

Department of Mathematics

MTL 145: Number Theory

PROBLEMS ON QUADRATIC RESIDUES

These problems are taken from *An Introduction to the Theory of Numbers* by NIVEN, ZUCKERMAN & MONTGOMERY with minor changes.

1. Let p be an odd prime, and let g be a primitive root modulo p . Prove that the quadratic residues are congruent to $g^2, g^4, g^6, \dots, g^{p-1}$ modulo p , and that the quadratic nonresidues are congruent to $g, g^3, g^5, \dots, g^{p-2}$ modulo p .
2. Let $m > 2$. Prove that if r is a quadratic residue modulo m , then $r^{\phi(m)/2} \equiv 1 \pmod{m}$.
3. Let p be a prime, $p > 3$. Prove that the sum of all quadratic residues modulo p is divisible by p .
4. Let $m > 1$. Show that if a is a quadratic residue modulo m and $ab \equiv 1 \pmod{m}$, then b is also a quadratic residue modulo m . Deduce that, if p is an odd prime, then the product of all quadratic residues modulo p is congruent to $+1$ or -1 according as $p \equiv 3 \pmod{4}$ or $p \equiv 1 \pmod{4}$.
5. Let $p = 4k + 3$ is a prime, and m is the number of quadratic residues less than $p/2$, then

$$1 \cdot 3 \cdot 5 \cdots (p-2) \equiv (-1)^{m+k+1} \pmod{p}, \quad 2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{m+k} \pmod{p}.$$

6. For all primes p , prove that $x^8 \equiv 16 \pmod{p}$ is solvable.
7. Let p be an odd prime. Prove that if there is an integer x such that

- $p \mid (x^2 + 1)$, then $p \equiv 1 \pmod{4}$.
- $p \mid (x^2 - 2)$, then $p \equiv \pm 1 \pmod{8}$.
- $p \mid (x^2 + 2)$, then $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$.
- $p \mid (x^4 + 1)$, then $p \equiv 1 \pmod{8}$.

Show that there are infinitely many primes of each of the forms $8k + 1$, $8k + 3$, $8k + 5$, $8k + 7$.

8. Show that if p and $2p + 1$ are primes and $0 < m < \sqrt{2p + 2}$, then m is a primitive root modulo p if and only if it is a quadratic nonresidue modulo p .
9. Show that if p is an odd prime, $\gcd(a, p) = 1$ and $\alpha \in \mathbb{N}$, then $x^2 \equiv a \pmod{p^\alpha}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions modulo p^α .
10. Which of the following congruences are solvable:

$$x^2 \equiv 5 \pmod{227}, \quad x^2 \equiv -7 \pmod{1009}.$$

11. Let p be an odd prime. Prove that $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$.
12. Let $q = 4k + 3$ be a prime. Prove that $x^2 \equiv -\frac{q+1}{4} \pmod{q}$ is not solvable.
13. Find all primes q such that $\left(\frac{5}{q}\right) = -1$.
14. Prove that there are infinitely many primes of the form $3k + 1$ and $3k - 1$.

15. Let $q = 4^n + 1$, $n \in \mathbb{N}$. Prove that q is a prime if and only if $3^{(q-1)/2} \equiv -1 \pmod{q}$.
16. Prove that if $19a^2 \equiv b^2 \pmod{7}$, then $19a^2 \equiv b^2 \pmod{7^2}$.
17. Show that $\frac{x^2-2}{2y^2+3}$ is never an integer when x and y are integers.
18. Show that if $3 \nmid x$, then $4x^2 + 3$ has at least one prime factor of the form $12k + 7$. Deduce that there are infinitely many primes of the form $12k + 7$.
19. Let p be an odd prime, and let $a, b \in \mathbb{Z}$ such that $p \nmid ab$. Show that the number of solutions (x, y) of the congruence $ax^2 + by^2 \equiv 1 \pmod{p}$ is $p - \left(\frac{-ab}{p}\right)$.
20. Determine all $n \in \mathbb{N}$ such that there exist integers x and y coprime to n with $n \mid (x^2 + y^2)$.
21. Let $p = 4k + 1$ be a prime, and let $p = a^2 + b^2$, with a odd and positive. Show that $\left(\frac{a}{p}\right) = 1$.
22. Let p be a prime, $p > 5$. Show that $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = 1$ for *at least one* $n \in \{1, 2, 3, \dots, 9\}$.
23. Let p be an odd prime, and $a, b \in \mathbb{Z}$ such that $p \nmid a$. Prove that $\sum_{n=1}^p \left(\frac{an+b}{p}\right) = 0$.
24. Let p be an odd prime. Define

$$s(a, p) = \sum_{n=1}^p \left(\frac{n(n+a)}{p}\right).$$

- (a) Show that $s(0, p) = p - 1$.
 - (b) Show that $\sum_{a=1}^p s(a, p) = 0$.
 - (c) If $p \nmid a$, prove that $s(a, p) = s(1, p)$. Deduce that $s(a, p) = -1$ if $p \nmid a$.
25. Let p be an odd prime, $a \in \mathbb{Z}$ such that $p \nmid a$. Prove that

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