METU MATH 365, Exam 2 *solutions*

David Pierce

Exam date: Thursday, December 16, 2010

Problem 1. *Exactly one of* 1458 *and* 1536 *has a primitive root. Which one, and why? Find a primitive root of the number that has one.*

Solution. $1458 = 2 \cdot 729 = 2 \cdot 3^6$ and $1536 = 3 \cdot 512 = 3 \cdot 2^9$.
The numbers with primitive roots are just 2, 4, p^k, and $2 \cdot p^k$, where p is an *odd* prime.
Therefore 1458, but not 1536, has a primitive root.
$\phi(9) = 6$, and

k	1	2	3	4	5	6	
5^k	5	-2	-1	4	2	1	mod9

so 5 is a primitive root of 9.
Then 5 is a primitive root of 3^6.
Since 5 is odd, it is a primitive root of 1458.

Remark. 1. A number of people computed $\phi(1458)$ and $\phi(1536)$, but this is of no practical use in this problem.
2. Some people pointed out that if a is a primitive root of n, then $a^{\phi(n)} \equiv 1 \pmod{n}$. This is logically correct, but useless, since by Euler's Theorem we have $a^{\phi(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$ (not just when a is a primitive root).
3. Our sequence of theorems about primitive roots of composite numbers is the following. Throughout, p is an odd prime.

(i) If r is a primitive root of p, then r or $r + p$ is a primitive root of p^2.
(ii) If r is a primitive root of p^2, then r is a primitive root of p^s whenever $s \geqslant 2$.
(iii) If r is a primitive root of p^s (where $s \geqslant 2$), then r or $r + p^s$ (whichever is odd) is a primitive root of $2p^s$.

Some people misremembered this sequence, or wrongly combined two of its theorems. For example, some wrote 'If r is a primitive root of p, then r or $r + p^s$ (whichever is odd) is a primitive root of $2p^s$.' This assertion is false. It would be correct to say for example, 'If r is a primitive root of p^2, then r or $r + p^2$ (whichever is odd) is a primitive root of $2p^s$.' Using this, one might observe that 2 is a primitive root of 9, and therefore 11 is a primitive root of 1458.

Problem 2. *Remembering that p is always prime, define the arithmetic function ω by*

$$\omega(n) = \sum_{p|n} 1.$$

a. *Define μ, preferably using ω.*

b. *Prove that, if m and n are co-prime, then $\omega(mn) = \omega(m) + \omega(n)$.*

c. *Prove that*

$$\sum_{d|n} \tau(d) \cdot \mu(d) = (-1)^{\omega(n)}.$$

d. *Find a simple description of the function f given by*

$$f(n) = \sum_{d|n} \omega(d) \cdot \mu\Big(\frac{n}{d}\Big).$$

Solution. a. $\mu(n) = \begin{cases} 0, & \text{if } p^2 \mid n \text{ for some } p, \\ (-1)^{\omega(n)}, & \text{if } p^2 \mid n \text{ for no } p. \end{cases}$.

b. Assume m and n are co-prime. If $p \mid mn$, then

$$p \mid m \iff p \nmid n.$$

Therefore

$$\omega(mn) = \sum_{p|mn} 1 = \sum_{p|m} 1 + \sum_{p|n} 1 = \omega(m) + \omega(n).$$

c. Each side of the equation is multiplicative, and

$$\sum_{d|p^k} \tau(d) \cdot \mu(d) = \tau(1) \cdot \mu(1) + \tau(p) \cdot \mu(p) = 1 - 2 = (-1)^{\omega(p^k)}.$$

d. By Möbius inversion,

$$\omega(n) = \sum_{d|n} f(d).$$

Since also $\omega(n) = \sum_{p|n} 1$, we have

$$f(n) = \begin{cases} 1, & \text{if } n \text{ is prime}, \\ 0, & \text{if } n \text{ is not prime}. \end{cases}$$

Remark. 1. In my solution to part a, the condition '$p^2 \mid n$ for no p' is equivalent to '$p^2 \nmid n$ for all p'. Similarly in part d.
2. For part a, some people wrote (as part of their answer) '$\mu(n) = (-1)^s$ if $n = p_1 \cdots p_s$'. Strictly, one must specify that the p_i are all distinct. The best way that I know to do this is to say $p_1 < \cdots < p_s$.

3. As an alternative solution to part b, one can write (as some people did) that, since m and n are co-prime, we have

$$m = {p_1}^{m(1)} \cdots {p_s}^{m(s)}, \qquad\qquad n = {q_1}^{n(1)} \cdots {q_t}^{n(t)},$$

where the exponents are positive, $p_1 < \cdots < p_s$, $q_1 < \cdots < q_t$, and $p_i \neq q_j$ in each case, and therefore

$$\omega(mn) = s + t = \omega(m) + \omega(n).$$

This may be a clearer argument than the one I wrote above. I don't know a good way to make the argument just with the Σ-notation. Some people wrote

$$\text{`}\omega(mn) = \sum_{pq|mn} 1\text{'},$$

which doesn't make sense. (If it means anything, it means $\omega(mn)$ is the number of factors d that mn has, where d is the product of two primes, possibly not distinct. This is not what $\omega(mn)$ is.) Others wrote

$$\text{`}\omega(mn) = \sum_{p|m} \sum_{q|n} 1\text{'};$$

this is meaningful, but false, since it makes $\omega(mn)$ equal to the *product* $\omega(m) \cdot \omega(n)$.

