In terminology to be developed later, the theorem is that -1 is a **quadratic residue** of an odd prime p if and only if $p \equiv 1 \pmod{4}$.

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, where $\sigma(n)$ is the sum of the (positive) divisors of n. Then n is perfect if and only if $\sigma(n) = 2n$. 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

$$\begin{array}{ccc} 2^0 \cdot 3^0, & 2^1 \cdot 3^0, & 2^2 \cdot 3^0, \\ 2^0 \cdot 3^1, & 2^1 \cdot 3^1, & 2^2 \cdot 3^1. \end{array}$$

So 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:

Theorem 20. *If $n = {p_1}^{k(1)} \cdot {p_2}^{k(2)} \cdots {p_n}^{k(n)}$, where $p_1 < p_2 < \cdots < p_n$, then*

$$\tau(n) = \prod_{j=1}^{n} (k(j) + 1), \qquad \sigma(n) = \prod_{j=1}^{n} \frac{{p_j}^{k(j)+1} - 1}{p_j - 1}.$$

We can abbreviate the definitions of σ and τ as follows:

$$\sigma(n) = \sum_{d|n} d, \qquad \tau(n) = \sum_{d|n} 1.$$

Implicitly here, d ranges over the *positive* divisors of n.

Is there a relation between $\sigma(n)$ and $\tau(n)$? We have

n	$\tau(n)$	$\sigma(n)$	$\prod_{d\|n} d$
1	1	1	1
2	2	3	2
3	2	4	3
4	3	7	$8 = 2^3 = 4^{3/2}$
5	2	6	5
6	4	12	$36 = 6^2$
7	2	8	7
8	4	15	$64 = 8^2$
9	3	13	$27 = 3^3 = 9^{3/2}$
10	4	18	$100 = 10^2$

It appears that

$$\prod_{d|n} d = n^{\tau(n)/2}.$$

We can prove it thus:

$$\Big(\prod_{d|n} d\Big)^2 = \Big(\prod_{d|n} d\Big) \cdot \Big(\prod_{d|n} d\Big) = \Big(\prod_{d|n} d\Big) \cdot \Big(\prod_{d|n} \frac{n}{d}\Big) = \prod_{d|n} n = n^{\tau(n)}.$$

Suppose $\gcd(n, m) = 1$. Then $n = {p_1}^{k(1)} \cdots {p_r}^{k(r)}$, and $m = {q_1}^{\ell(1)} \cdots {q_s}^{\ell(s)}$, where the p_i and q_j are all distinct primes. Hence the prime factorization of nm is

$${p_1}^{k(1)} \cdots {p_r}^{k(r)} \cdot {q_1}^{\ell(1)} \cdots {q_s}^{\ell(s)},$$

so we have

$$\begin{aligned}\sigma(nm) &= \frac{{p_1}^{k(1)+1} - 1}{p_1 - 1} \cdots \frac{{p_r}^{k(r)+1} - 1}{p_r - 1} \cdot \frac{{q_1}^{\ell(1)+1} - 1}{q_1 - 1} \cdots \frac{{q_s}^{k(s)+1} - 1}{q_s - 1} \\ &= \sigma(n) \cdot \sigma(m)\end{aligned}$$

by Theorem 20; similarly, $\tau(nm) = \tau(n) \cdot \tau(m)$. We say then that σ and τ are *multiplicative;* in general, a function f on the positive integers 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 in general. For example,

$$\sigma(2 \cdot 2) = \sigma(4) = 1 + 2 + 4 = 7 \neq 9 = (1 + 2) \cdot (1 + 2) = \sigma(2) \cdot \sigma(2).$$

The identify function $n \mapsto n$ and the constant function $n \mapsto 1$ are multiplicative. Since $\sigma(n) = \sum_{d|n} d$ and $\tau(n) = \sum_{d|n} 1$, the multiplicativity of σ and τ is a consequence of the following.

Theorem 21. *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. If $\gcd(m, n) = 1$, then every divisor of mn is uniquely of the form de, where $d \mid m$ and $e \mid n$. This is because every *prime* divisor of mn is uniquely a divisor of m or n. Hence

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d|m} \sum_{e|n} f(de) \\ &= \sum_{d|m} \sum_{e|n} f(d) \cdot f(e) \\ &= \sum_{d|m} f(d) \cdot \sum_{e|n} f(e) \\ &= \Big(\sum_{d|m} f(d)\Big) \cdot \sum_{e|n} f(e), \end{aligned}$$

which is $F(m) \cdot F(n)$ by $(*)$. □

8.2. Möbius

If F is defined from f as in $(*)$, can we recover f from F? For example, when f is $n \mapsto n$, so that F is σ, then

$$\begin{aligned} \sigma(12) &= 1 + 2 + 3 + 4 + 6 + 12 \\ \sigma(6) &= 1 + 2 + 3 + 6 \\ \sigma(4) &= 1 + 2 + 4 \\ \sigma(3) &= 1 + 3 \\ \sigma(2) &= 1 + 2 \\ \sigma(1) &= 1 \end{aligned}$$

so that

$$12 = \sigma(12) - \sigma(6) - \sigma(4) + \sigma(2).$$

Why are some terms added, others subtracted? Why didn't we need $\sigma(3)$ or $\sigma(1)$? Note that $12/3 = 4 = 2^2$, a square.

We have also

$$\begin{array}{rcl}
\sigma(30) &=& 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 \\
\sigma(15) &=& 1 \quad + \quad 3 + 5 \qquad + \qquad 15 \\
\sigma(10) &=& 1 + 2 \quad + \quad 5 \quad + \quad 10 \\
\sigma(6) &=& 1 + 2 + 3 \quad + \quad 6 \\
\sigma(5) &=& 1 \qquad + \qquad 5 \\
\sigma(3) &=& 1 \quad + \quad 3 \\
\sigma(2) &=& 1 + 2 \\
\sigma(1) &=& 1
\end{array}$$

so that

$$30 = \sigma(30) - \sigma(15) - \sigma(10) - \sigma(6) + \sigma(5) + \sigma(3) + \sigma(2) - \sigma(1).$$

Here we have $30/15 = 2$, $30/10 = 3$, and $30/6 = 5$: each of these numbers has one prime factor. But $30/5 = 2 \cdot 3$, $30/3 = 2 \cdot 5$, and $30/2 = 3 \cdot 5$; each number here has two prime factors.

The **Möbius function,** μ, (named for August Ferdinand MÃűbius, 1790–1868) 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, $\mu(1) = 1$.

Lemma. *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 $\mu(mn) = 0 = \mu(m) = \mu(m) \cdot \mu(n)$. But if $m = p_1 \cdots p_r$, and $n = q_1 \cdots q_s$, where all factors are distinct primes, then

$$\mu(mn) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m) \cdot \mu(n). \qquad \square$$

Theorem 22 (Möbius Inversion Formula)**.** *If f determines F by the rule $(*)$, then F determines f by the rule*

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot F(d). \tag{$\dagger$}$$

Proof. We just start calculating:

$$\begin{aligned}\sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot F(d) &= \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot \sum_{e \mid d} f(e) \\ &= \sum_{d \mid n} \sum_{e \mid d} \mu\left(\frac{n}{d}\right) \cdot f(e).\end{aligned}$$

For all factors d and e of n, we have

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

Therefore

$$\begin{aligned}\sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot F(d) &= \sum_{e \mid n} \sum_{c \mid (n/e)} \mu(c) \cdot f(e) \\ &= \sum_{e \mid n} f(e) \cdot \sum_{c \mid (n/e)} \mu(c).\end{aligned}$$

We want to obtain $f(n)$ from this. It will be enough if we can show that $\sum_{c \mid (n/e)} \mu(c)$ is 0 unless $e = n$, in which case the sum is 1. So it is enough to show

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{otherwise.} \end{cases} \tag{‡}$$

This is easy when $n = p^r$. Indeed, we have

$$\begin{aligned}\sum_{d \mid p^r} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) \\ &= \begin{cases} 1, & \text{if } r = 0; \\ 1 - 1, & \text{if } r \geqslant 1. \end{cases}\end{aligned}$$

But also μ is multiplicative by the lemma, so we have (‡) in general. For, if $n \neq 1$, then n has a prime factor p, and $n = p^r \cdot a$ for some positive r, where $\gcd(a, p) = 1$. Then $\mu(n) = \mu(p^r) \cdot \mu(a) = 0$. □

9. Euler

9.1. Chinese Remainder Theorem

The Chinese Remainder Theorem can be understood with a picture. Since $\gcd(5,6) = 1$ for example, the Theorem gives us a solution to

$$\begin{cases} x \equiv a_1 \pmod{5}, \\ x \equiv a_2 \pmod{6}, \end{cases}$$

—a solution that is unique *modulo* 30. In theory, we can find this solution by filling out a table diagonally as follows:

	0	1	2	3	4	5
0	0					
1		1				
2			2			
3				3		
4					4	

, then

	0	1	2	3	4	5
0	0					5
1		1				
2			2			
3				3		
4					4	

,

then

	0	1	2	3	4	5
0	0					5
1	6	1				
2		7	2			
3			8	3		
4				9	4	

, then

	0	1	2	3	4	5
0	0				10	5
1	6	1				11
2		7	2			
3			8	3		
4				9	4	

,

and ultimately

	0	1	2	3	4	5
0	0	25	20	15	10	5
1	6	1	26	21	16	11
2	12	7	2	27	22	17
3	18	13	8	3	28	23
4	24	19	14	9	4	29

.

Hence, for example, a solution to $x \equiv 2 \pmod{5}$ & $x \equiv 3 \pmod{6}$ is 27 (in row 2, column 3).

Making such a table is not always practical. But the possibility of making such a table will enable us to establish a generalization of Fermat's Theorem.

9.2. The Phi-Function

Fermat tells that, if $\gcd(a,p)=1$, then

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

Euler's Theorem will give us a certain function ϕ such that, if $\gcd(a,n)=1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

We have defined

$$\mu(n) = (-1)^r,$$

if n is the product of r *distinct* primes; otherwise, $\mu(n)=0$. In particular, $\mu(1)=(-1)^0=1$. We have shown that μ is multiplicative, that is,

$$\mu(mn) = \mu(m)\cdot\mu(n),$$

provided $\gcd(m,n)=1$. We have shown (‡). From this, we have established the Möbius Inversion Formula: if (∗), then (†).

Now we define a new multiplicative function, the **Euler phi-function,** named for Leonhard Euler, 1707–1783: $\phi(n)$ is the number of x such that $0 \leqslant x < n$ and x is prime to n. Then

a) $\phi(1)=1$;
b) $\phi(p)=p-1$;
c) $\phi(p^r)=p^r-p^{r-1}$ when $r>0$.

Indeed, suppose $\gcd(a,p^r)\neq 1$. Then $\gcd(a,p^r)=p^k$ for some positive k. In particular, $p \mid a$. Conversely, if $p \mid a$, then $p \mid \gcd(a,p^r)$, so $\gcd(a,p^r)\neq 1$. Therefore $\phi(p^r)$ is the number of integers x such that $0 \leqslant x < p^r$ and $p \nmid x$; so

$$\phi(p^r) = p^r - \frac{p^r}{p} = p^r \cdot \left(1-\frac{1}{p}\right).$$

If we can show ϕ is multiplicative, and $n = {p_1}^{k(1)} \cdots {p_r}^{k(r)}$, then

$$\begin{aligned}\phi(n) &= \phi({p_1}^{k(1)}) \cdots \phi({p_r}^{k(r)}) \\ &= {p_1}^{k(1)} \cdot \left(1 - \frac{1}{p_1}\right) \cdots {p_r}^{k(r)} \cdot \left(1 - \frac{1}{p_r}\right) \\ &= {p_1}^{k(1)} \cdots {p_r}^{k(r)} \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

But again, we must show ϕ is multiplicative. We do this with the Chinese Remainder Theorem.

Let us denote the set $\{x \in \mathbb{Z} \colon 0 \leqslant x < n\}$ by $[0, n)$. Assume $\gcd(m, n) = 1$. If $x \in [0, mn)$, then there is a unique a in $[0, m)$ such that $x \equiv a \pmod{m}$; likewise, there is a unique b in $[0, n)$ such that $x \equiv b \pmod{n}$. Thus we have a function $x \mapsto (a, b)$ from $[0, mn)$ into $[0, m) \times [0, n)$. Moreover, if x is prime to mn, then it is prime to m and to n, so a is prime to m, and b is prime to n.

