

## Homework V Solutions

**9C 43.** Find  $48^{322} \pmod{25}$ .

**Solution.** Since  $\phi(25) = 20$  (direct calculation, or see Problem 51(ii)), and  $\gcd(25, 48) = 1$ , Euler's Theorem tells us that

$$48^{20} \equiv 1 \pmod{25}.$$

Therefore,

$$48^{322} = (48^{20})^{16} \cdot 48^2 \equiv 1^{16} \cdot 48^2 \equiv 23^2 \equiv (-2)^2 \equiv 4 \pmod{25}.$$

**9C 48.** Verify that  $5^{11} \pmod{26} = 21$ , the inverse of 5  $\pmod{26}$ .

**Solution.** We have  $\phi(26) = \phi(2 \cdot 13) = \phi(2)\phi(13) = 1 \cdot 12 = 12$ , and since  $(5, 26) = 1$ , Euler's Theorem implies that

$$5^{12} \equiv 1 \pmod{26},$$

therefore  $5 \cdot 5^{11} \equiv 1 \pmod{26}$ , which exactly says that  $5^{11}$  is the inverse of 5  $\pmod{26}$ .

Alternative method:  $5^2 = 25 \equiv -1 \pmod{26}$ , therefore  $5^{10} = (5^2)^5 \equiv (-1)^5 \equiv -1 \pmod{26}$ , therefore  $5^{11} \equiv -5 \equiv 21 \pmod{26}$ .

**9C 51.** Prove that (i)  $\phi(p) = p - 1$  if  $p$  is prime; (ii)  $\phi(p^n) = p^n - p^{n-1}$  if  $p$  is prime.

**Solution.** (i) Recall that  $\phi(p)$  is, by definition, the number of integers between 1 and  $p$  which are coprime to  $p$ . If  $p$  is prime, then all the numbers from 1 to  $p - 1$  are coprime to  $p$  (and  $p$  itself is not), so  $\phi(p) = p - 1$ .

(ii) Now we want the number of integers between 1 and  $p^n$  which are coprime to  $p^n$ . Since  $p^n$  has only one prime factor— $p$ —the integers coprime to it are exactly those *not* divisible by  $p$ . How many of these are there between 1 and  $p^n$ ? It's easier to count how many integers are *not* coprime to  $p^n$ —these are exactly those that *are* divisible by  $p$ , and there are  $p^{n-1}$  of them between 1 and  $p^n$ :

$$1 \cdot p, 2 \cdot p, 3 \cdot p, \dots, p^{n-1} \cdot p.$$

Thus  $\phi(p^n)$  is the total number of integers in the range  $[1, p^n]$  minus the integers in that range *not* coprime to  $p^n$ , or just  $p^n - p^{n-1}$ .

**9F 78.** Find the least nonnegative residue (mod 34) of  $12^{87}$ .

**Solution.** We'll follow the textbook's method. First write the exponent 87 in base 2:  $87 = 64 + 16 + 4 + 2 + 1 = 1010111_2$ . Now write an  $S$  between each bit:  $1S0S1S0S1S1S1$ , and then erase 0's and replace 1's with  $X$ 's:  $XSSXSSXSSX$ . Now starting with 1, view this string as a sequence of operations to perform modulo 34 ( $X$  being the operation "multiply by 12" and  $S$  being the operation "square the current value"):

$$\begin{aligned} 1 \rightarrow^X 12 \rightarrow^S 144 = 8 \rightarrow^S 64 = -4 \rightarrow^X -48 = 20 \rightarrow^S 400 = 26 = -8 \rightarrow^S 64 = -4 \\ \rightarrow^X -48 = 20 \rightarrow^S 400 = -8 \rightarrow^X -96 = 6 \rightarrow^S 36 = 2 \rightarrow^X 24. \end{aligned}$$

So  $12^{87} \equiv 24 \pmod{34}$ .

**9F 79.** Find the least nonnegative number  $a$  congruent to  $2^{69} \pmod{71}$ . Verify that  $2a \equiv 1 \pmod{71}$ .

