# HW #7

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, March 5 by 11:59pm on Gradescope.

**Question 1.** Recall that, in the notes, it is proved that $h_{\mathbb{Q}(\sqrt{-14})} = 4$. Using this, we would like to know when a prime $p \neq 2, 7$ is of the form $p = x^2 + 14y^2$ for some integers $x, y \in \mathbb{Z}$.

Let $p \neq 2, 7$ be a rational prime number.

(1) Using the binary quadratic forms technique, show that $p$ is properly represented by either $X^2 + 14Y^2$, $2X^2 + 7Y^2$, $3X^2 + 2XY + 5Y^2$, or $3X^2 - 2XY + 5Y^2$, if and only if $-14$ is a square modulo $p$.

(2) Show that if either $p = X^2 + 14Y^2$ or $p = 2X^2 + 7Y^2$, then $p \equiv 1$ or $7 \pmod 8$.

**Hint.** $n^2 \equiv 0, 1, 4 \pmod 8$.

(3) Show that $p = 3X^2 \pm 2XY + 5Y^2$ for some $X, Y \in \mathbb{Z}$ if and only if $3p = Z^2 + 14W^2$ for some $Z, W \in \mathbb{Z}$. Deduce that, if $p = 3X^2 \pm 2XY + 5Y^2$, then $p \equiv 3$ or $5 \pmod 8$.

(4) Show that $p = 2X^2 + 7Y^2$ for some $X, Y \in \mathbb{Z}$ if and only if $2p = Z^2 + 14W^2$ for some $Z, W \in \mathbb{Z}$.

(5) Combining the above, show that, for $p \neq 2, 7$,

$$\text{Either } p \text{ or } 2p = X^2 + 14Y^2 \Leftrightarrow p \equiv 1, 7 \pmod 8 \text{ and } p \equiv 1, 2, 4 \pmod 7.$$

(6) Show that the two cases in the left side of (5) are mutually exclusive, namely that there is no $p \neq 2, 7$ such that $X^2 + 14Y^2$ represents both $p$ and $2p$.

**Question 2.** We will prove the following

**Claim.** If $p = 4q^2n^2 + 1$ is a prime, with $q$ prime and $n > 1$, then $h_{\mathbb{Q}(\sqrt{p})} > 1$.

(1) Suppose that $h_{\mathbb{Q}(\sqrt{p})} = 1$. Using the splitting of $(q)$ in $\mathbb{Q}(\sqrt{p})$, show that $q = \left|\frac{u^2 - pv^2}{4}\right|$ for some $u, v \in \mathbb{Z}$.

(2) We thus have an element $\alpha = u - v\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ such that $N(\alpha) = \pm 4q$. Take $\beta = x - y\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$, with $x \geq 0, y > 0$, such that $N(\beta) = \pm 4q$ with the smallest possible $y$. Use that $N(2qn + \sqrt{p}) = -1$ and the minimality of $y$ to show that $|x - 2qny| \geq y$.

(3) Deduce a contradiction from the conditions we have so far, $x \geq 0$, $y > 0$, $\pm 4q = x^2 - (4q^2n^2 + 1)y^2$, $n > 1$, and $|x - 2qny| \geq y$.

**Question 3.** Let $K$ be an imaginary quadratic field with $\mathrm{disc}(K) = -d < 0$. Recall that, in the notes, we have established

$$\mathrm{Cl}(K) = \left\{ z = \frac{-b + \sqrt{d}i}{2a} \in \mathbb{H},\ a, b, c \in \mathbb{Z},\ -d = b^2 - 4ac \right\} / (z \sim \gamma \cdot z,\ \gamma \in \mathrm{SL}_2(\mathbb{Z}))$$

$$= \left\{a, b, c \in \mathbb{Z},\ a, c > 0,\ d = 4ac - b^2,\ -a < b \leq a,\ c \geq a,\ \text{and if } b < 0, c > a\right\}.$$

For $z = \frac{-b+\sqrt{d}i}{2a} \in \mathbb{H}$ with $a, b, c \in \mathbb{Z}$ and $-d = b^2 - 4ac$, let $[z] \in \mathrm{Cl}(K)$ be its corresponding ideal class. For $a, b, c \in \mathbb{Z}$ with $a, c > 0$, $d = 4ac - b^2$, $-a < b \leq a$, $c \geq a$, and if $b < 0$, $c > a$, let $[a, b, c] \in \mathrm{Cl}(K)$ be its corresopnding ideal class.

(1) For $z = \frac{-b+\sqrt{d}i}{2a} \in \mathbb{H}$ with $a, b, c \in \mathbb{Z}$ and $-d = b^2 - 4ac$, show that $[-\overline{z}] = [z]^{-1}$ in $\mathrm{Cl}(K)$.

**Hint.** For $\mathfrak{a} \subset \mathcal{O}_K$, show that $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal, where $\overline{(\cdot)}$ is the nontrivial Galois conjugation of $K/\mathbb{Q}$.

(2) For $a, b, c \in \mathbb{Z}$ with $a, c > 0$, $d = 4ac - b^2$, $-a < b \leq a$, $c \geq a$, and if $b < 0$, $c > a$, show that $[a, b, c]^2 = 1$ in $\mathrm{Cl}(K)$ if and only if either $b = 0$, $b = a$ or $c = a$.

(3) Show that $h_K$ is an odd number if and only if either $K = \mathbb{Q}(\sqrt{-1})$, $K = \mathbb{Q}(\sqrt{-2})$, or $K = \mathbb{Q}(\sqrt{-p})$ with $p$ a rational prime $\equiv 3 \pmod 4$.

**Hint.** Divide into the cases where $K = \mathbb{Q}(\sqrt{m})$ with $m \equiv 1 \pmod 4$ and where $K = \mathbb{Q}(\sqrt{m})$ with $m \equiv 2, 3 \pmod 4$.