Quiz 2

CS 207 :: Autumn 2021
September 11, 2021

1. $\phi(120) =$ ____.

   Solution: $120 = 2^3 \cdot 3 \cdot 5$, so $\phi(120) = 2^2 \cdot (2-1)(3-1)(5-1) = 32$.

2. $\phi(540) =$ ____.

   Solution: $540 = 2^2 \cdot 3^3 \cdot 5$, so $\phi(540) = 2 \cdot 3^2 \cdot (2-1)(3-1)(5-1) = 144$.

3. $\phi(600) =$ ____.

   Solution: $600 = 2^3 \cdot 3 \cdot 5^2$, so $\phi(600) = 2^2 \cdot 5 \cdot (2-1)(3-1)(5-1) = 160$.

4. **Chinese Remainder Theorem**

   Find the smallest positive integer solution to:

$$x \equiv 2 \pmod{19}$$
$$x \equiv 5 \pmod{20}$$

   Show your work.

   Solution: We execute the Extended Euclidean Algorithm to find two integers u, v such that $19u+20v = 1$:

$$\gcd(19, 20) = \gcd(19, 1 = 20 - 19) = 1$$

   so that $1 = 1 \cdot 20 - 1 \cdot 19$. Therefore, $u = -1$ and $v = 1$.

   Alt: It is OK to just list the sequence of pairs as:

$$(19, 20) \rightarrow (19, 1 = 20 - 19)$$

   Then a solution for x is given by $19u \cdot 5 + 20v \cdot 2 = -19 \cdot 5 + 20 \cdot 2 = -55 = 380 - 55 \pmod{380} = 325 \pmod{380}$. This is the unique solution in the range $[0, 380)$.

   Alt: May derive this solution by considering, e.g., that $x_1 = 19u$ solves $x_1 \equiv 1 \pmod{20}$ and $x_1 \equiv 0 \pmod 19$, and similarly $x_2 = 20v$ solves $x_2 \equiv 0 \pmod{20}$ and $x_2 \equiv 1 \pmod 19$, and $x = 5x_1 + 2x_2$.

5. **Chinese Remainder Theorem**

   Find the smallest positive integer solution to:

$$x \equiv 3 \pmod{19}$$
$$x \equiv 10 \pmod{20}$$

   Show your work.

   Solution: We execute the Extended Euclidean Algorithm to find two integers u, v such that $19u+20v = 1$:

$$\gcd(19, 20) = \gcd(19, 1 = 20 - 19) = 1$$

   so that $1 = 1 \cdot 20 - 1 \cdot 19$. Therefore, $u = -1$ and $v = 1$.

Alt: It is OK to just list the sequence of pairs as:

$$(19, 20) \to (19, 1 = 20 - 19)$$

Then a solution for x is given by $19u \cdot 10 + 20v \cdot 3 = -19 \cdot 10 + 20 \cdot 3 = -130 = 380 - 130 \pmod{380} = 250 \pmod{380}$. This is the unique solution in the range $[0, 380)$.

Alt: May derive this solution by considering, e.g., that $x_1 = 19u$ solves $x_1 \equiv 1 \pmod{20}$ and $x_1 \equiv 0 \pmod{1}9$, and similarly $x_2 = 20v$ solves $x_2 \equiv 0 \pmod{20}$ and $x_2 \equiv 1 \pmod{1}9$, and $x = 10x_1 + 3x_2$.

6. **Chinese Remainder Theorem**

Find the smallest positive integer solution to:

$$x \equiv 2 \pmod{19}$$
$$x \equiv 10 \pmod{20}$$

Show your work.

Solution: We execute the Extended Euclidean Algorithm to find two integers u, v such that $19u + 20v = 1$:

$$\gcd(19, 20) = \gcd(19, 1 = 20 - 19) = 1$$

so that $1 = 1 \cdot 20 - 1 \cdot 19$. Therefore, $u = -1$ and $v = 1$.