Conversely, by the Chinese Remainder Theorem, for every a in $[0, m)$ and b in $[0, n)$, there is a unique x in $[0, mn)$ such that

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}. \end{cases}$$

Moreover, if a is prime to m, and b is prime to n, then x is prime to m and to n, hence to mn (that is, $\operatorname{lcm}(m, n)$). Therefore we have a bijection $x \mapsto (a, b)$ from the set

$$\{x \in [0, mn) \colon \gcd(x, mn) = 1\}$$

to the set that is the Cartesian product

$$\{a \in [0, m) \colon \gcd(a, m) = 1\} \times \{b \in [0, n) \colon \gcd(b, n) = 1\}.$$

Therefore the sizes of these sets are equal; but by definition of ϕ, these sizes are $\phi(mn)$ and $\phi(m) \cdot \phi(n)$.

The idea can be seen in a table as in § 9.1. Or consider now the table

	0	1	2	3	4	5	6
0	0	8	16	24	4	12	20
1	21	1	9	17	25	5	13
2	14	22	2	10	18	26	6
3	7	15	23	3	11	19	27

.

This gives the function $x \mapsto (a, b)$ from $[0, 28)$ to $[0, 4) \times [0, 7)$. For example, 18 is in row 2 and column 4, so the function takes 18 to $(2, 4)$. As 0 and 2 are not prime to 4, we delete rows 0 and 2; as 0 is not prime to 7, we delete column 0. The numbers remaining are prime to 28; and the *number* of these numbers—by definition, $\phi(28)$—is $2 \cdot 6$, which is $\phi(4) \cdot \phi(7)$.

	0	1	2	3	4	5	6
0							
1		1	9	17	25	5	13
2							
3		15	23	3	11	19	27

Burton [2] also uses a table of numbers, but written in the usual order:

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

We can apply to this a variant of the Sieve of Eratosthenes. First delete the multiples of 7; these compose the first column, so we delete this:

	1	2	3	4	5	6
	8	9	10	11	12	13
	15	16	17	18	19	20
	22	23	24	25	26	27

Then the number of remaining columns is $\phi(7)$. In each of these columns, just two numbers are prime to 4 (since each column contains a complete set of residues *modulo* 4). If we delete the numbers *not* prime to 4, what remains is the following:

	1		3		5	
		9		11		13
	15		17		19	
		23		25		27

Again, there are $\phi(4) \cdot \phi(7)$ numbers left, or $\phi(28)$.

For another example, say we want to find $\phi(30)$. As $30 = 2 \cdot 3 \cdot 5$, we write down the numbers from 0 to 29 (or 1 to 30) and eliminate the multiples of 2, 3, or 5:

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
	1		3		5		7		9
	11		13		15		17		19
	21		23		25		27		29
	1				5		7		
	11		13				17		19
			23		25				29
	1						7		
	11		13				17		19
			23						29

As 8 numbers remain, we have $\phi(30) = 8$.

Our list of numbers had 10 columns and 3 rows. When we eliminated multiples of 2 and 5, we eliminated the columns headed by 0, 2, 4, 5, 6, and 8. The remaining columns were headed by 1, 3, 7, and 9: four numbers. Therefore $\phi(10) = 4$. In each of the remaining columns, the entries are incongruent *modulo* 3. Indeed, the numbers differ by 10 or 20, and these are not divisible by 3. So, in each column, exactly one entry is a multiple of 3. When it is eliminated, there are $4 \cdot 2$ entries remaining: this is $\phi(10) \cdot \phi(3)$. Thus, multiplicativity of ϕ is established. Alternatively, considering the Chinese Remainder Theorem, we can tabulate the numbers from 0 to 29 thus:

	0	1	2	3	4	5	6	7	8	9
0	0	21	12	3	24	15	6	27	18	9
1	10	1	22	13	4	25	16	7	28	19
2	20	11	2	23	14	5	26	17	8	29

Eliminating multiples of 2, 3, and 5 means eliminating certain columns *and* rows:

	0	1	2	3	4	5	6	7	8	9
0										
1		1		13				7		19
2		11		23				17		29

9.3. Euler's Theorem

In general, we now have

$$\begin{aligned} \phi(p) &= p - 1; && \\ \phi(p^s) &= p^s - p^{s-1} = p \cdot \Big(1 - \frac{1}{p}\Big), && \text{if } s > 0; \\ \phi(mn) &= \phi(m) \cdot \phi(n), && \text{if } \gcd(m, n) = 1. \end{aligned}$$

Hence, if n has the distinct prime divisors $p_1, \dots, p_s$, then

$$\phi(n) = n \cdot \prod_{k=1}^{s} \Big(1 - \frac{1}{p_i}\Big).$$

We can write this more neatly as

$$\phi(n) = n \cdot \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big). \tag{$*$}$$

For example,

$$\phi(30) = 30 \cdot \Big(1 - \frac{1}{2}\Big) \cdot \Big(1 - \frac{1}{3}\Big) \cdot \Big(1 - \frac{1}{5}\Big) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$$

Since 180 has the same prime divisors as 30, we have

$$\frac{\phi(180)}{\phi(30)} = \frac{180}{30} = 6,$$

so $\phi(180) = 6\phi(30) = 48$. But 15 and 30 do not have the same prime divisors, and we cannot expect $\phi(15)/\phi(30)$ to be $15/30$, or $1/2$; indeed, $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8 = \phi(30)$.

Theorem 23 (Euler). *If* $\gcd(a, n) = 1$, *then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Fermat's Theorem is the special case when $n = p$. But we do *not* generally have $a^{\phi(n)+1} \equiv a \pmod{n}$ for arbitrary a. For example, $\phi(12) = 4$, but $2^5 = 32 \equiv 8 \pmod{12}$; so

$$2^{\phi(12)+1} \not\equiv 2 \pmod{12}.$$

Proof of Euler's Theorem. Assume $\gcd(a, n) = 1$. We can write $\{x \in \mathbb{Z}\colon 0 \leqslant x < n \;\&\; \gcd(x, n) = 1\}$ as

$$\{b_1, b_2, \dots, b_{\phi(n)}\}.$$

Then we can obtain $a^{\phi(n)}$ by solving the equation

$$\prod_{k=1}^{\phi(n)} (ab_k) = a^{\phi(n)} \cdot \prod_{k=1}^{\phi(n)} b_k.$$

As the two products $\prod_{k=1}^{\phi(n)}(ab_k)$ and $\prod_{k=1}^{\phi(n)} b_k$ are invertible *modulo* n, it is enough now to show that they are congruent *modulo* n. As a is invertible *modulo* n, there is a function f from $\{1, \dots, \phi(n)\}$ to itself such that

$$ab_i \equiv b_{f(i)} \pmod{n}$$

for each i. Moreover, if $f(i) = f(j)$, then

$$ab_i \equiv b_{f(i)} \equiv b_{f(j)} \equiv ab_j \pmod{n},$$

so $b_i \equiv b_j \pmod{n}$, hence $i = j$. So f is a permutation. Therefore

$$\prod_{k=1}^{\phi(n)} b_k \equiv \prod_{k=1}^{\phi(n)} b_{f(k)} \equiv \prod_{k=1}^{\phi(n)} (ab_k) \pmod{n}. \qquad \square$$

For example, to solve

$$369^{19587} x \equiv 1 \pmod{1000},$$

we compute

$$\phi(1000) = \phi(10^3) = \phi(2^3 \cdot 5^3) = \phi(2^3) \cdot \phi(5^3) = 4 \cdot 100 = 400.$$

Now reduce the exponent:

$$\frac{19587}{400} = 48 + \frac{387}{400}.$$

So we want to solve

$$369^{387} x \equiv 1 \pmod{1000},$$
$$x \equiv 369^{13} \pmod{1000}.$$

Now proceed, using that $13 = 8 + 4 + 1 = 2^3 + 2^2 + 1$. Multiplication *modulo* 1000 requires only three columns:

$$\begin{array}[t]{l} 369 \\ 369 \\ \hline 321 \\ 14 \\ 7 \\ \hline 161 \end{array} \quad \text{so } 369^2 \equiv 161 \quad (1000); \quad \begin{array}[t]{l} 161 \\ 161 \\ \hline 161 \\ 66 \\ 1 \\ \hline 921 \end{array} \quad \text{so } 369^4 \equiv 161^2 \equiv 921 \quad (1000);$$

$$\begin{array}[t]{l} 921 \\ 921 \\ \hline 921 \\ 42 \\ 9 \\ \hline 241 \end{array} \quad \text{so } 369^8 \equiv 921^2 \equiv 241 \quad (1000);$$

$$369^{13} \equiv 369^8 \cdot 369^4 \cdot 369 \equiv 241 \cdot 921 \cdot 369 \quad (1000);$$

$$\begin{array}[t]{l} 241 \\ 921 \\ \hline 241 \\ 82 \\ 9 \\ \hline 961 \end{array} \qquad \begin{array}[t]{l} 961 \\ 369 \\ \hline 649 \\ 66 \\ 3 \\ \hline 609 \end{array}$$

So the solution is $\boxed{x \equiv 609 \pmod{1000}.}$

Euler's Theorem gives a neat theoretical solution to Chinese-Remainder-Theorem problems: Suppose the integers $n_1, \ldots, n_s$ are pairwise co-prime. Say we want to solve the system

$$\begin{cases} x \equiv a_1 \pmod{n_1}, \\ \ldots \\ x \equiv a_s \pmod{n_s}. \end{cases}$$

Define

$$n = n_1 \cdots n_s;$$
$$N_i = \frac{n}{n_i}.$$

Then the system is solved by

$$x \equiv a_1 \cdot {N_1}^{\phi(n_1)} + \cdots + a_s \cdot {N_s}^{\phi(n_s)}$$

Indeed, we have

$$N_i^{\phi(n_i)} \equiv \begin{cases} 1 \pmod{n_i}; \\ 0 \pmod{n_j}, \quad \text{if } j \neq i. \end{cases}$$

9.4. Gauss's Theorem

As ϕ is a multiplicative function, so is the function

$$n \mapsto \sum_{d|n} \phi(d).$$

What *is* this function? The function is determined by its values at prime powers; so look at these. We have

$$\sum_{d|p^s} \phi(d) = \sum_{k=0}^{s} \phi(p^k) = 1 + \sum_{k=1}^{s} (p^k - p^{k-1})$$
$$= 1 + (p-1) + (p^2 - p) + \cdots + (p^s - p^{s-1}) = p^s.$$

Thus, the equation $\sum_{d|n} \phi(d) = n$ holds when n is prime power. As both sides are *multiplicative* functions of n, the equation holds for all n. Thus we have

Theorem 24 (Gauss). *For all positive integers n,*

$$\sum_{d|n} \phi(d) = n. \tag{†}$$

Note well the technique of our proof. Since both members of (†) are multiplicative functions, the equation is an identity, provided it holds when n is a prime power. This technique is frequently useful.

An alternative proof of Gauss's Theorem also demonstrates a useful technique. 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

$$0 \leqslant x < 12 \;\&\; \gcd(x, 12) = d \iff \gcd\Big(\frac{x}{d}, \frac{12}{d}\Big) = 1 \;\&\; 0 \leqslant \frac{x}{d} < \frac{12}{d}.$$

So the number of entries in row d is just $\phi(12/d)$. The number of entries in all rows together is 12, so $12 = \sum_{d\mid 12}\phi(d)$.

The last argument was not specific to 12. If $d \mid n$, let

$$S_d^n = \{x \colon 0 \leqslant x < n \;\&\; \gcd(x, n) = d\}.$$

Then $[0, n) = \bigcup_{d\mid n} S_d^n$, and the sets S_d^n are disjoint as d varies over the divisors of n. Therefore

$$n = |[0, n)| = \sum_{d\mid n} |S_d^n|. \tag{‡}$$

But we also have

$$\begin{aligned} x \in S_d^n &\iff 0 \leqslant x < n \;\&\; \gcd(x, n) = d \\ &\iff 0 \leqslant \frac{x}{d} < \frac{n}{d} \;\&\; \gcd\Big(\frac{x}{d}, \frac{n}{d}\Big) = 1 \\ &\iff \frac{x}{d} \in S_1^{n/d}. \end{aligned}$$

So we have a bijection $x \mapsto x/d$ from S_d^n to $S_1^{n/d}$, which means

$$|S_d^n| = |S_1^{n/d}|.$$

Also,

$$|S_1^{n/d}| = \phi\Big(\frac{n}{d}\Big).$$

So (‡) now becomes

$$n = \sum_{d\mid n} \phi\Big(\frac{n}{d}\Big) = \sum_{d\mid n} \phi(d).$$

Thus we have an alternative proof of Gauss's Theorem.

