MATH 311/521, FALL 2025 MIDTERM

OCTOBER 8, 2025

Each problem is worth 10 points.

Problem 1. Give the proof of Wilson's theorem, for a prime p, $(p-1)! \equiv -1 \bmod p$.

Solution. The theorem is trivial if $p = 2$, so assume p is odd. Let g be a primitive root mod p. Then the reduced residues mod p are $g, g^2, ..., g^{p-1}$ in some order, so their product is $g^{1+2+...+(p-1)} = g^{\frac{p(p-1)}{2}}$. Since p is odd, $p | \frac{p(p-1)}{2}$. By Fermat's little theorem $g^p \equiv g \bmod p$, so $(p-1)! \equiv g^{\frac{p-1}{2}} \bmod p$. Thus $(p-1)!^2 \equiv g^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem, so $g^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. It must be -1 since $g, g^2, ..., g^{p-1} \bmod p$ are all distinct, and $g^{p-1} \equiv 1 \bmod p$.

Alternatively, for each reduced residue $x \bmod p$ let $x\overline{x} \equiv 1 \bmod p$. If $x = \overline{x}$ then $x^2 \equiv 1 \bmod p$ so $x \equiv \pm 1 \bmod p$. Otherwise x and $\overline{x}$ may be paired in the product, which leaves a product of $1 \cdot (-1) \equiv -1 \bmod p$.

Problem 2. State the principle of inclusion and exclusion. Using this or otherwise prove a formula for the number of reduced residues to a modulus m with prime factorization $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $\alpha_i \geq 1$.

Solution. Given a finite set X and subsets $S_1, S_2, ..., S_k$, the principle of inclusion-exclusion states

$$\left| X \setminus \bigcup_{i=1}^{k} S_i \right| = |X| - \sum_i |S_i| + \sum_{i_1 < i_2} |S_{i_1} \cap S_{i_2}| + \cdots + (-1)^k |S_1 \cap ... \cap S_k|.$$

Let X be the set of residues modulo m, and for each p_i let S_{p_i} be those residues divisible by p_i. A residue is reduced if it is divisible by none of the p_i. Since $|S_{p_{i_1}} \cap ... \cap S_{p_{i_j}}| = \frac{m}{p_{i_1} \cdots p_{i_j}}$, the number of reduced residues is

$$m - \sum_i \frac{m}{p_i} + \sum_{i_1 < i_2} \frac{m}{p_{i_1} p_{i_2}} + ... + (-1)^k \frac{m}{p_1 ... p_k} = m \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right).$$

Problem 3.

a. State Fermat's little theorem.

b. Give the proof from lecture that the Legendre symbol to a prime p is given by $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Solution. a. Fermat's little theorem states that if $m > 1$ is a positive integer and $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \bmod m$, where $\phi(m)$ is the number of reduced residues modulo m.

b. We assume p is an odd prime. The claim is trivial if $a \equiv 0 \bmod p$, so we can assume $a \not\equiv 0 \bmod p$. The map $x \mapsto x^2$ is 2-to-1 on its image in the reduced residues since x and $-x$ have the same square. Thus if g is a primitive root $\bmod p$ then the even powers of g among $g, g^2, ..., g^{p-1}$ are quadratic residues and the odd powers are non-residues. We have $(g^k)^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \bmod p$ if k is odd, and $(g^k)^{\frac{p-1}{2}} \equiv g^{p-1} \equiv 1 \bmod p$ if k is even, which completes the proof.

Problem 4. Find a primitive root modulo $169 = 13^2$.

Solution. We'll check 2 is a primitive root. The powers of $2 \bmod 13$ are $2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$. As these are all of the reduced residues mod 13, 2 is a primitive root mod 13. We have $2^{12} = 4096 \equiv 40 \bmod 169$. Since the order of 2 mod 169 is 12 or 156, the order must be 156, and it is again a primitive root.