Homework #11. Solutions to selected problems.

2. Let $\alpha \in \mathbb{R}$, and assume that the continued fraction for α is infinite periodic. Prove that α is a quadratic irrational, that is, $\alpha \notin \mathbb{Q}$, but α is a root of a nonzero quadratic polynomial with integer coefficients. **Hint:** Start with the case when the continued fraction for α is purely periodic, that is, the periodic part starts from the very beginning ($\alpha = [\overline{a_0, \ldots, a_{k-1}}]$). Start by writing down some equation that α must satisfy (it will involve a finite continued fraction) and then conclude that α satisfies a quadratic equation. Then use the result in the purely periodic case to establish the general case.

Solution: Suppose first that the continued fraction for α is purely periodic. This means that there exists a finite sequence of positive integers $a_0, \ldots, a_{k-1}$ such that $\alpha = [a_0; a_1, \ldots, a_{k-1}, \alpha]$.

Lemma: *Let $a_0, \ldots, a_{k-1}$ be a finite integer sequence, with each $a_i > 0$. Then there exist non-negative integers x, y, z and w, with $x, z > 0$, such that for any real number $\alpha > 0$ we have $[a_0; a_1, \ldots, a_{k-1}, \alpha] = \frac{x\alpha+y}{z\alpha+w}$.*

Proof of the lemma: We use induction on k. In the base case $k = 1$ we have $[a_0; \alpha] = a_0 + \frac{1}{\alpha} = \frac{a_0\alpha+1}{\alpha}$, so the statement holds with $x = a_0$, $y = z = 1$ and $w = 0$.

Now assuming that lemma is true for some $k \geq 1$, we prove it for $k+1$. Let $\beta = [a_0; a_1, \ldots, a_k, \alpha]$. Then $\beta = [a_0; \gamma]$ where $\gamma = [a_1; a_2, \ldots, a_k, \alpha]$. By induction hypothesis $\gamma = \frac{x\alpha+y}{z\alpha+w}$ for some non-negative integers x, y, z and w, with $x, z > 0$. Then $\beta = a_0 + \frac{1}{\gamma} = a_0 + \frac{z\alpha+w}{x\alpha+y} = \frac{(a_0x+z)\alpha+(a_0y+w)}{x\alpha+y}$. Since $a_0 > 0$ and $x, z > 0$, the coefficients of α in both numerator and denominator are both positive, so β has required form. $\square$

Going back to our problem, since $\alpha = [a_0; a_1, \ldots, a_{k-1}, \alpha]$, by Lemma we have $\alpha = \frac{x\alpha+y}{z\alpha+w}$ for some $x, y, z, w \in \mathbb{Z}$ with $x, z > 0$. Multiplying both sides by $z\alpha + w$, we get $z\alpha^2 + (w-x)\alpha - y = 0$. Thus, α is a root of a polynomial of degree 2 (since $z > 0$). Since the continued fraction for α is infinite, α is irrational, so by definition α is a quadratic irrational.

Now assume that the continued fraction for α is periodic, but not purely periodic. Let l be the length of the "preperiodic" part of the continued fraction for α, that is, $\alpha = [a_0; a_1, \ldots, a_l; \overline{b_1, \ldots, b_k}]$. Thus, $\alpha = [a_0; a_1, \ldots, a_l, \gamma]$ where $\gamma = [\overline{b_1, \ldots, b_k}]$. The continued fraction for γ is purely periodic, so as we just proved, γ is a quadratic irrational. We will now prove that α is a quadratic irrational by induction on l.

In the base case $l = 0$ we have $\alpha = a_0 + \frac{1}{\gamma}$, so $\gamma = \frac{1}{\alpha - a_0}$. We know that there exist integers x, y, z with $z \neq 0$ such that $z\gamma^2 + y\gamma + x = 0$ (note that $x \neq 0$ as well since otherwise $\gamma \in \mathbb{Q}$). Hence $z\left(\frac{1}{\alpha-a_0}\right)^2 + y\left(\frac{1}{\alpha-a_0}\right) + x = 0$, whence $x(\alpha - a_0)^2 + y(\alpha - a_0) + z = 0$, so as before, α is a quadratic irrational.

Finally, we do the induction step. Assume that $l \geq 1$ and the assertion is true for $l - 1$. Then $\alpha = [a_0; \beta] = a_0 + \frac{1}{\beta}$ where $\beta = [a_1; \ldots, a_l, \gamma]$. By induction hypothesis, β is a quadratic irrational, and arguing as in the base case, we conclude that α is a quadratic irrational as well.

4. Find a non-trivial solution to Pell's equation $x^2 - dy^2 = 1$ in each of the following cases:

(i) $d = (a^2 - 1)$ for some $a \in \mathbb{N}$

(ii) $d = a^2 + 1$ for some $a \in \mathbb{N}$

(iii) $d = a(a + 1)$ for some $a \in \mathbb{N}$

Answer: (i) $(x, y) = (a, 1)$; (ii) $(x, y) = (2a^2 + 1, 2a)$; (iii) $(x, y) = (2a + 1, 2)$.

