

MATH 470 Homework 3 Solutions

1. If a and b are integers such that $ab \equiv 0 \pmod{p}$ where p is a prime, show that either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. Hence show that the only solutions to $x^2 \equiv 1 \pmod{p}$ for an odd prime p are $x \equiv \pm 1 \pmod{p}$.

For the first part since $ab \equiv 0 \pmod{p}$, $p|ab$ and hence that either $p|a$ (so that $a \equiv 0 \pmod{p}$) or $p|b$. (so that $b \equiv 0 \pmod{p}$). [This last statement follows from the Euclidean Algorithm: If a is not equivalent to $0 \pmod{p}$ then since p is prime $\gcd(p, a) = 1$ and so there are integers x and y with $ax + py = 1$. But then $axb + pyb = abx + pyb = b$. Now since p divides ab (we are given $ab \equiv 0 \pmod{p}$) and p divides pyb it must divide b - that is $b \equiv 0 \pmod{p}$]

For the second part, $x^2 \equiv 1 \pmod{p}$ gives $(x - 1)(x + 1) \equiv 0 \pmod{p}$ and so from part one that either $x - 1$ or $x + 1 \equiv 0 \pmod{p}$. Thus $x \equiv \pm 1 \pmod{p}$.

What if p is not a prime? If the modulus is 8 then it is easily seen that the solutions to $x^2 \equiv 1 \pmod{8}$ are $x = \pm 1$ $x = \pm 3$. Thus the result fails for non-prime moduli.

2. What are the last two digits of 123^{456} ?

We want to know the remainder after we divide this number by 100. That is, calculate $123^{456} \pmod{100}$. Now $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$. Also, $456 \equiv 16 \pmod{40}$, so by Euler's theorem we must compute $123^{16} \pmod{100}$. Now, this immediately simplifies to $23^{16} \pmod{100}$. Further, taking all values mod 100, $23^1 \equiv 23$, $23^2 \equiv 29$, $23^4 \equiv (29)^2 \equiv 41$, $23^8 \equiv (41)^2 \equiv 81 \equiv (-19)$, $23^{16} \equiv (-19)^2 \equiv 61$. Thus the last two digits are 61.

3. Use the Chinese Remainder theorem to solve the systems of congruences:

a. Find $x \pmod{77}$ if $x \equiv 2 \pmod{7}$ and $x \equiv 4 \pmod{11}$.

Note $\gcd(7, 11) = 1$. Thus there exists integers s, t such that $7s + 11t = 1$ - and these are computed from the Euclidean algorithm as $s = -3, t = 2$. The solution is now given by $x = 4.7.s + 2.11.t = 4.7.(-3) + 2.11.2 = -40 \equiv 37 \pmod{77}$.

b. $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{4}$, $x \equiv 1 \pmod{5}$.

We use the alternative method here just for something different. The first equation gives $x = 2 + 3s$ for some integer s . Now the second gives $2 + 3s \equiv 3 \pmod{4}$ or $3s \equiv 1 \pmod{4}$. Solving this, gives $s = 3$ and so $x \equiv 11 \pmod{12}$. But then $x = 11 + 12t$ and so putting this into the last equation gives $12t + 11 \equiv 1 \pmod{5}$, or $12t \equiv -10 \equiv 0 \pmod{5}$. Thus $t = 0$ and so the final solution is $x \equiv 11 \pmod{60}$.

4. An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Use the Chinese Remainder theorem to solve the puzzle by writing down the elements of the riddle as a sequence of congruences and then solving this system.

The conditions described amount to the following system of congruences: $x \equiv 1 \pmod{2}$, $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 1 \pmod{5}$, $x \equiv 1 \pmod{6}$ and $x \equiv 0 \pmod{7}$.

It is tempting to just apply the Chinese Remainder Theorem directly, but we cannot do this: a requirement is that each moduli m_j satisfy $\gcd(m_j, m_k) = 1$ and that is not the case here. The moduli 2, 3, 4, 6 are the problems. Note that if $x \equiv a \pmod{2n}$ then it is certainly so that $x \equiv a \pmod{n}$. Thus the two congruences $x \equiv 1 \pmod{2}$ and $x \equiv 1 \pmod{3}$ are subsumed by $x \equiv 1 \pmod{6}$. Can we combine this with the one mod 4? Certainly one solution would be $x \equiv 1 \pmod{24}$, but is this the *least* answer? We again cannot apply CRT since $\gcd(4, 6) = 2 > 1$. A little thought should convince that we should solve this latter pair $\pmod{12}$ instead, and there is the obvious solution $x \equiv 1 \pmod{12}$. Another way to view this is as follows. We note that $x \equiv 1 \pmod{2}$ is implied by $x \equiv 1 \pmod{6}$ so we can neglect the first of these. We can use CRT to combine those with moduli 3 and 4 since $\gcd(3, 4) = 1$. It is easy to see the solution is $x \equiv 1 \pmod{12}$. But this equation also implies the congruence $x \equiv 1 \pmod{6}$ and so we may replace all four congruences by the single $x \equiv 1 \pmod{12}$. With this preamble, we are now left with the three congruences that do satisfy the conditions of CRT:

$$x \equiv 1 \pmod{5} \quad x \equiv 0 \pmod{7} \quad x \equiv 1 \pmod{12}$$

Applying the CRT we construct the solution $x \equiv 301 \pmod{420}$ giving the answer $x = 301$.

This puzzle appears in *Brahma-Sphuta-Siddhanta* (Brahma's Correct System) by Brahmagupta (born 598 AD):

5. Use Euler's Theorem to calculate $17^{4567} \pmod{30}$

We calculate $\phi(30) = 8$ from $\phi(30) = 30(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})$. Then Euler's theorem gives $a^{\phi(30)} \equiv 1 \pmod{30}$. We then have $4567 \equiv 7 \pmod{8}$ and so $17^{4567} \pmod{30}$ reduces to $17^7 \pmod{30}$. Then $17^7 \pmod{30} \equiv 289^3 \cdot 17 \pmod{30} \equiv 19^3 \cdot 17 \pmod{30} \equiv -11^3 \cdot 17 \pmod{30} \equiv -121 \cdot 11 \cdot 17 \pmod{30} \equiv -1 \cdot 11 \cdot 17 \pmod{30} \equiv -1 \cdot 187 \pmod{30} \equiv -7 \pmod{30} \equiv 23 \pmod{30}$.

6. Compute $3^{4567} \pmod{89}$

Since 89 is prime we have $3^{88} \equiv 1 \pmod{89}$ and since $4567 \equiv 79 \pmod{88}$, we thus must now compute $3^{79} \pmod{89}$. Now $79 = 64 + 8 + 4 + 2 + 1$. Also, taking all congruences mod 89, we have $3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 81$, $3^8 \equiv 81^2 \equiv (-8)^2 \equiv 64$, $3^{16} \equiv 64^2 \equiv (-25)^2 \equiv 625 \equiv 2$, $3^{32} \equiv 2^2 \equiv 4$, $3^{64} \equiv 4^2 \equiv 16$. Thus $3^{79} \equiv 16 \cdot 64 \cdot 81 \cdot 9 \cdot 3 \pmod{89}$. Or, $3^{79} \equiv 16 \cdot (-25) \cdot (-8) \cdot 9 \cdot 3 \equiv 3200 \cdot 27 \equiv 85 \cdot 27 \equiv -4 \cdot 27 \pmod{89}$. Simplifying, we obtain $3^{4567} \equiv 70 \pmod{89}$.