M328K: Homework 6

Katherine Ho

October 22, 2024

1. (a) For $n > 1$, let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n that are relatively prime to n. Show that

$$a_1 + a_2 + \cdots + a_{\phi(n)} = \frac{1}{2} n\phi(n).$$

(Hint: $\gcd(a, n) = 1 \iff \gcd(n - a, n) = 1$)

Proof. For each integer a_i coprime to n, $n - a_i$ is also coprime to n because $\gcd(a, n) = 1 \iff \gcd(n-a, n) = 1$. We can pair these integers as so: $(a_1, n - a_1), (a_2, n - a_2), \ldots$. Since there are $\phi(n)$ such integers a_i, there are $\frac{\phi(n)}{2}$ such pairs.
Then, we know the sum of each pair is

$$a_i + (n - a_i) = n$$

So for all pairs, we have

$$a_1 + (n - a_1) + a_2 + (n - a_2) + \cdots + a_{\frac{\phi(n)}{2}} + (n - a_{\frac{\phi(n)}{2}}) = n \cdot \frac{\phi(n)}{2}$$

This is equivalent to

$$a_1 + a_2 + \cdots + a_{\phi(n)} = \frac{1}{2} n\phi(n)$$

□

(b) If $p \geq 5$ is prime, show that the product of the $\phi(p-1)$ primitive roots of p is congruent to 1 modulo p. (Hint: If a is a primitive root of p, then a^k is a primitive root of p iff $\gcd(k, p-1) = 1$. Now use part (a).)

Proof. Let g be a primitive root of p. The primitive roots of p are the powers g^k where $1 \leq k \leq p - 1$ and $\gcd(k, p-1) = 1$. The product P of all the primitive roots of p is:

$$P = g^{k_1} \cdot g^{k_1} \ldots g^{k_{\phi(p-1)}}$$

By the properties of exponents, this is equivalent to

$$P = g^{k_1 + k_2 + \cdots + k_{\phi(p-1)}}$$

From part (a), we can substitute:

$$P = g^{\frac{1}{2}(p-1)\phi(p-1)}$$

Then, since g is a primitive root of p, we know that $g^{p-1} \equiv 1 \pmod{p}$. So, we can reduce the exponent $\pmod{p-1}$:

$$P \equiv g^{\frac{1}{2}(p-1)\phi(p-1) \pmod{p-1}} \pmod{p}$$

We can see that the exponent is a multiple of $p-1$. So, we can say:

$$P \equiv 1 \pmod{p}$$

Thus the product of the $\phi(p-1)$ primitive roots of p is congruent to $1 \pmod{p}$. □

2. (a) Compute the table of indices modulo 17 relative to the primitive root 3.

Proof. First, compute all powers of $3 \pmod{17}$.

$$\begin{aligned}
3^1 &\equiv 3 \pmod{17} \\
3^2 &\equiv 9 \pmod{17} \\
3^3 &\equiv 10 \pmod{17} \\
3^4 &\equiv 13 \pmod{17} \\
3^5 &\equiv 5 \pmod{17} \\
3^6 &\equiv 15 \pmod{17} \\
3^7 &\equiv 11 \pmod{17} \\
3^8 &\equiv 16 \pmod{17} \\
3^9 &\equiv 14 \pmod{17} \\
3^{10} &\equiv 8 \pmod{17} \\
3^{11} &\equiv 7 \pmod{17} \\
3^{12} &\equiv 4 \pmod{17} \\
3^{13} &\equiv 12 \pmod{17} \\
3^{14} &\equiv 2 \pmod{17} \\
3^{15} &\equiv 6 \pmod{17} \\
3^{16} &\equiv 1 \pmod{17}
\end{aligned}$$

We can use these values to create the table of indices:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

□

Use the table to solve the following congruences:

(b) $x^{12} \equiv 13 \pmod{17}$

Proof. We can first take the index of both sides of the congruence.

$$\begin{aligned}
\operatorname{ind}(x^{12}) &\equiv \operatorname{ind}(13) \pmod{16} \\
12 \operatorname{ind}(x) &\equiv 4 \pmod{16} \\
3 \operatorname{ind}(x) &\equiv 1 \pmod{4}
\end{aligned}$$

Then, find the multiplicative inverse of 3 (mod 4):

$$\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 3x - 4y &= 1 \\ 4 &= 3(1) + 1 \\ 1 &= 4(1) - 3(1) \\ 1 &= 3(-1) - 4(-1) \end{aligned}$$

We have $x \equiv -1 \equiv 3 \pmod 4$. So $3^{-1} \pmod 4 = 3$. We can multiply both sides of the previous congruence by this value:

$$\operatorname{ind}(x) \equiv 3 \pmod 4$$

There are 4 solutions since we previously divided by a gcd of 4.

