Number Theory Example Sheet 5
Michaelmas 2004

Dr Alessio Corti

14th January, 2005

This sheet is made of old exam questions for revision purpuses. As in the exam, there are some short questions and some long questions. The short questions should be very straightforward and take about half the time of the long questions to complete.

Short questions

(1) State and prove the Chinese remainder Theorem. Show that each of the congruences:

$$x^2 \equiv 7 \mod 2, \quad x^3 \equiv 7 \mod 5, \quad x^4 \equiv 7 \mod 9,$$

is soluble, and find an integer x that satisfies the three equations simultaneously.

(2) Let $p > 0$ be a prime number. State and prove Euler's Theorem for the Legendre symbol $\left(\frac{a}{p}\right)$. Show that the number of quadratic residues $\mod p$ is equal to the number of quadratic non-residues $\mod p$, and that this is equal to $(p-1)/2$.

(3) State the law of quadratic reciprocity. State also its analogue in terms of Jacobi symbols.

Evaluate the symbols $\left(\frac{33}{755}\right)$ and $\left(\frac{5}{33}\right)$. Is 33 a quadratic residue mod 755?

(4) Let $\pi(x)$ denote the number of primes $\leq x$, where x is a positive real number. State and prove Legendre's formula relating $\pi(x)$ to $\pi(\sqrt{x})$. Use this formula to compute $\pi(100) - \pi(10)$.

(5) Let $n > 1$ be an odd composite natural number. Explain what it means for n to be a *pseudoprime*, an *Euler pseudoprime*, and a *strong pseudoprime*, respectively, with respect to a base b. Compute the number of bases b satisfying $1 \leq b \leq n$ and $(b, n) = 1$ with respect to which $n = 13 \times 37$ is a pseudoprime.

(6) State a necessary and sufficient condition for some positive definite integral binary form $q(x, y) = ax^2 + bxy + cy^2$ with discriminant D to represent an odd prime number p. Use this condition to show that an odd prime p can be written as the sum of the squares of two integers if and only if $p \equiv 1 \bmod 4$.

(7) What is meant by a *primitive root modulo n?*. State a result indicating the values of n for which primitive roots exist. Show that, for a prime number $p \neq 3$, the congruence $x^3 \equiv 1 \pmod{p}$ has one solution if $p \equiv 2 \pmod{3}$ and three solutions if $p \equiv 1 \pmod{3}$.

Long questions

(1) An integer n is called a *Carmichael number* if n is odd, composite, and if $b^{n-1} \equiv 1 \pmod{n}$ for all integers b prime to n. Show that if p is a prime, and if p^2 divides n, then n is not a Carmichael number. Deduce that n is a Carmichael number if and only if $n = p_1 \cdots p_k$ with distinct primes p_i satisfying $p_i > 2$ and $(p_i - 1)|(n - 1)$ for all $i = 1, \ldots, k$.

(2) Let $q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form. Define the discriminant D, and state the condition on a, b and c for $q(x, y)$ to be *reduced*. Prove that if $q(x, y)$ is positive definite, it is equivalent to some reduced form, and that there is at most a finite number $h(D)$ of reduced forms with given discriminant D. Show that $h(-3) = h(-7) = 1$ and determine $h(-5)$.

(3) Explain what is meant by the continued fraction of a real number $\theta > 1$. Define the convergents of θ and write down the recurrence relation satisfied by their numerators and denominators. Prove that the continued fraction expansion of θ converges to θ.

Use the continued fraction method to find two solutions in positive integers x, y of the equation $x^2 - 15y^2 = 1$.

(4) Write a short essay describing the factor base method for factorising a large odd positive integer n. You should define the notion of a factor base and discuss the theoretical underpinnings of the method. You do not need to discuss the problem of how to choose a factor base.