Math 342 Tutorial

July 9, 2025

Question 1. Show that if $n = p_1^{2e_1+1} \cdots p_k^{2e_k+1} q_1^{2f_1} \cdots q_m^{2f_m}$, and if r is an odd prime not dividing n, then

$$\left(\frac{n}{r}\right) = \left(\frac{p_1}{r}\right) \cdots \left(\frac{p_k}{r}\right).$$

Question 2. Show that if p is odd prime that is 3 (mod 4), then $[(p-1)/2]! \equiv (-1)^t \pmod{p}$ where t is the number of nonquadratic residues in the range 0 to $\lfloor p/2 \rfloor$ inclusive.

Question 3. Let p be an odd prime. Prove the following identities. **(a)** $\sum_{r=1}^{p-1} r(r \mid p) = 0$ if $p \equiv 1 \pmod{4}$. **(b)** $\sum_{\substack{r=1 \\ (r|p)=1}}^{p-1} r = \frac{p(p-1)}{4}$ if $p \equiv 1 \pmod{4}$. **(c)** $\sum_{r=1}^{p-1} r^2(r \mid p) = p \sum_{r=1}^{p-1} r(r \mid p)$ if $p \equiv 3 \pmod{p}$. **(d)** $\sum_{r=1}^{p-1} r^3(r \mid p) = \frac{3}{2} p \sum_{r=1}^{p-1} r^2(r \mid p)$ if $p \equiv 1 \pmod{4}$. **(e)** $\sum_{r=1}^{p-1} r^4(r \mid p) = 2p \sum_{r=1}^{p-1} r^3(r \mid p) - p^2 \sum_{r=1}^{p-1} r^2(r \mid p)$ if $p \equiv 1 \pmod{4}$.

Question 4. Show that if a is a quadratic residue of the prime p, then the solutions of $x^2 \equiv a \pmod{p}$ are **(a)** $x \equiv \pm a^{n+1} \pmod{p}$ if $p = 4n+3$, or **(b)** $x \equiv \pm a^{n+1}$ or $\pm\, 2^{2n+1} a^{n+1} \pmod{p}$ if $p = 8n+5$.

Question 5. Show there are infinitely many primes of the following forms **(a)** $8k+3$, **(b)** $8k+5$, and **(c)** $8k+7$. [Hint: For each part, assume there are only finitely many primes $p_1, p_2, \ldots, p_k$ of the required form. For (a), consider $(p_1 \cdots p_k)^2 + 2$; for (b), consider $(p_1 \cdots p_k)^2 + 4$; for (c), consider $(4p_1 \cdots p_k)^2 - 2$. Use what you know about $(-1 \mid p)$ and $(2 \mid p)$.]

Question 6. Show the following. **(a)** If $p = 4k+1$ is a prime, then there is an integer x such that $mp = 1 + x^2$ where $0 < m < p$. **(b)** If p is an odd prime, then there are integers x and y such that $1 + x^2 + y^2 = mp$ where again $0 < m < p$.

Question 7. Determine those primes for which 7 is a quadratic residue.

Let a and n be positive integers, and let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the prime power factorization of n. The Jocabi symbol is defined as $(a \mid n) = (a \mid p_1)^{e_1} \cdots (a \mid p_k)^{e_k}$.

Question 8. Prove the following properties of the Jacobi symbol. **(a)** If $a \equiv b \pmod{n}$, then $(a \mid n) = (b \mid n)$; **(b)** $(ab \mid n) = (a \mid n)(b \mid n)$; **(c)** $(-1 \mid n) = (-1)^{(n-1)/2}$; **(d)** $(2 \mid n) = (-1)^{(n^2-1)/8}$.

Question 9. Prove quadratic reciprocity holds for the Jacobi symbol, i.e., $(n|midm)(m \mid n) = (-1)^{(m-1)(n-1)/4}$.