Lecture 4

M. Klazar

October 21, 2025

In the last lecture we introduced the family of Pell equations. They are Diophantine equations

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

where $d \in \mathbb{N}$ is a non-square number. In today's lecture we prove that every Pell equation has a nontrivial solution. We saw in the last lecture that this implies that every Pell equation has infinitely many solutions. By "solutions" we mean, in the context of Diophantine equations, always solutions in integers, in $\mathbb{Z}$.

An automorphism of a field

We begin by making explicit the trick we used last time. Let d be as in Pell equation and

$$\mathbb{Q}[\sqrt{d}] := \{a + b\sqrt{d} \colon \ a,\, b \in \mathbb{Q}\} \ \ (\subset \mathbb{R})\,.$$

Note that representations of elements of $\mathbb{Q}[\sqrt{d}]$ in this form are unique: for every $a, b, a', b' \in \mathbb{Q}$ we have

$$a + b\sqrt{d} = a' + b'\sqrt{d} \iff a = a' \wedge b = b'\,.$$

It is also not hard to show that

$$\mathbb{Q}[\sqrt{d}]_{\mathrm{fi}} := \langle \mathbb{Q}[\sqrt{d}],\, 0,\, 1,\, +,\, \cdot \rangle\,,$$

where $+$ and $\cdot$ is the usual addition and multiplication of real numbers, is a field.

Lemma 1. *The map* $f \colon \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}]$,

$$f(a + b\sqrt{d}) := a - b\sqrt{d}\,,$$

is an automorphism of the field $\mathbb{Q}[\sqrt{d}]_{\mathrm{fi}}$.

Proof. We show that for every $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ we have $f(\alpha \pm \beta) = f(\alpha) \pm f(\beta)$ (same signs), $f(\alpha \cdot \beta) = f(\alpha) \cdot f(\beta)$ and $f(\alpha/\beta) = f(\alpha)/f(\beta)$ (for $\beta, f(\beta) \neq 0$). We also show that f is a bijection. Let $\alpha := a + b\sqrt{d}$ and $\beta := a' + b'\sqrt{d}$ $(a, b, a', b' \in \mathbb{Q})$. Then indeed,

$$\begin{aligned} f(\alpha \pm \beta) &= f((a \pm a') + (b \pm b')\sqrt{d}) = (a \pm a') - (b \pm b')\sqrt{d} \\ &= (a - b\sqrt{d}) \pm (a' - b'\sqrt{d}) = f(\alpha) \pm f(\beta) \end{aligned}$$

(same signs),

$$\begin{aligned} f(\alpha\cdot\beta) &= f(aa'+bb'd+(ab'+a'b)\sqrt{d}) = aa'+bb'd-(ab'+a'b)\sqrt{d} \\ &= (a-b\sqrt{d})\cdot(a'-b'\sqrt{d}) = f(\alpha)\cdot f(\beta) \end{aligned}$$

and

$$\begin{aligned} f(\alpha/\beta) &= f((a+b\sqrt{d})/(a'+b'\sqrt{d})) = f\big(\tfrac{(a+b\sqrt{d})(a'-b'\sqrt{d})}{(a')^2-(b')^2d}\big) \\ &= \tfrac{(a-b\sqrt{d})(a'+b'\sqrt{d})}{(a')^2-(b')^2d} = (a-b\sqrt{d})/(a'-b'\sqrt{d}) = f(\alpha)/f(\beta)\,. \end{aligned}$$

In the last computation we used the two previous identities for $\pm$ and $\cdot$. Injectivity and surjectivity of f follow easily from its definition. □

Lagrange's theorem

Theorem 2 (Lagrange, 1770). *Every Pell equation has a nontrivial solution. In more detail, for every non-square number $d\in\mathbb{N}$ there exist numbers $p,q\in\mathbb{Z}$ such that $q\neq 0$ and*

$$p^2-dq^2=1\,.$$

Proof. Let $d\in\mathbb{N}$ be a non-square number. By Corollary 3 in Lecture 1 there exist infinitely many distinct numbers $\frac{p}{q}\in\mathbb{Q}$ such that

$$\left|\sqrt{d}-\frac{p}{q}\right|<\frac{1}{q^2}\,.$$

For each of these fractions $\frac{p}{q}$ we have

$$\left|p^2-dq^2\right| = q^2\cdot\left|\sqrt{d}-\tfrac{p}{q}\right|\cdot\left|\sqrt{d}+\tfrac{p}{q}\right| \le 2\sqrt{d}+1\,.$$