The idea behind the last equation is frequently useful. For any arithmetic function f, we have

$$\sum_{d\mid n} f\Big(\frac{n}{d}\Big) = \sum_{d\mid n} f(d).$$

This is because the function $x \mapsto n/x$ is a permutation of the set of divisors of n. We shall use this for Theorem 26 below.

Is there anything noticeable about the table for $n = 12$? Try $n = 20$:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
20	0																			
10											10									
5						5										15				
4					4				8				12				16			
2			2				6								14				18	
1		1		3				7		9		11		13				17		19

The entries are symmetric about a vertical axis, except for 0. Is there a theorem here?

Theorem 25. *When $n > 1$ and $d \mid n$, the average member of S_d^n is $n/2$:*

$$\frac{1}{|S_d^n|} \sum_{x \in S_d^n} x = \frac{n}{2}.$$

Proof. When $n > 1$, then S_d^n has the permutation $x \mapsto n - x$, so

$$2 \cdot \sum_{x \in S_d^n} x = \sum_{x \in S_d^n} x + \sum_{x \in S_d^n} (n - x) = \sum_{x \in S_d^n} (x + (n - x)) = \sum_{x \in S_d^n} n = n \cdot |S_d^n|. \quad \square$$

Theorem 26. *For all n,*

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Proof. Applying the Möbius Inversion Formula to (†) yields

$$\phi(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot d = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n \cdot \sum_{d|n} \frac{\mu(d)}{d}. \qquad \square$$

Recalling $(*)$, namely $\phi(n) = n \cdot \prod_{p|n}(1 - 1/p)$, we have now

$$\prod_{p|n}\Big(1 - \frac{1}{p}\Big) = \sum_{d|n} \frac{\mu(d)}{d}.$$

For example,

$$\begin{aligned}
\sum_{d|12} \frac{\mu(d)}{d} &= \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(6)}{6} + \frac{\mu(12)}{12} \\
&= 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6} \\
&= 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{2 \cdot 3} \\
&= \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = \prod_{p|12} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

10. Primitive roots

10.1. Order

Recall Euler's Theorem:

$$\gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \pmod{n}.$$

This can be improved in some cases. For example, $255 = 3 \cdot 5 \cdot 17$, so $\phi(255) = \phi(3) \cdot \phi(5) \cdot \phi(17) = 2 \cdot 4 \cdot 16 = 128$, and hence

$$\gcd(a, 255) = 1 \implies a^{128} \equiv 1 \pmod{255}.$$

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

$$a^k \equiv 1 \pmod{n}.$$

If such k does exist, 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 $a^{\phi(n)} \equiv 1 \pmod{n}$, 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 $\mathrm{ord}_{17}(2)$? Just compute powers of 2 *modulo* 17:

$$2,\ 4,\ 8,\ 16 \equiv -1,\ -2,\ -4,\ -8,\ -16 \equiv 1.$$

Then $\mathrm{ord}_{17}(2) = 8$. We also have

$$3,\ 9 \equiv -8,\ -24 \equiv -7,\ -21 \equiv -4,\ -12 \equiv 5,\ 15 \equiv -2,\ -6,\ -18 \equiv -1,$$
$$-3,\ 8,\ 7,\ 4,\ -5,\ 2,\ 6,\ 1.$$

So $\mathrm{ord}_{17}(3) = 16$. Note how, in each computation, halfway through, we just change signs. In the latter case, we computed

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

From this table, 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 $\mathrm{ord}_{17}(-8) = 8$. Likewise, $\mathrm{ord}_{17}(-4) = 4$, and $\mathrm{ord}_{17}(-1) = 2$. So we have

a	1	2	3	4	5	6	7	8
$\mathrm{ord}_{17}(a)$	1		16					
$\mathrm{ord}_{17}(-a)$	2			4				8

How can we complete the table? For example, what is $\mathrm{ord}_{17}(-7)$? Since $-7 \equiv 3^3 \pmod{17}$, and $\gcd(3, 16) = 1$, we have $\mathrm{ord}_{17}(-7) = 16$. Likewise, $\mathrm{ord}_{17}(5) = 16$. But $\mathrm{ord}_{17}(-2) = 16/\gcd(6, 16) = 8$, since $-2 \equiv 3^6 \pmod{17}$. This is by a general theorem to be proved presently. We complete the table thus:

a	1	2	3	4	5	6	7	8
$\mathrm{ord}_{17}(a)$	1	8	16	4	16	16	16	8
$\mathrm{ord}_{17}(-a)$	2	8	16	4	16	16	16	8

Theorem 27. *Suppose* $\gcd(a, n) = 1$. *Then*

a) $a^k \equiv 1 \pmod{n}$ *if and only if* $\mathrm{ord}_n(a) \mid k$;

b) $\mathrm{ord}_n(a^s) = \mathrm{ord}_n(a)/\gcd(s, \mathrm{ord}_n(a))$;

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

$$\frac{\operatorname{ord}_n(a)}{\gcd(s, \operatorname{ord}_n(a))} = \operatorname{ord}_n(a^s).$$

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.) $\square$

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
$\mathrm{ord}_{19}(a)$	1	18	18	9	9	9	3	6	9
$\mathrm{ord}_{19}(-a)$	2	9	9	18	18	18	6	3	18

since

$$\begin{aligned}
\mathrm{ord}_{19}(2^k) = 18 &\iff \gcd(k, 18) = 1 \\
&\iff k \equiv 1, 5, 7, 11, 13, 17 \pmod{18} \\
&\iff 2^k \equiv 2, -6, -5, -4, 3, -9 \pmod{19}; \\
\mathrm{ord}_{19}(2^k) = 9 &\iff \gcd(k, 18) = 2 \\
&\iff k \equiv 2, 4, 8, 10, 14, 16 \pmod{18} \\
&\iff 2^k \equiv 4, -3, 9, -2, 6, 5 \pmod{19}, \\
\mathrm{ord}_{19}(2^k) = 6 &\iff \gcd(k, 18) = 3 \\
&\iff k \equiv 3, 15 \pmod{18} \\
&\iff 2^k \equiv 8, -7 \pmod{19}, \\
\mathrm{ord}_{19}(2^k) = 3 &\iff \gcd(k, 18) = 6 \\
&\iff k \equiv 6, 12 \pmod{18} \\
&\iff 2^k \equiv 7, -8 \pmod{19}, \\
\mathrm{ord}_{19}(2^k) = 2 &\iff \gcd(k, 18) = 9 \\
&\iff k \equiv 9 \pmod{18} \\
&\iff 2^k \equiv -1 \pmod{19}.
\end{aligned}$$

If $d \mid 18$, let $\psi_{19}(d)$ be the number 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

Note that $\psi_{19}(d) = \phi(d)$ here. This is no accident, by Theorem 29 below.

10.2. Groups

We can understand what we are doing algebraically as follows. The set of congruence classes *modulo* n is denoted by

$$\mathbb{Z}_n$$

or $\mathbb{Z}/(n)$ or $\mathbb{Z}/n\mathbb{Z}$. On this set, by Theorem 6, addition and multiplication are well-defined: the set is a **ring.** The set of multiplicatively invertible elements of the ring is denoted by

$$\mathbb{Z}_n{}^{\times}.$$

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 $\bar{k}$.) 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 $\mathbb{Z}_{19}{}^{\times}$:

$$\mathbb{Z}_{18} \cong \mathbb{Z}_{19}{}^{\times},$$
$$(\{0, 1, 2, \dots, 17\}, +) \cong (\{1, 2, 3, \dots, 18\}, \cdot).$$

We have

x	0	1	2	3	4	5	6	7	8
$f_2(x)$	1	2	4	8	16	13	7	14	9
$f_2(x+9)$	18	17	15	11	3	6	12	5	10

10.3. Primitive roots of primes

If $\gcd(a, n) = 1$, and $\operatorname{ord}_n(a) = \phi(n)$, then a is called a **primitive root** of n. So we have shown that 3, but not 2, is a primitive root of 17, and 2 is a primitive root of 19. There is 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 $\phi(18)$.

To prove generally that the number of primitive roots of p is $\phi(p-1)$, we shall need the following (attributed to Joseph-Louis Lagrange, 1736–1813.)

Theorem 28 (Lagrange)**.** *Every congruence of the form*

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod{p}$$

*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

$$x^{k+1} + a_1x^k + \cdots + a_kx + a_{k+1} \equiv 0 \pmod{p} \tag{$*$}$$

has a solution b. Then we can factorize the left member, and rewrite the congruence as

$$(x-b)\cdot(x^k + c_1x^{k-1} + \cdots + c_{k-1}x + c_k) \equiv 0 \pmod{p}.$$

Any solution to this that is different from b is a solution of

$$x^k + c_1x^{k-1} + \cdots + c_{k-1}x + c_k \equiv 0 \pmod{p}.$$

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. □

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.

Theorem 29. *If $d \mid p-1$, let $\psi_p(d)$ be the number of incongruent residues* modulo *p that have order d. Then*

$$\psi_p(d) = \phi(d).$$

Proof. Every number prime to p has an order *modulo* p, and this order divides $\phi(p)$, which is $p-1$; so

$$\sum_{d\mid p-1} \psi_p(d) = p-1.$$

By Gauss's Theorem, 24, we have $\sum_{d\mid p-1}\phi(d)=p-1$; therefore

$$\sum_{d\mid p-1}\psi_p(d)=\sum_{d\mid p-1}\phi(d). \tag{$\dagger$}$$

Hence, to establish $\psi_p(d)=\phi(d)$, it is enough to show that $\psi_p(d)\leqslant\phi(d)$ whenever $d\mid p-1$. Indeed, if we show this, but $\psi_p(e)<\phi(e)$ for some divisor e of $p-1$, then

$$\sum_{d\mid p-1}\psi_p(d)=\sum_{\substack{d\mid p-1\\ d\neq e}}\psi_p(d)+\psi_p(e)<\sum_{\substack{d\mid p-1\\ d\neq e}}\phi(d)+\phi(e)=\sum_{d\mid p-1}\phi(d),$$

contradicting ($\dagger$).

If $\psi_p(d)=0$, then certainly $\psi_p(d)\leqslant\phi(d)$. 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

$$x^d-1\equiv 0 \pmod{p}. \tag{$\ddagger$}$$

But then every power of a is a solution, since $(a^k)^n=(a^n)^k$. Moreover, if $0<k<\ell\leqslant d$, then

$$a^k\not\equiv a^\ell \pmod{p}$$

by Theorem 27. Hence the numbers a, a^2, …, a^d are incongruent solutions to the congruence ($\ddagger$). Moreover, by Lagrange's Theorem, 28, 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 27. The number of such powers is just $\phi(d)$. Therefore $\psi_p(d)=\phi(d)$, under the assumption $\psi_p(d)>0$; in any case, $\psi_p(d)\leqslant\phi(d)$. □

Corollary. *Every prime number has a primitive root.*

Proof. $\psi_p(p-1)=\phi(p-1)\geqslant 1$. □

From analysis, we have the exponential function $x\mapsto \mathrm{e}^x$ or exp from $\mathbb{R}$ to $\mathbb{R}^\times$, where $\mathbb{R}^\times=\mathbb{R}\smallsetminus\{0\}$ (the 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 have been 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 $\mathbb{Z}_{\phi(n)}$ to $\mathbb{Z}_n{}^{\times}$. In particular, a prime p does have a primitive root a, and then $x \mapsto a^x$ is an isomorphism from $\mathbb{Z}_{p-1}$ to $\mathbb{Z}_p{}^{\times}$. Therefore $\mathbb{Z}_p{}^{\times}$ is a cyclic group, and $\mathbb{Z}_n{}^{\times}$ is cyclic if and only if n has a primitive root.

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 have shown that primes have primitive roots, but the converse fails: not every number with a primitive root is prime. In fact, we shall show in § 10.5 that the following numbers have primitive roots:

a) powers of odd primes;
b) 2 and 4;
c) doubles of powers of odd primes.

