Catalan’s conjecture is Mihăilescu’s theorem

Martin Klazar

(KAM MFF UK Praha)

dedicated to my parents Blanka and Jiří

– 520 –

48. ***Théorème.*** **Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes. (Catalan.)**

See [5].

192

13.
Note

extraite d'une lettre adressée à l'éditeur par Mr. *E. Catalan*, Répétiteur à l'école polytechnique de Paris.

„Je vous prie, Monsieur, de vouloir bien énconcer, dans votre recueil, le
„théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à
„le démontrer complètement: d'autres seront peut-être plus heureux:
„Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être
„des puissances exactes; autrement dit: l'équation $\mathbf{x^m - y^n = 1}$, dans
„laquelle les inconnues sont entières et positives, n'admèt qu'une seule
„solution."

See [6].

— written according to [1, pp. 1–2]. In 1842, the Belgian-French mathematician Eugène Ch. Catalan (1814–1894) (see [13]) put forth without a proof a theorem asserting that 8 and 9 are the only consecutive pure powers. Two years later he corrected himself and changed it to a conjecture. Catalan's conjecture was proven in 2004 by the Romanian mathematician Preda Mihăilescu (1955). In this text, we present a complete proof of Catalan's conjecture. In particular, we give in entirety Mihăilescu's proof.

Introduction

One can state Catalan's conjecture [6] (1844) as follows. For integers $m, n \geq 2$ the only solution of the Diophantine equation

$$x^m - y^n = 1$$

in nonzero integers x, y is $m = y = 2$, $x = \pm 3$ and $n = 3$. After many partial results by many authors, Catalan's conjecture was proven in 2004 by P. Mihăilescu [25].

Three excellent books on the subject are [30] by P. Ribenboim, [32] by R. Schoof and [1] by Yu. Bilu, Y. Bugeaud and M. Minotte. The first book is from the pre-Mihăilescu era; the other two present Mihăilescu's proof. They are far from self-contained, though. In this text our aim is to give a complete and self-contained presentation of Mihăilescu's proof, and in fact of the proof of Catalan's conjecture (which has to include many things Mihăilescu took for granted). The initial part in Chapters 1–**??** corresponds to my lectures in the course *Algebraic Number Theory* in 2024/25 and 2025/26.

It is easy to see that the exponents $m = p$ and $n = q$ can be assumed to be distinct primes. The resolution of Catalan's conjecture naturally divides in the elementary part with $p = 2$ or $q = 2$, and the non-elementary part with $p, q \geq 3$. "Elementary" does not mean easy, and "non-elementary" means hard. The elementary part is covered by the first three chapters, and the rest of our text is devoted to the non-elementary case. If it is not said else, a solution is always an integral solution.

In Chapter 1, we resolve the equation $x^2 - y^3 = 1$; the only solutions are $\langle \pm 3, 2 \rangle$, $\langle \pm 1, 0 \rangle$, and $\langle 0, -1 \rangle$. We present three resolutions of the equation. The historically first due to L. Euler (1737) is in Section 1.4. It makes use of the fact that, in the modern view, $x^2 = y^3 + 1$ is an elliptic curve. Euler actually proved that the five mentioned solutions are the only rational solutions. The second resolution of $x^2 - y^3 = 1$ in Section 1.3 is due to this author in 1989; the factorization $x^2 = (y + 1)(y^2 - y + 1)$ leads to investigation of properties of solutions of the Pell equation $x^2 - 3y^2 = 1$. Another way how to solve $x^2 - y^3 = 1$ is to start with the factorization $(x + 1)(x - 1) = y^3$; one is then led to equations $x^3 - 2y^3 = \pm 1$. In 1957, in a little known article, A. Wakulicz provided an elementary resolution of the more general equation $x^3 + y^3 = 2z^3$; we present his result in Section 1.5. All three resolutions of $x^2 - y^3 = 1$ are completely elementary in the sense that they take place in the field $\mathbb{Q}$.

Praha and Louny, December 2025 to ?? Martin Klazar

Contents

(^{c} . . . means a relatively complete section.)

Chapter 1

Euler's theorem

We begin our long journey on the mountain range of the proof of Catalan's conjecture in the first elementary case: the only integral solutions of the equation

$$x^2 - y^3 = 1$$

are pairs $\langle \pm 3, 2\rangle$, $\langle \pm 1, 0\rangle$ and $\langle 0, -1\rangle$. We give three proofs. Section 1.1 collects auxiliary results on Pell equations $x^2 - dy^2 = 1$ needed in this chapter and in Chapter 3. In Section 1.2 we survey unique factorization domains and principles of powers. In Section 1.3 we present the resolution of $x^2 - y^3 = 1$ in [18], found by this author in 1989. Section 1.4 is devoted to a modern proof of the result due to Leonhard Euler (1707–1783) ([14]) in [15] in 1738 that the five pairs are the only *rational* solutions of the equation. In the last Section 1.5 we present the elementary proof of A. Wakulicz [34] that the equation $x^3 + y^3 = 2z^3$ has no solution with $x \neq \pm y$. Thus the only solutions of $x^3 - 2y^3 = \pm 1$ are $\langle \pm 1, 0\rangle$ and $\langle \pm 1, \pm 1\rangle$ (equal signs). Using the factorization

$$(x-1)(x+1) = y^3$$

one deduces that $x^2 - y^3 = 1$ has just the five mentioned solutions. The existence of the nontrivial (nonzero) solution $\langle \pm 3, 2\rangle$ gives this elementary case of Catalan's conjecture a distinct flavor compared to the elementary cases in the next two chapters. In Sections 1.3, 1.4 and 1.5 we follow [18], [9] and [34], respectively.

1.1 Pell equations

Pell equation is any Diophantine equation of the form

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

with unknowns x, y and parameter $d \in \mathbb{N}$ that is not a square: $d = 2$, 3, 5, 6, 7, 8, 10 and so on. We say that a pair $a, b \in \mathbb{N}$ is a *minimal solution* of the equation if $a^2 - db^2 = 1$ and there is no solution $x, y \in \mathbb{N}$ with $x < a$. Minimal solutions, if they exist, are unique.

Proposition 1.1.1 *Let $a, b \in \mathbb{N}$ be the minimal solution of the Pell equation*

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

Then natural solutions $x, y \in \mathbb{N}$ of the equation form an infinite set

$$\{\langle x,\, y\rangle \in \mathbb{N}^2\colon\ x + y\sqrt{d} = \big(a + b\sqrt{d}\big)^n \ \textit{for some}\ n \in \mathbb{N}\}\,.$$

Proof. Let $x_i, y_i \in \mathbb{Z}$, $i = 1, 2$, be two solutions of the equation and $x_3, y_3 \in \mathbb{Z}$ be defined by

$$x_3 + y_3\sqrt{d} = \big(x_1 + y_1\sqrt{d}\big)\big(x_2 + y_2\sqrt{d}\big)\,.$$

Then also

$$x_3 - y_3\sqrt{d} = \big(x_1 - y_1\sqrt{d}\big)\big(x_2 - y_2\sqrt{d}\big)\,.$$

Multiplying the displayed equalities we get

$$x_3^2 - dy_3^2 = \big(x_1^2 - dy_1^2\big)\big(x_2^2 - dy_2^2\big) = 1 \cdot 1 = 1\,.$$

Thus x_3, y_3 is a solution of the equation as well. Even more easily, if x, y is a solution of the equation, then the reciprocal

$$\frac{1}{x + y\sqrt{d}} = x - y\sqrt{d}$$

produces solution $x, -y$. Note that if $x_i, y_i \in \mathbb{N}$, $i = 1, 2$, are solutions of the equation, then

$$x_1 < x_2 \iff x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}\,.$$

Also, if $x, y \in \mathbb{Z}$ is a solution of the equation, then $x, y \in \mathbb{N}$ iff $x + y\sqrt{d} > 1$.

Now let a, b be as stated and $x, y \in \mathbb{N}$ be such that $x^2 - dy^2 = 1$. We take the unique $m \in \mathbb{N}_0$ such that

$$\alpha := \big(a + b\sqrt{d}\big)^m < x + y\sqrt{d} \le \big(a + b\sqrt{d}\big)^{m+1}\,.$$

If the last inequality were strict, then

$$1 < u + v\sqrt{d} := \alpha^{-1} \cdot (x + y\sqrt{d}) < a + b\sqrt{d}$$

would give a solution $u, v \in \mathbb{N}$ of the equation, in contradiction with the minimality of a, b. Thus $x + y\sqrt{d} = \big(a + b\sqrt{d}\big)^{m+1}$. □

In 1770, Lagrange proved that every Pell equation has a minimal solution, and hence infinitely many solutions. Probably, we do not need this result to resolve Catalan's conjecture. But we need some properties of the solutions of the Pell equation $x^2 - 3y^2 = 1$.

Corollary 1.1.2 *The solutions of Pell equation*

$$x^2 - 3y^2 = 1$$

are exactly the pairs $\langle \pm x_n, \pm y_n \rangle$, $n \in \mathbb{N}_0$, *where*

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

Also, $x_0 = 1$, $y_0 = 0$ *and* $x_{n+1} = 2x_n + 3y_n$, $y_{n+1} = x_n + 2y_n$.

Proof. This follows from Proposition 1.1.1 because $x^2 - 3y^2 = 1$ has the minimal solution $\langle 2, 1 \rangle$. □

Proposition 1.1.3 *If* $\langle x_n, y_n \rangle$, $n \in \mathbb{N}_0$, *are as in the previous corollary, then for every* $n \in \mathbb{N}_0$ *we have*

$$x_{2n} = 2x_n^2 - 1,\ y_{2n} = 2x_ny_n,\ x_{2n+1} = (y_n + y_{n+1})^2 + 1,\ y_{2n+1} = 2x_ny_{n+1} - 1 .$$

The numbers x_n *and* y_n *have different parity, and* x_n *is odd iff* n *is even.*

Proof. Since $x_n^2 - 3y_n^2 = 1$,

$$\begin{aligned} x_{2n} + y_{2n}\sqrt{3} &= \big(2 + \sqrt{3}\big)^{2n} = \big(x_n + y_n\sqrt{3}\big)^2 \\ &= x_n^2 + 3y_n^2 + 2x_ny_n\sqrt{3} = 2x_n^2 - 1 + 2x_ny_n\sqrt{3} . \end{aligned}$$

Similarly,

$$\begin{aligned} x_{2n+1} + y_{2n+1}\sqrt{3} &= (2 + \sqrt{3})(x_n^2 + 3y_n^2 + 2x_ny_n\sqrt{3}) \\ &= 2x_n^2 + 6x_ny_n + 6y_n^2 + (x_n^2 + 4x_ny_n + 3y_n^2)\sqrt{3} . \end{aligned}$$

Now $2x_n^2 + 6x_ny_n + 6y_n^2 = x_n^2 + 6x_ny_n + 9y_n^2 + 1 = (y_n + x_n + 2y_n)^2 + 1 = (y_n + y_{n+1})^2 + 1$ and $x_n^2 + 4y_ny_n + 3y_n^2 = 2x_n^2 + 4x_ny_n - 1 = 2x_n(x_n + 2y_n) - 1 = 2x_ny_{n+1} - 1$. The last claim is immediate from the just proven formulas. □

1.2 UFD and PP

These acronyms refer to *unique factorization domain(s)* and *principle(s) of powers*, respectively. PP propel resolutions of Diophantine equations, and therefore deserve more than the usual glossing over. Here we treat them in detail.

