MTH215 $\star\star$ 2019-20 $\star\star$ ASSIGNMENT – 3

1. Let $a \geq 2$ be an integer. Show that $n \mid \varphi(a^n - 1)$ for all integers $n \geq 2$.
2. Let a has order 3 modulo prime p. Show that order of $a+1$ modulo p is 6.
3. Let n be a positive integer. Show that
   (a) Odd prime divisors of n^2+1 are of form $4k+1$.
   (b) Odd prime divisors of n^4+1 are of form $8k+1$.
   (c) A prime divisors of n^2+n+1 is either 3 or of the form $6k+1$.
4. Show that there are infinitely many primes each of the form $4k+1$, $6k+1$ and $8k+1$.
5. Find all primitive roots of 43. Find all positive integers $n < 43$ such that order of n is 6 modulo 43.
6. Let a and b be primitive roots of odd prime p. Show that $a^{(p-1)/2} \equiv -1 (\bmod\ p)$ and that ab is not a primitive root modulo p.
7. Let a be a primitive root of prime p. Show that $(p-1)! \equiv a^{p(p-1)/2} (\bmod\ p)$. Hence establish that $(p-1)! \equiv -1 (\bmod\ p)$.
8. Let p be an odd prime and $n \in \mathbb{N}$. Show that $\sum_{i=1}^{p-1} i^n \equiv 0$ or 1 according as $(p-1) \mid n$ or $(p-1) \nmid n$.
9. Find all primitive roots of 25.
10. Let a be a primitive root of p^n where p is prime and $n \geq 2$. Show that a is also a primitive root of p^{n-1}.
11. Let a be a primitive root of p^2. Find all b such that $b^{p-1} = 1 (\bmod\ p^2)$.
12. Prove that 3 is primitive root for 17^k and 2×17^k for all $k \in \mathbb{N}$.
13. Solve
    (a) $x^2 + 7x + 10 \equiv 0 (\mod 11)$
    (b) $3x^2 + 9x + 7 \equiv 0 (\mod 13)$
    (c) $5x^2 + 6x + 1 \equiv 0 (\mod 23)$
14. Find all quadratic residues of prime 23.
15. Let a be a quadratic residue of p, where p is an odd prime. Show that
    (a) a is not a primitive root of p,
    (b) $p - a$ is a quadratic residue iff $p \equiv 1 (\bmod\ 4)$,
    (c) if $p \equiv 3 (\bmod\ 4)$ then then $x = \pm a^{(p+1)/4}$ are the solutions of $x^2 \equiv a (\bmod\ 4)$.
16. Let a be a primitive root of p. Find all quadratic residues of p in terms of a.
17. Let $a, b \in \mathbb{Z}$ such that $\gcd(ab, p) = 1$ Show that one of the a, b, ab is a quadratic residue modulo p.
18. Let $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$. Let $b \in \mathbb{Z}$ such that $ab \equiv 1 (\bmod\ p)$. Show that $(a/p) = (b/p)$.

19. Show that $\sum_{i=1}^{p-2} \left(\frac{i(i+1)}{p}\right) = -1$. Further show that there exist $a, b \in \{1, 2, \ldots, p-2\}$ such that $(a/p) = 1 = ((a+1)/p)$ and $(b/p) = -1 = ((b+1)/p)$.

20. If p and $q = 2p+1$ are both primes then show that -4 is a primitive root of q.

21. If $p \equiv 1 (\text{mod } 4)$ then show that -4 and $(p-1)/4$ are quadratic residues of p.

22. Let p be of type $8k+7$. Show that $p \mid 2^{(p-1)/2} - 1$.

23. Let a be a primitive root for p. Show that the product of all quadratic residues is congruent to $a^{(p^2-1)/4}$ and that the product of quadratic nonresidues is congruent to $a^{(p-1)^2/4}$ modulo p.

24. Show that the product of all quadratic residues is congruent to -1 or 1 modulo p according as $p \equiv (1 \bmod 4)$ or $p \equiv (3 \bmod 4)$.

25. Let $p > 3$. Show that p divides sum of its quadratic residues.

26. Let $p > 5$. Show that p divides sum of squares of its quadratic nonresidues.

27. Let $p = 4k+1$. Show that sum of its quadratic residues in $\{1, 2, \ldots, p-1\}$ is $p(p-1)/4$.

28. Let $p = 8k+1$ and let a be primitive root of p. Show that the solutions of $x^2 \equiv 2 (\text{mod } p)$ are $\pm(a^{7(p-1)/8} + a^{(p-1)/8})$.

29. Show that $(-1/p) = (-1)^{(p-1)/2}$ and $(-2/p) = (-1)^{\frac{(p-1)}{2} + \frac{p^2-1}{8}}$.

30. Show that $(-3/p)$ is 1 or -1 according as $p \equiv 1 (\text{mod } 6)$ or $p \equiv 5 (\text{mod } 6)$.

31. Let $n \in \mathbb{N}$. Find the forms of the prime which divide n^2+1, n^2+2 and n^2+3.

32. Find a prime which is expressible in the form of $x_1^2 + y_1^2$, $x_2^2 + 2y_2^2$ and $x_3^2 + 3y_3^2$, where $x_i, y_i \in \mathbb{Z}$.

33. Let p and q be odd primes such that $q = p + 4n$. Show that $(n/p) = (q/p)$.

34. Let p be an odd prime.

    (a) If $p \neq 5$, then $(5/p) = 1$ iff $p \equiv 1, 9, 11$ or 19 (mod 20).
    (b) If $p \neq 3$, then $(6/p) = 1$ iff $p \equiv 1, 5, 19$ or 23 (mod 24).
    (c) If $p \neq 7$, then $(7/p) = 1$ iff $p \equiv 1, 3, 9, 19, 25$ or 27 (mod 28).