10.4. Discrete logarithms

The inverse of the function exp from $\mathbb{R}$ onto $(0, \infty)$ is the logarithm function log, where as noted in § 4.5, $\log x = \int_1^x (\mathrm{d}t/t)$. More precisely, this function log is $\log_{\mathrm{e}}$ or ln, since the notation log is sometimes used for $\log_{10}$, that is, the inverse of $x \mapsto 10^x$.

We can use similarly 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

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^k	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Reordering, we have

3^k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

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,

$$\log_3(11 \cdot 14) \equiv \log_3 11 + \log_3 14 \equiv 7 + 9 \equiv 16 \equiv 0 \pmod{16},$$

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* $\phi(n)$. Indeed, by Theorem 27,

$$b^x \equiv b^y \pmod{n} \iff x \equiv y \pmod{\phi(n)}.$$

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

$$\log_b(x^d) \equiv \log_b a \pmod{\phi(n)},$$
$$d \log_b x \equiv \log_b a \pmod{\phi(n)}.$$

If this is to have a solution, then we must have

$$\gcd(d, \phi(n)) \mid \log_b a.$$

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 the 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	$\log_2 \ell \mod 10$
$2^k \mod 11$	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 30. *Suppose n has a primitive root, $\gcd(a,n) = 1$, and*

$$d = \gcd(k, \phi(n)).$$

The following are equivalent:

a) *The congruence*
$$x^k \equiv a \pmod{n} \qquad (\S)$$
is soluble.

b) *The congruence (§) has d solutions.*

c) $a^{\phi(n)/d} \equiv 1 \pmod{n}$.

Proof. The following are equivalent:

$$x^k \equiv a \text{ is soluble} \pmod{n};$$
$$k\log x \equiv \log a \text{ is soluble} \pmod{\phi(n)};$$
$$d \mid \log a;$$
$$\phi(n) \mid \frac{\phi(n)}{d}\cdot \log a;$$
$$\frac{\phi(n)}{d}\cdot \log a \equiv 0 \pmod{\phi(n)};$$
$$\log(a^{\phi(n)/d}) \equiv 0 \pmod{\phi(n)};$$
$$a^{\phi(n)/d} \equiv 1 \pmod{n}.$$

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

$$\begin{aligned} x^k \equiv a \pmod{n} &\iff k \log x \equiv \log a \pmod{\phi(n)} \\ &\iff \frac{k}{d} \cdot \log x \equiv \frac{\log a}{d} \pmod{\frac{\phi(n)}{d}} \\ &\iff \log x \equiv \frac{\log a}{k} \pmod{\frac{\phi(n)}{d}} \\ &\iff \log x \equiv \frac{\log a}{k} + \frac{\phi(n)}{d} \cdot j \pmod{\phi(n)}, \\ &\qquad \text{where } j \in \{0, 1, \dots, d-1\} \\ &\iff x \equiv r^{(\log a)/k} \cdot (r^{\phi(n)/d})^j \pmod{n}, \\ &\qquad \text{where } j \in \{0, 1, \dots, d-1\}. \end{aligned}$$

These d solutions are incongruent, as $\operatorname{ord}_n(r) = \phi(n)$. □

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:

$$2, 4, p^s, 2 \cdot p^s,$$

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 $2 \mid \phi(k)$.*

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, $\phi(k) = 2^s - 2^{s-1} = 2^{s-1}$, which is even. In the second case, $\phi(k) = \phi(p^s) \cdot \phi(m)$, which is even, since $\phi(p^s) = p^s - p^{s-1}$, the difference of two odd numbers. □

Theorem 31. *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

$$a^{\phi(m)} \equiv 1 \pmod{m}; \qquad a^{\phi(n)} \equiv 1 \pmod{n};$$
$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{m, n},$$
$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{\operatorname{lcm}(m,n)},$$
$$a^{\operatorname{lcm}(\phi(m),\phi(n))} \equiv 1 \pmod{mn}.$$

By the lemma, 2 divides both $\phi(m)$ and $\phi(n)$, so

$$\operatorname{lcm}(\phi(m),\phi(n)) \mid \frac{\phi(m)\phi(n)}{2},$$

that is, $\operatorname{lcm}(\phi(m),\phi(n)) \mid \phi(mn)/2$. Therefore

$$\operatorname{ord}_{mn}(a) \leqslant \frac{\phi(mn)}{2},$$

so a is not a primitive root of mn. □

Theorem 32. *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

$$a^{\phi(2^{2+k})/2} \equiv 1 \pmod{2^{2+k}}.$$

Since $\phi(2^{2+k}) = 2^{2+k} - 2^{1+k} = 2^{1+k}$, 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 $k = \ell$: 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:

$$a^{2^{1+\ell}} = (a^{2^\ell})^2 = (1 + 2^{2+\ell} \cdot m)^2 = 1 + 2^{3+\ell} \cdot m + 2^{4+2\ell} \cdot m^2.$$

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*

$$\mathrm{ord}_{p^k}(r) = (p-1)p^{\ell}$$

for some ℓ, where $0 \leqslant \ell < k$.

Proof. Let $\mathrm{ord}_{p^k}(r) = n$. Then $n \mid \phi(p^k)$. But $\phi(p^k) = p^k - p^{k-1} = (p-1)\cdot p^{k-1}$. 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 $\mathrm{ord}_p(r) \mid n$. But r is a primitive root of p, so $\mathrm{ord}_p(r) = \phi(p) = p-1$. Therefore

$$p - 1 \mid n.$$

The claim now follows. □

Theorem 33. *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 $\mathrm{ord}_{p^2}(r) = p-1$, 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 $\mathrm{ord}_{p^2}(r+p) \neq p-1$, so by the lemma, the order must be $(p-1)\cdot p$, that is, $\phi(p^2)$. This means r is a primitive root of p^2. □

Theorem 34. *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 $k = \ell$. This means

$$\mathrm{ord}_{p^{1+\ell}}(r) = (p-1) \cdot p^{\ell}.$$

In particular,

$$r^{(p-1)\cdot p^{\ell-1}} \not\equiv 1 \pmod{p^{1+\ell}}.$$

However, since $\phi(p^{\ell}) = (p-1) \cdot p^{\ell-1}$, 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:

$$\begin{aligned} r^{(p-1)\cdot p^{\ell}} &= (1 + p^{\ell} \cdot m)^p \\ &= 1 + p^{1+\ell} \cdot m + \binom{p}{2} \cdot p^{2\ell} \cdot m^2 + \binom{p}{3} \cdot p^{3\ell} \cdot m^3 + \cdots . \end{aligned}$$

Since $p > 2$, so that $p \mid \binom{p}{2}$, we have

$$\begin{aligned} r^{(p-1)\cdot p^{\ell}} &\equiv 1 + p^{1+\ell} \cdot m \pmod{p^{2+\ell}} \\ &\not\equiv 1 \pmod{p^{2+\ell}}. \end{aligned}$$

Therefore we must have

$$\mathrm{ord}_{p^{2+\ell}}(r) = (p-1) \cdot p^{1+\ell} = \phi(p^{2+\ell}),$$

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 33. 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 $\phi(9)$. By Theorem 34 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, $\phi(27) = 18$ 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 $\phi(18) = 6$ 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 35. *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, so that $\gcd(r, 2p^s) = 1$. Let $n = \operatorname{ord}_{2p^s}(r)$. We want to show $n = \phi(2p^s)$. We have

$$n \mid \phi(2p^s).$$

Also $r^n \equiv 1 \pmod{2p^s}$, so $r^n \equiv 1 \pmod{p^s}$, and therefore

$$\operatorname{ord}_{p^s}(r) \mid n.$$

But $\operatorname{ord}_{p^s}(r) = \phi(p^s) = \phi(2p^s)$. Hence

$$\phi(2p^s) \mid n.$$

So $n = \phi(2p^s)$. □

11. Quadratic reciprocity

11.1. Quadratic equations

Now we return to high-school-like problems. With respect to the modulus 11, let us solve

$$x^2 - 4x - 1 \equiv 0. \tag{$*$}$$

We have $x^2-4x-1 \equiv x^2-4x-12 \equiv (x-6)(x+2)$, so the solutions to $(*)$ include 6 and -2, or rather 6 and 9. Since the modulus is prime, these are the *only* incongruent solutions, by Lagrange's Theorem, 28. Alternatively, $x^2 - 4x - 1 \equiv x^2 + 7x + 10 \equiv (x+5)(x+2)$, so x is -5 or -2, that is, 6 or 9 again.

To solve

$$3x^2 - 4x - 6 \equiv 0 \pmod{13},$$

we can search for a factorization as before; but we can also **complete the square:**

$$\begin{aligned}
3x^2 - 4x - 6 \equiv 0 &\iff x^2 - \frac{4}{3}x - 2 \equiv 0\\
&\iff x^2 - \frac{4}{3}x + \frac{4}{9} \equiv 2 + \frac{4}{9}\\
&\iff \left(x - \frac{2}{3}\right)^2 \equiv \frac{22}{9} \equiv 1\\
&\iff x - \frac{2}{3} \equiv \pm 1\\
&\iff x \equiv \frac{2}{3} \pm 1\\
&\iff x \equiv \frac{5}{3} \text{ or } \frac{-1}{3}\\
&\iff x \equiv 6 \text{ or } 4.
\end{aligned}$$

Here we can divide by 3 and 9 because they are invertible *modulo* 13; indeed, $3 \cdot 9 \equiv 1 \pmod{13}$, so $1/3 \equiv 9$ and $1/9 \equiv 3 \pmod{13}$.

If we take this approach with the first problem, we have, *modulo* 11,

$$\begin{aligned}
x^2 - 4x - 1 \equiv 0 &\iff x^2 - 4x + 4 \equiv 5\\
&\iff (x-2)^2 \equiv 5.
\end{aligned}$$

If 5 is a square *modulo* 11, then there is a solution; if not, not. But $5 \equiv 16 \equiv 4^2$, so we have

$$\begin{aligned} x^2 - 4x - 1 \equiv 0 &\iff (x-2)^2 \equiv 4^2 \\ &\iff x - 2 \equiv \pm 4 \\ &\iff x \equiv 2 \pm 4 \\ &\iff x \equiv 6 \text{ or } 9, \end{aligned}$$

as before. But the congruence

$$x^2 \equiv 5 \pmod{13}$$

has no solution. How do we know? One way is by trial. As 2 is a primitive root of 13, and 0 is not a solution of the congruence, every solution would be a power of 2. But we have, *modulo* 13,

k	0	1	2	3	4	5	6	7	8	9	10	11
2^k	1	2	4	-5	3	6	-1	-2	-4	5	-3	-6
2^{2k}	1	4	3	-1	-4	-3	1	4	3	-1	-4	-3

and 5 does not appear on the bottom row. So 5 is not a square *modulo* 13. Now we shall work out an easier way to find such results.

11.2. Quadratic residues

Henceforth let p be an odd prime, and $\gcd(a, p) = 1$. If $p \nmid a$, we say a is a **quadratic residue** of p if the congruence

$$x^2 \equiv a \pmod{p}$$

is soluble; otherwise, a is a **quadratic non-residue** of p. So we have just seen that the quadratic residues of 13 are ± 1, ± 3, and ± 4, or rather 1, 3, 4, 9, 10, and 12; the quadratic non-residues are 2, 5, 6, 7, 8, and 11. So there are six residues, and six non-residues. We shall see that this equality is not accidental (by Theorem 39 below).

Theorem 36 (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*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Proof. Let r be a primitive root of p. If $x^2 \equiv a \pmod{p}$ has a solution, then that solution is r^k for some k. Then

$$a^{(p-1)/2} \equiv ((r^k)^2)^{(p-1)/2} \equiv (r^k)^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Theorem (§ 7.2).

In any case, $a \equiv r^\ell \pmod{p}$ for some ℓ. Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Then

$$1 \equiv (r^\ell)^{(p-1)/2} \equiv r^{\ell\cdot(p-1)/2} \pmod{p},$$

so $\mathrm{ord}_p(r) \mid \ell \cdot (p-1)/2$, that is,

$$p-1 \mid \ell \cdot \frac{p-1}{2}.$$

Therefore $\ell/2$ is an integer, that is, ℓ is even. Say $\ell = 2m$. Then $a \equiv r^{2m} \equiv (r^m)^2 \pmod{p}$. □

What other congruence class can $a^{(p-1)/2}$ belong to, besides 1? Only -1, since $a^{p-1} \equiv 1 \pmod{p}$, by Fermat's Theorem. So $a^{(p-1)/2} \equiv -1 \pmod{p}$ if and only if a is a quadratic non-residue of p.

