Math 573 Problem Set 5 Solutions

1. List the primitive roots modulo 14.

The primitive roots modulo 14 are 3 and 5. They were found using SAGE.

2. **(a)** Prove that for $n > 1$, the sum of the positive integers less then n and relatively prime to n is $\frac{1}{2}n\phi(n)$.

Proof: Let $j > 0$ be an integer relatively prime to n that is less then n. Observe that $n - j$ satisfies $0 < n - j < n$ and is relatively prime to n as well. (If not, there would be a common divisor of n and j!). If $n > 2$, then $\phi(n)$ is even and so we can pair off the terms j and $n - j$ to obtain all of the integers less then n relatively prime to n. Each pair sums to give n and there are $\frac{1}{2}\phi(n)$ such pairs. This gives the result for $n > 2$. The case of $n = 2$ is clear. ■

(b) Let p be a prime. Show that the product of the $\phi(p-1)$ primitive roots modulo p is congruent modulo p to $(-1)^{\phi(p-1)}$.

Proof: Let $r_1, \ldots, r_{\phi(p-1)}$ be the primitive roots modulo p. Recall that for each j we can write $r_j = r_1^{k_j}$ for some k_j with $0 < k_j < p - 1$, k_j relatively prime to $p - 1$. Thus we have

$$\begin{aligned} r_1 \cdots r_{\phi(p-1)} &= r_1 \cdot r_1^{k_2} \cdots r_1^{k_{\phi(p-1)}} \\ &= r_1^{\sum_{j=1}^{\phi(p-1)} k_j} \\ &= r^{\frac{1}{2}(p-1)\phi(p-1)} \end{aligned}$$

where the last equality uses part (a). Applying the result that if r is a primitive root modulo p then $r^{(p-1)/2} \equiv -1 (\operatorname{mod} p)$ we have the result. ■

3. Prove that $\operatorname{ord}_n(ab) = \operatorname{ord}_n(a) \operatorname{ord}_n(b)$ if $\gcd(\operatorname{ord}_n(a), \operatorname{ord}_n(b)) = 1$.

Proof: Let $r = \operatorname{ord}_n(ab), s = \operatorname{ord}_n(a), t = \operatorname{ord}_n(b)$. Observe that

$$\begin{aligned} (ab)^{st} &= a^{st} b^{st} \\ &= (a^s)^t (b^t)^s \\ &\equiv 1 (\operatorname{mod} n). \end{aligned}$$

Thus, we have $r \mid st$. Note that this did not use that $\gcd(s,t) = 1$. Observe that

$$\begin{aligned} a^{rt} &\equiv a^{rt} b^{rt} \pmod{n} \qquad (\text{since } b^t \equiv 1 \pmod{n}) \\ &\equiv (ab)^{rt} \pmod{n} \\ &\equiv 1 \pmod{n} \qquad (\text{since } \operatorname{ord}_n(ab) = 1). \end{aligned}$$

Thus, we have that $s \mid rt$. However, $\gcd(s,t) = 1$ implies that $s \mid r$. Similarly, we get that $t \mid r$. Since $\gcd(s,t) = 1$, we have that $st \mid r$ and hence they are equal. ■

4. Let $a, n \in \mathbb{Z}_{>1}$ and let p be a prime. If $p \mid a^{2^n} + 1$, prove that $p = 2$ or $p \equiv 1 \pmod{2^{n+1}}$.

Proof: If $p = 2$ we are done, so assume $p > 2$. The fact that $p \mid a^{2^n} + 1$ gives that $a^{2^n} \equiv -1 \pmod{p}$. Thus, $a^{2^{n+1}} = (a^{2^n})^2 \equiv 1 \pmod{p}$. Thus, we must have $2^{n+1} \mid p - 1$ by Euler's theorem, i.e., $p \equiv 1 \pmod{2^{n+1}}$. ■

5. (a) Let p and q be odd primes. If $q \mid a^p - 1$, then either $q \mid (a-1)$ or $q = 2kp + 1$ for some $k \in \mathbb{Z}$.

