Elliptic Curves
Example Sheet 5

We prove the **Four Squares Theorem**: every positive integer can be written as the sum of four integer squares.

(a) Let p be an odd prime. Show that there are integers a, b such that

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

(**Hint:** Count the elements in $\mathbb{F}_p$ of the form u^2 and those of the form $-1 - v^2$.)

(b) Let p be an odd prime, and let a, b be as above. Let

$$\Lambda = \{(x, y, z, w) \in \mathbb{Z}^4 \; : \; x \equiv az + bw \pmod{p}, \; y \equiv bz - aw \pmod{p}\}.$$

Show that Λ is a subgroup of $\mathbb{Z}^4$ of index p^2. Moreover, show that if $(x, y, z, w) \in \Lambda$ then

$$x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{p}.$$

(c) Let

$$C = \{(x, y, z, w) \in \mathbb{R}^4 \; : \; x^2 + y^2 + z^2 + w^2 < 2p\}.$$

Compute the volume of C.

(d) Use Minkowski's Theorem to show that every odd prime p can be written as

$$p = x^2 + y^2 + z^2 + w^2$$

for some x, y, z, $w \in \mathbb{Z}$.

(e) Use the identity

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) =$$

$$(ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+(az-bw+cx+dy)^2+(aw+bz-cy+dx)^2$$

to complete the proof of the Four Squares Theorem.

please turn over

Notes:

- The Four Squares Theorem was proved by Joseph Louis Lagrange in 1770, though the theorem appears–without proof–in the Arithmetica of Diophantus (probably written around 250AD). We have followed Davenport's proof of the Four Squares Theorem (1941).
- Another fascinating question is, in how many ways can we write a positive integer n as the sum of four squares? This was answered in 1834 by Carl Jacobi. He showed that this number is eight times the sum of the divisors of n if n is odd, and 24 times the sum of the odd divisors of n if n is even. Jacobi's theorem has remarkable proof using modular forms.
- Where does identity in (e) come from? You are surely familiar with the multiplicative property of norms of Gaussian integers. If $\alpha = a + bi \in \mathbb{Z}[i]$ then the norm of α is defined by $N(\alpha) = a^2 + b^2$, and you know $N(\alpha\beta) = N(\alpha)N(\beta)$. The identity in (e) is the corresponding identity for quaternion norms.