Proposition 1.2.1 (PP0) *Let* $a, b, c \in \mathbb{Z}$ *and* $k \in \mathbb{N}$. *If* a *divides* bc^k *and* a, c *are coprime, then* a *divides* b.

Proposition 1.2.2 (PP1) *Let $k, l \in \mathbb{N}$ with $k, l \geq 2$. If $a_i, b \in \mathbb{N}_0$ for $i \in [k]$ are $k+1$ numbers such that the a_i are pairwise coprime and if*

$$a_1 a_2 \dots a_k = b^l\ ,$$

then there exist k pairwise coprime numbers $b_i \in \mathbb{N}_0$ such that for every $i \in [k]$,

$$a_i = b_i^l\ .$$

If l is odd then this result holds also when $\mathbb{N}_0$ is replaced with $\mathbb{Z}$.

Proposition 1.2.3 (PP2) *Let p be a prime and $k \in \mathbb{N}$ with $k \geq 2$. If a, b, c in $\mathbb{N}_0$ are numbers such that*

$$\gcd(a, b) = p \wedge ab = c^k\ ,$$

then there exist coprime numbers $d, e \in \mathbb{N}_0$ such that

$$\{a,\, b\} = \{pd^k,\, p^{k-1}e^k\}\ .$$

If k is odd then this result holds also when $\mathbb{N}_0$ is replaced with $\mathbb{Z}$.

In order to generalize PP0, PP1 and PP2 to domains and to prove them, we review the notion of a unique factorization domain. We also introduce irreducible factorizations. Recall that an *(integral) domain*

$$R = \langle R,\, 0_R,\, 1_R,\, +,\, \cdot\rangle$$

is a commutative ring with 1_R such that for every $a, b \in R^*$ $(= R \setminus \{0_R\})$ we have $ab \neq 0_R$. For $a, b \in R$ we say that *a divides b (in R)*, written $a \,|\, b$, if $b = ac$ $(= a \cdot c)$ for some $c \in R$. We say that $a \in R$ is a *unit* if $a \,|\, 1_R$, that is, a is multiplicatively invertible. The set of units in R is denoted by $R^\times$. It is easy to see that

$$\langle R^\times,\, 1_R,\, \cdot\rangle$$

is an Abelian group, the *group of units* of the domain R. For $a, b \in R$ we write $a \sim b$ if $a = bc$ for some $c \in R^\times$; we say that the elements a and b are *associated.* For example, in the domain of integers

$$\mathbb{Z} = \langle \mathbb{Z},\, 0,\, 1,\, +,\, \cdot\rangle$$

we have $m \sim n$ iff $m = \pm n$. It is easy to see that $\sim$ is an equivalence relation, and that it is congruent with respect to multiplication. For $a \in R$ we denote by

$$[a]_\sim \quad (= \{b \in R\colon\ b \sim a\})$$

the *block* of the element a in the equivalence $\sim$. We get the (commutative) monoid of blocks

$$\langle R/\!\sim,\, [1_R]_\sim = R^\times,\, \cdot\rangle\ .$$

Proposition 1.2.4 *In any domain R, two elements are associated if and only if each divides the other.*

Proof. Let $a, b \in R$. Suppose that $a \sim b$. Thus $a = bc$ and $ac^{-1} = b$ for some $c, c^{-1} \in R^{\times}$. Hence $b \,|\, a$ and $a \,|\, b$.

Suppose that $a \,|\, b$ and $b \,|\, a$. Thus $b = ac$ and $a = bd$ for some $c, d \in R$. We get the equality

$$b \cdot (1_R - d \cdot c) = 0_R\,.$$

Thus, since we are in a domain, $b = a = 0_R$ and $a \sim b$, or $dc = 1_R$ and again $a \sim b$. □

Two elements $a, b \in R$ are *coprime*, written $(a, b) = 1_R$, if they can be simultaneously divided only by units.

Definition 1.2.5 (gcd) *Let R be a domain and $a, b \in R$. We say that $c \in R$ is the greatest common divisor of a and b, and write $c = \gcd(a, b)$, if c divides a and b, and every simultaneous divisor of a and b divides c.*

If $c = \gcd(a, b)$ and $c' \sim c$, then $c' = \gcd(a, b)$. If $a \sim a'$, $b \sim b'$, $c = \gcd(a, b)$ and $c' = \gcd(a', b')$, then $c \sim c'$. Also, a and b are coprime iff $\gcd(a, b) = 1_R$.

Let R be a domain. An element $a \in R$ is *irreducible* if $a \in R^* \setminus R^{\times}$ and if in every multiplicative decomposition $a = bc$ with $b, c \in R$, b or c is a unit. If $a, b \in R$, $a \sim b$ and a is irreducible, then so is b. We denote the set of irreducibles in R by R^{ir}.

Definition 1.2.6 (UFD 1) *R is a unique factorization domain, or* UFD*, if every element in $R^* \setminus R^{\times}$ is a product of irreducibles, and this product is unique up to the order of factors and the relation $\sim$.*

In more details, R is UFD if for every element $a \in R^* \setminus R^{\times}$ there exist $m \in \mathbb{N}$ irreducibles a_i such that

$$a = a_1 \cdot a_2 \cdot \ldots \cdot a_m\,,$$

and if any equality

$$c_1 \cdot c_2 \cdot \ldots \cdot c_l = b_1 \cdot b_2 \cdot \ldots \cdot b_m\,,$$

where $l, m \in \mathbb{N}$ and b_i and c_i are irreducibles, implies that $l = m$ and that there exists a permutation π of the numbers $1, 2, \ldots, l$ such that for every $i \in [l]$ we have $c_i \sim b_{\pi(i)}$. A prototypical example of UFD is $\mathbb{Z}$, which we prove in Section 2.3.

Recall that if A and B are sets and $X \subset A \times B$, then the relation X is a *partial function* (from A to B) if for every $a \in A$ there exists at most one $b \in B$ such that $\langle a, b\rangle \in X$. We formalize (actually, set-theorize) irreducible factorizations.

Definition 1.2.7 (irreducible factorizations) *Let R be a domain, $\mathbb{I} = R^{\mathrm{ir}}/\!\sim$ and let $a \in R^*$. Irreducible factorizations (in R) are finite partial functions X*

from $\mathbb{I}$ to $\mathbb{N}$. If $X \neq \emptyset$, we say that X is an irreducible factorization of the element a if

$$[a]_\sim = \prod_{\langle\alpha,\, m\rangle \in X} \alpha^m \,.$$

We say that $X = \emptyset$ is an irreducible factorization of a if $a \in R^\times$.

For any irreducible factorization X we set

$$(X)_1 = \{\alpha \in \mathbb{I}\colon\ \exists m \in \mathbb{N} :\ \langle\alpha,\, m\rangle \in X\}\,,$$

and for $\alpha \in (X)_1$ we denote by $X(\alpha)$ the unique $m \in \mathbb{N}$ such that $\langle\alpha, m\rangle \in X$.

Let $a, b \in R$ and X, Y be the respective irreducible factorizations. We define that X *divides* Y, written $X \,|\, Y$, if $(X)_1 \subset (Y)_1$ and for every $\alpha \in (X)_1$ we have $X(\alpha) \le Y(\alpha)$. It is easy to see that $a \,|\, b$ iff $X \,|\, Y$. We restate the definition of UFD.

Definition 1.2.8 (UFD 2) *A domain R is a unique factorization domain, or* UFD*, if every element in R^* has a unique irreducible factorization.*

Proposition 1.2.9 *In every* UFD *R every two elements $a, b \in R^*$ have the greatest common divisor c. If a and b are coprime then $c = 1_R$. Else, denoting by X and Y the irreducible factorization of a and b, respectively, we have*

$$[c]_\sim = \prod_{\alpha \in X_1 \cap Y_1} \alpha^{\min(X(\alpha),\, Y(\alpha))} \,.$$

Proof. This is immediate from the interpretation of divisibility of elements in R^* in terms of their irreducible factorizations. □

As for the pairs a, b with $ab = 0_R$, we have $\gcd(0_R, a) = a$ for every $a \in R^*$, and $\gcd(0_R, 0_R)$ does not exist.

We generalize PP0, PP1 and PP2 to UFD. Let R be UFD, $a, b \in R^*$ and let X and Y be the respective irreducible factorizations of a and b. Then a and b are coprime iff $(X)_1 \cap (Y)_1 = \emptyset$. The product ab has the irreducible factorization

$$\begin{aligned} XY \;\; := \;\; & \{\langle\alpha,\, X(\alpha)\rangle\colon\ \alpha \in (X)_1 \setminus (Y)_1\} \cup \{\langle\alpha,\, Y(\alpha)\rangle\colon\ \alpha \in (Y)_1 \setminus (X)_1\} \,\cup \\ & \cup \{\langle\alpha,\, X(\alpha) + Y(\alpha)\rangle\colon\ \alpha \in (X)_1 \cap (Y)_1\}\,. \end{aligned}$$

If a and b are coprime then we have the disjoint union $XY = X \cup Y$. For $l \in \mathbb{N}$ the power a^l has the irreducible factorization

$$X^l := \{\langle\alpha,\, lX(\alpha)\rangle\colon\ \alpha \in (X)_1\}\,.$$

Proposition 1.2.10 (PP0′) *Let R be* UFD*, $a, b, c \in R$ and let $k \in \mathbb{N}$. If a divides bc^k and a, c are coprime, then a divides b.*

Proof. It is not hard to check that the proposition holds if $abc = 0_R$. We assume that $a, b, c \in R^*$ and denote by X, Y and Z their respective irreducible factorizations. Since $(X)_1 \cap (Z)_1 = \emptyset$, also $(X)_1 \cap (Z^k)_1 = \emptyset$. From the previous description of divisibility on the level of irreducible factorizations it then follows that since $X \,|\, YZ^k$, we in fact have $(X)_1 \subset (Y)_1 \setminus (Z)_1$ and $X \,|\, Y$. □

Proposition 1.2.11 (PP1′) *Let R be* UFD *and let $k, l \in \mathbb{N}$ with $k, l \geq 2$. If $a_i, b \in R$ for $i \in [k]$ are $k+1$ elements such that the a_i are pairwise coprime and if*

$$a_1 a_2 \dots a_k \sim b^l \,,$$

then there exist k pairwise coprime elements $b_i \in R$ such that for every $i \in [k]$,

$$a_i \sim (b_i)^l \,.$$

Proof. Let R, k, l, a_i, and b be as stated. If one of the a_i is 0_R, then every a_j with $j \neq i$ is a unit. The proposition then holds because $0_R = (0_R)^l$ and for every $a \in R^\times$ we have $a \sim (1_R)^l$. So we may omit every $a_i \in R^\times$ and may assume that $a_i, b \in R^* \setminus R^\times$. Let X_i $(\neq \emptyset)$ be the irreducible factorization of a_i, and Y $(\neq \emptyset)$ be that of b. Since

$$X_1 X_2 \dots X_k = X_1 \cup X_2 \cup \dots \cup X_k = Y^l \,,$$

we have $X_i \subset Y^l$ for every $i \in [k]$. Thus l divides m for every $\langle \alpha, m \rangle \in X_i$, and it follows that $a_i \sim (b_i)^l$ for some $b_i \in R^* \setminus R^{\mathrm{ir}}$. Since the a_i are pairwise coprime, so are the b_i. □

We use the following notation. If R is a domain and $A, B \subset R$ are two equinumerous finite sets, then $A \sim B$ means that there is a bijection $f\colon A \to B$ such that $a \sim f(a)$ for every $a \in A$.