Alt: It is OK to just list the sequence of pairs as:

$$(19, 20) \to (19, 1 = 20 - 19)$$

Then a solution for x is given by $19u \cdot 10 + 20v \cdot 2 = -19 \cdot 10 + 20 \cdot 2 = -150 = 380 - 150 \pmod{380} = 230 \pmod{380}$. This is the unique solution in the range $[0, 380)$.

Alt: May derive this solution by considering, e.g., that $x_1 = 19u$ solves $x_1 \equiv 1 \pmod{20}$ and $x_1 \equiv 0 \pmod{1}9$, and similarly $x_2 = 20v$ solves $x_2 \equiv 0 \pmod{20}$ and $x_2 \equiv 1 \pmod{1}9$, and $x = 10x_1 + 2x_2$.

7. **Chinese Remainder Theorem**

Find the smallest positive integer solution to:

$$x \equiv 3 \pmod{19}$$
$$x \equiv 5 \pmod{20}$$

Show your work.

Solution: We execute the Extended Euclidean Algorithm to find two integers u, v such that $19u + 20v = 1$:

$$\gcd(19, 20) = \gcd(19, 1 = 20 - 19) = 1$$

so that $1 = 1 \cdot 20 - 1 \cdot 19$. Therefore, $u = -1$ and $v = 1$.

Alt: It is OK to just list the sequence of pairs as:

$$(19, 20) \to (19, 1 = 20 - 19)$$

Then a solution for x is given by $19u \cdot 5 + 20v \cdot 3 = -19 \cdot 5 + 20 \cdot 3 = -35 = 380 - 35 \pmod{380} = 345 \pmod{380}$. This is the unique solution in the range $[0, 380)$.

Alt: May derive this solution by considering, e.g., that $x_1 = 19u$ solves $x_1 \equiv 1 \pmod{20}$ and $x_1 \equiv 0 \pmod{1}9$, and similarly $x_2 = 20v$ solves $x_2 \equiv 0 \pmod{20}$ and $x_2 \equiv 1 \pmod{1}9$, and $x = 5x_1 + 3x_2$.

8. **System of Linear Equations**

Solve the following system of equations modulo 10:

$$\begin{aligned} x + 4y &\equiv 2 \pmod{10} \\ 2x + 5y &\equiv 3 \pmod{10} \end{aligned}$$

Show your work.

Solution: After multiplying the first equation by 2 and then subtracting the second equation from it, we get

$$3y \equiv 1 \pmod{10}$$

Since 3 and 10 are co-prime, the inverse of 3 exists modulo 10. It is not hard to see that 7 is the inverse of 3 modulo 10. Therefore, multiplying both sides of the above equation by 7, we get

$$y \equiv 7 \pmod{10}$$

Putting this in the first equation, we get

$$\begin{aligned} x + 28 &\equiv 2 \pmod{10} \\ x &\equiv -26 \pmod{10} \\ x &\equiv 4 \pmod{10} \end{aligned}$$

9. **System of Linear Equations**

Solve the following system of equations modulo 10:

$$\begin{aligned} 2x + 5y &\equiv 4 \pmod{10} \\ x + 4y &\equiv 3 \pmod{10} \end{aligned}$$

Show your work.

Solution:
After multiplying the second equation by 2 and then subtracting the first equation from it, we get

$$3y \equiv 2 \pmod{10}$$

Since 3 and 10 are co-prime, the inverse of 3 exists modulo 10. It is not hard to see that 7 is the inverse of 3 modulo 10. Therefore, multiplying both sides of the above equation by 7, we get

$$y \equiv 14 \equiv 4 \pmod{10}$$

Putting this in the second equation, we get

$$\begin{aligned} x + 16 &\equiv 3 \pmod{10} \\ x &\equiv -13 \pmod{10} \\ x &\equiv 7 \pmod{10} \end{aligned}$$

10. Suppose for integers a, b we have $au + bv = g$, where $g = \gcd(a, b)$, and u, v are integers. Then, describe the set of all integer solutions (x, y) for the equation

$$ax + by = c,$$

where c is some integer. You may consider different cases for c, and write your solution separately for each case. Justify your answer.

