AC, 1st December 2008

M3P14 Elementary Number Theory—Problem Sheet 4.

This is assessed coursework. Please hand in solutions to the starred questions by **Monday 15th December.**

(1) (i) Prove that if n is an odd integer then $(n^2-1)/8$ is also an integer, and that this integer is even, odd, odd, even respectively in the cases $n \equiv 1, 3, 5, 7 \bmod 8$.
(ii) Prove that if a and b are odd integers, then $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{(ab)^2-1}{8} \bmod 2$.
(iii) Prove that if a_i are odd integers then $\sum_i \frac{(a_i)^2-1}{8} \equiv \frac{(\prod_i a_i)^2-1}{8} \bmod 2$.
(iv) Deduce that

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$$

(this is the Jacobi symbol; recall its formal definition...).

(2) Evaluate the following Jacobi symbols: $\left(\frac{5}{13}\right), \left(\frac{13}{13}\right), \left(\frac{456}{123}\right), \left(\frac{11}{10001}\right)$.

(3) For each n in $\{7, 14, 28, 10001\}$, decide whether or not 2 is a square mod n.

(4) (i) Say $a, b, c \in \mathbb{Z}$ and p is an odd prime with $p \nmid a$. Prove, by completing the square or otherwise, that the quadratic equation $aX^2 + bX + c \equiv 0 \bmod p$ has no roots mod p iff $\left(\frac{b^2-4ac}{p}\right) = -1$. How many roots does it have when $\left(\frac{b^2-4ac}{p}\right) = 0$, and how many does it have when $\left(\frac{b^2-4ac}{p}\right) = +1$?
(ii) Does the congruence

$$x^2 - 3x - 1 \equiv 0 \mod 31957$$

have any solutions?

(5) A prime number of the form $F_n = 2^{2^n} + 1$ is called a *Fermat prime*. For example $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ are prime. Let $p > 2$ be a prime. Consider the following property (F), which may or may not be true for p: the property is that for all $a \in \mathbb{Z}$,

$$\left(\frac{a}{p}\right) = -1 \iff a \text{ is a primitive root mod } p.$$

Prove that p is a Fermat prime iff p has property (F).

(6) Let $n > 1$ be odd. Which of the following can happen? Proofs or examples required!
(i) $\left(\frac{a}{n}\right) = 1$ and a is a square mod n.
(ii) $\left(\frac{a}{n}\right) \neq 1$ and a is a square mod n.
(iii) $\left(\frac{a}{n}\right) = 1$ and a is not a square mod n.
(iv) $\left(\frac{a}{n}\right) \neq 1$ and a is not a square mod n.

(7) The Euler's criterion states that if p is prime, then

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p$$

Use successive squaring to compute $11^{864} \mod 1729$ and use standard properties of the Jacobi symbol to compute $\left(\frac{11}{1729}\right)$. Do they agree? What can you conclude about the possible primality of 1729?

(8*) Prove that there are no integers x and y such that $y^2 = x^3 + 23$.

[*Hint.* Assume there is a solution; first prove that $x \equiv 1 \mod 4$ and then prove that there is a prime $p \equiv 3 \mod 4$ such that $y^2 + 4 \equiv 0 \mod p$ and deduce a contradiction.]

(9) Use Fermat descent starting with

$$557^2 + 55^2 = 26 \times 12049$$

to write the prime 12049 as a sum of two squares.

(10*) Make a list of all primes $p < 50$ that can be written in the form a^2+2b^2. Try to find a pattern and make a guess as to exactly which primes have this form.

Use the technique of Fermat descent to prove that your guess is correct. The only places that you are likely to get stuck is that at one stage you might find a prime p such that $2p = a^2 + 2b^2$ and you will want to deduce that p is of the form $c^2 + 2d^2$. This can be done though—if $2p = a^2 + 2b^2$ then a must be even so you can divide the entire equation by 2.

(11) For each of the following numbers m, either write m as a sum of two squares, or explain why it is not possible to do so:

$$4370, \quad 1885, \quad 1189, \quad 3185.$$

(12*) (i) Find $\mathrm{hcf}(8 + 38i, 9 + 59i)$ and $\mathrm{hcf}(-9 + 19i, -19 + 4i)$ in $\mathbb{Z}[i]$.
(ii) Find the decomposition of $23 - 11i$ into *normalised* Gaussian primes.

(13) (i) Make a list of residues of smallest norm in $\mathbb{Z}[i]/(2 + 3i)$. [*Hint: consider the square in the complex plane with vertices at the points* 3, $2i$, $-2 - i$, $1 - 3i$.]

(ii†) Show that $\mathbb{Z}[i]/(a+bi)$ has $N(a+bi) = a^2+b^2$ elements. [*Hint: consider integer points in the square with vertices at* 0,$a + bi$,$-b + ai$, $(a - b) + (b + a)i$.]

(14*) Make a list of all divisors of $n = 2925$; use this to calculate $D_1(n)$ and $D_3(n)$ (the number of divisors of n congruent to 1 and 3 mod 4); hence calculate in how many ways can n be written as sum of two squares; make a list of all integer solutions $(x, y) \in \mathbb{Z}$ of the equation:

$$x^2 + y^2 = 2925$$