Proposition 1.2.12 (PP2′) *Let R be* UFD, *$p \in R^{\mathrm{ir}}$ and let $k \in \mathbb{N}$ with $k \geq 2$. If a, b, c in R are such that*

$$\gcd(a,\, b) = p \wedge ab \sim c^k \,,$$

then there exist coprime elements $d, e \in R$ such that

$$\{a,\, b\} \sim \{pd^k,\, p^{k-1}e^k\} \,.$$

Proof. Let R, p, k, a, b and c be as stated. If one of a and b is 0_R, then the other is associated with p. We are done because $0_R = p^{k-1}(0_R)^k$ and $p = p(1_R)^k$. We may therefore assume that $a, b, c \in R^*$. Let X, Y and Z be the irreducible factorizations of a, b and c, respectively. We may assume that $\langle [p]_\sim, 1 \rangle \in X$, $\langle [p]_\sim, m \rangle \in Y$ with $m \in \mathbb{N}$ and that $(X)_1 \cap (Y)_1 = \{[p]_\sim\}$. Since

$$XY = \big(X \setminus \{\langle [p]_\sim,\, 1 \rangle\}\big) \cup \big(Y \setminus \{\langle [p]_\sim,\, m \rangle\}\big) \cup \{\langle [p]_\sim,\, m+1 \rangle\} = Z^k \,,$$

we get that k divides both $X(\alpha)$ and $Y(\alpha)$ for every $\alpha \in ((X)_1 \cup (Y)_1) \setminus \{[p]_\sim\}$, and that k divides $m+1$. Thus $m = k - 1 + km_0$ for some $m_0 \in \mathbb{N}_0$. It follows that $a \sim pd^k$ and $b \sim p^{k-1}e^k$ for coprime $d, e \in R^*$. □

Assuming that $\mathbb{Z}$ is UFD, we leave the deduction of PP0 from PP0′, PP1 from PP1′ and PP2 from PP2′ as easy exercises for the interested reader.

1.3 Klazar's resolution of $x^2 - y^3 = 1$

We follow the article [18]. In the next result, we obtain well known formulas for Pythagorean triples. These formulas reverse the polynomial identity

$$\big(x^2 - y^2\big)^2 + (2xy)^2 = \big(x^2 + y^2\big)^2 \ \ (\text{in } \mathbb{Z}[x,\, y])\,.$$

Proposition 1.3.1 *If $x, y, z \in \mathbb{N}_0$ are numbers such that*

$$x^2 + y^2 = z^2$$

— they form a Pythagorean triple — and are pairwise coprime, then they express for some coprime numbers $u, v \in \mathbb{N}_0$ as

$$z = u^2 + v^2 \ \ \textit{and} \ \{x,\, y\} = \{u^2 - v^2,\, 2uv\}\,.$$

Proof. Let x, y and z be as stated. Reduction modulo 4 shows that z and exactly one of x and y, say x, is odd. Then, since $(z-x)/2$ and $(z+x)/2$ are coprime, from the equality

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

we get by PP1 (Proposition 1.2.2) coprime numbers $u, v \in \mathbb{N}_0$ such that $(z - x)/2 = v^2$, $(z + x)/2 = u^2$ and $uv = y/2$. Hence $x = u^2 - v^2$, $y = 2uv$ and $z = u^2 + v^2$. □

Corollary 1.3.2 *If $x, y \in \mathbb{N}_0$ are numbers such that*

$$2x^2 - y^2 = 1\,,$$

then there exist numbers $a, b \in \mathbb{N}_0$ such that $a^2 - 2b^2 = 1$ and

$$x \in \{a^2 + 2b^2 + 2ab,\, a^2 + 2b^2 - 2ab\} = \{2a^2 - 1 + 2ab,\, 2a^2 - 1 - 2ab\}\,.$$

Proof. Let x, y be as stated. Then y is odd, $y = 2y_0 + 1$ with $y_0 \in \mathbb{N}_0$. So $x^2 = 2y_0^2 + 2y_0 + 1 = y_0^2 + (y_0 + 1)^2$. By Proposition 1.3.1 there exist $u, v \in \mathbb{N}_0$ such that

$$x = u^2 + v^2 \ \text{ and } \{y_0,\, y_0 + 1\} = \{2uv,\, u^2 - v^2\}\,.$$

Thus $1 = u^2 - v^2 - 2uv = (u - v)^2 - 2v^2$ or $1 = 2uv - u^2 + v^2 = (u + v)^2 - 2u^2$. We set $a = u - v$, $b = v$, respectively $a = u + v$, $b = u$, and get $a, b \in \mathbb{N}_0$ as stated. □

We took the following result from Sierpinski's book [**?**].

Proposition 1.3.3 *The only solutions of the Diophantine equation*

$$x^4 - 2y^2 = 1$$

are $\langle \pm 1, 0 \rangle$.

Proof. Let $x, y \in \mathbb{Z}$ be a solution of the equation. Then x is odd and $x^2 = 1+4k$ for some $k \in \mathbb{N}_0$. We get from the factorization

$$(x^2-1)(x^2+1) = 2y^2$$

that $4k(2k+1) = y^2$. Since the numbers $4k$ and $2k+1$ are coprime, by PP1 (Proposition 1.2.2) we have $4k = a^2$, $a \in \mathbb{N}_0$. Thus $(x-a)(x+a) = 1$ and $x = \pm 1, y = 0$. □

The following auxiliary result is of an independent interest.

Theorem 1.3.4 *The Diophantine equation*

$$x^4 - 3y^2 = 1$$

has only the trivial solutions $\langle \pm 1, 0 \rangle$.

Proof. We need to solve $x_n = m^2$, where $n, m \in \mathbb{N}_0$ and x_n are as in Proposition 1.1.2. If $n = 2n_0 + 1$ is odd then Proposition 1.1.3 gives

$$(m - y_{n_0} - y_{n_0+1})(m + y_{n_0} + y_{n_0+1}) = 1\,.$$

Thus $m = \pm 1$ and $y_{n_0} + y_{n_0+1} = 0$. This is impossible because always $y_{n_0} + y_{n_0+1} > 0$.

Let $n = 2n_0$ be even. Then by Proposition 1.1.3, $2x_{n_0}^2 - 1 = x_{2n_0} = x_n = m^2$ and $2x_{n_0}^2 - m^2 = 1$. Reduction modulo 4 gives that x_{n_0} is odd. By Proposition 1.1.3, $x_{n_0} = x_{2n_1} = 2x_{n_1}^2 - 1$. Corollary 1.3.2 shows that there are numbers $a, b \in \mathbb{N}_0$ such that $a^2 - 2b^2 = 1$ and

$$2x_{n_1}^2 - 1 = x_{n_0} = 2a^2 - 1 \pm 2ab\,.$$

Hence $x_{n_1}^2 = a(a \pm b)$. Since a, b are coprime, so are $a, a \pm b$, and by PP1 (Proposition 1.2.2) the number a is a square. By Proposition 1.3.3 we have $a = 1$. Thus $b = 0$, $x_n = x_{n_0} = 1$ and $x = \pm 1, y = 0$. □

Theorem 1.3.5 (Euler, 1737) *The only integral solutions of the Diophantine equation*

$$x^2 - y^3 = 1$$

are $\langle \pm 3, 2 \rangle$, $\langle \pm 1, 0 \rangle$ *and* $\langle 0, -1 \rangle$.

Proof. (Klazar) Let $x, y \in \mathbb{Z}$ be such that $x^2 - y^3 = 1$. Then

$$x^2 = (y+1) \cdot (y^2 - y + 1) = (y+1) \cdot ((y+1)(y-2) + 3)\,.$$

Since $y^2 - y + 1 \geq 0$, we have $y + 1 \geq 0$. Also, $\gcd(y+1, y^2 - y + 1) \in \{1, 3\}$. If the gcd is 1 we have by PP1 (Proposition 1.2.2) that $y + 1$ and $y^2 - y + 1$ are squares. Thus $4y^2 - 4y + 4 = (2a)^2$ for some $a \in \mathbb{N}_0$. We get that

$$3 = (2a - 2y + 1)(2a + 2y - 1)\,.$$

Hence $\langle a, y\rangle = \langle \pm 1, 1\rangle$ or $\langle \pm 1, 0\rangle$. For $y = 1$ the number $y + 1$ is not a square and for $y = 0$ we get the solution $\langle \pm 1, 0\rangle$.

Let $\gcd(y+1, y^2 - y + 1) = 3$. By PP2 (Proposition 1.2.3) there are numbers $a, b \in \mathbb{N}_0$ such that

$$y + 1 = 3a^2 \;\text{ and }\; y^2 - y + 1 = 3b^2\,.$$

Thus $3(2b)^2 - (2y - 1)^2 = 3$ and $2y - 1 = 3Y$ for some $Y \in \mathbb{Z}$. With $X = 2b$ ($\in \mathbb{N}_0$) we get

$$X^2 - 3Y^2 = 1 \;\text{ and }\; Y = 2a^2 - 1\,.$$

The triple $\langle X, Y, a\rangle = \langle 2, -1, 0\rangle$ solves this system. We get $y = -1$ and the solution $\langle 0, -1\rangle$.

Thus we can assume that $Y \geq 0$. We look for a number $n \in \mathbb{N}_0$ such that $Y = y_n = 2a^2 - 1$, where $a \in \mathbb{N}_0$ and y_n is as in Proposition 1.1.2. Since y_n is odd, so is n. By Proposition 1.1.3 we have

$$2a^2 - 1 = y_n = y_{2m+1} = 2x_m y_{m+1} - 1,\; m \in \mathbb{N}_0\,.$$

Thus

$$a^2 = x_m y_{m+1}\,.$$

We have

$$\gcd(x_m,\, y_{m+1}) = \gcd(x_m,\, x_m + 2y_m) \in \{1,\, 2\}\,.$$

If $\gcd(x_m, y_{m+1}) = 1$, by PP1 (Proposition 1.2.2) the number x_m is a square. Theorem 1.3.4 gives $x_m = 1$. Thus $m = 0$, $n = 1$, $y_n = Y = 1$ and $y = 2$. We get the solution $\langle \pm 3, 2\rangle$.