4. In part c, it doesn't hurt to say *why* the two sides are multiplicative. The left-hand side is multiplicative because the product of two multiplicative functions is multiplicative (we didn't prove this, but it's fairly obvious), and if g is multiplicative, so is $n \mapsto \sum_{d|n} g(d)$ (we did prove this). The right-hand side is multiplicative by part b.

5. In notation introduced in class, the function f in part d is given by $f = \omega * \mu$, and therefore $\omega = f * 1$ by Möbius inversion. It may not be immediately obvious that f *must* be as in the solution above. But if f *is* that function, then indeed $\omega = f * 1$, and therefore $f = \omega * \mu$, as required. So f must be as given in the solution.

Problem 3. *Find the least positive x such that*

$$11^{5117}x \equiv 57 \pmod{600}.$$

Solution. $600 = 2^3 \cdot 3 \cdot 5^2$, so $\phi(600) = 4 \cdot 2 \cdot 20 = 160$. We compute $\boxed{\begin{array}{r} 31 \\ 160\overline{)5117} \\ 480 \\ \hline 317 \\ 160 \\ \hline 157 \end{array}}$. Hence

$$5117 \equiv 157 \equiv -3 \pmod{160}.$$

Therefore

$$\begin{aligned} & 11^{1557}x \equiv 5 \pmod{600} \\ \iff\ & 11^{-3}x \equiv 5 \pmod{600} \\ \iff\ & x \equiv 5 \cdot 11^3 \pmod{600}. \end{aligned}$$

But

$$\begin{aligned} 11^3 = 121 \cdot 11 = 1331 \equiv 131 \pmod{600}, \\ 5 \cdot 131 = 655 \equiv 55 \pmod{600}, \end{aligned}$$

so the least positive solution is $\boxed{55}$.

Remark. Not too many problems here. I'm guessing this is the sort of problem that the *dershane* prepares one for. According to the Wikipedia article 'Long division', my notation for long division is what used in Anglophone countries; the notation I see on papers, Francophone. But the symbolism b) a (used in the former notation) for a/b is traced to Michael Stifel of the University of Jena in Germany in 1544 (see the Wikipedia article 'Division (mathematics)').

Problem 4. *a. Since* 2 *is a primitive root of* 29*, the function* $x \mapsto \log_2 x$ *from* $\mathbb{Z}_{29}{}^\times$ *to* $\mathbb{Z}_{28}$ *is defined. Considering this as a function from* $\{-14, \dots, -1, 1, \dots 14\}$ *to* $\{-14, \dots, 14\}$*, fill out the table below.*

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$														
$\log_2(-m)$														

b. With respect to the modulus 29*, exactly one of the two congruences*

$$x^{400} \equiv 13, \qquad\qquad x^{400} \equiv -13$$

*has a solution. Find all of its solutions (*modulo 29*), and explain why the other congruence has no solutions.*

Solution. a.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$	0	1	5	2	-6	6	12	3	10	-5	-3	7	-10	13
$\log_2(-m)$	14	-13	-9	-12	8	-8	-2	-11	-4	9	11	-7	4	-1

b. For the first congruence, we have

$$\begin{aligned} & x^{400} \equiv 13 \pmod{29} \\ \iff & 400 \log x \equiv -10 \pmod{28} \\ \iff & 200 \log x \equiv -5 \pmod{14}; \end{aligned}$$

the congruence has no solution since $\gcd(200, 14) = 2$, and $2 \nmid -5$. For the second congruence:

$$\begin{aligned} & x^{400} \equiv -13 \pmod{29} \\ \iff & 400 \log x \equiv 4 \pmod{28} \\ \iff & 100 \log x \equiv 1 \pmod{7} \\ \iff & 2 \log x \equiv 1 \pmod{7} \\ \iff & \log x \equiv 4 \pmod{7} \\ \iff & \log x \equiv 4, 11, -10, -3 \pmod{28} \\ \iff & x \equiv -13, -11, 13, 11 \pmod{29}. \end{aligned}$$

Remark. The quickest way I know to fill out the table is, keeping in mind

$$\log_2 m \equiv k \bmod 28 \iff 2^k \equiv m \bmod 29,$$

to start out as follows,

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$	0	1		2				3						
$\log_2(-m)$													4	

continuing to get

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\log_2 m$	0	1	5	2		6	12	3	10			7		13
$\log_2(-m)$	14				8					9	11		4	

then filling in the remaining spaces by using

$$\log m - \log(-m) \equiv \log(-1) \equiv \pm 14 \pmod{28}.$$

Some people may have done something like this, but they put the logarithms into the set $\{0, \ldots, 27\}$ rather than $\{-14, \ldots, 14\}$ as requested (this set could have been $\{-13, \ldots, 14\}$. Other people gave negative logarithms, but they were off by 1, as if the modulus had been taken as 29 rather than 28. In solving the congruences, there were various confusions about modulus.