Solution: Let $L(a, b)$ denote the set of all linear combinations of a and b. Similarly let $M(g)$ denote the set of all multiples of g. In class, it was shown that $L(a, b) = M(g)$, where $g = \gcd(a, b)$. Since c is also a linear combination of a and b, we can say that there exists an integer h s.t. $c = gh$. Upon expanding as linear combinations of a and b, we get

$$\begin{aligned} ax + by &= (au + bv)h \\ a(x - uh) &= b(vh - y) \end{aligned}$$

Dividing both sides of the above equation by g, we get

$$m(x - uh) = n(vh - y)$$

where m and n are co-prime to each other. This is only possible if $m|(vh - y)$ and $n|(x - uh)$. In other words, $a|g(vh - y)$ and $b|g(x - uh)$. In modulo terms, the first equation implies

$$\begin{aligned} g(vh - y) &\equiv 0 \pmod{a} \\ gy &\equiv vc \pmod{a} \end{aligned}$$

Similarly, the second equation implies

$$gx \equiv uc \pmod{b}$$

The above two equations describe the set of all integer solutions to the equation $ax + by = c$.

11. For integers $x, m > 1$, we say that x is *nil potent* modulo m if there exists a positive integer n such that

$$x^n \equiv 0 \pmod{m}.$$

We define the "square-free part" of a positive integer m, denoted as $\mathrm{SFP}(m)$, as the smallest positive integer z for which there exists an integer y such that $m = zy^2$.

Characterize all numbers that are nil potent modulo m (where $m > 1$), in terms of $\mathrm{SFP}(m)$. Justify your answer.

Solution: First of all, if x is nil potent modulo m, then all prime factors of m are also factors of x. In fact, any integer x which is divided by all prime factors of m is nil potent modulo m. Therefore, one needs to extract the product of all prime factors of m in terms of SFP. For instance, define $F(m)$ as the largest number z such that $z|m$ and $\mathrm{SFP}(z) = z$. Then, a recursive definition would work:

$$F(1) = 1, \quad F(m) = \operatorname{lcm}\left(\mathrm{SFP}(m), F\left(\sqrt{\frac{m}{\mathrm{SFP}(m)}}\right)\right)$$

Then the final characterisation required would be "all multiples of $F(m)$".

12. **Unique Cube-Root**

Give an explicit characterization of all prime numbers p such that there is a unique cube-root of 1 modulo p. That is, give a necessary and sufficient condition for a prime p to satisfy the following:

$$\forall x \in \mathbb{Z},\ x^3 \equiv 1 \pmod p \to x \equiv 1 \pmod p.$$

Make your condition as simple as you can, and prove your claim.

Solution: Using Euler's Totient theorem, we can restate the above condition as

$$\forall x \in \mathbb{Z},\ x^{3 \mod \phi(p)} \equiv 1 \pmod p \to x \equiv 1 \pmod p.$$

It is easy to see that a necessary and sufficient condition for this to hold is that $\gcd(3, \phi(p)) = 1$. Since p is a prime, we can re-write this as $\gcd(3, p-1) = 1$. Therefore, either $p - 1 = 3k + 1$ or $p-1 = 3k+2$ for some integer k. Since p is a prime, we cannot have $p-1 = 3k+2$ as that would imply $p = 3k+3 = 3(k+1)$. Therefore, the only valid solutions are $p = 3k+2$ and $p = 3$, for all integers k.

13. **Square Roots**

Find all integers x in the range $[0, 199]$ such that

$$x^2 \equiv 1 \pmod{200}$$

You should prove that these are the only solutions.

Solution: By CRT, $x^2 \equiv 1 \pmod{200}$ if and only if x satisfies the system of congruences $x^2 \equiv 1 \pmod 8$ and $x^2 \equiv 1 \pmod{25}$.