Another way to prove this is the following: 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 may 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 $(b_1, \dots, b_{p-1})$ recursively. If b_k has been chosen when $k < \ell < p-1$, 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

$$\{1, \dots, p-1\} = \left\{b_1, \frac{a}{b_1}, \dots, b_{p-1}, \frac{a}{b_{p-1}}\right\}.$$

Now multiply everything together:

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}.$$

But we know $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem, 18. Thus

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

when a is a quadratic non-residue of p.

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 $p - b_1$. Multiplication now gives us

$$\begin{aligned}(p-1)! &\equiv b_1 \cdot (p-b_1) \cdot b_2 \cdot a/b_2 \cdots b_{(p-1)/2} \cdot a/b_{(p-1)/2} \\ &\equiv -a \cdot a^{(p-1)/2-1} \\ &\equiv -a^{(p-1)/2} \pmod{p}.\end{aligned}$$

By Wilson's Theorem again, we have

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

when a is a quadratic residue of p.

11.3. The Legendre symbol

Again, p is an odd prime, and $p \nmid a$. We define the **Legendre symbol** (a/p), by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p; \\ -1, & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

(This is named for Adrien-Marie Legendre, 1752–1833.)

Then by Euler's Criterion we have immediately

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{$\dagger$}$$

The Legendre symbol easily has the following properties:

$$\begin{gathered} a \equiv b \pmod{p} \implies (a/p) = (b/p), \\ (a^2/p) = 1, \\ (1/p) = 1, \\ (-1/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \end{gathered} \tag{$\ddagger$}$$

The last equation is equivalent to Theorem 19 above; but it now follows also by direct computation by means of (†). Finally, we have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

since $(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}$, and equality of (ab/p) and $(a/p)(b/p)$ follows since each is ± 1 and $p > 2$. With these properties, we can calculate many Legendre symbols. For example,

$$\left(\frac{50}{19}\right) = \left(\frac{12}{19}\right) = \left(\frac{2}{19}\right)^2 \left(\frac{3}{19}\right) = \left(\frac{3}{19}\right),$$
$$3^{(19-1)/2} \equiv 3^9 \equiv 3^8 \cdot 3 \equiv 9^4 \cdot 3 \equiv 81^2 \cdot 3 \equiv 5^2 \cdot 3 \equiv 6 \cdot 3 \equiv 18 \equiv -1 \pmod{19},$$

so $(50/19) = -1$, which means the congruence $x^2 \equiv 50 \pmod{19}$ has no solution.

We may ask whether (‡) has a simpler form, owing to the existence of only finitely many p satisfying one of the case. This possibility fails.

Theorem 37. *There are infinitely many primes p such that $p \equiv 3 \pmod{4}$.*

Proof. Suppose $(q_1, q_2, \dots, q_n)$ 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. □

This argument fails when 3 is replaced by 1, since $3^2 \equiv 1 \pmod{4}$. Nonetheless, we still have:

Theorem 38. *There are infinitely many primes p such that $p \equiv 1 \pmod{4}$.*

Proof. Suppose $(q_1, q_2, \dots, q_n)$ 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: $(-1)^{(13-1)/2} = (-1)^6 = 1$. Hence the table will be symmeti $(13 - a/13) = (-a/13) = (-1/13) \cdot (a/13) = (a/13)$; 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 39. *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

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{r^k}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{r}{p}\right)^k = \sum_{k=1}^{p-1} (-1)^k = 0,$$

since $r^{(p-1)/2} \equiv -1 \pmod{p}$, since r is a primitive root. □

So now we have

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

Lemma (Gauss). *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 of the set

$$\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

whose remainders after division by p are greater than $p/2$.

For example, to find (3/19), we can look at

$$3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27,$$

whose remainders on division by 19 are, respectively,

$$3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 2,\ 5,\ 8.$$

Of those, 12, 15, and 18 exceed 19/2, and these are three; so

$$\left(\frac{3}{19}\right) = (-1)^3 = -1.$$

Proof of Gauss's Lemma. If $1 \leqslant k \leqslant p-1$, let b_k be such that

$$1 \leqslant b_k \leqslant p-1, \qquad\qquad ka \equiv b_k \pmod{p}.$$

Then $\{1, 2, \dots, p-1\} = \{b_1, b_2, \dots, b_{p-1}\}$, because the b_k are distinct:

$$b_k = b_\ell \iff ka \equiv \ell a \iff k \equiv \ell.$$

In the set $\{b_1, b_2, \dots, b_{(p-1)/2}\}$, let n be the number of elements that are greater than $p/2$. We want to show

$$(-1)^n = \left(\frac{a}{p}\right).$$

There is some permutation σ of $\{1, 2, \dots, (p-1)/2\}$ such that

$$b_{\sigma(1)} > b_{\sigma(2)} > \cdots > b_{\sigma(n)} > \frac{p}{2} > b_{\sigma(n+1)} > \cdots > b_{\sigma((p-1)/2)}.$$

Observe now that

$$b_{p-k} = p - b_k;$$

indeed, both numbers are in $\{1, 2, \dots, p-1\}$, and

$$b_{p-k} \equiv (p-k)a \equiv -ka \equiv -b_k \equiv p - b_k \pmod{p}.$$

In particular, if $1 \leqslant k \leqslant (p-1)/2$, then $p - b_k \notin \{b_1, b_2, \dots, b_{(p-1)/2}\}$. Since σ just permutes the set of such k, we have

$$\{p - b_{\sigma(1)}, p - b_{\sigma(2)}, \dots, p - b_{\sigma(n)}, b_{\sigma(n+1)}, \dots b_{\sigma((p-1)/2)}\} = \left\{1, 2, \dots, \frac{p-1}{2}\right\}.$$

Now take products:

$$\begin{aligned}\frac{p-1}{2}! &\equiv (p-b_{\sigma(1)})(p-b_{\sigma(2)})\cdots(p-b_{\sigma(n)})b_{\sigma(n+1)}\cdots b_{\sigma((p-1)/2)}\\ &\equiv (-1)^n \cdot b_{\sigma(1)}\cdots b_{\sigma((p-1)/2)}\\ &\equiv (-1)^n \cdot b_1 \cdots b_{(p-1)/2}\\ &\equiv (-1)^n \cdot a \cdot 2a \cdot 3a \cdots \frac{p-1}{2}a\\ &\equiv (-1)^n \cdot \frac{p-1}{2}! \cdot a^{(p-1)/2} \pmod{p}.\end{aligned}$$

Therefore, since $p \nmid ((p-1)/2)!$, we have

$$1 \equiv (-1)^n \cdot a^{(p-1)/2} \equiv (-1)^n \cdot (a/p) \pmod{p}.$$

As both $(-1)^n$ and (a/p) are ± 1, the claim follows. □

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:

Theorem 40. *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

$$2 \cdot 1,\ 2 \cdot 2,\ \ldots,\ 2 \cdot \frac{p-1}{2}.$$

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 $p/4 < k \leqslant (p-1)/2$. This means

$$n = \frac{p-1}{2} - \left[\frac{p}{4}\right],$$

where $x \mapsto [x]$ is the **greatest-integer function.** Now consider the possibilities:

a) $p = 8k+1 \implies n = 4k - [2k+1/4] = 2k$, even;
b) $p = 8k+3 \implies n = 4k+1 - [2k+3/4] = 2k+1$, odd;
c) $p = 8k+5 \implies n = 4k+2 - [2k+5/4] = 4k+1$, odd;
d) $p = 8k+7 \implies n = 4k+3 - [2k+7/4] = 4k+2$, even.

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. We can also use the result about $(2/p)$ to find some primitive roots. A **Germain prime** (named for Sophie Germain, 1776–1831) is an odd prime p such that $2p+1$ is also prime.

Theorem 41. *If p is a Germain prime, then $2p+1$ has the primitive root $(-1)^{(p-1)/2} \cdot 2$, which is 2 if $p \equiv 1 \pmod 4$, and is otherwise -2.*

Hence, for example, we have

p	3	5	11	23	29	41	53	83	89	113	131	173	179	191	233
$2p+1$	7	11	23	47	59	83	107	167	179	227	263	347	359	383	467
p.r. of $2p+1$	-2	2	-2	-2	2	2	2	-2	2	2	-2	2	-2	-2	2

Proof of theorem. Denote $2p+1$ by q. Then $\phi(q) = 2p$, whose divisors are 1, 2, p, and $2p$. Let $r = (-1)^{(p-1)/2} \cdot 2$. We want to show $\operatorname{ord}_q(r) \notin \{1, 2, p\}$. But $p \geqslant 3$, so $q \geqslant 7$, and hence $r^1, r^2 \not\equiv 1 \pmod q$. Hence $\operatorname{ord}_q(r) \notin \{1, 2\}$. It remains to show $\operatorname{ord}_q(r) \neq p$. But we know, 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. If $p \equiv 1 \pmod 4$, then $r = 2$, but also $q \equiv 3 \pmod 8$, so $(r/q) = (2/q) = -1$. If $p \equiv 3 \pmod 4$, then $r = -2$, but also $q \equiv 7 \pmod 8$, and $(-1/q) = (-1)^{(q-1)/2} = (-1)^p = -1$, so $(r/q) = (-2/q) = (-1/q)(2/q) = -1$. □

It is not known whether there infinitely many Germain primes.

Another consequence of Theorem 40 is:

Theorem 42. *There are infinitely many primes congruent to -1 modulo 8.*

Proof. Let $q_1, \dots, q_n$ 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. $\square$

11.5. The Law of Quadratic Reciprocity

We now aim to establish the Law of Quadratic Reciprocity: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^n, \qquad \text{where} \qquad n = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Equivalently,

$$\left(\frac{q}{p}\right) = \begin{cases} (p/q), & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod{4}; \\ -(p/q), & \text{if } q \equiv 3 \equiv p \pmod{4}. \end{cases}$$

Then we shall be able to compute as follows:

$$\begin{aligned}
\left(\frac{365}{941}\right) &= \left(\frac{5}{941}\right)\left(\frac{73}{941}\right) && [\text{factorizing}] \\
&= \left(\frac{941}{5}\right)\left(\frac{941}{73}\right) && [5, 73 \equiv 1 \pmod{4}] \\
&= \left(\frac{1}{5}\right)\left(\frac{65}{73}\right) && [\text{dividing}] \\
&= \left(\frac{5}{73}\right)\left(\frac{13}{73}\right) && [\text{factorizing}] \\
&= \left(\frac{73}{5}\right)\left(\frac{73}{13}\right) && [5, 13 \equiv 1 \pmod{4}] \\
&= \left(\frac{3}{5}\right)\left(\frac{8}{13}\right) && [\text{dividing}] \\
&= \left(\frac{5}{3}\right)\left(\frac{2}{13}\right)^3 && [5 \equiv 1 \pmod{4}; \text{ factorizing}] \\
&= \left(\frac{2}{3}\right)\left(\frac{2}{13}\right) && [(p/q)^2 = 1] \\
&= (-1)(-1) = 1 && [3 \equiv 3 \pmod{8};\ 13 \equiv -3 \pmod{8}].
\end{aligned}$$

To prove the Law, we shall use the following consequence of Gauss's Lemma:

Lemma. *If p is an odd prime, $p \nmid a$, and a is odd, then*

$$\left(\frac{a}{p}\right) = (-1)^n, \qquad \textit{where} \qquad n = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right].$$

Proof. As in the proof of Gauss's Lemma, if $1 \leqslant k \leqslant p-1$, we define b_k by

$$1 \leqslant b_k \leqslant p-1 \qquad \& \qquad ka \equiv b_k \pmod p.$$

Then

$$ka = p \cdot \left[\frac{ka}{p}\right] + b_k,$$

so

$$\sum_{k=1}^{(p-1)/2} ka = p \cdot \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] + \sum_{k=1}^{(p-1)/2} b_k. \tag{§}$$

For Gauss's Lemma, we introduced a permutation σ of $\{1, \ldots, (p-1)/2\}$ such that, for some n,

$$b_{\sigma(1)} > \cdots > b_{\sigma(n)} > \frac{p}{2} > b_{\sigma(n+1)} > \cdots b_{\sigma((p-1)/2)},$$

and we showed $(a/p) = (-1)^n$ after first showing

$$\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{p - b_{\sigma(1)}, \ldots, p - b_{\sigma(n)}, b_{\sigma(n+1)}, \ldots b_{\sigma((p-1)/2)}\}.$$

Now take sums:

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{n} (p - b_{\sigma(k)}) + \sum_{\ell=n+1}^{(p-1)/2} b_{\sigma(\ell)}.$$

Subtracting this from (§) (and using that $\sum_{k=1}^{(p-1)/2} b_{\sigma(k)} = \sum_{k=1}^{(p-1)/2} b_k$) gives

$$(a-1) \cdot \sum_{k=1}^{(p-1)/2} k = p \cdot \Big(\sum_{k=1}^{n} \left[\frac{ka}{p}\right] - n\Big) + 2 \cdot \sum_{k=1}^{n} b_{\sigma(k)}.$$

Since $a-1$ is even, but p is odd, we conclude

$$\sum_{k=1}^{n} \left[\frac{ka}{p}\right] \equiv n \pmod 2,$$

which yields the claim. □

Theorem 43 (Law of Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^n, \tag{¶}$$

where

$$n = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

This Law 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.

