

MATH 567 NUMBER THEORY I, SOLUTIONS 7

Throughout this problem sheet, p denotes an odd prime number.

1. Let g be a primitive root modulo p . Prove that the quadratic residues are precisely the residue classes g^{2k} with $0 \leq k < \frac{1}{2}(p-1)$. Show that the sum of the quadratic residues modulo p is the 0 residue. (Correction. False for $p=3$!) There are $\frac{p-1}{2}$ QR. The $\frac{p-1}{2}$ residues g^{2k} with $0 \leq k < \frac{p-1}{2}$ are QR and distinct modulo p . Now assume $p > 3$. Then $(g^2 - 1) \sum_{n \text{ QR}} n \equiv (g^2 - 1) \sum_{k=0}^{\frac{p-1}{2}} g^{2k} = g^{p-1} - 1 \equiv 0 \pmod{p}$ but $g^2 \not\equiv 1$ when $p > 3$.

2. Show that if $p \equiv \pm 1 \pmod{8}$, then 2 is a quadratic residue and otherwise 2 is a quadratic non-residue. By considering the polynomial $x^2 - 2$, or otherwise, show that there are infinitely many primes in the residue class 7 (mod 8). $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}} = 1$ iff $p \equiv \pm 1 \pmod{8}$. Suppose that p_1, \dots, p_k are all the primes $\equiv 7 \pmod{8}$. Let $x = p_1 \dots p_k$. Then $x \geq 7$, $x^2 - 2$ is odd and > 1 . Moreover all the prime factors of $x^2 - 2$ will be $\equiv \pm 1 \pmod{8}$ and $x^2 - 2 \equiv -1 \pmod{8}$. Thus there are an odd number of primes $p \equiv -1 \pmod{8}$ with $p|x^2 - 2$. But then for any such p , $p|2$.

3. Of which primes is -2 a quadratic residue? $\left(\frac{-2}{p}\right)_L = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = 1$ iff $p \equiv 1$ or $3 \pmod{8}$.

4. Decide whether $x^2 \equiv 150 \pmod{1009}$ is soluble or not. 1009 is prime. (Obviously not divisible by 2, 3, 5, 11 and checked by trial division for 7, 13, 17, 19, 23, 29 and 31.) Moreover $\left(\frac{150}{1009}\right)_L = \left(\frac{2}{1009}\right)_L \left(\frac{3}{1009}\right)_L = \left(\frac{1009}{3}\right)_L = \left(\frac{1}{3}\right)_L = 1$.

5. Find all primes p such that $x^2 \equiv 13 \pmod{p}$ has a solution. $\left(\frac{13}{p}\right)_L = \left(\frac{p}{13}\right)_L$. The QR modulo 13 are 1, 3, 4, 9, 10, 12. Thus the congruence is soluble when $p = 2, 13$ or lies in one of these residue classes modulo 13.

6. Prove that every quadratic non-residue modulo p is a primitive root modulo p if and only if $p = 2^{2^n} + 1$ for some non-negative integer n . We assume $p > 2$. The number of primitive roots is $\phi(p-1)$. The number of QNR is $\frac{p-1}{2}$. No QR is a primitive root. Thus every QNR is a primitive root iff $\phi(p-1) = \frac{p-1}{2}$. Write $p-1 = 2^a \prod_{j=1}^s p_j^{b_j}$ where $a \geq 1$ and the product is taken to be empty when $s = 0$. Then $\phi(p-1) = (p-1) \frac{1}{2} \prod_{j=1}^s (1 - 1/p_j)$. Now $\phi(p-1) < \frac{p-1}{2}$ unless $s = 0$. Hence $p-1 = 2^a$ with $a \geq 1$. If a has an odd prime factor, say q , then $a = bq$, $1 < 2^b + 1 < 2^{bq} + 1 = p$ and $p \equiv (-1)^q + 1 \equiv 0 \pmod{2^b + 1}$ contradicting the primality of p . Hence a is a power of 2.

7. Show that $(x^2 - 2)/(2y^2 + 3)$ is never an integer when x and y are integers. $2y^2 + 3 \equiv 3$ or $5 \pmod{8}$. Hence $2y^2 + 3$ cannot have 2 as a prime factor and not all of its prime factors can be $\equiv \pm 1 \pmod{8}$. Hence $2y^2 + 3$ has a prime factor $p \equiv \pm 3 \pmod{8}$. But $x^2 - 2$ can have no such prime factor.