6. Use continued fractions to find a solution to Pell's equation $x^2 - dy^2 = 1$ for $d = 19$ and $d = 41$.

Solution: The continued fraction for $\sqrt{19}$ is $[4; \overline{2, 1, 3, 1, 2, 8}]$. It has even period 6, so the continued fraction $[4; 2, 1, 3, 1, 2]$ gives us a solution. We have $[4; 2, 1, 3, 1, 2] = [4; 2, 1, 3, 3/2] = [4; 2, 1, 11/3] = [4; 2, 14/11] = [4; 39/14] = 170/39$, so $(170, 39)$ is a solution.
The continued fraction for $\sqrt{41}$ is $[6; \overline{2, 2, 12}]$. It has odd period 3, so the continued fraction $[6; 2, 2]$ give us an element of $\mathbb{Z}[\sqrt{41}]$ of norm -1. We have $[6; 2, 2] = [6; 5/2] = 32/5$, so $N(32 + 5\sqrt{41}) = -1$ and therefore $N((32 + 5\sqrt{41})^2) = 1$. Since $(32 + 5\sqrt{41})^2 = (32^2 + 25 \cdot 41 + 320\sqrt{41}) = 2049 + 320\sqrt{41}$, the pair $(2049, 320)$ is a solution.

7. Prove that for every $n \in \mathbb{N}$ there exists a solution to the equation $x^2 - 3y^2 = 1$ satisfying $10^n < x < 10^{n+1}$.

Solution: Clearly, $(x, y) = (2, 1)$ is a solution (in fact, the fundamental solution). Let $z = 2 + \sqrt{3}$, and for each $k \in \mathbb{N}$ let x_k and y_k be unique integers such that $z^k = x_k + y_k\sqrt{3}$. We know that (x_k, y_k) is a solution for each k, and we just need to show that $10^n < x_k < 10^{n+1}$ for some k.
We claim that for each k,

(i) $x_k < z^k < 2x_k$

(ii) $x_{k+1} < 8x_k$

(iii) $x_k \to \infty$ as $k \to \infty$

The inequality $x_k < z^k$ is clear. On the other hand, $3y_k^2 = x_k^2 - 1 < x_k^2$, so $y_k\sqrt{3} < x_k$ and therefore $z^k = x_k + y_k\sqrt{3} < 2x_k$. This proves (i).

Since $z < 4$, from (i) we get $x_{k+1} < z^{k+1} < 4z^k < 8x_k$ by (i). Thus we proved (ii).

Finally, it is clear that $z^k \to \infty$ as $k \to \infty$. Since $x_k > z^k/2$ by (i), this implies (iii).

Now fix $n \in \mathbb{N}$. Since $x_k \to \infty$ as $k \to \infty$, the set $\{k \in \mathbb{N} : x_k \leq 10^n\}$ is finite. Note that this set is also non-empty since $x_1 = 2 < 10$. Hence there exists the largest k for which $x_k \leq 10^n$. Since k is the largest with this property, $x_{k+1} > 10^n$; on the other hand, $x_{k+1} < 8x_k < 10^{n+1}$, so $10^n < x_{k+1} < 10^{n+1}$, as desired.

8. Let (x, y, z) be a primitive integer solution for the equation $x^2 + 2y^2 = z^2$. Prove that there exist integers u and v such that $(x, y, z) = (2u^2 - v^2, 2uv, 2u^2 + v^2)$ or $(u^2 - 2v^2, 2uv, u^2 + 2v^2)$.

Note: As in the case of Pythagorean triples, we call the solution (x, y, z) primitive if $gcd(x, y, z) = 1$. Also, the problem was stated slightly incorrectly – I forgot to require that x, y and z are positive.

Solution: We start by making a few observations about x and z. Since $z^2 - x^2 = 2y^2$, x and z must have the same parity. If x and z are both even, then $4 \mid z^2$ and $4 \mid x^2$, so $4 \mid (z^2 - x^2) = 2y^2$, whence $2 \mid y^2$, and therefore y is even. Hence, x, y, z are all even, contradicting the assumption $gcd(x, y, z) = 1$. Thus, x and z are both odd.

Next we prove that x and z are coprime. If not, there exists a prime p which divides both x and z, hence also divides $2y^2$. Since x is odd, p is also odd, and therefore $p \mid y$, again contradicting $gcd(x, y, z) = 1$.

Since x and z are both odd, $x \equiv \pm z \mod 4$, so either $\frac{z-x}{4}, \frac{z+x}{2} \in \mathbb{Z}$ or $\frac{z+x}{4}, \frac{z-x}{2} \in \mathbb{Z}$.

In the first case, from the equation $2y^2 = z^2 - x^2 = (z - x)(z + x)$, we get $8 \mid 2y^2$, so y is even. Dividing both sides by 8, we get

$$\left(\frac{y}{2}\right)^2 = \frac{z-x}{4} \cdot \frac{z+x}{2}. \qquad (***)$$

Since x and z are coprime, as in the proof of the classification of Pythagorean triples, $\frac{z-x}{2}$ and $\frac{z+x}{2}$ are coprime, hence $\frac{z-x}{4}$ and $\frac{z+x}{2}$ are also coprime.

Since $x, z > 0$ and $x^2 < z^2$, we have $z - x > 0$ and $z + x > 0$, so by the result of Problem 7 in HW#1 applied to (***), there exist $u, v \in \mathbb{N}$ such that $\frac{z-x}{4} = v^2$ and $\frac{z+x}{2} = u^2$. Hence $z = u^2 + 2v^2$ and $x = u^2 - 2v^2$. Since $(y/2)^2 = u^2v^2$ and $y, u, v > 0$, we get $y = 2uv$. So, $(x, y, z) = (u^2 - 2v^2, 2uv, u^2 + 2v^2)$, as desired.

Similarly, in the second case (when $\frac{z+x}{4}, \frac{z-x}{2} \in \mathbb{Z}$), we get $(x, y, z) = (2u^2 - v^2, 2uv, 2u^2 + v^2)$ for some $u, v \in \mathbb{N}$.