ASSIGNMENT 8 - NUMBER THEORY, WINTER 2009

Submit by Monday, March 23, 16:00.

Solve following questions:

(35) Using a calculator only (the period of the continued fraction of $\sqrt{79}$ is 4), solve the equations

$$x^2 - 79 * y^2 = 1, \qquad x^2 - 79 * y^2 = 2.$$

(36) Show that a rational number $\frac{m}{n}$, where $(m, n) = 1$ has an expansion into a finite continued fraction and relate the continued fraction to the Euclidean algorithm for calculating (m, n).

In the following two questions follow the strategy we used to prove that two infinite simple continued fractions $[a_0, a_1, \dots], [b_0, b_1, \dots]$ that converge to the same number must be equal: $a_i = b_i$ for all i.

(37) Show that the expansion into continued fraction of a rational number is unique up to the following:

$$[a_0, a_1, \dots, a_n] = \begin{cases} [a_0, \dots, a_n - 1, 1] & a_n > 1 \text{ or } n = 0; \\ [a_0, \dots a_{n-1} + 1] & a_n = 1. \end{cases}$$

(38) Show that we cannot have an equality

$$[a_0, \dots, a_n] = [b_0, b_1, b_2, \dots],$$

between a finite continued fraction and an infinite one (where as usual the $a_i, b_i \in \mathbb{Z}$ and are positive for $i > 0$).

(39) Find which integers are both a square and a triangular number. (You may find it useful to note that a is a triangular number if and only if $8a + 1$ is a square.) First find one non-zero example and then, making use of exercise (L) below, find all such integers.

The honors students need to submit also the following problem.

(L) In this exercise we shall analyze the group of units $\mathbb{Z}[\sqrt{d}]^\times$ of $\mathbb{Z}[\sqrt{d}]$.

Let d be a positive integer which is not a square. Consider the ring

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b, \in \mathbb{Z}\}.$$

Prove that $x + y\sqrt{d}$ is a unit in this ring if and only if $x^2 - dy^2 = \pm 1$.

Now, prove that every discrete subgroup Γ of $\mathbb{R}$ (namely, a subgroup Γ, relative to the addition, such that for some $\epsilon > 0$ we have $\Gamma \cap (-\epsilon, \epsilon) = 0$) is cyclic. More precisely, there exists $\gamma \in \Gamma$ such that $\Gamma = \gamma\mathbb{Z}$.

Consider the map

$$\mathbb{Z}[\sqrt{d}]^\times \to \mathbb{R}^2.$$

$x + y\sqrt{d} \mapsto (\log(|x + y\sqrt{d}|), \log(|x - y\sqrt{d}|)$. Show that this is a homomorphism, whose kernel is ± 1, and whose image is a discrete subgroup of $\{(s, t) \in \mathbb{R}^2 : s + t = 0\} \cong \mathbb{R}$. Conclude that the image is an infinite cyclic group with some generator γ. Let $\eta = x_0 + y_0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^\times$ be an element mapping to $\pm\gamma$. We may assume without loss of generality that x_0, y_0 are positive – explain why! (Hint: consider $\pm\eta^{\pm 1}$.) This determines η uniquely; it is called the fundamental unit.

Conclude from the above that any element of $\mathbb{Z}[\sqrt{d}]^\times$ can be written uniquely as $\pm(x_0 + y_0\sqrt{d})^m, m \in \mathbb{Z}$. Conclude that if $x_0^2 - dy_0^2 = -1$ (we say that the fundamental unit has negative sign) then the solutions to the equation

$$x^2 - dy^2 = -1,$$

are given by $\pm(x_0 + y_0\sqrt{d})^{2m+1}$ and the solutions to

$$x^2 - dy^2 = 1,$$

are given by $\pm(x_0 + y_0\sqrt{d})^{2m}$. On the other hand, if $x_0^2 - dy_0^2 = 1$ (we say that the fundamental unit has positive sign) then there are no solutions to the equation

$$x^2 - dy^2 = -1,$$

and the solutions to

$$x^2 - dy^2 = 1,$$

are given by $\pm(x_0 + y_0\sqrt{d})^m$.

It is a fact that the continued fraction of $\sqrt{d}$ has (p_{n-1}, q_{n-1}) corresponding to η as defined above.