Proof: Let q, p be odd primes so that $q \mid a^p - 1$. i.e., $a^p \equiv 1 \pmod{q}$. This says that $\operatorname{ord}_q(a) \mid p$. Thus, we must have either $\operatorname{ord}_q(a) = 1$, in which case $q \mid (a-1)$ or we must have $\operatorname{ord}_q(a) = p$ in which case $p \mid \phi(q) = q - 1$. Thus, we have the result. ■

(b) Prove that if p is an odd prime, then the prime divisors of $2^p - 1$ are of the form $2kp + 1$.

Proof: We use part (a) here with $a = 2$. In this case it is clear that $q \nmid (2-1) = 1$, so it must be that any prime divisor of $2^p - 1$ is of the form $q = 2kp + 1$, as desired. ■

(c) Find the smallest prime divisor of $2^{29} - 1$.

Part (b) tells us that all prime divisors of $2^{29} - 1$ must be of the form $q = 58k + 1$. Thus, we just need to run through these for $k > 0$. Using SAGE we quickly find that $k = 4$ gives the smallest prime divisor, i.e., 223 is the smallest prime divisor.

6. Let p be a prime and $a \in \mathbb{Z}$ so that $\gcd(a, p) = 1$. Show that the congruence

$$x^n \equiv a \pmod{p}$$

has $\gcd(n, p-1)$ solutions if

$$a^{(p-1)/\gcd(n,p-1)} \equiv 1 \pmod{p}$$

and no solutions otherwise. (Hint: Think primitive roots! Write $a = r^j$ for some j with r a primitive root.)

Proof: Observe that since $\gcd(a, p) = 1$, if there is a solution x then we must have $\gcd(x, p) = 1$ as well. Let r be a primitive root modulo p and write $a = r^j$. For each x with $\gcd(x, p) = 1$, there is a k_x so that $x \equiv r^{k_x} \pmod{p}$. We have that x is a solution to the congruence if and only if r^{k_x} is a solution to the congruence. In turn, this is equivalent to $r^{k_x n} \equiv r^j \pmod{p}$. Since r is primitive, this is equivalent to $k_x n \equiv j \pmod{p-1}$. Thus, we have reduced the problem to looking for solutions to the linear congruence $k_x n \equiv j \pmod{p-1}$. From our work on linear congruences, we know this has exactly $\gcd(n, p-1)$ solutions if $\gcd(n, p-1) \mid j$ and no solutions otherwise. If $\gcd(n, p-1) \mid j$, then

$$\begin{aligned} a^{(p-1)/\gcd(n,p-1)} &\equiv (r^j)^{(p-1)/\gcd(n,p-1)} \pmod{p} \\ &\equiv (r^{p-1})^{j/\gcd(n,p-1)} \pmod{n} \qquad (\text{since } \gcd(n, p-1) \mid j) \\ &\equiv 1 \pmod{p}. \end{aligned}$$

On the other hand, if $\gcd(n, p-1) \nmid j$, then $j(p-1)/\gcd(n, p-1) \not\equiv 0 \pmod{p-1}$ and so $a^{(p-1)/\gcd(n,p-1)} \equiv r^{j(p-1)/\gcd(n,p-1)} \not\equiv 1 \pmod{p}$. Thus we have the result. ■

7. Prove that $1^k, 2^k, \ldots, (p-1)^k$ form a reduced residue system modulo p if and only if $\gcd(k, p-1) = 1$.

Proof: Note that there are clearly $p-1$ elements here, so what we need to prove is that they are distinct if and only if $\gcd(k, p-1) = 1$. Let r be a primitive root modulo p and let $a, b \in \{1, 2, \ldots, p-1\}$ with $a \neq b$. We show a^k and b^k are distinct modulo p if and only if $\gcd(k, p-1) = 1$. Write $a = r^i$, $b = r^j$ for some $i, j \in \{1, \ldots, p-1\}$. We have that $a^k \equiv b^k \pmod{p}$ if and only if $r^{ik} \equiv r^{jk} \pmod{p}$, which is equivalent to $ik \equiv jk \pmod{p-1}$. This is satisified if and only if $p-1 \mid (i-j)k$. If $\gcd(k, p-1) = 1$, then this gives that $p-1 \mid (i-j)$, which is a contradiction. If $\gcd(k, p-1) = d > 1$, then we will have $r^d \not\equiv 1 \pmod{p}$ and $1^k \equiv (r^d)^k \pmod{p}$. Thus, in this case we do not get a reduced residue system. ■

8. (a) Let r be a primitive root modulo p. Express $-r$ as a power of r.

