Solutions to Midterm Exam

Problem 1. a) Find the prime factorizations of 192 and of 150.

b) Use your answer for part a) to find the GCD $(192, 150)$.

c) Use your answer for part a) to find the sum of the factors of 150.

Solution. a) $192 = 2^6 \cdot 3$, $150 = 2 \cdot 3 \cdot 5^2$.

b) $(192, 150) = 2^{\min(6,1)} \cdot 3^{\min(1,1)} \cdot 5^{\min(0,2)} = 2 \cdot 3 = 6$.

c) The sum of the factors is $(1 + 2)(1 + 3)(1 + 5 + 5^2) = 372$.

Problem 2. a) Solve the equation $7x \equiv 1 \pmod{101}$.

b) Find the general solution (with integers x, y) of the equation $22x + 60y = 6$.

Solution. a) We seek the inverse of 7 mod 101. This can be found since $(7, 101) = 1$. By the Euclidean Algorithm,

$$\begin{aligned} 101 &= 14 \cdot 7 + 3, & 3 &= 101 - 14 \cdot 7 \\ 7 &= 2 \cdot 3 + 1, & 1 &= 7 - 2 \cdot 3 = 7 - 2(101 - 14 \cdot 7) = 29 \cdot 7 - 2 \cdot 101 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

This confirms that $(7, 101) = 1$ and that in fact $1 = 29 \cdot 7 - 2 \cdot 101$, thus $1 \equiv 29 \cdot 7 \pmod{101}$ and the desired answer is

$$x \equiv 29 \pmod{101}.$$

b) Here there is a solution because 6 is a multiple of the GCD $(22, 60) = 2$. Once again, by the Euclidean Algorithm:

$$\begin{aligned} 60 &= 2 \cdot 22 + 16, & 16 &= 60 - 2 \cdot 22 \\ 22 &= 1 \cdot 16 + 6, & 6 &= 22 - 16 = 22 - (60 - 2 \cdot 22) = 3 \cdot 22 - 60 \ (*) \\ 16 &= 2 \cdot 6 + 4, & 4 &= 16 - 2 \cdot 6 = 60 - 2 \cdot 22 - 2(3 \cdot 22 - 60) = 3 \cdot 60 - 8 \cdot 22 \\ 6 &= 1 \cdot 4 + 2, & 2 &= 6 - 4 = 3 \cdot 22 - 60 - (3 \cdot 60 - 8 \cdot 22) = 11 \cdot 22 - 4 \cdot 60 \ (**) \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

We could actually have stopped the calculation at the identity $(*)$ because it gives us a particular solution:

$$x_0 = 3, \quad y_0 = -1.$$

Otherwise, we could multiply equation $(**)$ by 3 to get another particular solution, with $x_0 = 33$ and $y_0 = -12$. Let's stick to the first particular solution given above, though.

The general solution is then written in terms of the particular solution, as well as the coefficients 22 and 60 and their GCD $(22, 60) = 2$:

$$\begin{cases} x = x_0 + (60/2)\ell = 3 + 30\ell, \\ y = y_0 - (22/2)\ell = -1 - 11\ell, \end{cases} \quad \text{where } \ell \text{ is an integer.}$$

Problem 3. a) Find the remainder of 4^{183} mod 61.

b) Find the remainder of 2^{264} mod 25.

c) How many primitive roots are there mod 61?

(Remark: parts (a), (b), and (c) are independent.)

Solution. a) Note that 61 is prime, so by the Little Fermat Theorem, $4^{60} \equiv 1 \pmod{61}$. Thus

$$4^{183} \equiv 4^{3 \cdot 60 + 3} \equiv (4^{60})^3 \cdot 4^3 \equiv 4^3 \equiv 64 \equiv 3 \pmod{61}.$$

(mod 25). Thus

$$2^{264} \equiv 2^{13\cdot 20+4} \equiv (2^{20})^{13} \cdot 2^4 \equiv 2^4 \equiv 16 \pmod{25}.$$

c) If g is a primitive root mod 61, then the other primitive roots are the numbers $g^i \pmod{61}$ where i is a number mod 60 and i is relatively prime to 60. Thus the number of such i is

$$\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = (2^2 - 2)(3-1)(5-1) = 16.$$

Problem 4. Assume given a and m such that a has order ℓ mod m. Let k be given. Find, with proof, the order (mod m) of a^k.

Solution. The order of a^k is the smallest number $h > 0$ such that $(a^k)^h \equiv 1 \pmod{m}$. We first find which h satisfy the above equation. As a preliminary, write $d = (k, \ell)$, $k = dk'$, $\ell = d\ell'$; thus $(k', \ell') = 1$. Then we obtain:

$$(a^k)^h \equiv 1 \pmod{m} \Leftrightarrow a^{kh} \equiv 1 \pmod{m} \Leftrightarrow kh \equiv 0 \pmod{\ell} \Leftrightarrow dk'h \equiv 0 \pmod{d\ell'}$$

$$\Leftrightarrow k'h \equiv 0 \pmod{\ell'} \Leftrightarrow h \equiv 0 \pmod{\ell'}, \text{ because } (k', \ell') = 1.$$

Thus the smallest solution for h is $h = \ell' = \ell/d$, so the order of a^k is $\ell/(k, \ell)$.

Problem 5. a) Carefully state the Chinese remainder theorem.

b) Use the Chinese remainder theorem to show that if $(a, 77) = 1$, then $a^{30} \equiv 1 \pmod{77}$.

