SPRING 2025 MATH 540: QUIZ 6

Name:

1. Given positive integers n, a with $\gcd(n, a) = 1$, define what it means for a to be a primitive root of 1 modulo n. (2 points)

Solution. If the order of a modulo n equals $\phi(n)$, then a is a primitive root of 1 modulo n. Equivalently, $\phi(n)$ is the least positive integer such that $a^{\phi(n)} \equiv 1 \bmod n$.

2. Solve the system of congruences (4 points)

$$x \equiv 1 \bmod 5$$
$$x \equiv 2 \bmod 7$$
$$x \equiv 3 \bmod 11$$

Solution. Set $N = 3 \cdot 7 \cdot 11 = 385$, $N_1 = \frac{385}{5} = 77, N_2 = \frac{385}{7} = 55, N_3 = \frac{385}{11} = 35$. The inverse of 77 mod 5 is the inverse of 2 mod 5 equals 3. The inverse of 55 mod 7 is the inverse of 6 mod 7 equals 6. The inverse of 35 mod 11 is the inverse of 2 mod 11 euqals 6. For the solution we take

$$x = 1 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 3 \cdot 35 \cdot 6 = 1521,$$

which is congruent to 366 mod 385, which is the proper way to write the solution.

3. Prove that there is no primitive root of one modulo 2^n, for all $n \geq 1$. Hint: First prove by induction on n that if $n \geq 3$ and $a \in \mathbb{Z}$, odd, then $a^{2^{n-2}} \equiv 1 \bmod 2^n$. Then explain why this shows there is no primitive root of one modulo n. (4 points)

Solution. We first prove by induction in $n \geq 3$ that if a is odd, then $a^{2^{n-2}} \equiv 1 \bmod 2^n$. For this, if $n = 3$, we clearly have that $1^2, 3^2, 5^2, 7^2$ are congruent to 1 modulo 8. Now suppose the statement is true for $n - 1$. Then for any odd a we have $a^{2^{n-3}} = 1 + t \cdot 2^{n-1}$, for some $t \in \mathbb{Z}$. Squaring both sides, we get $a^{2^{n-2}} = 1 + t \cdot 2 \cdot 2^{n-1} + t^2 \cdot 2^{2n-2} = 1 + h \cdot 2^n$, for some $h \in \mathbb{Z}$, since $2^{2n-2} > 2^n$. Thus, $a^{2^{n-2}} \equiv 1 \bmod 2^n$. Thus the order of any odd a modulo 2^n is less than or equal to 2^{n-2} which is strictly less than $2^{n-1} = \phi(2^n)$. Therefore, there are no primitive roots of 1 modulo 2^n.