Proof of Quadratic Reciprocity. By the lemma, we have (¶), where

$$n = \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2} \left[\frac{\ell q}{p}\right].$$

So it is enough to show

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2} \left[\frac{\ell q}{p}\right].$$

First consider the example where $p = 5$ and $q = 7$. Then

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = 2 \cdot 3 = 6;$$

$$\begin{aligned}\sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2} \left[\frac{\ell q}{p}\right] &= \left[\frac{5}{7}\right] + \left[\frac{10}{7}\right] + \left[\frac{15}{7}\right] + \left[\frac{7}{5}\right] + \left[\frac{14}{5}\right] \\ &= 0 + 1 + 2 + 1 + 2 = 6.\end{aligned}$$

Here 6 is the number of certain points in a lattice, as in Fig. 11.1. In general, $((p-1)/2) \cdot ((q-1)/2)$ is the number of ordered pairs (ℓ, k) of integers such that

$$1 \leqslant \ell \leqslant \frac{p-1}{2}, \qquad 1 \leqslant k \leqslant \frac{q-1}{2}.$$

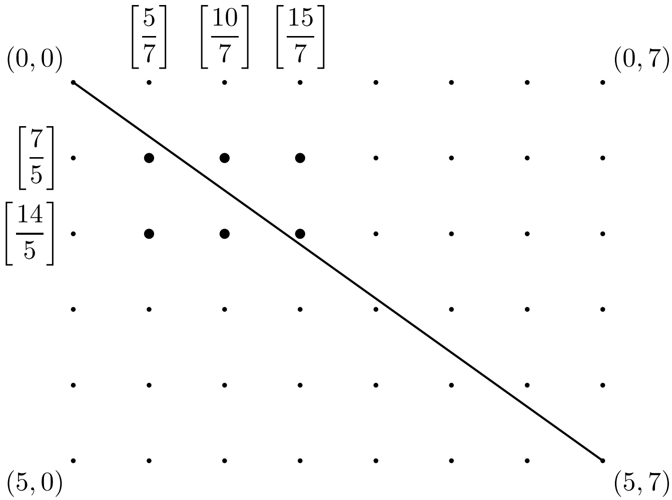


Figure 11.1. Quadratic reciprocity in case $p = 5$, $q = 7$. The diagonal separates sets A and B. The label $\left[\frac{10}{7}\right]$, for example, is also the number (which is 1) of points of A that lie below it.

Then $\ell/k \neq p/q$, since p and q are co-prime. Hence the set of these pairs (ℓ, k) is a disjoint union $A \cup B$, where

$$\begin{aligned}
(\ell, k) \in A &\iff \frac{\ell}{k} < \frac{p}{q};\\
(\ell, k) \in B &\iff \frac{\ell}{k} > \frac{p}{q} \iff \frac{k}{\ell} < \frac{q}{p}.
\end{aligned}$$

Hence

$$\begin{aligned}
A &= \left\{(\ell, k) \in \mathbb{Z} \times \mathbb{Z} \colon 1 \leqslant k \leqslant \frac{q-1}{2} \;\&\; 1 \leqslant \ell \leqslant \left[\frac{kp}{q}\right]\right\},\\
B &= \left\{(\ell, k) \in \mathbb{Z} \times \mathbb{Z} \colon 1 \leqslant \ell \leqslant \frac{p-1}{2} \;\&\; 1 \leqslant k \leqslant \left[\frac{\ell q}{p}\right]\right\},
\end{aligned}$$

so

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = |A \cup B| = |A| + |B| = \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] + \sum_{\ell=1}^{(p-1)/2} \left[\frac{\ell q}{p}\right]. \qquad \square$$

Again, the more useful form of the theorem is

$$\left(\frac{q}{p}\right) = \begin{cases} (p/q), & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4; \\ -(p/q), & \text{if } q \equiv 3 \equiv p \pmod 4. \end{cases}$$

Hence, for example,

$$\left(\frac{47}{199}\right) = -\left(\frac{199}{47}\right) = -\left(\frac{11}{47}\right) = \left(\frac{47}{11}\right) = \left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

We have used here the formula for $(2/p)$ in Theorem 40. What about $(3/p)$? We can compute:

$$\left(\frac{3}{p}\right) = \left\{ \begin{aligned} \left(\frac{p}{3}\right), &\text{ if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right), &\text{ if } p \equiv 3 \pmod 4 \end{aligned} \right\}, \qquad \left(\frac{p}{3}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 3 \\ -1, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

By the Chinese Remainder Theorem, we have

$$\left\{ \begin{array}{ll} p \equiv 1 & (4) \\ p \equiv 1 & (3) \end{array} \right\} \iff p \equiv 1 \quad (12), \qquad \left\{ \begin{array}{ll} p \equiv 1 & (4) \\ p \equiv 2 & (3) \end{array} \right\} \iff p \equiv 5 \quad (12),$$
$$\left\{ \begin{array}{ll} p \equiv 3 & (4) \\ p \equiv 1 & (3) \end{array} \right\} \iff p \equiv 7 \quad (12), \qquad \left\{ \begin{array}{ll} p \equiv 3 & (4) \\ p \equiv 2 & (3) \end{array} \right\} \iff p \equiv 11 \quad (12).$$

Actually this is not by the CRT. Direct computation gives the leftward implications $\Leftarrow$; then the rightward implications $\Rightarrow$ follow by contraposition, so to speak. But the CRT establishes the rightward implication in any one case, without consideration of the others.) Therefore

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod p, \\ -1, & \text{if } p \equiv \pm 5 \pmod p. \end{cases}$$

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

$$\begin{cases} x^2 \equiv a \pmod{m}, \\ x^2 \equiv a \pmod{n} \end{cases}$$

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:

$$\left\{\begin{array}{l} x \equiv 4 \pmod{23}, \\ x \equiv 10 \pmod{29} \end{array}\right\}, \qquad \left\{\begin{array}{l} x \equiv 4 \pmod{23}, \\ x \equiv -10 \pmod{29} \end{array}\right\},$$
$$\left\{\begin{array}{l} x \equiv -4 \pmod{23}, \\ x \equiv 10 \pmod{29} \end{array}\right\}, \qquad \left\{\begin{array}{l} x \equiv -4 \pmod{23}, \\ x \equiv -10 \pmod{29} \end{array}\right\}.$$

One finds $x \equiv \pm 19, \pm 280 \pmod{667}$, or $x \equiv 648, 280, 387, 19 \pmod{667}$.

So now $x^2 \equiv a \pmod{n}$ is soluble if and only if the congruences

$$x^2 \equiv a \pmod{p^{k(p)}}$$

are soluble, where $n = \prod_{p|n} p^{k(p)}$.

Theorem 44. *If p is odd, and a is prime to p, then the following are equivalent:*

a) $(a/p) = 1$,

b) *the congruence*
$$x^2 \equiv a \pmod{p^k} \tag{$\|$}$$
is soluble for some positive k,

c) *the congruence* ($\|$) *is soluble for all positive k.*

Proof. Suppose $b^2 \equiv a \pmod{p^\ell}$ for some positive ℓ. This means

$$b^2 = a + c \cdot p^\ell$$

for some c. Then

$$\begin{aligned} (b + p^\ell \cdot y)^2 &= b^2 + 2bp^\ell \cdot y + p^{2\ell} \cdot y^2 \\ &= a + (c + 2by)p^\ell + p^{2\ell} \cdot y^2 \end{aligned}$$

Therefore $(b+p^\ell \cdot y)^2 \equiv a \pmod{p^{\ell+1}} \iff c+2by \equiv 0 \pmod{p}$. But the latter congruence is soluble, since p is odd. $\square$

We must finally consider powers of 2.

Theorem 45. *Suppose a is odd. Then:*

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) $x^2 \equiv a \pmod 8$ *is soluble;*
   (ii) $x^2 \equiv a \pmod{2^{2+k}}$ *is soluble for some positive* k*;*
   (iii) $x^2 \equiv a \pmod{2^{2+k}}$ *is soluble for all positive* k*;*
   (iv) $a \equiv 1 \pmod 8$.

Proof. The first two parts are easy. So, are (ci)⇔(civ) and (ciii)⇒(cii)⇒(ci). We shall show (ci)⇒(ciii) by induction. Suppose $b^2 \equiv a \pmod{2^{2+\ell}}$ for some positive ℓ. 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* $p^{3+\ell}$ if and only if $c + by \equiv 0 \pmod 2$. But this congruence is soluble, since b is odd (since a is odd). □

12. Lagrange

A **Diophantine equation** (named after Diophantus, of the 3rd century C.E.) is a polynomial equation with integer coefficients for which the solutions sought are integers. Then

$$x^2 + y^2 = z^2$$

is a Diophantine equation among whose solutions are $(3, 4, 5)$ and $(5, 12, 13)$ are solutions. The additional condition $x = y$ yields the Diophantine equation

$$2x^2 = z^2,$$

which we know from § 1.3 is not soluble. We considered Diophantine equations $ax + by = c$ in Chapter 3.

Now we shall show that, if n is a natural number, then the Diophantine equation

$$x^2 + y^2 + z^2 + w^2 = n$$

is soluble.

If p is an odd prime, we know that the congruence $x^2 \equiv -1 \pmod{p}$ is soluble if and only if $(-1/p) = 1$, that is, $(-1)^{(p-1)/2} = 1$, that is, $p \equiv 1 \pmod{4}$.

Lemma. *For every prime p, the congruence*

$$x^2 + y^2 \equiv -1 \pmod{p}$$

is soluble.

Proof. The claim is easy when $p = 2$. So assume now p is odd. We define two sets:

$$A = \left\{x^2 : 0 \leqslant x \leqslant \frac{p-1}{2}\right\},$$
$$B = \left\{-y^2 - 1 : 0 \leqslant x \leqslant \frac{p-1}{2}\right\}.$$

We shall show that A and B have elements representing the same congruence class *modulo* p; that is, A contains some a, and B contains some b, such that $a \equiv b \pmod{p}$. To prove this, note first that distinct elements of A are incongruent, and likewise of B. Indeed, if a_0 and a_1 are between 0 and $(p-1)/2$ inclusive, and ${a_0}^2 \equiv {a_1}^2 \pmod{p}$, then $a_0 \equiv \pm a_1 \pmod{p}$. If $a_0 \equiv -a_1$, then $a_0 = p - a_1$, which is absurd. Hence $a_0 \equiv a_1 \pmod{p}$, so $a_0 = a_1$.