Using the pigeonhole principle (with infinitely many pigeons and finitely many pigeonholes) we see that there exists a nonzero number $m\in\mathbb{Z}$ ($|m|\le 2\sqrt{d}+1$) and infinitely many numbers $\frac{p}{q}\in\mathbb{Q}$ such that

$$p^2-dq^2=m\,.$$

By the same pigeonhole principle there exist two distinct fractions p_1/q_1 and p_2/q_2 such that

$$p_1^2-dq_1^2=p_2^2-dq_2^2=m$$

and

$$p_1\equiv p_2,\ q_1\equiv q_2\ (\mathrm{mod}\,|m|)\,.$$

We define $p,q\in\mathbb{Q}$ by the relation

$$\begin{aligned} p+q\sqrt{d} &:= \frac{p_1+q_1\sqrt{d}}{p_2+q_2\sqrt{d}} = \frac{(p_1+q_1\sqrt{d})(p_2-q_2\sqrt{d})}{m} \\ &= \frac{p_1p_2-q_1q_2d}{m}+\frac{p_2q_1-p_1q_2}{m}\sqrt{d}\,. \end{aligned}$$

Modulo $|m|$ we have

$$p_1p_2 - q_1q_2d \equiv p_1^2 - dq_1^2 = m$$

and

$$p_2q_1 - p_1q_2 \equiv p_2q_2 - p_2q_2 = 0\,.$$

Thus the numerators $p_1p_2 - q_1q_2d$ and $p_2q_1 - p_1q_2$ are divisible by m and we see that $p, q \in \mathbb{Z}$.

We show that p, q is a solution of $x^2 - dy^2 = 1$. Indeed, using the automorphism f in Lemma 1, we get from

$$p + q\sqrt{d} = \frac{p_1 + q_1\sqrt{d}}{p_2 + q_2\sqrt{d}}$$

that

$$p - q\sqrt{d} = f(p + q\sqrt{d}) = f\big(\tfrac{p_1+q_1\sqrt{d}}{p_2+q_2\sqrt{d}}\big) = \tfrac{f(p_1+q_1\sqrt{d})}{f(p_2+q_2\sqrt{d})} = \tfrac{p_1-q_1\sqrt{d}}{p_2-q_2\sqrt{d}}\,,$$

and therefore

$$p^2 - dq^2 = (p + q\sqrt{d})(p - q\sqrt{d}) = \tfrac{p_1+q_1\sqrt{d}}{p_2+q_2\sqrt{d}} \cdot \tfrac{p_1-q_1\sqrt{d}}{p_2-q_2\sqrt{d}} = \tfrac{p_1^2-dq_1^2}{p_2^2-dq_2^2} = \tfrac{m}{m} = 1\,.$$

It remains to show that $q \neq 0$. This is clear,

$$0 = q = \frac{p_2q_1 - p_1q_2}{m}$$

yields the contradiction that $\frac{p_2}{q_2} = \frac{p_1}{q_1}$. □

Generalized Pell equations

Generalized Pell equations are Diophantine equations

$$x^2 - dy^2 = m$$

with unknowns x, y and parameters $d \in \mathbb{N}$ and $m \in \mathbb{Z}$ such that d is a non-square number. The equation $x^2 - dy^2 = 0$ has clearly just one solution $0, 0$. For nonzero m we have the following dichotomy.

Corollary 3. *For every non-square $d \in \mathbb{N}$ and nonzero $m \in \mathbb{Z}$ the equation*

$$x^2 - dy^2 = m$$

has either no solution or infinitely many solutions $x, y \in \mathbb{Z}$.

Proof. Suppose that d and m are as stated and that numbers $a, b \in \mathbb{Z}$ are such that $a^2 - db^2 = m$. For every of the infinitely many solutions $x, y \in \mathbb{N}$ of the Pell equation $x^2 - dy^2 = 1$ we define numbers $a(x), b(y) \in \mathbb{Z}$ by the relation

$$a(x) + b(y)\sqrt{d} := (a + b\sqrt{d}) \cdot (x + y\sqrt{d})\,.$$

Using the automorphism f in Lemma 1, we get

$$a(x) - b(y)\sqrt{d} = f\big(a(x) + b(y)\sqrt{d}\big) = \cdots = (a - b\sqrt{d}) \cdot (x - y\sqrt{d})\,.$$

Thus

$$\begin{aligned} &a(x)^2 - d \cdot b(y)^2 = \big(a(x) + b(y)\sqrt{d}\big) \cdot \big(a(x) - b(y)\sqrt{d}\big) \\ &= (a + b\sqrt{d}) \cdot (x + y\sqrt{d}) \cdot (a - b\sqrt{d}) \cdot (x - y\sqrt{d}) \\ &(a^2 - db^2) \cdot (x^2 - dy^2) = m \cdot 1 = m \end{aligned}$$

and we see that $a(x), b(y)$ is a solution of the equation $x^2 - dy^2 = m$. It remains to show that if $x', y' \in \mathbb{N}$ is another solution of the Pell equation, so that $(x')^2 - d(y')^2 = 1$, then

$$\langle x',\, y' \rangle \neq \langle x,\, y \rangle \Rightarrow \langle a(x'),\, b(y') \rangle \neq \langle a(x),\, b(y) \rangle$$

and we really get infinitely many distinct solutions of $x^2 - dy^2 = m$. This implication in fact fails for $m = 0$. For $m \neq 0$ it holds because $a + b\sqrt{d} \neq 0$. $\square$

