MATH 365, FINAL EXAMINATION SOLUTIONS

DAVID PIERCE

The following table of powers of 3 *modulo* 257 was provided for use in several problems:

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

Problem 1. *For positive integers n, let $\omega(n) = |\{p\colon p \mid n\}|$, the number of primes dividing n.*

(a) *Show that the function $n \mapsto 2^{\omega(n)}$ is multiplicative.*
(b) *Define the Möbius function μ in terms of ω.*
(c) *Show $\displaystyle\sum_{d\mid n} |\mu(d)| = 2^{\omega(n)}$ 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 $n \mapsto \sum_{d\mid n} |\mu(d)|$. Hence it is enough to establish the equation when n is a prime power. We have
$$\sum_{d\mid p^s} |\mu(d)| = \sum_{k=0}^{s} \left|\mu(p^k)\right| = |\mu(1)| + |\mu(p)| = 1 + 1 = 2 = 2^1 = 2^{\omega(p^s)}.$$

Problem 2. *Fill out the following table of Legendre symbols:*

a	1	2	3	5	7	11	13	17	19
$\left(\dfrac{a}{257}\right)$									

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
$\left(\dfrac{a}{257}\right)$	1	1	−1	−1	−1	1	1	1	−1

Date: January 11, 2008.

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 3. *In the following table, in the box below each number a, write the least positive integer n such that* $\operatorname{ord}_{257}(n) = a$.

1	2	4	8	16	32	64	128	256

Solution. If r is a primitive root of 257, then $\operatorname{ord}_{257}(r^{256/a}) = a$. The primitive roots of 257 are 3^s, where s is odd. So below a we want the least n such that $n \equiv 3^{(256/a)\cdot s}$ for some odd s. (In searching the table of powers, since $3^{k+128} \equiv -3^k$, we can ignore signs, except when $a \leqslant 2$. For example, when $a = 4$, then $3^{(256/a)\cdot s} = 3^{64s}$, so n can only be $|3^{64}|$. When $a = 32$, then $3^{(256/a)\cdot s} = 3^{8s}$, so n will be the absolute value of an entry in the column of powers that is headed by 8.)

1	2	4	8	16	32	64	128	256
1	256	16	4	2	15	11	9	3

Remark. Another way to approach the problem is to note that

$$\operatorname{ord}_{257}(3^k) = \frac{256}{\gcd(256, k)}.$$

Then one must look among those powers 3^k such that $\gcd(256, k) = 256/a$. *Some* explanation is necessary, though it need not be so elaborate as what I gave above.

Some people apparently misread the problem as asking for the orders of the given numbers. Others provided numbers that had the desired orders; but they weren't the *least positive* such numbers.

Problem 4. *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 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 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 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:

$$\begin{aligned} &x^2 \equiv 59 \pmod{5} & &x^2 \equiv 59 \pmod{17} \\ &\iff x^2 \equiv 4 \pmod{5} & &\iff x^2 \equiv 8 \pmod{17} \\ &\iff x \equiv \pm 2 \pmod{5}; & &\iff x^2 \equiv 25 \pmod{17} \\ & & &\iff x \equiv \pm 5 \pmod{17}. \end{aligned}$$

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 $85/2$).

Mathematics Dept, Middle East Technical University, Ankara 06531, Turkey
E-mail address: dpierce@metu.edu.tr
URL: http://www.math.metu.edu.tr/~dpierce/