Finally, let $\gcd(x_m, y_{m+1}) = 2$. By PP2 (Proposition 1.2.3), $y_{m+1} = 2c^2$ for some $c \in \mathbb{N}_0$. By Proposition 1.1.3,

$$2c^2 = y_{m+1} = y_{2k} = 2x_k y_k,\; k \in \mathbb{N}\,.$$

Hence $c^2 = x_k y_k$. Since x_k, y_k are coprime, by PP1 (Proposition 1.2.2) the number x_k is a square. Theorem 1.3.4 shows that it is not possible because $k \geq 1$. We do not get any more solutions of $x^2 - y^3 = 1$, and the proof is complete. □

This was the 1989 resolution of $x^2 - y^3 = 1$ in [18]. In 2003, a similar resolution was obtained by Ch. Notari in [29].

1.4 Modern completion of Euler's argument

We give a modern version of Euler's resolution of the equation $x^2 - y^3 = 1$ in the domain of fractions. We follow (and complete) the write-up [9] of Conrad. First we resolve an auxiliary Diophantine equation.

Theorem 1.4.1 *The only triple $\langle x, y, z\rangle \in \mathbb{N}^3$ such that $(x, y) = 1$, $(3, x) = 1$ and*

$$x^4 - 3x^2y^2 + 3y^4 = z^2\,,$$

is $\langle 1, 1, 1\rangle$. Said equivalently, the only coprime numbers $u, v \in \mathbb{N}$ such that $(3, u) = 1$ and that all three numbers

$$u,\ v\ \textit{and}\ u^2 - 3uv + 3v^2$$

are squares, are $u = v = 1$.

Proof. (Conrad) First, we show that in the latter problem, if $v = 1$ then $u = 1$. Indeed, since $u^2 - 3uv + 3v^2$ is a square, there is an $a \in \mathbb{Z}$ such that

$$u^2 - 3u + 3 = a^2\ \text{ and }\ (2a)^2 - (2u - 3)^2 = 3\,.$$

Thus $a = \pm 1$ and $u = 1$ or 2. Since $u = 2$ is not a square, $u = 1$.

We therefore assume that $u, v \in \mathbb{N}$ and $w \in \mathbb{Z}$ are numbers such that $(u, v) = 1$, $(3, u) = 1$, u and v are squares,

$$u^2 - 3uv + 3v^2 = w^2\,,$$

$v > 1$ and that v is the minimum possible (with respect to the stated properties). We obtain a contradiction and show that no such triple $\langle u, v, w\rangle$ in fact exists.

Thus $(3, w) = 1$ and we may select the sign of w so that $w \equiv -u \pmod 3$. Let $r := \frac{w-u}{v}$ $(\in \mathbb{Q})$, so that $u + rv = w$. By the choice of w we have $r \neq 0$. Let $r = \frac{m}{n}$ be in lowest terms, so that $m \in \mathbb{Z}$, $n \in \mathbb{N}$ and $(m, n) = 1$. We see that $m \mid (w - u)$, $n \mid v$ and $(3, m) = 1$. Substituting $w = u + rv$ in the previous displayed equation we get

$$u^2 - 3uv + 3v^2 = u^2 + 2urv + r^2v^2\ \text{ and }\ (3 - r^2)v^2 = (2r + 3)uv\,.$$

We see that $2r + 3 \neq 0$. Dividing by $v^2(2r + 3)$ and substituting $r = \frac{m}{n}$ we get

$$\frac{u}{v} = \frac{3n^2 - m^2}{n(2m + 3n)}\,.$$

We show that the fraction on the right-hand side is in lowest terms. From $(m, n) = 1$ we get that n is coprime with $3n^2 - m^2$. To show that $3n^2 - m^2$ and $2m + 3n$ are coprime, we argue by contradiction. Suppose that a prime p divides $3n^2 - m^2$ and $2m + 3n$. Then $m^2 \equiv 3n^2$ and $2m \equiv -3n$ modulo p. Squaring the second congruence and comparing it with the first we get $4m^2 \equiv 3m^2$ and

$12n^2 \equiv 9n^2$. Thus p divides both m^2 and $3n^2$. Since m and n are coprime, $p = 3$ and p divides m, which is a contradiction.

Thus

$$u = \varepsilon(3n^2 - m^2) \text{ and } v = \varepsilon n(2m + 3n),\ \varepsilon \in \{-1,\, 1\}\,.$$

Modulo 3, $u \equiv -\varepsilon m^2 \equiv -\varepsilon$. Since u is a square, we get that $\varepsilon = -1$. Hence

$$u = m^2 - 3n^2 \text{ and } v = -n(2m + 3n)\,.$$

Since u is a square, we have

$$m^2 - 3n^2 = k^2,\ k \in \mathbb{Z}\,.$$

Thus $(3, k) = 1$ and we select the sign of k so that $k \equiv -m$ modulo 3.

Let $s = \frac{k-m}{n}$ $(\in \mathbb{Q})$, so that $m + sn = k$. It follows from the choice of k that $s \neq 0$. Let $s = \frac{u'}{v'}$ be in lowest terms, so that $u' \in \mathbb{Z}$, $v' \in \mathbb{N}$ and $(u', v') = 1$. We see that $u' \mid (k - m)$, $v' \mid n$ and $(3, u') = 1$. Substituting $k = m + sn$ in the previous displayed equation we get

$$m^2 - 3n^2 = m^2 + 2mns + s^2n^2 \text{ and } 2mns = -(3 + s^2)n^2\,.$$

We know that $sn \neq 0$. Dividing by sn^2 and substituting $s = \frac{u'}{v'}$ we get

$$\frac{2m}{n} = -\frac{3 + s^2}{s} \text{ and } v = -n^2\Big(\frac{2m}{n} + 3\Big) = n^2 \cdot \frac{(u')^2 - 3u'v' + 3(v')^2}{u'v'}\,.$$

Since v is a square, multiplying by $(u'v')^2$ we get that

$$u' \cdot v' \cdot \big((u')^2 - 3u'v' + 3(v')^2\big)$$

is a square. Since $(u', v') = 1$ and $(3, u') = 1$, the three displayed factors are pairwise coprime and by PP1 (Proposition 1.2.2) all three are squares; note that $v' > 0$ and $(u')^2 - 3u'v' + 3(v')^2 > 0$, hence also $u' > 0$.

We show that $0 < v' \leq v$. We have

$$\frac{v}{n} = \frac{n\big((u')^2 - 3u'v' + 3(v')^2\big)}{u'v'}\,.$$

Now $n \mid v$, and u' and v' are coprime with $(u')^2 - 3u'v' + 3(v')^2$. Thus $u'v' \mid n$ and $u'v' \mid v$. Hence $0 < u'v' \leq v$ and $0 < v' \leq v$. The minimality of v implies two cases: either $v' = 1$ or $v' = v$. We show that both lead to the contradiction that $v = 1$.

Case 1 when $v' = 1$. As we know from the beginning, $u' = 1$. Thus $s = \frac{u'}{v'} = 1$, $k = m + sn = m + n$, $m^2 - 3n^2 = k^2 = (m + n)^2$ and $m = -2n$. So $r = \frac{m}{n} = -2$ and $w = u + rv = u - 2v$. We get

$$u^2 - 3uv + 3v^2 = (u - 2v)^2 \text{ and } uv = v^2\,.$$

Hence $(u-v)v=0$ and $u=v$. Since $(u,v)=1$, we get the contradiction that $v=1$.

Case 2 when $v'=v$**.** Thus $u'=1$. We have $s=\frac{k-m}{n}=\frac{u'}{v'}=\frac{1}{n}$. Since $n\,|\,v$ and $v'\,|\,n$, we get $v=v'=n$ and $k=m+1$. Then $m^2-3n^2=k^2=m^2+2m+1$ and $2m+1=-3n^2$. But from

$$n=v=-n(2m+3n)$$

we get that $2m+3n=-1$ and $2m+1=-3n$. Thus $-3n^2=-3n$ and $n=v=1$, which is a contradiction. □

In the previous proof we followed [9], but we corrected/completed the conclusion of the proof; [9] misses case 1.

From the previous theorem we deduce the main result of this section

Theorem 1.4.2 (Euler, 1737) *The only rational solutions* $x,y\in\mathbb{Q}$ *of the equation*

$$x^2-y^3=1$$

are the pairs $\langle\pm3,2\rangle$, $\langle\pm1,0\rangle$ *and* $\langle0,-1\rangle$.

Proof. (Conrad) Let $x,y\in\mathbb{Q}$ be such that $x^2-y^3=1$. Since $x^2, y^2-y+1=(y-\frac{1}{2})^2+\frac{3}{4}\geq0$, from

$$x^2=y^3+1=(y+1)(y^2-y+1)$$

we deduce that $y\geq-1$. As $y=-1$ yields the solution $\langle0,-1\rangle$, we assume from now on that $y>-1$.

Let $y=\frac{a}{b}$ with coprime $a\in\mathbb{Z}$ and $b\in\mathbb{N}$. From $y>-1$ we get $a+b>0$. Since

$$x^2=y^3+1=\frac{b(a^3+b^3)}{b^4}\,,$$

$b(a^3+b^3)$ is a square. With $c=a+b$ $(\in\mathbb{N})$ we write

$$b(a^3+b^3)=b(a+b)(a^2-ab+b^2)=b\cdot c\cdot(c^2-3bc+3b^2)\,.$$

Case 1 when $(3,c)=1$**.** The three displayed factors are pairwise coprime and positive. By PP1 (Proposition 1.2.2) they are squares. Using Theorem 1.4.1 we get that $b=c=1$ and $a=0$. Thus $y=\frac{a}{b}=0$ and we get the solution $\langle\pm1,0\rangle$.

Case 2 when $3\,|\,c$**.** Let $c=3d$. From $(b,c)=1$ we get $(3,b)=1$ and $(b,d)=1$. Then

$$bc(c^2-3bc+3b^2)=9bd(b^2-3bd+3d^2)$$

is a square. Thus

$$b\cdot d\cdot(b^2-3bd+3d^2)$$

is a square. As before we deduce by means of PP1 (Proposition 1.2.2) and Theorem 1.4.1 that $b=d=1$. Thus $c=3d=3$, $a=c-b=2$ and $y=\frac{a}{b}=2$. We get the solution $\langle\pm3,2\rangle$. □

1.5 Wakulicz's resolution of $x^3 + y^3 = 2z^3$

Antoni Wakulicz (1902–1988) ([33])

Chapter 2

V. Lebesgue's theorem

In the second chapter, we tackle the second elementary case of Catalan's conjecture, that of equations

$$x^m - y^2 = 1$$

with odd $m \geq 3$ (for even m, it is a trivial problem). Section 2.1 contains results on p-adic order that we use later in Section 2.2, where we present the theorem of V. Lebesgue (1791–1875) that the only solution of the equation is $\langle 1, 0 \rangle$. For a biography of V. Lebesgue, see [22]. In Section 2.3 we prove in Theorem 2.3.2 that every Euclidean domain is UFD. In particular, $\mathbb{Z}[i]$ is UFD, which is needed for Lebesgue's proof. This theorem plays a more important role in the resolution of Catalan's conjecture than one might think. We show by means of it that the class numbers of the cyclotomic fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_5)$ are $h_3 = h_5 = 1$, which is a key result in Chapter 8. In Section 2.2 we follow [32, Chapter 2].