Hence the elements of A represent $(p-1)/2+1$ distinct congruence classes *modulo* p, and so do the elements of B. Since $2((p-1)/2+1) = p+1$, and there are only p distinct congruence classes *modulo* p, there must be a class represented both in A and in B, by the **Pigeonhole Principle.** □

Another way to express the lemma is that, for all primes p, there are a, b, and m such that

$$a^2 + b^2 + 1 = mp.$$

Hence there are a, b, c, d, and m such that

$$a^2 + b^2 + c^2 + d^2 = mp.$$

We shall show that we can require $m = 1$. We can combine this with the following:

Theorem 46 (Euler)**.** *The product of two sums of four squares is the sum of four squares.*

Proof. One can confirm that

$$\begin{aligned}(a^2+b^2+c^2+d^2)(q^2+r^2+s^2+t^2) = \; & (aq+br+cs+dt)^2 + \\ & (ar-bq+ct-ds)^2 + \\ & (as-bt-cq+dr)^2 + \\ & (at+bs-cr-dq)^2\end{aligned}$$

by expanding each side. □

Theorem 47 (Lagrange)**.** *Every positive integer is the sum of four squares.*

Proof. By the lemma and Euler's Theorem (46), it is now enough to show the following. Let p be a prime. Suppose m is a positive integer such that

$$a^2 + b^2 + c^2 + d^2 = mp \tag{$*$}$$

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
$$\left(\frac{a+b}{2}\right)^2+\left(\frac{a-b}{2}\right)^2=\frac{n}{2},$$
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

$$\left(\frac{a+b}{2}\right)^2+\left(\frac{a-b}{2}\right)^2+\left(\frac{c+d}{2}\right)^2+\left(\frac{c-d}{2}\right)^2=\frac{m}{2}\cdot p.$$

Henceforth we may assume m is odd. Then there are q, r, s and t *strictly* between $-m/2$ and $m/2$ such that

$$q\equiv a,\quad r\equiv b,\quad s\equiv c,\quad t\equiv d \pmod{m}.$$

Then
$$q^2+r^2+s^2+t^2\equiv 0 \pmod{m},$$
but also $q^2+r^2+s^2+t^2<m^2$, so

$$q^2+r^2+s^2+t^2=km$$

for some positive k less than m. We now have

$$(a^2+b^2+c^2+d^2)(q^2+r^2+s^2+t^2)=km^2p.$$

By Euler's Theorem, we know the left-hand side as a sum of four squares. Moreover, by checking the proof of Euler's Theorem, we can see that each of the squared numbers in that sum is divisible by m:

$$\begin{aligned}
&aq+br+cs+dt\equiv q^2+r^2+s^2+t^2\equiv 0 \pmod{m},\\
&ar-bq+ct-ds\equiv qr-rq+st-ts=0,\\
&as-bt+cq+dr\equiv qs-rt-sq+tr=0,\\
&at+bs-cr-dq\equiv qt+rs-sr-tq=0.
\end{aligned}$$

Therefore we obtain kp as a sum of four squares. □

A. Foundations of Number-Theory

Theorems about natural numbers have been known for thousands of years. Some of these theorems come down to us in Euclid's *Elements* [5], for example, or Nicomachus's *Introduction to Arithmetic* [10]. 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 Axiom 48 below. This axiom lists five conditions that the natural numbers meet. Richard Dedekind published these conditions in 1888 [3, II, § 71, p. 67]. In 1889, Giuseppe Peano [11, § 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 A.9). Others suggest that the possibility of definition by recursion (Theorem A.1) can be proved by induction (Axiom 48(e)) 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 why I have written these notes.

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 $f(a) = b$. Finally, f can also be written as $x \mapsto f(x)$.

Axiom and definition 48. *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) *Zero is not a successor: if* $n \in \mathbb{N}$*, then* $\mathrm{s}(n) \neq 0$*.*
d) *Distinct natural numbers have distinct successors: if* $n, m \in \mathbb{N}$ *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 49. 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 A.1. *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 A.1 (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 50. In its statement (though not the proof), the Recursion Theorem assumes only parts (a) and (b) of Axiom 48. 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 51 (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,

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

Lemma A.2. *For all n and m in $\mathbb{N}$,*
a) $1 + n = \mathrm{s}(n)$;
b) $\mathrm{s}(m) + n = \mathrm{s}(m + n)$.

Theorem A.2. *For all n, m, and k in $\mathbb{N}$,*
a) $n + m = m + n$;
b) $(n + m) + k = n + (m + k)$;

Remark 52. It is possible to prove by induction alone that an operation of addition with the properties described in ¶¶51–A.2 exists uniquely.

Definition 53 (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,

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

Lemma A.3. *For all n and m in $\mathbb{N}$,*
a) $1 \cdot n = n$;
b) $(m + 1) \cdot n = m \cdot n + n$.

Theorem A.3. *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 54. As with addition, so with multiplication, one can prove by induction alone that it exists uniquely as described in ¶¶53–A.3. However, the next theorem requires also Axioms 48(c)–(d).

Theorem A.4 (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 55 (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,

$$\begin{aligned} m^1 &= m, \\ m^{n+1} &= m^n \cdot m. \end{aligned}$$

Theorem A.5. *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 56. In contrast with addition and multiplication, exponentiation requires more than induction for its existence.

Definition 57 (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 A.6. *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* $m \cdot k \leqslant n \cdot k$.

Lemma A.4. *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 A.7. *The binary relation $\leqslant$ is a **total 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* $n \leqslant m$.

Theorem A.8 (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 Lemma A.4(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 58. 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 A.9. *The set of natural numbers is* ***well ordered*** *by $\leqslant$: 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, $\mathbb{N} \smallsetminus A = \mathbb{N}$. 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 $\mathbb{N} \smallsetminus A$, then $n \in \mathbb{N} \smallsetminus A$. By strong induction, we are done. □

Remark 59. We have now shown, in effect, that if a total order $(A, \leqslant)$ admits proof by strong recursion, then it is well-ordered. The converse is also true.

Theorem A.10 (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 60. Recursion with Parameter allows us to define the set of predecessors of n as $\operatorname{pred}(n)$, where $x \mapsto \operatorname{pred}(x)$ 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 $m \in \operatorname{pred}(n)$ and prove the foregoing theorems about the ordering.

Definition 61 (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,

$$\begin{aligned} 1! &= 1, \\ (n+1)! &= (n+1) \cdot n! \end{aligned}$$

B. 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 [2, Ch. 2].

Exercise 1. Prove the unproved propositions in Appendix A.

Exercise 2. An integer n is a triangular number if and only if $8n+1$ is a square 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 $1, 5, 12, \dots$: 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.

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 7. $\gcd(a, a + 1) = 1$.

Exercise 8. $(k!)^n \mid (kn)!$ for all k and n in $\mathbb{N}$.

Exercise 9. If a and b are co-prime, and a and c are co-prime, then a and bc are co-prime.

Exercise 10. Let $\gcd(204, 391) = n$.

a) Compute n.

b) Find a solution of $204x + 391y = n$.

Exercise 11. 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 12. $\gcd(a, b) \mid \operatorname{lcm}(a, b)$.

Exercise 13. When are $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ the same?

Exercise 14. The binary operation $(x, y) \mapsto \gcd(x, y)$ on $\mathbb{N}$ is commutative and associative.

Exercise 15. 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 16. Give complete solutions, or show that they do not exist, for:
a) $14x - 56y = 34$;
b) $10x + 11y = 12$.

Exercise 17. 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 18. $p \equiv \pm 1 \pmod 6$ if $n > 3$.

Exercise 19. If $p \equiv 1 \pmod 3$ then $p \equiv 1 \pmod 6$.

Exercise 20. If $n \equiv 2 \pmod 3$, then n has a factor p such that $p \equiv 2 \pmod 3$.

Exercise 21. Find all primes of the form $n^3 - 1$.

Exercise 22. Find all p such that $3p + 1$ is square.

Exercise 23. Find all p such that $p^2 + 2$ is prime.

Exercise 24. $n^4 + 4$ is composite unless $n = \pm 1$.

Exercise 25. If n is positive, then $8^n + 1$ is composite.

Exercise 26. Find all integers n such that the equation

$$x^2 = ny^2$$

has only the zero solution. Prove your findings.

Exercise 27. If $p_0 < \cdots < p_n$, prove that the sum

$$\frac{1}{p_0} + \cdots + \frac{1}{p_n}$$

is not an integer.

Exercise 28. 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 29. Infinitely many primes are congruent to -1 *modulo* 6.

Exercise 30. Find all n such that
a) $n!$ is square;
b) $n! + (n+1)! + (n+2)!$ is square.

Exercise 31. Determine whether $a^2 \equiv b^2 \pmod{n} \implies a \equiv b \pmod{n}$.

Exercise 32. Compute $\sum_{k=1}^{1001} k^{365} \pmod{5}$.

Exercise 33. $39 \mid 53^{103} + 103^{53}$.

Exercise 34. Solve $6^{n+2} + 7^{2n+1} \equiv x \pmod{43}$.

Exercise 35. Determine whether $a \equiv b \pmod{n} \implies c^a \equiv c^b \pmod{n}$.

Exercise 36. Determine r such that $a \equiv b \pmod{r}$ whenever $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.

Exercise 37. Solve the system

$$\begin{cases} x \equiv 1 \pmod{17}, \\ x \equiv 8 \pmod{19}, \\ x \equiv 16 \pmod{21}. \end{cases}$$

Exercise 38. The system

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

has a solution if and only if $\gcd(n, m) \mid b - a$.

Exercise 39. The number 32 970 563 is the product of two primes. Find them.

Exercise 40. Factorize 1 003 207 (the product of two primes) knowing

$$1\,835^2 \equiv 598^2 \pmod{1\,003\,207}.$$

Exercise 41. Compute 16200 *modulo* 19.

Exercise 42. 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 43. Show $a^{13} \equiv a \pmod{70}$.

Exercise 44. Assuming $\gcd(a, p) = 1$, and $0 \leqslant n < p$, solve the congruence

$$a^n x \equiv b \pmod{p}.$$

Exercise 45. Solve $2^{14}x \equiv 3 \pmod{23}$.

Exercise 46. Show $\displaystyle\sum_{k=1}^{p-1} k^p \equiv 0 \pmod{p}$.

Exercise 47. 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 48. 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 49. 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 50. $\tau(n) \leqslant 2\sqrt{n}$.

Exercise 51. $\tau(n)$ is odd if and only if n is square.

Exercise 52. Assuming n is odd: $\sigma(n)$ is odd if and only if n is square.

Exercise 53. $\displaystyle\sum_{d\mid n}\frac{1}{d} = \frac{\sigma(n)}{n}$.

Exercise 54. $\{n\colon \tau(n)=k\}$ is infinite (when $k>1$), but $\{n\colon \sigma(n)=k\}$ is finite.

Exercise 55. Let $m\in\mathbb{Z}$. The number-theoretic function $n\mapsto n^m$ is multiplicative.

Exercise 56. 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 57. Let $\Lambda(n) = \begin{cases}\log p, & \text{if } n=p^m \text{ for some positive } m;\\ 0, & \text{otherwise.}\end{cases}$

a) $\displaystyle\log n = \sum_{d\mid n}\Lambda(d)$.
b) $\displaystyle\Lambda(n) = \sum_{d\mid n}\mu\Big(\frac{n}{d}\Big)\log d$.
c) $\displaystyle\Lambda(n) = -\sum_{d\mid n}\mu(d)\log d$.

Exercise 58. Suppose $n = {p_1}^{k(1)}\cdots {p_r}^{k(r)}$, where the p_i are distinct.

a) If f is multiplicative and non-zero, then $\displaystyle\sum_{d\mid n}\mu(d)\cdot f(d) = \prod_{i=1}^{r}(1-f(p_i))$;
b) $\displaystyle\sum_{d\mid n}\mu(d)\cdot\tau(d) = (-1)^r$.

Exercise 59. $f(568) = f(638)$ when $f\in\{\tau,\sigma,\phi\}$.

Exercise 60. Solve:
a) $n = 2\phi(n)$.
b) $\phi(n) = \phi(2n)$.
c) $\phi(n) = 12$. (Do this without a table. There are 6 solutions.)

Exercise 61. Find a sequence $(a_n : n \in \mathbb{N})$ of positive integers such that

$$\lim_{n\to\infty} \frac{\phi(a_n)}{a_n} = 0.$$

(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 $\displaystyle\lim_{n\to\infty} \prod_{k=1}^{n} \frac{1}{1-\frac{1}{p_k}} = \infty$ if $(p_k : k \in \mathbb{N})$ is the list of primes.)

Exercise 62. 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 63. 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 64. If $\gcd(m, n) = 1$, show $m^{\phi(n)} \equiv n^{\phi(m)} \pmod{mn}$.