The fact that r is a primitive root modulo p gives that $r^{p-1} \equiv 1 \pmod{p}$ and $r^j \not\equiv 1 \pmod{p}$ for all $0 < j < p-1$. Thus, we have $(r^{(p-1)/2})^2 \equiv 1 \pmod{p}$ with $r^{(p-1)/2} \not\equiv 1 \pmod{p}$. By our earlier work, we know the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x = \pm 1$. Thus, we must have $r^{(p-1)/2} \equiv -1 \pmod{p}$. Using this we can write $-r = (-1)r \equiv r^{(p-1)/2} r \equiv r^{(p+1)/2} \pmod{p}$.

(b) If $p \equiv 3 \pmod{4}$, prove that $-r$ is not a primitive root modulo p.

and

(c) If $p \equiv 1 \pmod{4}$, prove that $-r$ is a primitive root modulo p.

Proof: Recall that the order of an element a^k modulo n is precisely

$$\text{ord}_n(a)/\gcd(k, \text{ord}_n(a)).$$

Thus, the order of $-r$ is precisely $p - 1/\gcd((p+1)/2, p-1)$. Thus we need to determine $\gcd((p+1)/2, p-1)$. Let d be a divisor of $(p+1)/2$. There exists $e \in \mathbb{Z}$ so that $de = (p+1)/2$, i.e., $p = 2de - 1$. Thus, $p + 1 = 2de + 2$. Thus, the only possible common divisor is 2. If $p \equiv 3 \pmod{4}$, then we have that $2 \mid (p+1)/2$ and so $2 \mid \gcd((p+1)/2.p-1)$ and so the order of $-r$ is strictly less then $p-1$ and so it cannot be a primitive root. If $p \equiv 1 \pmod{4}$, then $2 \nmid (p+1)/2$ and so it must be that the greatest common divisor is 1. ■

9. Use Euler's criterion to prove that if $2^k + 1$ is a prime, then all quadratic nonresidues are primitive roots modulo $2^k + 1$.

Proof: Let $p = 2^k + 1$ be a prime and a a quadratic nonresidue. We know that $\text{ord}_p(a) \mid \phi(p) = p - 1 = 2^k$. If a is a quadratic nonresidue, then Euler's criterion says that $a^{(p-1)/2} \equiv -1 \pmod{p}$. However, in this case $(p-1)/2 = 2^{k-1}$. Thus, if we had $\text{ord}_p(a) < p - 1$, we would have that $a^{(p-1)/2} \equiv 1 \pmod{p}$, a contradiction. Thus it must be that $\text{ord}_p(a) = p - 1$. Note here that we are using that $p - 1 = 2^k$ to conclude that if $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, then no power other then $p - 1$ could possibly work. ■

10. (a) Consider the polynomial $f(x) = x^{2^m n} + 1$ for $m \geq 1$, $n > 1$ with n odd. Prove that the polynomial is not irreducible. In other words, show that the polynomial factors into two polynomials each of degree greater then or equal to 1.

Proof: The polynomial factors as:

$$f(x) = (x^{2^m} + 1)(x^{(n-1)2^m} - x^{(n-2)2^m} + \cdots - x^{2^m} + 1).$$

Thus, as long as $n > 1$, this is a nontrivial factorization. ■

(b) Let $a \in \mathbb{Z}_{>1}$, $k \in \mathbb{Z}_{>0}$ and suppose $p = a^k + 1$ is a prime. Prove that $\mathrm{ord}_p(a)$ must be a power of 2.

Proof: The definition of p gives that $a^{2k} \equiv 1 (\bmod p)$, so we must have $\mathrm{ord}_p(a) \mid 2k$. Thus, we are reduced to showing that k must be a power of 2. If k is not a power of 2, then one writes $k = 2^m n$ with $n > 1$. Now apply part (a) with $x = a$ to contradict that p is prime. Just note that since $a \neq 1$, we have $a^{(n-1)2^m} - a^{(n-2)2^m} + \cdots - a^{2^m} + 1 > 1$ because $a^{(n-1)2^m} > a^{(n-2)2^m}$, etc so that $(a^{(n-1)2^m} - a^{(n-2)2^m} + \cdots - a^{2^m}) > 0$. Thus, a must have order a power of 2. ■