ASSIGNMENT 3

MMATH FIRST YEAR, 2025

Problems

1. Solve the congruence $x^3 \equiv 3(\text{mod } 25)$.
2. Solve the congruence $x^3 + x^2 - 5 \equiv 0(\text{mod } 343)$.
3. For which primes p do we have $\left(\frac{11}{p}\right) = \left(\frac{13}{p}\right)$?
4. Show that

$$\sum_{x(\text{mod } p)} \left(\frac{ax+b}{b}\right) = 0$$

whenever $p > 2$ is a prime and a, b are integers, $(a, p) = 1$.

5. If p is a prime and $p \equiv 1(\text{mod } 4)$, then show that

$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = 0 \quad \text{and} \quad \sum_{1 \le r \le p, \left(\frac{r}{p}\right)=1} r = \frac{p(p-1)}{4}.$$

6. Is $21^{36} + 36^{21}$ square of an integer? Justify.
7. Show that the congruence $ax^2 + bx + c \equiv 0(\text{mod } p)$, where p is an odd prime and $(p, a) = 1$, has a solution if and only if $\left(\frac{b^2-4ac}{p}\right)$=1.
8. Suppose n is a quadratic nonresidue of p. Then show that

$$\sum_{d|n} d^{\frac{p-1}{2}} \equiv 0(\text{mod } p).$$

9. Show that there are infinitely many primes of the form $3k + 2$.
10. Let $h(n)$ denote the number of distinct solutions modulo n to the congruence $x^2 + 1 \equiv 0(\text{mod } n)$. Evaluate $h(39)$ and $h(65)$.
11. Suppose a is a positive integer and $p \nmid a$. If $p \equiv \pm 1(\text{mod } 4a)$, then show that a is a quadratic residue of p.
12. Suppose $p = 2^{2^n} + 1$ is a prime. Show that every quadratic nonresidue modulo p is a generator for the cyclic group of invertible residue classes modulo p, i.e., $U(p)$.
13. Show that the representation of a prime as a sum of two squares, if any, must be unique (up to signs and ordering).
14. Prove the supplementary law to the Quadratic Reciprocity Law of Gauss.
15. Let $p > 2$ be a prime. Given an integer $a, (a, p) = 1$, the map $x \to ax(\text{mod } p)$ defines a permutation of the elements $\{1, 2, \cdots, p-1\}$. Show that the sign of the permutation is $\left(\frac{a}{p}\right)$.
16. Following the proof of Gauss lemma, show that

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

17. Following Euclid's proof of infnititude of primes and properties of the Legendre symbol, show that
(a) There are infinitely many primes $p \equiv 1 (\text{mod } 4)$ (Hint: Suppose $p_1, p_2, cdots, p_k$ are all such primes. Then consider a prime factor of $N := (2p_1p_2 \cdots p_k)^2 + 1$.)
(b) There are infinitely many primes $p \equiv 7 (\text{mod } 8)$ (Hint: similar idea but different N).
18. Show that $y^2 = x^3 + 7$ has no integer solution.
19. Show that the smallest positive integer that is a quadratic non-residue modulo a prime p is smaller than $1 + \sqrt{p}$.