$$\operatorname{ind}(x) \equiv 3, 7, 11, 15 \pmod{16}$$

$$\boxed{x \equiv 10, 11, 7, 6 \pmod{17}}$$

□

(c) $9x^8 \equiv 8 \pmod{17}$

Proof. We can first take the index of both sides of the congruence.

$$\begin{aligned} \operatorname{ind}(9x^8) &\equiv \operatorname{ind}(8) \pmod{16} \\ \operatorname{ind}(9) + \operatorname{ind}(x^8) &\equiv 10 \pmod{16} \\ 2 + 8\operatorname{ind}(x) &\equiv 10 \pmod{16} \\ 8\operatorname{ind}(x) &\equiv 8 \pmod{16} \\ \operatorname{ind}(x) &\equiv 1 \pmod 2 \\ \operatorname{ind}(x) &\equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16} \end{aligned}$$

$$\boxed{x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}}$$

□

(d) $7^x \equiv 7 \pmod{17}$

Proof. Since 17 is prime, the multiplicative group of integers (mod 17) has order 16. So the exponents x and 1 are congruent (mod 16).

$$x \equiv 1 \pmod{16}$$

So,

$$x = 1 + 16y$$

for some $y \in \mathbb{Z}$.
The smallest solution is $x = 1$. So, $x = 1$ satisfies the congruence.

□

3. Determine whether the congruences $x^{14} \equiv 3 \pmod{23}$ and $x^{14} \equiv 5 \pmod{23}$ are solvable.

Proof. $x^{14} \equiv 3 \pmod{23}$ is not solvable. $x^{14} \equiv 5 \pmod{23}$ is solvable. □

4. In this problem, we will establish the existence of primitive roots for odd prime powers. Throughout, let p be an odd prime. Prove the following assertions.

   (a) If g is a primitive root of p such that $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root of p^2.

   Proof. Let d be the order of $g \pmod{p^2}$. We know
   $$g^d \equiv 1 \pmod{p^2}$$
   This implies
   $$\begin{aligned} p^2 \mid g^d - 1 \\ p \mid g^d - 1 \\ g^d \equiv 1 \pmod{p} \end{aligned}$$
   Since p is prime, either $d \mid p-1$ or $d \mid p(p-1)$. If $d \mid p-1$, then since $p-1 \mid d$ we have $d = p-1$. However this can't be true given $g^{p-1} \not\equiv 1 \pmod{p^2}$.
   So, $d \mid p(p-1)$. Thus g is a primitive root $\pmod{p^2}$. □

   (b) If g is a primitive root of p, then either g or $g+p$ (or both) is a primitive root of p^2.

   Proof. If g is a primitive root of p, then the order of $g \pmod{p^2}$ is either $p-1$ or $p(p-1)$. If g has order p, then $g+p$ will be a primitive root of p^2. □

   (c) If g is a primitive root of p^2, then for each positive integer $k \geq 2$,
   $$g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$
   (Hint: Argue by induction on k. For the induction step, assume it holds for k and show that $g^{p^{k-2}(p-1)} = 1 + ap^{k-1}$, for some $a \in \mathbb{Z}$, where $p \nmid a$. Finish by raising both sides to the pth power and then reduce mod p^{k+1}.)

   Proof. This holds for $k = 2$.
   IH: Assume this is true for some $k \geq 2$. Since $\gcd(g, p^{k-1}) = \gcd(g, p^k) = 1$, Euler's Theorem states:
   $$g^{p^{k-2}(p-1)} = g^{\phi(p^k-1)} \equiv 1 \pmod{p^{k-1}}$$
   There exists an $a \in \mathbb{Z}$ such that
   $$g^{p^{k-2}(p-1)} = 1 + ap^{k-1}$$
   Raising both sides to the pth power, we get
   $$g^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}$$
   Since a is not divisible by p, we have
   $$g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$
   Thus proving the induction step. □

(d) If p is an odd prime and $k \geq 1$, then there exists a primitive root for p^k. In fact, there exists an integer g that is a primitive root for all positive powers of p.

Proof. Let g be a primitive root of p and $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Let n be the order of $g \pmod{p^k}$. n divides $\phi(p^k) = p^{k-1}(p-1)$.
Since $g^n \equiv 1 \pmod{p^k}$ implies $g^n \equiv 1 \pmod{p}$, we have $p-1 \mid n$. Then, $n = p^m(p-1)$ where $0 \leq m \leq k-1$. If $n \neq p^{k-1}(p-1)$, then $p^{k-2}(p-1)$ would be divisible by n and we would have

$$g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$$

However this contradicts how we set g above. Therefore, $n = p^m(p-1)$ and g is a primitive root for p^k.

□