Let us first find all possible solutions to $x^2 \equiv 1 \pmod 8$. Bringing 1 to the left and using a common identity, we can write

$$(x-1)(x+1) \equiv 0 \pmod 8$$

Therefore, $x^2 \equiv 1 \pmod 8$ iff $(x+1)(x-1) \equiv 0 \pmod 8$. That is $8|(x+1)(x-1)$. This means that $2^i|(x+1)$ and $2^j|(x-1)$ for some i, j such that $i + j \geq 3$. Suppose $2^i|(x+1)$ and $2^j|(x-1)$. Note that if $i \geq 2$ and $j \geq 2$, then $4|(x+1)$ and $4|(x-1)$, which implies that $4|2$, a contradiction. So we have the following 4 cases where at least one of i, j is < 2:

- $i = 0$. In this case $j \geq 3$, and so $8|(x-1)$. That is $x \equiv 1 \pmod 8$.
- $i = 1$. In this case $j \geq 2$, and so $4|(x-1)$. That is $x - 1 = 4q$. If q is even, have $x \equiv 1 \pmod 8$ as in the previous case. Otherwise, $x \equiv 5 \pmod 8$.
- $i \geq 2, j = 1$. In this case, working as above, we get $x \equiv -1 \pmod 8$ or $x \equiv 4 - 1 \equiv 3 \pmod 8$.
- $i \geq 3, j = 0$. In this case, working as above, we get $x \equiv -1 \equiv 7 \pmod{2^k}$.

Therefore, the solutions to $x^2 \equiv 1 \pmod 8$ are $x \equiv 1, 3, 5, 7 \pmod 8$. Similarly, the solutions for $x^2 \equiv 1 \pmod{25}$ will be given by all x's s.t. $25|(x+1)(x-1)$. Since 5 cannot divide both $x-1$ and $x+1$, as that would imply that $5|2$, we can say that either $25|x-1$ or $25|x+1$. Therefore, the only solutions to this are $x \equiv \pm 1 \pmod{25}$.

Therefore, the set of solutions of $x^2 \equiv 1 \pmod{200}$ are exactly those which satisfy

$$x \equiv 1, -1, 3, 5 \pmod 8$$
$$x \equiv 1, -1 \pmod{25}.$$

Each of the 8 pairs in $\{\pm 1, 4 \pm 1\} \times \{\pm 1\}$ corresponds to the CRT representation of a unique x modulo 200. Using the fact that $8 \cdot (-3) + 25 \cdot (1) = 1$, we obtain these 8 solutions as 1, 49, 51, 99, 101, 149, 151, 199.

14. **Speed of Euclid's Algorithm.**

The Euclidean algorithm zooms into the answer quite quickly. This is because, at each step one of the numbers is replaced by a number which is at most half of it. To see this, prove the following. If x, y are positive integers with $y \leq x$, and r is the remainder on dividing x by y, then $r < x/2$. That is, prove that if

$$x \equiv r \pmod{y} \text{ and } 0 \leq r < y$$

then

$$r < \frac{x}{2}.$$

Solution: By division lemma. Let $x = yq + r$, where $0 < r < y$ and $q \geq 0$. As, $x \geq y$, we have, $q \geq 1$.

Proof 1: Proof by contradiction.
Suppose, $r \geq \frac{x}{2}$.
Then, we have, $x = yq + r \geq yq + \frac{x}{2}$. This implies, $\frac{x}{2} \geq yq \geq y > r$, which is a contradiction. Hence proved.

Proof 2: Case study.
case 1: $y \leq \frac{x}{2}$.
Then as, $y > r$, we have, $r < \frac{x}{2}$.

case 2: $\frac{x}{2} < y \leq x$.
In this case, q has to be 1.
This implies, $r = x - y < \frac{x}{2}$.

Thus, in all cases we have the desired output.