Number theory I: Problem sheet 7

1. (a) Let $p \equiv 1 \pmod 4$ be an odd prime, and let u satisfy $u^2 \equiv -1 \pmod p$. Define the lattice Λ to consist of all pairs $(a, b) \in \mathbb{Z}^2$ such that $b \equiv ua \pmod p$. Show that Λ is a subgroup of $\mathbb{Z}^2$ of index $p/$

   (b) Let $u, v \in \mathbb{Z}$ such that $u^2 + v^2 + 1 \equiv 0 \pmod p$. Let $\Lambda \subseteq \mathbb{Z}^4$ be the lattice of points (a, b, c, d) which satisfy

$$c \equiv ua + vb \pmod p \qquad \text{and} \qquad d \equiv ub - va \pmod p.$$

   Then Λ has index p^2 in $\mathbb{Z}^4$

2. Let K be a number field with ring of integers O_K, and let I_1, I_2 be comprime ideals such that $I_1 I_2 = J^k$ for some ideal J and some $k > 0$. Then there exist ideals J_1, J_2 such that $I_1 = J_2^k$ and $I_2 = J_2^k$.

3. Calculate the ideal class group of the following fields:

   (a) $\mathbb{Q}(\sqrt{\pm 3})$,

   (b) $\mathbb{Q}(\sqrt{-11})$,

   (c) $\mathbb{Q}(\sqrt{-13})$,

   (d) $\mathbb{Q}(\sqrt{-23})$,

   (e) $\mathbb{Q}(\sqrt{-65})$.

4. (a) Determine all integer solutions of the equation $Y^3 = X^2 + 13$.

   (b) Does the equation $Y^3 = X^2 + 30$ have any integer solutions? Justify your answer.