2.1 Properties of p-adic order

For a prime p and $\alpha \in \mathbb{Q}$, the p-adic order $\mathrm{ord}_p(\alpha)$ of α is $+\infty$ if $\alpha = 0$. For $\alpha \neq 0$, it is the unique $k \in \mathbb{Z}$ such that $\alpha = p^k \beta$ for some $\beta \in \mathbb{Q}$ with numerator and denominator coprime to p.

Proposition 2.1.1 *For every $\alpha, \beta \in \mathbb{Q}$, the following holds.*

1. $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$. *Here for $a, b \in \mathbb{Z} \cup \{+\infty\}$ we set $a + b := +\infty$ if a or b is $+\infty$.*

2. $\mathrm{ord}_p(\alpha + \beta) \geq \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta))$*, with equality if* $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$. *Here $+\infty > m$ for every $m \in \mathbb{Z}$.*

Proof. 1. If α or β is 0 then the equality holds, and we may assume that $\alpha, \beta \neq 0$. Let $\alpha = p^k \alpha_0$ and $\beta = p^l \beta_0$ in $\mathbb{Q}^*$ be two arbitrary fractions, where

$k = \mathrm{ord}_p(\alpha)$, $l = \mathrm{ord}_p(\beta)$ and the fractions α_0 and β_0 have numerators and denominators coprime to p. Then

$$\alpha\beta = p^{k+l}\alpha_0\beta_0 =: p^{k+l}\gamma$$

where $\gamma \in \mathbb{Q}^*$ has numerator and denominator coprime to p. Thus

$$\mathrm{ord}_p(\alpha\beta) = k + l = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)\,.$$

2. Again, if α or β is 0 then the claim holds. We take $\alpha, \beta \in \mathbb{Q}^*$ as in item 1 and assume without loss of generality that $k \leq l$. Then

$$k = \min(\mathrm{ord}_p(\alpha),\, \mathrm{ord}_p(\beta))$$

and

$$\alpha + \beta = p^k(\alpha_0 + p^{l-k}\beta_0) =: p^k\gamma\,.$$

If $k < l$ then γ can be written as a fraction with numerator and denominator coprime to p, so that $\mathrm{ord}_p(\alpha + \beta) = k$. If $k = l$ then γ can be written with denominator coprime to p, and it follows that $\mathrm{ord}_p(\alpha + \beta) \geq k$. □

Corollary 2.1.2 *If p is a prime and $\alpha_1, \ldots, \alpha_n$ are $n \geq 2$ fractions such that*

$$\mathrm{ord}_p(\alpha_n) < \mathrm{ord}_p(\alpha_i) \text{ for every } i \in [n-1]\,,$$

then $\sum_{j=1}^{n} \alpha_j \neq 0$.

Proof. Let $k := \min(\{\mathrm{ord}_p(\alpha_i)\colon\ i \in [n-1]\})$ $(\in \mathbb{Z} \cup \{+\infty\})$ and let $\alpha := \sum_{j=1}^{n-1} \alpha_j$. Applying repeatedly item 2 of Proposition 1 we get that $\mathrm{ord}_p(\alpha) \geq k$. Since $\mathrm{ord}_p(\alpha_n) < k$, we have $\mathrm{ord}_p(\alpha_n) < +\infty$ and

$$\mathrm{ord}_p\big(\textstyle\sum_{j=1}^{n} \alpha_j\big) = \mathrm{ord}_p(\alpha + \alpha_n) = \mathrm{ord}_p(\alpha_n) < +\infty\,.$$

Thus $\sum_{j=1}^{n} \alpha_j \neq 0$. □

2.2 V. Lebesgue's resolution of $x^m - y^2 = 1$

We work in the domain

$$\mathbb{Z}[i] = \langle \mathbb{Z}[i],\, 0,\, 1,\, +,\, \cdot,\, \rangle\,,$$

where the base set $\mathbb{Z}[i] = \{a + bi\colon\ a, b \in \mathbb{Z}\}$ is the set of complex numbers with both real and imaginary part integral.

Theorem 2.2.1 (V. Lebesgue, 1850) *Let $m \geq 3$ be an odd integer. The Diophantine equation*

$$x^m - y^2 = 1$$

has only the solution $\langle 1, 0\rangle$.

Proof. (V. Lebesgue) Let m be as stated and $a, b \in \mathbb{Z}$ with $b \neq 0$ be such that $a^m - b^2 = 1$. We derive a contradiction. If b is odd then $a^m \equiv 2$ modulo 4, which is impossible. Thus b is even, $b \neq 0$ and a is odd. In $\mathbb{Z}[i]$, we consider the factorization

$$a^m = (1+bi)(1-bi)\,.$$

The elements $1+bi$ and $1-bi$ are coprime: if $\alpha \in \mathbb{Z}[i]$ divides both $1+bi$ and $1-bi$, then $n = \alpha\overline{\alpha}$ ($\in \mathbb{N}$) divides, in $\mathbb{Z}$, the number $2 \cdot \overline{2} = 4$ and the odd number $(1+bi)(1-bi) = a^m$. Thus $n = 1$, α is a unit, and $1+bi$ and $1-bi$ are coprime. Since $\mathbb{Z}[i]$ is UFD (Corollary 2.3.3 in the next section), by PP1$'$ (Proposition 1.2.11) there exist an element $\alpha \in \mathbb{Z}[i]$, units $\epsilon, \epsilon' \in \mathbb{Z}[i]^\times$ and numbers $u, v \in \mathbb{Z}$ such that

$$1+bi = \epsilon\alpha^m = (\epsilon'\alpha)^m = (u+vi)^m \text{ and } 1-bi = \overline{\epsilon}(\overline{\alpha})^m = (\overline{\epsilon'\alpha})^m = (u-vi)^m\,,$$

because every unit in $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ (Proposition 2.3.4 in the next section) is an m-th power. Since m is odd, we have

$$2 = (u+vi)^m + (u-vi)^m = 2u \cdot \beta,\ \beta \in \mathbb{Z}[i]\,,$$

and deduce that $u = \pm 1$. We exclude the possibility $u = -1$. Since $(1+v^2)^m = (u^2+v^2)^m = 1+b^2$ is odd, the number v is even. From

$$1+bi = (u+vi)^m = \textstyle\sum_{j=0}^{m} \binom{m}{j} u^{m-j}(vi)^j \equiv u^m + mu^{m-1}vi \pmod 4$$

(congruence in $\mathbb{Z}[i]$) we deduce that $u^m \equiv 1$ modulo 4 (congruence in $\mathbb{Z}$), which excludes $u = -1$.

Thus $u + vi = 1 + vi$ with even and nonzero v (since $b \neq 0$). Comparing the real parts in $1 + bi = (1+vi)^m$ we get an identity in $\mathbb{Z}$,

$$1 = \textstyle\sum_{j=0}^{(m-1)/2} (-1)^j \binom{m}{2j} v^{2j}, \text{ or } -\binom{m}{2}v^2 + \sum_{j=2}^{(m-1)/2} (-1)^j \binom{m}{2j} v^{2j} = 0\,.$$

For $m = 3$ the last sum is empty (zero) and the equality is impossible as $v \neq 0$. For odd $m \geq 5$ we show that the equality does not hold by means of Corollary 2.1.2 and prime $p = 2$. We set $A = \binom{m}{2}v^2$ and $B_j = \binom{m}{2j} \cdot v^{2j}$ for $j = 2, 3, \ldots, \frac{m-1}{2}$, and show that $\mathrm{ord}_2(A) < \mathrm{ord}_2(B_j)$ for every j. Indeed,

$$B_j = A \cdot \tfrac{1}{j(2j-1)} \tbinom{m-2}{2j-2} v^{2j-2} =: A \cdot C_j$$

and $\mathrm{ord}_2(C_j) \geq 2j - 2 - \lfloor \log_2(j) \rfloor > 0$, so that by the additivity of $\mathrm{ord}_2(\cdot)$ (item 1 of Proposition 2.1.1) we have $\mathrm{ord}_2(A) = \mathrm{ord}_2(B_j) - \mathrm{ord}_2(C_j) < \mathrm{ord}_2(B_j)$. We get a contradiction □

2.3 Euclidean domains are UFD

We begin by reviewing Euclidean domains. A *well ordering* $\langle W, \prec \rangle$ is a linear order $\prec$ on a set W such that every nonempty set $V \subset W$ has the *minimum element* $m \in V$, an element such that $m \preceq x$ for every $x \in V$. Minima are unique.

Definition 2.3.1 (Euclidean domain) *A domain*

$$R = \langle R,\, 0_R,\, 1_R,\, +,\, \cdot\rangle$$

is called Euclidean if there is a well ordering $\langle W, \prec\rangle$ and a function $f\colon R^* \to W$ such that

$$\forall\, a,\, b \in R,\, b \ne 0_R\, \exists\, c,\, d \in R\, \big(a = b \cdot c + d \wedge (d = 0_R \vee f(d) \prec f(b))\big)\,.$$

Note that the last disjunction is an exclusive or. For instance, the domain of integers $\mathbb{Z}$ is Euclidean: $\langle W, \prec\rangle$ is $\langle \mathbb{N}, <\rangle$ and $f(n) = |n|$. One can often prove that a domain is UFD by using the next classical theorem.

Theorem 2.3.2 *Every Euclidean domain is* UFD*.*

Proof. Let R be a Euclidean domain with a well ordering $\langle W, \prec\rangle$ and a map $f\colon R^* \to W$ as in Definition 2.3.1.

Existence of irreducible factorizations. We show that every $x \in R^* \setminus R^\times$ is a product of irreducibles. Suppose for the contrary that the set

$$A \subset R^* \setminus R^\times$$

of elements that are not products of irreducibles is nonempty. Let $a \in R^*$ be such that a has a divisor $b \in A$, and that the value $f(a)$ is $\prec$-minimum among all such values in W. Thus $a = bc$ where $b \in A$ and $c \in R^*$. Since b is not irreducible, $b = de$ with $d, e \in R^* \setminus R^\times$. But $b \in A$ and hence d or e is in A. We assume that $d \in A$, the case with $e \in A$ is similar. Thus $a = d(ec)$ where $d \in A$ and $ec \in R^* \setminus R^\times$ (because $e \in R^* \setminus R^\times$). This means by Proposition 1.2.4 that a does not divide d, and if we divide d by a with a remainder we get

$$d = ag + h \text{ where } g \in R,\, h \in R^* \text{ and } f(h) \prec f(a)\,.$$

Since d divides a, it divides h too. So $d \in A$ and divides h, and $f(h) \prec f(a)$. This contradicts the choice of a.