**Solution.** Write  $69 = 64 + 4 + 1 = 1000101_2$ . Then, as in the previous problem,  $1000101 \rightarrow 1S0S0S0S1S0S1 \rightarrow XSSSSXSSX$ , and we perform the specified operations modulo 71:

$$1 \rightarrow^X 2 \rightarrow^S 4 \rightarrow^S 16 \rightarrow^S 64 = -7 \rightarrow^S 49 \rightarrow^X 98 = 27 \rightarrow^S 729 = 19 \rightarrow^S 361 = 6 \rightarrow^X 36.$$

Thus  $2^{69} \equiv 36 \pmod{71}$ , and indeed  $2 \cdot 36 \equiv 1 \pmod{71}$  (as required by Fermat's Theorem).

**10A 5 (encode only).** Let  $m = 3337$ ,  $e = 11$ ,  $d = 1171$ . Encode and decode the message NO.

**Solution.** First step is to translate NO into a number using the encoding  $A \leftrightarrow 01$ ,  $A \leftrightarrow 02$ ,  $\dots$ ,  $Z \leftrightarrow 26$ . This gives the number 1415. To encode using RSA, we simply raise the message to the power  $e$  modulo  $m$ :

$$1415^{11} \pmod{3337} = 2551,$$

so the encoding of *NO* under RSA with these parameters is 2551. (I recommend not doing the previous calculation by hand—there are online calculators for modular exponentiation, e.g. <http://www.math.umn.edu/~garrett/crypto/a01/FastPow.html>.)

**10A 7.** Suppose  $m$  is a product of two prime numbers  $p$  and  $q$ , and suppose  $m$  and  $\phi(m)$  are known. Show that  $p$  and  $q$  can be found as the roots of an appropriate quadratic equation.

**Solution.** If  $p$  and  $q$  are the roots, the equation must be  $(x-p)(x-q) = 0$ ; expanding we get  $x^2 - (p+q)x + pq = 0$ . We know  $pq = m$ , so this is the same as  $x^2 - (p+q)x + m = 0$ . Also we know  $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1) = pq - p - q + 1 = m - (p+q) + 1$ .

Therefore  $-(p+q) = \phi(m) - m - 1$ , and the appropriate quadratic equation is  $x^2 + (\phi(m) - m - 1)x + m = 0$ .

**12A 19.** There is an unknown number of objects. When counted by threes, the remainder is 2; when counted by fives, the remainder is 3; and when counted by sevens, the remainder is 2. How many objects are there?

**Solution.** We seek to solve the system

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

Looking just at the first two to begin with, we hope to combine them into a single congruence mod 15. We write

$$x = 3s + 2 = 5t + 3 \implies 3s - 5t = 1.$$

Looking at this equation mod 3 (the smaller of the two moduli 3 and 5), we get  $-5t \equiv 1 \pmod{3}$ , or just  $t \equiv 1 \pmod{3}$ . Taking  $t = 1$ , we obtain  $x = 5t + 3 = 5(1) + 3 = 8$ . (As a sanity check, we can quickly confirm that indeed  $8 \equiv 2 \pmod{3}$  and  $8 \equiv 3 \pmod{5}$ .) So we've reduced three congruences to two, namely:

$$x \equiv 8 \pmod{15}$$

$$x \equiv 2 \pmod{7}$$

Following the same procedure, we write

$$x = 15s + 8 = 7t + 2 \implies 15s - 7t = -6$$

and viewing this mod 7 yields  $15s \equiv -6 \pmod{7}$ , or just  $s \equiv 1 \pmod{7}$ . Taking  $s = 1$ , we have  $x = 15(1) + 8 = 23$ , and we confirm that indeed 23 is congruent to 8 mod 15 and to 2 mod 7. Thus the final answer is

$$x \equiv 23 \pmod{105}.$$

(Of course the answer to the actual question “How many objects are there?” is underdetermined—there could be 23, or 128, or...)