Solution. a) If m and n are relatively prime, then there is a one-to-one correspondence between numbers x mod mn on the one hand, and between pairs of numbers (b mod m, c mod n) on the other hand. The correspondence is given by the two congruences

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv c \pmod{n} \end{cases}. \qquad (*)$$

Put differently: if $(m, n) = 1$, and given b and c, then the simultaneous congruences $(*)$ have a solution x, and x is unique mod mn.

b) Since $(a, 77) = 1$, it follows that $(a, 7) = 1$ and $(a, 11) = 1$. Now by the Little Fermat Theorem, we conclude that

$$a^6 \equiv 1 \pmod{7}, \qquad a^{10} \equiv 1 \pmod{11}.$$

Raising the first equation to the 5th power, and the second equation to the 3rd power, we obtain

$$a^{30} \equiv 1 \pmod{7}, \qquad a^{30} \equiv 1 \pmod{11}.$$

But the number 1 is also congruent to 1 mod both 7 and 11; so by the Chinese Remainder Theorem, a^{30} and 1 must be congruent mod 77 (since they both satisfy the congruences $(*)$ with $x = a^{30}, b = c = 1, m = 7$, and $n = 11$).

Problem 6. a) Find a solution of $x^2 \equiv -1 \pmod{5}$.

b) Find a solution of $x^2 \equiv -1 \pmod{25}$.

c) Find a solution of $x^2 \equiv -1 \pmod{125}$.

(Remark: I am not asking you to find the most general solution; just find one particular solution in each case.)

Solution. a) x is congruent to one of $0, 1, 2, 3$, or 4 mod 5. The squares of these (taken mod 5) are $0, 1, 4, 4$, and 1; thus $x \equiv 2$ or $x \equiv 3 \pmod{5}$. We'll stick with the choice $x \equiv 2$ (but the other one works as well.)

to the equation mod 5, we try x of the form $2 + 5\ell$, where ℓ only matters mod 5. Thus we want

$$(2+5\ell)^2 \equiv -1 \pmod{25} \Leftrightarrow 4 + 20\ell + 25\ell^2 \equiv -1 \pmod{25} \Leftrightarrow 20\ell \equiv -5 \pmod{25}$$

$$\Leftrightarrow 4\ell \equiv -1 \pmod 5 \Leftrightarrow \ell \equiv 1 \pmod 5.$$

Thus we can take as our solution

$$x = 2 + 5 \cdot 1 = 7.$$

(Alternative method: if we want $x \equiv 2 \pmod 5$, then the possibilities for x mod 25 are $2, 7, 12, 17$, and 22, and a little trial and error also gives the solution $x = 7$. Another remark: if you had started with the solution $x = 3$ to part (a), you would have obtained a solution $x = 18$ to part (b).)

c) This is much the same as before; we try $x = 7 + 25k$, where k only matters mod 5. Once again,

$$(7+25k)^2 \equiv -1 \pmod{5^3} \Leftrightarrow 49 + 350k + 5^4k \equiv -1 \pmod{5^3} \Leftrightarrow 350k \equiv -50 \pmod{5^3}$$

$$\Leftrightarrow 14k \equiv -2 \pmod 5 \Leftrightarrow k \equiv 2 \pmod 5.$$

Thus we can take

$$x = 7 + 25 \cdot 2 = 57.$$

(Once again, the other solution mod 125 is $x = 68$. Also, you could have found the solution $x = 57$ by trial and error, by trying for x all the numbers mod 125 that are congruent to 7 mod 25; this is again a short list, consisting of $7, 32, 57, 82, 107$.)

Problem 7. Let p be a prime number, and let k be a number such that $(k, p-1) = 1$. Let a be given (you may assume $a \not\equiv 0 \pmod p$ if you like). Show that the equation

$$x^k \equiv a \pmod p$$

has exactly one solution $x \pmod p$.

(Hint: Either raise the equation to the mth power for a suitable m, or use indices.)

Solution. (Preliminary remark: If $a \equiv 0 \pmod p$, then the only solution for x is $x \equiv 0 \pmod p$. Otherwise, if $a \not\equiv 0$, we can see that $x \not\equiv 0$ as well. We assume that we are in this latter case throughout this problem.)

Here is one way to solve this problem. First, find m such that $km \equiv 1 \pmod{p-1}$; this is possible since $(k, p-1) = 1$; thus $km = (p-1)n + 1$ for some n. Now raise the original equation to the mth power to obtain

$$x^k \equiv a \pmod p \Rightarrow x^{km} \equiv a^m \pmod p \Rightarrow x \equiv a^m \pmod p.$$

The second implication holds because $x^{p-1} \equiv 1 \pmod p$. Thus if x is a solution, it must be congruent to a^m. This establishes uniqueness of x, provided we can show that x exists. To do this, just check that $x = a^m$ genuinely is a solution:

$$(a^m)^k \equiv a^{mk} \equiv a \pmod p,$$

where once again the second equivalence holds because $a^{p-1} \equiv 1 \pmod p$.

Here is another solution, totally independent of the first: choose a primitive root g mod p, and write $a \equiv g^i \pmod p$, where i is the index of a relative to g. Instead of looking for y, we look for its index y; so write $x = g^y$ and try to solve for j. Remember that the index y is really a number mod $(p-1)$. The equation becomes

$$(g^y)^k \equiv g^i \pmod p \Leftrightarrow g^{yk} \equiv g^i \pmod p \Leftrightarrow yk \equiv i \pmod{p-1}.$$

This last equation has a unique solution for y mod $(p-1)$, since k is invertible mod $(p-1)$. Since y exists and is unique, the same can be said for $x = g^y$.