Michaelmas Term 2012 J. M. E. Hyland

Number Theory: Example Sheet 2

The first 12 questions are intended for the supervisions. Further questions are designed to encourage mathematical investigation without any examination emphasis.

1. For which odd primes p is 15 a quadratic residue modulo p?

2. Evaluate the following Jacobi symbols (in fact, they are Legendre symbols):

$$\left(\frac{20964}{1987}\right) \qquad \left(\frac{741}{9283}\right) \qquad \left(\frac{5}{160465489}\right) \qquad \left(\frac{3083}{3911}\right)$$

   (Did it help to know they were Legendre symbols?)

3. Prove that 3 is a quadratic non-residue modulo any Mersenne prime $2^n - 1$, with $n > 2$.

4. Let p be a prime with $p \equiv 1 (\operatorname{mod} 4)$. Prove that the sum of the quadratic residues in the interval $[1, p-1]$ is equal to the sum of the quadratic non-residues in this interval. Does this hold if $p \equiv 3 (\operatorname{mod} 4)$?

5. Let p be a prime with $p \equiv 3 (\operatorname{mod} 4)$. Suppose that m of the quadratic non-residues of p are in the range $1, \cdots, P = \frac{p-1}{2}$. Show that $P! \equiv (-1)^m (\operatorname{mod} p)$.

6. Let a be a positive integer that is not a square. Prove that there are infinitely many odd primes p such that a is not a quadratic residue modulo p.

7. Are the forms $3x^2 + 2xy + 23y^2$ and $2x^2 + 4xy + 5y^2$ equivalent under the action of $SL_2(\mathbb{Z})$? Are the forms $15x^2 - 15xy + 4y^2$ and $3x^2 + 9xy + 8y^2$ equivalent?

8. Find the smallest positive integer that can be represented by the form $4x^2 + 17xy + 20y^2$. What is the next largest? And the next?

9. Make a list of all reduced positive definite quadratic forms of discriminant $-d$, where $d = 8, 11, 12, 16, 19, 23, 163$.

10. Establish necessary and sufficient conditions for a prime p to be represented by the form $x^2 + xy + y^2$. Do the same for $x^2 + 3y^2$.

11. Is there a positive definite binary quadratic form that represents 2 and the primes congruent to 1 or 3 modulo 8, but no other primes? What about 1 and 5 modulo 8 only? What about 1 and 7 modulo 8 only?

12. Find a necessary and sufficient condition for a positive integer n to be properly represented by at least one of the two forms $x^2 + xy + 4y^2$ and $2x^2 + xy + 2y^2$.

    Suppose that the positive integer n is coprime to 15, and properly represented by at least one of the forms. Show that congruence conditions modulo 15 allow one to decide which form represents n.

That ends the official part of the sheet. As before the remaining questions are intended to encourage investigation so don't bother your supervisor with them.

(A) Show that if a is a quadratic residue of an odd prime p, then it is a quadratic residue for all p^k with $k \geqslant 1$. Can you say anything about quadratic residues modulo an arbitrary positive integer n?

(B) One classical topic which I do not cover in lectures is the question of the number of representations by a given form.
Suppose that n is odd. Can you determine how many representations there are of n by the form $x^2 + y^2$ in terms of its prime factorization? What about the number of representations of $2n$? So what about representations of $2^k n$?
Investigate the number of representation by the form $x^2 + xy + y^2$.

(C) It is a famous elementary question to consider which numbers can be represented by the indefinite form $x^2 - y^2$. So can you do the same for the indefinite form $x^2 - 2y^2$?

(D) In lectures I mentioned some observations of Fermat and Euler.
(Fermat) If primes p and q are each congruent to one of 3 or 7 modulo 20 then there product is expressible by the form $x^2 + 5y^2$.
(Euler) If a prime p is congruent to 1 or 9 mod 20 then it is expressible by the form $x^2 + 5y^2$, while if it is congruent to 3 or 7 mod 20 then $2p$ is so expressible.
What can you say about these observations?

Email any comments, suggestions and queries to `m.hyland@dpmms.cam.ac.uk`.