For example, since $10^2 - 2 \cdot 7^2 = 2$, the equation

$$x^2 - 2y^2 = 2$$

has infinitely many solutions. On the other hand, for example, since x^2 modulo 5 is 0, 1 or 4, for every $m \in \mathbb{Z}$ that is 2 or 3 modulo 5 the equation

$$x^2 - 5y^2 = m$$

has no solution. Can one decide for which pairs d and m there is a solution, and hence infinitely many solutions? Yes, one can, and the late result [2] of the German mathematician Carl Ludwig Siegel (1896–1981) is much more general.

Theorem 4 (C. L. Siegel, 1972). *There is an algorithm $\mathcal{A}$ that for every n and every input polynomial*

$$p \in \mathbb{Z}[x_1,\, x_2,\, \ldots,\, x_n]$$

with $\deg p \leq 2$ *decides if* $Z(p) \neq \emptyset$.

Last time we proved Skolem's theorem that solvability of any Diophantine equation is reducible to solvability of an equation with degree at most 4. What about cubic, i.e. degree 3, equations? The recent preprint [1] claims to prove that their solvability is also undecidable.

The infinite cyclic group

In the last result on Pell equations that we discuss we show that their solution sets have a simple group structure. For non-square $d \in \mathbb{N}$ let

$$M_d := \{a + b\sqrt{d} \in (0,\, +\infty) \colon\ a,\, b \in \mathbb{Z},\, a^2 - db^2 = 1\} \quad (\subset \mathbb{R}^+)\,.$$

Theorem 5. *The set M_d is an Abelian group with respect to multiplication of real numbers. In fact, every group*

$$M_{d,\mathrm{gr}} = \langle M_d,\, 1,\, \cdot \rangle$$

is isomorphic to the infinite cyclic group $\mathbb{Z}_{\mathrm{gr}} = \langle \mathbb{Z}, 0, + \rangle$.

Proof. Let M_d be as stated. We have $1 = 1 + 0\sqrt{d} \in M_d$ and M_d is closed to multiplication and division. We proved the former in the last lecture. Division is easy: if $a + b\sqrt{d} \in M_d$, then

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - db^2} = a - b\sqrt{d} \in M_d\,.$$

Thus $\langle M_d, 1, \cdot \rangle$ is an Abelian group, the remaining group properties are inherited from the group $\langle \mathbb{R}^+, 1, \cdot \rangle$.

We complete the proof by defining

$$\alpha := \min(M_d \cap (1,\, +\infty))$$

and showing that

$$M_d = \{\alpha^n \colon\ n \in \mathbb{Z}\}\,.$$

Then

$$g \colon M_d \to \mathbb{Z},\ g(\alpha^n) := n\,,$$

is an isomorphism of groups $M_{d,\mathrm{gr}}$ and $\mathbb{Z}_{\mathrm{gr}}$.

The intersection $M_d \cap (1,\, +\infty)$ is nonempty by Lagrange's theorem. It is not hard to see that if $\alpha := a + b\sqrt{d}$ and $\alpha' := a' + b'\sqrt{d}$ lie in $M_d \cap (1, +\infty)$, then $a, b, a', b' \in \mathbb{N}$ and

$$\alpha < \alpha' \iff a < a' \iff b < b'\,.$$

Thus the minimum exists. Finally, let $\beta \in M_d$. We show that $\beta = \alpha^n$ for some $n \in \mathbb{Z}$. If $\beta = 1$ then $n = 0$. If $\beta < 1$, we replace β with $1/\beta$. So let $\beta > 1$ and $n \in \mathbb{N}_0$ be maximum such that

$$\alpha^n \le \beta < \alpha^{n+1}\,.$$

For strict inequality here we would get from $\alpha^n < \beta < \alpha^{n+1}$ that $1 < \beta\alpha^{-n} < \alpha$. Since $\beta\alpha^{-n}$ is in M_d, we have a contradiction with the definition of α. Thus $\beta = \alpha^n$. □

References

[1] M. Rosko, Cubic Incompleteness: Hilbert's Tenth Problem Over N Starts at $\delta = 3$, arXiv:2510.00759v3 [math.LO], 2025, 33 pp.

[2] C. L. Siegel, Zur Theorie der quadratischen Formen, *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl.* II 1972, 21–46