Elementary Number Theory - Exercise 10a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. Show that, if $d = m^2$ is a square, then Pell's equation $x^2 - dy^2 = 1$ only has the trivial solutions $(x, y) = (\pm 1, 0)$.

Solution 1. We can factor

$$(x^2 - dy^2) = (x^2 - m^2y^2) = (x - my)(x + my).$$

If $(x - my)(x + my) = 1$, then both factors equal 1 or -1. Replacing (x, y) with $(-x, -y)$ we can assume that both factors are 1, that is

$$\begin{aligned} x - my &= 1, \\ x + my &= 1. \end{aligned}$$

Adding and subtracting the two equations, we get $x = 1$ and $my = 0$, hence $y = 0$.

Problem 2. Determine some non-trivial solutions of Pell's equation $x^2 - 2y^2 = 1$ and use them to find a rational approximation $\frac{x}{y}$ to $\sqrt{2}$ with $|\frac{x}{y} - \sqrt{2}| \leq 10^{-6}$.

Solution 2. We have the trivial solutions $(\pm 1, 0)$. Moreover, by replacing x, y with their negatives if necessary, it suffices to look for solutions $(x, y) \in \mathbb{N}^2$. By trying $(x, y) = (1, 1), (x, y) = (1, 2), (x, y) = (2, 1)$, and so on, we find the non-trivial solution

$$(x_1, y_1) = (3, 2).$$

Since the tuples $(x, y) \in \mathbb{N}^2$ with $x < 3$ do not give solutions, this is the fundamental solution. By Lagrange's Theorem, all non-trivial solutions are given by (x_n, y_n), where

$$x_n + y_n\sqrt{2} = (x_1 + y_2\sqrt{2})^n = (3 + 2\sqrt{2})^n.$$

For example, we obtain the solutions

$$(3, 2), \quad (17, 12), \quad (99, 70), \quad (577, 408), \quad (3363, 2378).$$

We have seen in the lecture that each solution (x, y) to Pell's equation $x^2 - dy^2 = 1$ gives a rational approximation to $\frac{x}{y}$ to $\sqrt{d}$ with

$$|\tfrac{x}{y} - \sqrt{d}| \leq \frac{1}{2y^2}.$$

Hence, if we want to achieve that $|\frac{x}{y} - \sqrt{2}| \leq 10^{-4}$, it suffices to find a solution (x, y) with $y \geq 10^3$. Above, we found the solution $(x_5, y_5) = (3363, 2378)$, which leads to the rational approximation

$$\frac{x_5}{y_5} = \frac{3363}{2378} = 1.41421362489487.$$

Comparing this with

$$\sqrt{2} = 1.41421356237310,$$

we see that the first 7 digits are correct, so this is the desired rational approximation.

Problem 3. Let $d > 0$ be a non-square. Consider the set

$$\mathbb{Q}(\sqrt{d}) = \{x + \sqrt{d}y \,:\, x, y \in \mathbb{Q}\}.$$

1. Show that $\mathbb{Q}(\sqrt{d})$ is closed under addition and multiplication.
2. Show that $(x + \sqrt{d}y)^{-1} = \frac{x-\sqrt{d}y}{x^2-dy^2}$ for $(x, y) \neq (0, 0)$, and deduce that $\mathbb{Q}(\sqrt{d})$ is a field.
3. If $(x, y) \in \mathbb{Q}^2$ solves Pell's equation $x^2 - dy^2 = 1$, then we have

$$(x + \sqrt{d}y)^{-n} = (x - \sqrt{d}y)^n$$

   for every $n \in \mathbb{Z}$.

Solution 3. 1. We have

$$(x + \sqrt{d}y)(a + \sqrt{d}b) = (x + a) + \sqrt{d}(y + b)$$

   and

$$(x + \sqrt{d}y)(a + \sqrt{d}b) = (xa + dyb) + \sqrt{d}(xb + ya)$$

2. We have

$$(x + \sqrt{d}y) \cdot \frac{x - \sqrt{d}y}{x^{-}dy^2} = 1$$

   which implies the result. This works whenever $x + \sqrt{d}y \neq 0$, so every non-zero element in $\mathbb{Q}(\sqrt{d})$ is invertible. Since $\mathbb{Q}(\sqrt{d})$ contains 0 and 1, is closed under addition and multiplication, and every non-zero element is invertible, it is a field.

3. We compute

$$(x + \sqrt{d}y)^n(x - \sqrt{d}y)^n = ((x + \sqrt{d}y)(x - \sqrt{d}y))^n = (x^2 - dy^2)^n = 1^n = 1,$$

   which implies the stated formula.

Problem 4. Compute the continued fraction expansion and the convergents of $\frac{128}{1527}$.

Solution 4. We compute

$$\begin{aligned}
\frac{128}{1527} &= \frac{1}{\frac{1527}{128}} = \frac{1}{11 + \frac{119}{128}} = \frac{1}{11 + \frac{1}{\frac{128}{119}}} = \frac{1}{11 + \frac{1}{1+\frac{9}{119}}} \\
&= \frac{1}{11 + \frac{1}{1+\frac{1}{\frac{119}{9}}}} = \frac{1}{11 + \frac{1}{1+\frac{1}{13+\frac{2}{9}}}} = \frac{1}{11 + \frac{1}{1+\frac{1}{13+\frac{1}{\frac{9}{2}}}}} \\
&= \frac{1}{11 + \frac{1}{1+\frac{1}{13+\frac{1}{4+\frac{1}{2}}}}} = [0, 11, 1, 13, 4, 2].
\end{aligned}$$

The convergents are given by

$$
\begin{aligned}
c_0 &= [0] = 0,\\
c_1 &= [0, 11] = \frac{1}{11},\\
c_2 &= [0, 11, 1] = \frac{1}{11 + \frac{1}{1}} = \frac{1}{12},\\
c_3 &= [0, 11, 1, 13] = \frac{1}{11 + \frac{1}{1+\frac{1}{13}}} = \frac{14}{167}\\
c_4 &= [0, 11, 1, 13, 4] = \frac{1}{11 + \frac{1}{1+\frac{1}{13+\frac{1}{4}}}} = \frac{57}{680}.
\end{aligned}
$$

Problem 5. Show the identities

$$
\begin{aligned}
[a_0, \dots, a_n] &= a_0 + \frac{1}{[a_1, \dots, a_n]},\\
[a_0, \dots, a_n] &= [a_0, \dots, a_{n-1} + \tfrac{1}{a_n}],\\
[a_0, \dots, a_n] &= [a_0, \dots, a_n - 1, 1],\\
[a_0, \dots, a_n]^{-1} &= [0, a_0, \dots, a_n].
\end{aligned}
$$

Solution 5. We have

$$
[a_0, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = a_0 + \frac{1}{[a_1, \dots, a_n]}
$$

and

$$
[a_0, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{\left(a_{n-1} + \cfrac{1}{a_n}\right)}}} = [a_0, \dots, a_{n-1} + \tfrac{1}{a_n}].
$$

and

$$
[a_0, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{(a_n - 1) + \frac{1}{1}}}}} = [a_0, \dots, a_n - 1, 1],
$$

and

$$
[a_0, \dots, a_n]^{-1} = 0 + \frac{1}{[a_0, \dots, a_n]} = [0, a_0, \dots, a_n].
$$

Problem 6 (sage)**.** Write programs that

1. finds the fundamental solution to Pell's equation (apply it to $d = 43$).
2. lists solutions to Pell's equation using Lagrange's Theorem.
3. computes the continued fraction expansion and the convergents of a rational number.