Bachet's identity. We prove that if $a, b \in R$ are coprime, then there exist $c, d \in R$ such that $ca + db = 1_R$. We consider the set

$$I = \{ca + db:\ c,\, d \in R\}\ (\subset R)\,,$$

which is the ideal in R generated by the elements a, b. Let $e \in I \setminus \{0_R\}$ have $\prec$-minimum value $f(e)$. Clearly, $I \ne \emptyset$. Note that $I \ne \{0_R\}$ because we do not have $a = b = 0_R$, the element 0_R is not a unit and therefore $0_R, 0_R$ are not coprime. We show that e divides every $x \in I$. Indeed, we express any $x \in I$ as $x = ec + d$ where $c, d \in R$ and $d = 0_R$ or $f(d) \prec f(e)$. Due to $d = x - ec \in I$ we have $d = 0_R$. Thus e divides every element of I and since $a, b \in I$ and are coprime, $e \in R^\times$. It follows that $1_R \in I$, there exist $c, d \in R$ such that $1_R = ca + db$.

Primes are prime divisors. We show that if $a, b, c \in R$, $a\,|\,bc$ and $a \in R^{\mathrm{ir}}$, then $a\,|\,b$ or $a\,|\,c$. Suppose that $a, b, c \in R$ and that a is irreducible, divides bc

but does not divide b. Then a, b are coprime and by the second step there are $d, e \in R$ such that

$$da + eb = 1_R\,.$$

We multiply it by c and get $dac + ebc = c$. Hence a divides c.

Finally, we prove that in R every element $a \in R^*$ has a unique irreducible factorization X ($\subset \mathbb{I} \times \mathbb{N}$). It means to prove that if

$$a_1 a_2 \dots a_k \sim b_1 b_2 \dots b_l\,,$$

where $a_i, b_i \in R^{\mathrm{ir}}$ and $k, l \in \mathbb{N}$, then always $k = l$ and there always exists a bijection $f\colon [k] \to [l]$ such that

$$a_i \sim b_{f(i)},\ i \in [k]\,.$$

Suppose that the above displayed equality is a shortest counterexample. Then $k, l \geq 2$ and, by the previous step, $a_k \sim b_m$ for some $m \in [l]$. Canceling a_k and b_m we get that

$$a_1 a_2 \dots a_{k-1} \sim b_1 b_2 \dots b_{m-1} b_{m+1} \dots b_l\,.$$

Now we have $k - 1 = l - 1$ and a map $g\colon [k-1] \to [l] \setminus \{m\}$ with the above property. But then $k = l$ and we easily extend g to $f\colon [k] \to [l]$ so that f has the above property. We get a contradiction and deduce that no counterexample actually exists. □

Corollary 2.3.3 *The domain* $\mathbb{Z}[i]$ *is Euclidean and hence* UFD.

Proof. Recall that for $z = u + vi$ ($\in \mathbb{C}$), the norm (absolute value) of z is $|z| = \sqrt{z \cdot \overline{z}} = \sqrt{u^2 + v^2}$. We have $|z \cdot z'| = |z| \cdot |z'|$ and $|z + z'| \leq |z| + |z'|$. We take the well ordering $\langle \mathbb{N}, < \rangle$, i.e. the usual linear order on natural numbers, and the map

$$f\colon \mathbb{Z}[i]^* \to \mathbb{N},\ f(z) = |z|^2\,.$$

Let $z, z' \in \mathbb{Z}[i]$ with $z' \neq 0$. We define $\alpha, \beta \in \mathbb{Q}$ by

$$\frac{z}{z'} = \alpha + \beta i\,.$$

Let $a, b \in \mathbb{Z}$ be such that $|a - \alpha| \leq \frac{1}{2}$ and $|b - \beta| \leq \frac{1}{2}$. Let $w := a + bi$ and $w' = z - z' \cdot w$. Then $z = z' \cdot w + w'$, of course, and

$$f(w') = |w'|^2 = |z'|^2 \cdot \left|\frac{z}{z'} - w\right|^2 \leq f(z')\Big(\frac{1}{4} + \frac{1}{4}\Big) < f(z')\,.$$

□

Proposition 2.3.4 $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$.

Proof. Let $f(z) = |z|^2 \colon \mathbb{Z}[i]^* \to \mathbb{N}$ be the map in the previous proof. If $z = a + bi, z' \in \mathbb{Z}[i]$ are such that $zz' = 1$, then

$$1 = f(1) = f(z)f(z') = (a^2 + b^2)f(z')$$

and $a^2 + b^2 = 1$. Thus $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$, and we get the stated units. □

Chapter 3

Chao Ko's theorem

The third chapter is devoted to the last elementary case of Catalan's conjecture, that of the equation

$$x^2 - y^q = 1$$

in which $q \geq 5$ is a prime number. In 1965, the Chinese mathematician Chao Ko (1910–2002) ([17]) proved in [19] that for every q the only solutions are $\langle \pm 1, 0 \rangle$ and $\langle 0, -1 \rangle$. Another well-known mathematical result due to Chao Ko is the Erdős–Ko–Rado theorem in extremal combinatorics [10, 11].

Section 3.1 contains two auxiliary lemmas. In Section 3.2 we present a resolution of the equation due to E. Z. Chein [7]. In this chapter we follow [32, Chapter 3].

3.1 Two lemmas

Lemma 3.1.1 *Let q be a prime number and $a, b \in \mathbb{Z}$, $a \neq b$, be coprime numbers. Then*

$$d := \gcd\big(\tfrac{a^q - b^q}{a - b},\, a - b\big) = \gcd\big(\textstyle\sum_{i=0}^{q-1} a^i b^{q-1-i},\, a - b\big)$$

divides q.

Proof. By the binomial theorem, $\frac{a^q-b^q}{a-b} = \frac{(a-b+b)^q - b^q}{a-b}$ equals

$$\textstyle\sum_{i=1}^{q} \binom{q}{i}(a-b)^{i-1} b^{q-i} = qb^{q-1} + \sum_{i=2}^{q} \binom{q}{i}(a-b)^{i-1} b^{q-i}\,.$$

Thus $d \mid qb^{q-1}$. Since a, b are coprime, so are $b, a - b$ and $(d, b) = 1$. By PP0 (Proposition 1.2.1) the number d divides q. □

Lemma 3.1.2 *Let $q \in \mathbb{N}$ with $q \geq 3$ be odd and x, y be nonzero integers such that $x^2 - y^q = 1$. Then y is even and replacing x with $-x$ if necessary, we have expressions*

$$x - 1 = 2^{q-1} a^q \text{ and } x + 1 = 2b^q\,,$$

where $a, b \in \mathbb{Z}$ are coprime and b is odd.

Proof. In the factorization $(x-1)(x+1) = y^q$ the two factors are coprime or their gcd is 2. In the former case we get by PP1 (Proposition 1.2.2) two q-th powers differing by 2. The only such powers are -1 and 1, and $x = 0$. Since this is impossible, we see that $\gcd(x-1, x+1) = 2$ and y is even. Hence x is odd. Changing the sign of x we may assume that $\frac{x+1}{2}$ is odd. Applying PP2 (Proposition 1.2.3) we get the stated expressions. □

3.2 Chein's resolution of $x^2 - y^q = 1$

Proposition 3.2.1 *Let $q \geq 3$ be prime and x, y be nonzero integers such that $x^2 - y^q = 1$. Then q divides x.*

Proof. We may assume that $y \in \mathbb{N}$. We assume that $\neg(q \mid x)$ and obtain a contradiction. By Lemma 3.1.1, in the factorization

$$x^2 = (y+1) \cdot \tfrac{y^q-(-1)}{y-(-1)}$$

the gcd of the two factors divides q. By the assumption on x they are therefore coprime. By PP1 (Proposition 1.2.2) we have $y + 1 = u^2$ for $u \in \mathbb{N}$. Since y is even, u is odd. From the equalities

$$x^2 - y \cdot \left(y^{(q-1)/2}\right)^2 = 1 \text{ and } u^2 - y \cdot 1^2 = 1$$

we see that $\langle x, y^{(q-1)/2}\rangle$ and $\langle u, 1\rangle$ are two solutions of Pell equation

$$X^2 - yY^2 = 1\,.$$

(Since $y = u^2 - 1 \geq 3$ and is not a square, it is really a Pell equation.) It is clear that $\langle u, 1\rangle \in \mathbb{N}^2$ is the minimal solution. By Proposition 1.1.1 there is an $m \in \mathbb{N}$ such that in the domain $\mathbb{Z}[\sqrt{y}]$ we have the equality

$$x + y^{(q-1)/2}\sqrt{y} = \left(u + \sqrt{y}\right)^m.$$

Thus in $\mathbb{Z}[\sqrt{y}]$ we have the congruence

$$x \equiv u^m + mu^{m-1}\sqrt{y} \pmod{y}\,.$$

Hence, in $\mathbb{Z}$, the number y divides mu^{m-1}. But y is even and u is odd, so m is even. In $\mathbb{Z}[\sqrt{y}]$ we therefore have equality

$$x + y^{(q-1)/2}\sqrt{y} = \left(u^2 + y + 2u\sqrt{y}\right)^{m/2},$$

from which we get the congruence $x + y^{(q-1)/2}\sqrt{y} \equiv y^{m/2} \pmod{u}$. Thus in $\mathbb{Z}$ the number u divides $y^{(q-1)/2}$. But $y+1 = u^2$, so y, u are coprime and $u = \pm 1$. Hence $y = 0$, in contradiction with the assumption. □

Proposition 3.2.2 *Let $q \geq 3$ be prime and x, y be nonzero integers such that $x^2 - y^q = 1$. Then $x \equiv \pm 3 \pmod{q}$.*

Proof. Let q, x and y be as stated. Changing the sign of x if necessary, by Lemma 3.1.2 we have coprime $a, b \in \mathbb{Z}$ with odd b such that $x - 1 = 2^{q-1}a^q$ and $x + 1 = 2b^q$. Hence

$$b^{2q} - (2a)^q = \Big(\frac{x+1}{2}\Big)^2 - 2(x-1) = \Big(\frac{x-3}{2}\Big)^2$$

and

$$(b^2 - 2a) \cdot \Big(\frac{b^{2q} - (2a)^q}{b^2 - 2a}\Big) = \Big(\frac{x-3}{2}\Big)^2 .$$

The numbers $2a, b^2$ are coprime and by Lemma 3.1.1 the gcd of the last two factors divides q.

