Number Theory Example Sheet 2
Michaelmas 2003

Dr Alessio Corti

5th November, 2004

(Questions marked with a $*$ are optional.)

(1) (a) Prove that, for an odd prime p:

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 3 \mod 8, \quad \text{and} \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \mod 8 \end{cases}$$

(b) Prove that, for odd primes p, q,

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

if either $p \equiv q \mod 4a$ or $p \equiv -q \mod 4a$.

(2) Evaluate the Legendre symbol

$$\left(\frac{1801}{8191}\right)$$

(a) using the reciprocity law only for the Legendre symbol, and (b) without factoring any odd integers, instead using the reciprocity law for the Jacobi symbol.

(3) Use the Euclidean argument for the existence of infinitely many primes to show that $p_n < 2^{2^n}$ for all $n \geq 1$, where p_n is the n-th prime.

(4) For each integer $n \geq 1$, and each prime p, prove that the power of p dividing $n!$ is $\sum_{m=1}^{\infty} \lfloor \frac{n}{p^m} \rfloor$. Find the power of each prime $2, 3, 5, 7$ which exactly divides $100!$

(5) (a) If a and b are relatively prime positive integers, prove that every odd prime divisor of $a^2 + b^2$ must be $\equiv 1 \mod 4$.

(b) Use part (a) to show that there are infinitely many primes $\equiv 1 \mod 4$ (consider $2^2 + 5^2(13)^2 \cdots$).

(6) Deduce from the statement of the prime number theorem that

$$\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$$

where, as usual, p_n denotes the n-th prime.

(7∗) Define the function $\theta(x)$ as follows:

$$\theta(x) = \sum_{p\le x} \log p$$

(the sum is over primes). Prove that the prime number theorem is equivalent to the statement that

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$$

[Hint. The proof is similar to what we did in class with the function $\psi(x)$, only slightly easier. You should use the Abel summation formula in two different ways.]

(8) Make a list of all quadratic residues for the primes $p = 17$ and 37.

(9) If n is a positive integer such that $(n-1)! \equiv -1 \pmod{n}$, prove that n is prime.

(10) Define a *cubic residue* (mod p) to be an element a of $\mathbb{F}_p^\times$ such that the equation $x^3 \equiv a \pmod{p}$ is soluble.

(i) If p is a prime of the form $3m+1$, prove that $\mathbb{F}_p^\times$ contains exactly m cubic residues.

(ii) If p is a prime of the form $3m+2$, prove that every element of $\mathbb{F}_p^\times$ is a cubic residue.

(11) Are the forms $3x^2 + 2xy + 23y^2$ and $7x^2 + 6xy + 11y^2$ equivalent?

(12) Determine the set of prime numbers represented by one of the two forms $x^2 + xy + 4y^2$, $2x^2 + xy + 2y^2$.

(13∗) Find all reduced positive definite quadratic forms of discriminant Δ for the following values: $\Delta = -1, -3, -4, -12, -23, -35, -163$.

(14∗) If $ax^2+bxy+cy^2$ is a reduced form, show that the roots of the quadratic equation $az^2 + bz + c = 0$ satisfy $-1/2 \le \mathrm{Re}(z) \le 1/2$ and $|z| \ge 1$. Does the converse hold?

(15) Show that there are two inequivalent reduced forms of discriminant -20. Prove that the primes represented by $x^2 + 5y^2$ are 5 and those congruent to 1 or 9 mod 20.