MAT3434

UNIVERSITY OF EXETER

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

NUMBER THEORY: SUMMER 1998 EXAMINATION

1. (a) Show that if p is a prime and if $x^2 \equiv y^2 \pmod{p}$ then $x \equiv \pm y \pmod{p}$. Given that $x = 2515$ and $y = 6135$ satisfy $x^2 \equiv y^2 \equiv -1 \pmod{31313}$, deduce that 31313 is composite, and find a proper factorisation.

   (b) Find all solutions to each of the following congruences, or show that none exist:

   (i) $x^2 \equiv 1 \pmod{85}$;

   (ii) $x^2 \equiv -1 \pmod{55}$;

   (iii) $x^2 \equiv 5 \pmod{11^3}$;

   (iv) $x^3 - 3x \equiv 5 \pmod{7^2}$.

2. (a) State Fermat's Little Theorem, and use it to show that the number $m = 6601 = 7 \cdot 23 \cdot 41$ has the following property: if $\gcd(a, m) = 1$ then $a^{m-1} \equiv 1 \pmod{m}$.

   (b) Define Euler's totient function φ, and write down a formula for $\varphi(n)$ in terms of the prime factorisation of n. Hence find all solutions of $\varphi(n) = 18$ and $\varphi(n) = 20$.

   (c) State the law of quadratic reciprocity, including the assertions giving the values of the Legendre symbols $\left(\dfrac{-1}{p}\right)$ and $\left(\dfrac{2}{p}\right)$ for an odd prime p. Use it to evaluate the following Legendre symbols, showing your working and justifying each intermediate step:

   $$\text{(i)}\ \left(\frac{2}{37}\right); \qquad \text{(ii)}\ \left(\frac{15}{37}\right); \qquad \text{(iii)}\ \left(\frac{-21}{71}\right); \qquad \text{(iv)}\ \left(\frac{43}{103}\right).$$

3. (a) Let $m, n \in \mathbf{N}$ with $\gcd(m, n) = 1$. Show that the positive divisors d of mn are precisely the numbers of the form kl where k, l are any positive divisors of m, n respectively, and that each d can be represented in this form in only one way.

   (b) Let $\sigma(n)$ denote the sum of the positive divisors of n. Show that if $\gcd(m, n) = 1$ then $\sigma(mn) = \sigma(m)\sigma(n)$. Show also that if p is prime then $\sigma(p^e) = (p^{e+1} - 1)/(p - 1)$. Hence obtain a formula for $\sigma(n)$ in terms of the prime factorisation of n. Use your formula to evaluate $\sigma(30)$ and $\sigma(100)$.

   (c) A *perfect number* is a natural number n whose positive divisors (excludng n itself) add up to n. Thus for example 28 is a perfect number since $1+2+4+7+14 = 28$. Show that n is a perfect number if and only if $\sigma(n) = 2n$. Hence show that if $n = 2^{m-1}p$ where $p = 2^m - 1$ is a prime, then n is a perfect number.

(d) Suppose that n is an *even* perfect number. Then n may be written $n = 2^{m-1}k$ where k is odd and $m \geq 2$. Show that $\sigma(k) = 2^m a$ and $k = (2^m - 1)a$ for some odd number a. By considering $\sigma((2^m - 1)a)$, show that $a = 1$ and that $2^m - 1$ is prime. Deduce that every even perfect number has the form $n = 2^{m-1}p$ where $p = 2^m - 1$ is prime.

4. (a) Give an account of Pollard's rho method of factorising a given integer n. Your answer should contain a clear step-by-step description of the algorithm. (This may be expressed in pseudocode, or as a procedure in Maple or some other computer language, if you wish.) You should explain briefly why the algorithm works, what parameters may be varied, and under what circumstances it fails to find a proper factor of n.

Illustrate the algorithm by using it to obtain a proper factor of $n = 667$, starting with seed $x_0 = 2$ and iteration function $f(x) = x^2 + 1$.

(b) Describe the RSA public key cryptosystem, indicating what information is published, and what calculations must be performed by the sender and the recipient of a message. On what assumptions does the security of the system depend?

5. (a) Let $n \in \mathbf{N}$ and let a be an integer with $\gcd(a, n) = 1$. Define the *order* of a modulo n. What does it mean to say that a is a *primitive root* modulo n? Show that a is a primitive root modulo n if and only if $a^{\varphi(n)/q} \not\equiv 1 \pmod{n}$ for every prime q dividing $\varphi(n)$.

(b) Let p be an odd prime, and let g be a primitive root modulo p. Show that either g or $g + p$ is a primitive root modulo p^2, and deduce that this same number is a primitive root modulo p^r for all $r \geq 1$.

(c) Show that 2 is a primitive root modulo 37, but that 3 is not. How many of the integers g with $0 \leq g < 37$ are primitive roots modulo 37?

(d) Show that the congruence $x^4 \equiv -1 \pmod{37}$ has no solutions, and find all solutions of $x^4 \equiv -11 \pmod{37}$.

6. (a) Let p be an odd prime and let a be an integer not divisible by p. State Gauss' lemma concerning the Legendre symbol $\left(\frac{a}{p}\right)$. Use it to evaluate $\left(\frac{2}{p}\right)$ and $\left(\frac{-2}{p}\right)$ for all odd primes p.

(b) Show that an odd prime p can be written as the sum of two squares if and only if $p \equiv 1 \pmod{4}$. (You may assume without proof that the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.) Express 61 and 89 as sums of two squares, and hence find two inequivalent expressions for $5429 = 61 \cdot 89$ as the sum of two squares. (The expression $a^2 + b^2$ is to be counted as equivalent to $(\pm a)^2 + (\pm b)^2$ and to $(\pm b)^2 + (\pm a)^2$ with any combination of signs.)

(c) Determine a necessary and sufficient condition for a prime p to be expressible in the form $a^2 + 2b^2$.

Examiner: Dr. N.P. Byott