If it is q then $x \equiv 3 \pmod{q}$ and for the original x, before the possible change of sign, we have $x \equiv \pm 3 \pmod{q}$. We assume for the contrary that the gcd is 1. Hence we assume that $b^2 - 2a$ and $\frac{b^{2q}-(2a)^q}{b^2-2a}$ are coprime numbers. From $b^{2q} - (2a)^q \geq 0$ (it is a square) we get $b^2 - 2a \geq 0$ ($f(X) = X^q$ is an increasing function) and by PP1 (Proposition 1.2.2) there is a $c \in \mathbb{N}$ such that $b^2 - 2a = c^2$. Since $y \neq 0$, also $a \neq 0$ and $c^2 \neq b^2$. The nearest squares to b^2 different from it are $(b \pm 1)^2$. Thus $2|a| = |b^2 - c^2| \geq 2|b| - 1$ and hence $|a| \geq |b|$. On the other hand,

$$|a|^q = \frac{|x-1|}{2^{q-1}} \leq \frac{|x-1|}{16} < \frac{|x+1|}{2} = |b|^q .$$

For $x \in \mathbb{Z}$ the crucial strict inequality $|x - 1| < 8|x + 1|$ does not hold only for $x = -1$. This value of x is excluded by the fact that $y \neq 0$. Hence also $|a| < |b|$ and we have a contradiction. □

Theorem 3.2.3 (Chao Ko, 1965) *Let $q \geq 5$ be a prime number. The Diophantine equation*

$$x^2 - y^q = 1$$

has only the solutions $\langle \pm 1, 0\rangle$ and $\langle 0, -1\rangle$.

Proof. (Chein) Suppose that q is as stated and $x, y \in \mathbb{Z}^*$ satisfy $x^2 - y^q = 1$. By Proposition 3.2.1 we have $x \equiv 0 \pmod{q}$. Also $x \equiv \pm 3 \pmod{q}$ by Proposition 3.2.2. For $q > 3$ these congruences are contradictory. □

Chapter 4

Two relations of Cassels

In Sections 4.2 and 4.3 we deduce two divisibility relations for hypothetical nonzero solutions $x, y \in \mathbb{Z}^*$ of the equation

$$x^p - y^q = 1\,,$$

where $p > q > 2$ are primes, namely that q divides x and p divides y. Since we eventually show that no such numbers x and y exist, these are properties of non-existing objects. These relations are important in Mihăilescu'c proof, and they were obtained in [3, 4] by the British mathematician John W. S. Cassels (1922–2015) ([2]). Section 4.1 contains auxiliary results needed to prove both relations, and in Section 4.4 we obtain their corollaries. In this chapter we follow [32, Chapter 6].

4.1 Five lemmas

Lemma 4.1.1 *For $u \in \mathbb{R}$ the following hold.*

1. *If $u \ge 1$ then the function*

$$f(x) = \big(u^x + 1\big)^{1/x} \colon (0,\, +\infty) \to (0,\, +\infty)$$

decreases.

2. *If $u > 1$ then the function*

$$f(x) = \big(u^x - 1\big)^{1/x} \colon (0,\, +\infty) \to (0,\, +\infty)$$

increases.

Proof. 1. We have

$$f'(x) = f(x)\Big(\frac{u^x \log u}{x(u^x + 1)} - \frac{\log(u^x + 1)}{x^2}\Big)$$

and $(\cdots) < 0$ because $xu^x \log u = u^x \log(u^x) < (u^x+1)\log(u^x+1)$.

2. Similarly,

$$f'(x) = f(x)\Big(\frac{u^x \log u}{x(u^x-1)} - \frac{\log(u^x-1)}{x^2}\Big)$$

and $(\cdots) > 0$ because $xu^x \log u = u^x \log(u^x) > (u^x-1)\log(u^x-1)$. □

Definition 4.1.2 **($F_{m,n}(X)$)** *Let $m, n \in \mathbb{N}$ with odd n. We define the function*

$$F_{m,n}(X) = \big((1+X)^m - X^m\big)^{1/n} \colon \mathbb{R} \to \mathbb{R}\,.$$

Lemma 4.1.3 *Let $l, m, n \in \mathbb{N}$ and $l < m$. Then*

$$F_{m,\,n}(X) = \sum_{j=0}^{l} \binom{m/n}{j} X^j + o(X^l) \quad (X \to 0)\,.$$

Proof.

□

Lemma 4.1.4 *Let $a \in \mathbb{Z}$, $m, d \in \mathbb{N}$, p be a prime with $(p, d) = 1$ and let*

$$P_m(a,\, d) := \prod_{j=0}^{m-1} (a + jd)\,.$$

Then

$$\mathrm{ord}_p\big(P_m(a,\, d)\big) = \sum_{j \ge 1} \Big(\Big\lfloor \frac{m}{p^j} \Big\rfloor + \varepsilon_j \Big), \ \ \varepsilon_j \in \{0,\, 1\}\,.$$

If $P_m(a, d) = m!$ then $\varepsilon_j = 0$ for every j.

Proof. Let a, m, d and p be as stated. For $j \in \mathbb{N}$ let m_j ($\in \mathbb{N}_0$) be the number of multiples of p^j among the numbers $a + id$, $i = 0, 1, \ldots, m-1$. A double counting argument shows that

$$\mathrm{ord}_p\big(P_m(a,\, d)\big) = \sum_{j \ge 1} m_j\,.$$

If integers i and i' are non-congruent modulo p^j, then so are $a + id$ and $a + i'd$. Hence if $I \subset \{0, 1, \ldots, m-1\}$ is an interval with length $|I| \le p^j$, then for at most one $i \in I$ the number $a + id$ is divisible by p^j, and if $|I| = p^j$ then there is exactly one such number. Thus

$$m_j = \Big\lfloor \frac{m}{p^j} \Big\rfloor + \varepsilon_j$$

with ε_j equal to 0 or 1, because we have the partition

$$\{0,\,1,\,\ldots,\,m-1\} = I_1 \cup I_2 \cup \cdots \cup I_k \cup I_0$$

into intervals $I_1 < I_2 < \cdots < I_k < I_0$ such that $k = \lfloor m/p^j \rfloor$, $|I_i| = p^j$ for $i > 0$ and $|I_0| < p^j$. This proves the first claim. □

Lemma 4.1.5 *Let q be prime, $a \in \mathbb{Z}$ with $(q,a) = 1$ and $k \in \mathbb{N}_0$. Then there exists $b \in \mathbb{Z}$ with $(q,b) = 1$ such that*

$$\binom{a/q}{k} = \frac{b}{q^{k+\mathrm{ord}_q(k!)}}\,.$$

4.2 The relation $q \,|\, x$

The following theorem was proven by Cassels in [3]. We follow [32, Chapter 6].

Theorem 4.2.1 (Cassels, 1953) *If $p > q > 2$ are primes and $x, y \in \mathbb{Z}^*$ are such numbers that*

$$x^p - y^q = 1\,,$$

then q divides x.

Proof. Suppose that p, q, x and y are as stated and that $\neg(q \,|\, x)$. Then by Lemma 3.1.1 the two factors in

$$(y+1)\cdot\frac{y^q+1}{y+1} = x^p$$

are coprime. By PP1 (Proposition 1.2.2 we have $y+1 = b^p$ with $b \in \mathbb{Z}$. Since $x \neq 0$, also $b \neq 0$. Hence

$$x^p - (b^p-1)^q = 1\,.$$

We show that this equality cannot hold.

For $X \in \mathbb{R}$, we consider the function

$$g(X) = X^p - (b^p-1)^q$$

and show that $g(X) \neq 1$ for every $X \in \mathbb{Z}$. Suppose that $b > 0$. Since $y \neq 0$, we have $b \geq 2$. Then

$$g(b^q) = \sum_{j=0}^{q-1} b^{jp}(b^p-1)^{q-1-j} \geq q > 1$$

and

$$g(b^q-1) = (b^q-1)^p - (b^p-1)^q < 0\,,$$

because, since $q < p$, by item 2 of Lemma 4.1.1 we have

$$\big((b^q-1)^p\big)^{\frac{1}{pq}} = (b^q-1)^{\frac{1}{q}} < (b^p-1)^{\frac{1}{p}} = \big((b^p-1)^q\big)^{\frac{1}{pq}}\,.$$

The function $g(X)$ increases on $\mathbb{R}$ and we see that there is no $X \in \mathbb{Z}$ with $g(X) = 1$.

Suppose that $b < 0$, thus $b \leq -1$. Then, similarly,

$$g(b^q) = \sum_{j=0}^{q-1} (b^p)^j (b^p-1)^{q-1-j} \geq q > 1$$

(each summand has sign $(-1)^{q-1} = 1$) and

$$g(b^q-1) = -((-b)^q+1)^p - ((-b)^p+1)^q < 0\,,$$

because, since $q < p$, by part 1 of Lemma 4.1.1 it holds that

$$\big(((-b)^q+1)^p\big)^{\frac{1}{pq}} = ((-b)^q+1)^{\frac{1}{q}} > ((-b)^p+1)^{\frac{1}{p}} = \big(((-b)^p+1)^q\big)^{\frac{1}{pq}}\,.$$

Again, $g(X)$ increases on $\mathbb{R}$ and we see that there is no $X \in \mathbb{Z}$ with $g(X) = 1$. We reached a contradiction and see that q divides x. □

4.3 The relation $p \,|\, y$

The following theorem was proved by Cassels in [4]. We follow [32, Chapter 6].

Theorem 4.3.1 (Cassels, 1960) *If $p > q > 2$ are primes and $x, y \in \mathbb{Z}^*$ are such numbers that*

$$x^p - y^q = 1\,,$$

then p divides y.

Proof. Let p, q, x and y be as stated and let $(p, y) = 1$. By Lemma 3.1.1, the two factors in

$$(x-1) \cdot \frac{x^p-1}{x-1} = y^q$$

are coprime. We deduce from this a contradiction. By PP1 (Proposition 1.2.2), $x - 1 = a^q$ with $a \in \mathbb{Z}$. Clearly $a \neq 0$. Thus $y^q = (a^q+1)^p - 1$ and with $F_{p,q}(X)$ in Definition 4.1.2 we express y as

$$y = a^p \cdot F_{p,q}(1/a^q)\,.$$

We set $m = \lfloor p/q \rfloor + 1$ (≥ 2), $D = q^{m+\mathrm{ord}_q(m!)}$ and

$$z = a^{mq-p} y - a^{mq} \cdot T_0^m(F_{p,q})(1/a^q) \;\; (\in \mathbb{Q})\,.$$

Using Lemmas 4.1.3 and 4.1.5 and the inequality $mq - p \geq 0$ (following from $m > \frac{p}{q}$) we see that

$$Dz = Da^{mq-p}y - \textstyle\sum_{k=0}^{m} D\binom{p/q}{k}a^{mq-qk} \in \mathbb{Z}\,.$$

We obtain a contradiction by proving that the integer $Dz \neq 0$ but at the same time $|Dz| < 1$. Non-vanishing of Dz follows from the non-divisibility $\neg(q \,|\, Dz)$: in the displayed expression for Dz all terms are divisible by q except for the summand with $k = m$, which by Lemma 4.1.5 is the integer $D\binom{p/q}{m}$ not divisible by q.