Exercise 65. If n is odd, and is not a prime power, and if $\gcd(a, n) = 1$, show $a^{\phi(n)/2} \equiv 1 \pmod{n}$. (This generalizes Exercise 63(b).)

Exercise 66. Solve $5^{10000}x \equiv 1 \pmod{153}$.

Exercise 67. Prove $\displaystyle\sum_{d|n} \mu(d)\phi(d) = \prod_{p|n}(2-p)$. (This is a special case of Exercise 58(a).)

Exercise 68. If n is **squarefree** (has no factor p^2), and $k \geqslant 0$, show

$$\sum_{d|n} \sigma(d^k)\phi(d) = n^{k+1}.$$

Exercise 69. $\sum_{d|n} \sigma(d)\phi\left(\frac{n}{d}\right) = n\tau(n)$.

Exercise 70. $\sum_{d|n} \tau(d)\phi\left(\frac{n}{d}\right) = \sigma(n)$.

Exercise 71. We have $(\pm 3)^2 \equiv 2 \pmod{7}$. Compute the orders of 2, 3, and -3, *modulo* 7.

Exercise 72. 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 73. 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 74. 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 75. Find all elements of $[-30, 30]$ having order 4 *modulo* 61.

Exercise 76. $f(x) \equiv 0 \pmod{n}$ 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 77. If $\mathrm{ord}_n(a) = n - 1$, then n is prime.

Exercise 78. If $a > 1$, show $n \mid \phi(a^n - 1)$.

Exercise 79. If $2 \nmid p$ and $p \mid n^2 + 1$, show $p \equiv 1 \pmod{4}$.

Exercise 80.
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 $\operatorname{ord}_p(-r)$?

Exercise 81. 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 82. If n has primitive roots r and s, and $\gcd(a, n) = 1$, prove

$$\log_s a \equiv \frac{\log_r a}{\log_r s} \pmod{\phi(n)}.$$

Exercise 83. In $(\mathbb{Z}/(337))^\times$, for any base, show

$$\log(-a) \equiv \log a + 168 \pmod{336}.$$

Exercise 84. Solve $4^x \equiv 13 \pmod{17}$.

Exercise 85. How many primitive roots has 22? Find them.

Exercise 86. Find a primitive root of 1250.

Exercise 87. Define the function λ by the rules

$$\lambda(2^k) = \begin{cases} \phi(2^k), & \text{if } 0 < k < 3; \\ \phi(2^k)/2, & \text{if } k \geqslant 3; \end{cases}$$
$$\lambda(2^k \cdot {p_1}^{\ell(1)} \cdots {p_m}^{\ell(m)}) = \operatorname{lcm}(\phi(2^k), \phi({p_1}^{\ell(1)}), \ldots, \phi({p_m}^{\ell(m)})).$$

where the p_i are distinct odd primes.

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 88. 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 89. 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:

- $a \equiv b \pmod{p} \implies (a/p) = (b/p)$;
- $(1/p) = 1$;
- $(-1/p) = (-1)^{(p-1)/2}$;
- $(a^2/p) = 1$;
- $(2/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$

Exercise 90. Compute all of the Legendre symbols $(n/17)$ and $(m/19)$ by means of Gauss's Lemma.

Exercise 91. Find all primes of the form $5 \cdot 2^n + 1$ that have 2 as a primitive root.

Exercise 92. 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 93.
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 94. Assuming p is an odd prime, and $2p + 1$ is a prime q, show that -4 is a primitive root of q. (*Hint:* Show $\mathrm{ord}_q(-4) \notin \{1, 2, p\}$.)

Exercise 95. Compute the Legendre symbols $(91/167)$ and $(111/941)$.

Exercise 96. Find $(5/p)$ in terms of the class of p *modulo* 5.

Exercise 97. Find $(7/p)$ in terms of the class of p *modulo* 28.

Exercise 98. 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 99. Solve the congruence $x^2 \equiv 11 \pmod{35}$.

Exercise 100. 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

$$\left(\frac{a}{n}\right) = \prod_p \left(\frac{a}{p}\right)^{k(p)}, \qquad \text{where} \qquad n = \prod_p p^{k(p)}.$$

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

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^k, \qquad \text{where} \qquad k = \frac{m-1}{2} \cdot \frac{n-1}{2}.$$

C. Examinations

C.1. In-term examination

The exam lasts 90 minutes. All answers must be justified to the reader.

The set $\mathbb{N}$ of natural numbers is $\{0, 1, 2, \dots\}$.

Problem 1.1. *For all natural numbers k and integers n, prove*

$$k! \mid n \cdot (n+1) \cdots (n+k-1).$$

Solution.

$$\frac{n \cdot (n+1) \cdots (n+k-1)}{k!} = \begin{cases} \dbinom{n+k-1}{k}, & \text{if } n > 0; \\ 0, & \text{if } n \leqslant 0 < n+k; \\ (-1)^k \cdot \dbinom{-n}{k}, & \text{if } n+k \leqslant 0. \end{cases}$$

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

$$(\ell+1)! \mid n \cdot (n+1) \cdots (n+\ell) \tag{$*$}$$

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 Little 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 $\mathbb{N}$, 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.

C.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 $\mathbb{N}$ 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 $\mathbb{N}$.*

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 $\mathbb{N}$ 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 $35 \cdot \phi(n) \leqslant 8n$.*

Solution. We want $\dfrac{\phi(n)}{n} \leqslant \dfrac{8}{35}$. We have

$$\frac{\phi(n)}{n} = \prod_{p|n} \frac{p-1}{p}.$$

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 $\mathbb{N} \setminus \{0\}$. Define h and H by $h(n) = f(n) \cdot g(n)$ and $H(n) = \displaystyle\sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right)$. 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

$$\begin{aligned}
H(mn) &= \sum_{d \mid mn} f(d) \cdot g\Big(\frac{mn}{d}\Big) \\
&= \sum_{d \mid m} \sum_{e \mid n} f(de) \cdot g\Big(\frac{mn}{de}\Big) \\
&= \sum_{d \mid m} \sum_{e \mid n} f(d) \cdot f(e) \cdot g\Big(\frac{m}{d}\Big) \cdot g\Big(\frac{n}{e}\Big) && \text{[mult. of } f, g\text{]} \\
&= \sum_{d \mid m} f(d) \cdot \Big(\frac{m}{d}\Big) \cdot \sum_{e \mid n} f(e) \cdot g\Big(\frac{m}{d}\Big) \cdot g\Big(\frac{n}{e}\Big) && \text{[distributivity]} \\
&= \Big(\sum_{d \mid m} f(d) \cdot \Big(\frac{m}{d}\Big)\Big) \cdot \sum_{e \mid n} f(e) \cdot g\Big(\frac{m}{d}\Big) \cdot g\Big(\frac{n}{e}\Big) && \text{[distributivity]} \\
&= H(m) \cdot H(n),
\end{aligned}$$

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 $\sum_{d \mid n} f(d)$ is a multiplicative function of n. Hence $\sum_{d \mid n} f(n/d)$ is also multiplicative, since it is the same function. Likewise, once we know that fg is multiplicative, then we know that $\sum_{d \mid n} f(d)g(d)$ is multiplicative. But we *cannot* conclude so easily that $\sum_{d \mid n} f(d)g(n/d)$ 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 $\phi(365) = \phi(5) \cdot \phi(73) = 4 \cdot 72 = 288$. And 288 goes into 3164 ten times, with remainder 284. Therefore, *modulo* 365, we have

$$\begin{aligned} 6^{3164}x \equiv 2 \iff & 6^{284}x \equiv 2 \\ \iff & x \equiv 2 \cdot 6^4 \\ & \equiv 2 \cdot 36^2 \\ & \equiv 2 \cdot 1296 \\ & \equiv 2 \cdot 201 \\ & \equiv 402 \\ & \equiv 37. \end{aligned}$$

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. $\phi(41) = 40 = 2^3 \cdot 5 = 8 \cdot 5$, so the proper divisors of $\phi(41)$ 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 2^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 $\{6^k : 0 < k \leqslant 40 \ \&\ \gcd(k, 40) = 1\}$. 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.

C.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 [95]) refer to related homework exercises.

Problem 3.1. *Compute the Legendre symbol* $\left(\dfrac{63}{271}\right)$. [95]

Solution. $\left(\dfrac{63}{271}\right) = \left(\dfrac{7 \cdot 3^2}{271}\right) = \left(\dfrac{7}{271}\right) = -\left(\dfrac{271}{7}\right) = -\left(\dfrac{5}{7}\right) = -\left(\dfrac{7}{5}\right) = -\left(\dfrac{2}{5}\right) = -(-1) = 1.$

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 [100].

Problem 3.2 (3 points). *Find the Legendre symbol* $(a/29)$, *given that* [90]

$$\left\{ka - 29 \cdot \left[\frac{ka}{29}\right] : 1 \leqslant k \leqslant 14\right\} = \{1, 2, 5, 6, 7, 10, 11, 12, 15, 16, 20, 21, 25, 26\}.$$

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. [94]

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 $\phi(\phi(q))$, 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) $\mathrm{ord}_q(r) \notin \{1, 2, p\}$;
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.)* [81(a)]

k	1	2	3	4	5	6	7	8	9	10	11	(mod 23)
$\log_5 k$												(mod 22)
$\log_5(-k)$												(mod 22)

Solution. First compute powers of 5, then rearrange:

ℓ	0	1	2	3	4	5	6	7	8	9	10	(mod 22)
5^ℓ	1	5	2	10	4	-3	8	-6	-7	11	9	(mod 23)
$5^{\ell+11}$	-1	-5	-2	-10	-4	3	-8	6	7	-11	-9	(mod 23)

k	1	2	3	4	5	6	7	8	9	10	11	(mod 23)
$\log_5 k$	0	2	16	4	1	18	19	6	10	3	9	(mod 22)
$\log_5(-k)$	11	13	5	15	12	7	8	17	21	14	20	(mod 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 [89]), or by Gauss's Lemma (as in [90]); 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. [81(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

$$\begin{array}{r|l} & \,16 \\ \hline 22 &)\,369 \\ & \,\underline{22} \\ & \,149 \\ & \,\underline{132} \\ & \,17 \end{array}$$

$$\begin{aligned} x^{369} \equiv 7 \pmod{23} &\iff x^{17} \equiv 7 \pmod{23} \\ &\iff 17 \log_5 x \equiv 19 \pmod{22} \\ &\iff \log_5 x \equiv \frac{19}{17} \equiv \frac{-3}{-5} \equiv \frac{3}{5} \pmod{22} \\ &\iff \log_5 x \equiv 3 \cdot 9 \equiv 27 \equiv 5 \pmod{22} \\ &\iff x \equiv 5^5 \equiv -3 \pmod{23} \\ &\iff \boxed{x \equiv 20} \pmod{23} \end{aligned}$$

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* $x^2 - x + 5 \equiv 0 \pmod{23}$. [88]

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.* [86]

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	(mod 10)
2^k	2	4	-3	-6	-1	(mod 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.

C.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 Figure C.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.*

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

Figure C.1.

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, $(-1/257) = 1$, 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* $\mathrm{ord}_{257}(n) = a$.

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 $x \equiv 2 \cdot 17^{\phi(5)} + 5 \cdot 5^{\phi(17)} \pmod{85}$; but this is not *useful* (the number is not between 0 and 85, or between $-85/2$ and $85/2$).

Bibliography

[1] V. I. Arnol′d. On the teaching of mathematics. *Uspekhi Mat. Nauk*, 53(1(319)):229–234, 1998.

[2] David M. Burton. *Elementary Number Theory*. McGraw-Hill, Boston, sixth edition, 2007.

[3] 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.

[4] 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.

[5] 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.

[6] Graham Everest and Thomas Ward. *An introduction to number theory*, volume 232 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2005.

[7] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, 1986. Translated into English by Arthur A. Clarke, revised by William C. Waterhouse.

[8] D. A. Goldston, J. Pintz, and C. Y. Yıldırım. `http://arxiv.org`, 2005. arXiv:math/0508185v1 [math.NT].

[9] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. `http://arxiv.org`, 2004. arXiv:math/0404188v6 [math.NT].

[10] 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.

[11] 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.

[12] 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.

[13] Jean van Heijenoort. *From Frege to Gödel. A source book in mathematical logic, 1879–1931.* Harvard University Press, Cambridge, Mass., 1967.

Index