

Number Theory: Problem sheet 5

1. Find all quadratic residues modulo 29.
2. Evaluate $\left(\frac{5}{p}\right)$ using Gauss's Lemma, in the same way that $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$ were done in lectures.
3. Evaluate (showing your working) the following Legendre symbols:
(i) $\left(\frac{29}{43}\right)$; (ii) $\left(\frac{84}{89}\right)$; (iii) $\left(\frac{71}{197}\right)$; (iv) $\left(\frac{341}{1013}\right)$; (v) $\left(\frac{1729}{2011}\right)$.
4. Prove that the congruence

$$x^8 \equiv 16 \pmod{p}$$

is soluble for **all** primes p .

[Hint: what are the solutions of $z^8 = 16$ in the complex numbers?]

5. Prove that the **Jacobi** symbol

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

Also prove that the Jacobi symbol

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

6. Prove that if N is an even integer, all prime factors p of $N^2 + 1$ satisfy $p \equiv 1 \pmod{4}$. By considering $N = n!$, or otherwise, prove that there are infinitely many primes congruent to 1 modulo 4.
Similarly, by considering $3(n!)^2 + 1$ or otherwise, prove that there are infinitely many primes congruent to 1 modulo 3.
7. In each case, the prime p is congruent to 3 modulo 4. By computing $a^{(p+1)/4}$ (using **MAPLE** if necessary) solve the congruence $x^2 \equiv a \pmod{p}$.
(i) $p = 83$, $a = 11$; (ii) $p = 199$, $a = -41$; (iii) $p = 2011$, $a = 5$.
8. Suppose that a has order 8 modulo the prime p . Prove that $a^4 \equiv -1 \pmod{p}$ and deduce that $t = a + a^3$ satisfies $t^2 \equiv -2 \pmod{p}$. Also find an similar expression for a solution of $u^2 \equiv 2 \pmod{p}$.

9. For each of the following numbers n , determine whether n can be written as the sum of two squares of integers, and if so write n in that form.
 (i) $n = 122$; (ii) $n = 490$, (iii) $n = 515$, (iv) $n = 2700$, (v) $n = 40885$.
10. Find two essentially different representations of $n = 3977 = 41 \times 97$ as a sum of two squares, and four essentially different representations of $n = 3445 = 5 \times 13 \times 53$ as a sum of two squares. (Representations $n = a^2 + b^2 = c^2 + d^2$ are essentially different if $(a, b) \neq (\pm c, \pm d)$ and $(a, b) \neq (\pm d, \pm c)$).
11. Let (x, y, z) be a Pythagorean triple (that is, $x^2 + y^2 = z^2$). Show that $3 \mid xy$ and that $5 \mid xyz$. [Hint: reduce to the case of primitive Pythagorean triples, and use the parameterization.]
12. Let p be an odd prime. Show that if $a \equiv b \pmod{p}$ then $a^p \equiv b^p \pmod{p^2}$. [Hint: write $a = b + pc$ and use the binomial theorem.]

Hence show that the Diophantine equation

$$x^5 + y^5 = z^5$$

has no integer solutions with $5 \nmid xyz$.

13. (Challenge problem) Let p be an odd prime number. Define

$$\tau_p = \sum_{a=0}^{p-1} \left(\frac{a}{p} \right) \exp(2\pi i a/p).$$

Prove that $\tau_p^2 = \left(\frac{-1}{p} \right) p$. (Much harder!) Determine the value of τ_p .