We show that $|Dz| < 1$. We have $z = a^{mq}\big(F_{p.q}(1/a^q) - T_0^m(F_{p.q})(1/a^q)\big)$. Since $x \neq 0$ but $q \,|\, x$ by Theorem 4.2.1, $a \neq 0, \pm 1$ and $|a| \geq 2$. We can use Lemma **??** with $X = 1/a^q$ and get the bound

$$|z| \leq \frac{|a|^{mq} \cdot |a|^{-(m+1)q}}{(1 - |a|^{-q})^2} = \frac{|a|^q}{(|a|^q - 1)^2} \leq \frac{1}{|a|^q - 2} \leq \frac{1}{|x| - 3}\,.$$

By Proposition **??**, $|x| \geq q^{p-1} + q$. Thus

$$|Dz| \leq q^{m + \mathrm{ord}_q(m!) - (p-1)}\,.$$

If the exponent is negative, we are done. And indeed, by Lemma **??**, the inequality $m < \frac{p}{q} + 1$ and since $p \geq 5$ and $q \geq 3$, it is negative:

$$\begin{array}{rcl} m + \mathrm{ord}_q(m!) - (p-1) & \leq & m\big(1 + \frac{1}{q-1}\big) - (p-1) \\ & < & \big(\frac{p}{q} + 1\big)\big(1 + \frac{1}{q-1}\big) - (p-1) \\ & = & \frac{3-(p-2)(q-2)}{q-1} \leq 0\,. \end{array}$$

□

4.4 Corollaries

Chapter 5

Mihăilescu's theorem, an outline of the proof

5.1 Theorems M0.95–M4

Catalan' conjecture claims that for integers $m, n \geq 2$ the only nonzero solutions $x, y \in \mathbb{Z}^*$ of the Diophantine equation

$$x^m - y^n = 1$$

occur for $m = 2$ and $n = 3$ as $\langle x, y \rangle = \langle \pm 3, 2 \rangle$. In the first three chapters, we described the resolution of the conjecture in the case when $m = 2$ or $n = 2$. It is clear that to prove the whole conjecture, it remains to show that for every two distinct odd primes p and q, the Diophantine equation

$$x^p - y^q = 1$$

has no nonzero solution. This is what P. Mihăilescu accomplished in 2004, and in the present chapter we outline his solution. We also describe the content of the remaining chapters of our book. Recall that if $x, y \in \mathbb{Z}$ and $m, n \in \mathbb{N}$ are odd, then

$$x^m - y^n = 1 \iff (-y)^n - (-x)^m = 1\,,$$

so that we may assume, if needed, that $p > q$.

In the first part of the chapter, we follow [32, Chapter 1], but we are more precise and clear about the assumptions in Theorems M1–M4. This pays off because then we can simplify the deduction of Theorem 5.1.1 from the four theorems compared to the argument given in [32, p. 5].

Theorem 5.1.1 (Mihăilescu, 2004) *If p and q are distinct odd primes, then the Diophantine equation*

$$x^p - y^q = 1$$

has no nonzero solution $x, y \in \mathbb{Z}^*$.

Theorems 5.1.1, 1.3.5 (or 1.4.2), 2.2.1 and 3.2.3 together prove Catalan's conjecture.

Theorem 5.1.1 follows from the next four Theorems M1–M4, all of which are due to P. Mihăilescu.

Theorem 5.1.2 (M1, [24]) *If $p > q > 2$ are primes such that $x^p - y^q = 1$ for some numbers $x, y \in \mathbb{Z}^*$, then*

$$p^{q-1} \equiv 1 \pmod{q^2} \ \textit{ and } \ q^{p-1} \equiv 1 \pmod{p^2}\,.$$

These congruences follow easily from the actual thing, which we dub as Theorem M0.95.

Theorem 5.1.3 (M0.95, [24]) *If $p > q > 2$ are primes such that $x^p - y^q = 1$ for some numbers $x, y \in \mathbb{Z}^*$, then*

$$p^2 \,|\, y \ \textit{ and } \ q^2 \,|\, x\,.$$

Theorem 5.1.4 (M2, [25]) *If $p, q \geq 7$ are distinct primes such that $x^p - y^q = 1$ for some numbers $x, y \in \mathbb{Z}^*$, then*

$$p \equiv 1 \pmod{q} \ \textit{ or } \ q \equiv 1 \pmod{p}\,.$$

This is the hardest theorem of M1–M4 to prove. The original theorem in [25] holds for the primes 3 and 5 as well, but the present slightly restricted version has simpler proof and suffices to establish Theorem 5.1.1.

Theorem 5.1.5 (M3, [26]) *If $p, q \geq 7$ are distinct primes such that $x^p - y^q = 1$ for some numbers $x, y \in \mathbb{Z}^*$, then*

$$p < 4q^2 \ \textit{ and } \ q < 4p^2\,.$$

Again, the original theorem in [26] holds for the primes 3 and 5 too.

Theorem 5.1.6 (M4, [26]) *If p and q are distinct odd primes and $p \in \{3, 5\}$ or $q \in \{3, 5\}$, then the Diophantine equation*

$$x^p - y^q = 1$$

has no nonzero solution $x, y \in \mathbb{Z}^*$.

In [26, 32] the theorem is proven for the larger set of primes $\{3, 5, 7, 11, \ldots, 41\}$, but this restricted version suffices for our purposes.

To deduce Theorem 5.1.1 from Theorems M1–M4 we need a simple lemma.

Lemma 5.1.7 *Let q be prime, $x \in \mathbb{Z}$, $x \equiv 1 \pmod{q}$ and $x^{q-1} \equiv 1 \pmod{q^2}$. Then $x \equiv 1 \pmod{q^2}$.*

Proof. We have $x = 1 + kq$ with $k \in \mathbb{Z}$. From

$$x^{q-1} = (1+kq)^{q-1} = 1 + \sum_{j=1}^{q-1} \binom{q-1}{j} (kq)^j \equiv 1 \pmod{q^2}$$

we deduce that $q^2 \mid (q-1)kq$. Thus $q \mid k$, as stated. □

Deduction of Theorem 5.1.1 from Theorems M1–M4. In view of theorem M4 (Theorem 5.1.6) we may assume that $p, q \geq 7$ are distinct primes such that $x^p - y^q = 1$ for some nonzero integers x and y. We deduce a contradiction. By Theorems M1 (Theorem 5.1.2), M2 (Theorem 5.1.4), Lemma 5.1.7 and the symmetry we have $p = 1+kq^2$ for some $k \in \mathbb{N}$. By Theorem M3 (Theorem 5.1.5), $k \in \{1, 2, 3\}$. The values $k = 1$ and 3 are excluded because they give an even p. Thus $p = 1 + 2q^2$. The values $q \neq 3$ are excluded because they give a p divisible by 3. We are left with the single pair $\langle p, q\rangle = \langle 19, 3\rangle$. It is excluded by the assumption that $p, q \geq 7$ (that is, by Theorem 5.1.6). □

5.2 Overview of Chapters 6–A

Chapter 6

An obstruction group

6.1 Number fields

A field L *extends* another field K, written L/K, if the base set of K is a subset of that of L, if both fields share neutral elements, which means that $0_K = 0_L$ and $1_K = 1_L$, and if addition and multiplication in L extend these operations in K. In this situation L is a K-vector space. We denote its dimension by $[L : K]$.

Definition 6.1.1 (number fields) *A field extension K of the field of fraction $\mathbb{Q}_{\text{fi}}$ with finite dimension $d := [K : \mathbb{Q}_{\text{fi}}]$ $(\in \mathbb{N})$ is called a number field (with degree d).*

Let K be a number field with degree d and let $\alpha \in K$. Then the $d+1$ powers 1_K, α, α^2, …, α^d are linearly dependent over $\mathbb{Q}$, and α is a root of a nonzero polynomial in $\mathbb{Q}[x]$ of degree at most d.

Definition 6.1.2 (rings of integers) *Let K be a number field. We define the subset*

$$\mathcal{O}_K = \{\alpha \in K\colon\ p(\alpha) = 0_K \textit{ for a monic polynomial } p(x) \in \mathbb{Z}[x]\}\,.$$

We say that $\mathcal{O}_K$ is the (base set of the) ring of integers of K.

Proposition 6.1.3 *The set $\mathcal{O}_K$ contains the neutral elements 0_K and 1_K, and is closed under addition and multiplication in K. It forms a subdomain of K.*

Proof.

□

Proposition 6.1.4 *For every number field K its ring of integers is* UFD *if and only if the class number $h_K = 1$.*

Proof.

□

6.2 Cyclotomic fields

Proposition 6.2.1 *For every prime p the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_p)_{\text{fi}}$ equals $\mathbb{Z}[\zeta_p]_{\text{do}}$.*

Proof.

□

Theorem 6.2.2 *The domains*

$$\mathbb{Z}[\zeta_3]_{\text{do}} \ \text{ and } \ \mathbb{Z}[\zeta_5]_{\text{do}}$$

are Euclidean. In view of Propositions 6.1.4 and 6.2.1, and of Theorem 2.3.2 the class numbers of cyclotomic fields $\mathbb{Q}(\zeta_3)_{\text{fi}}$ and $\mathbb{Q}(\zeta_5)_{\text{fi}}$ are

$$h_3 = h_5 = 1\,.$$

Proof.

□

6.3 The obstruction group

Chapter 7

Super–Cassels relations

7.1 The Stickelberger ideal

7.2 Theorems M0.95 and M1

Chapter 8

Theorem M4

Theorem 8.0.1 (M4) *If p and q are distinct odd primes and $p \in \{3, 5\}$ or $q \in \{3, 5\}$, then the Diophantine equation*

$$x^p - y^q = 1$$

has no nonzero solution $x, y \in \mathbb{Z}^*$.

Proof.

□

Appendix A

Results from mathematical analysis

Theorem A.0.1 (on Taylor polynomials) *Let $n \in \mathbb{N}$, $I \subset \mathbb{R}$ be an open interval, $a \in I$ and $f\colon I \to \mathbb{R}$ be a function that has n derivatives*

$$f',\, f'',\, \ldots,\, f^{(n)}\colon I \to \mathbb{R}\,.$$

Then the (Taylor) polynomial

$$T_f^{n,\,a}(x) := \sum_{j=0}^{n} \frac{f^{(j)}(a)}{j!}(x-a)^j$$

is a unique polynomial $P \in \mathbb{R}[x]$ with degree at most n and the property that

$$f(x) = P(x) + o((x-a)^n) \quad (x \to a)\,.$$

Proof.

□

Bibliography

[1] Yu. Bilu, Y. Bugeaud and M. Mignotte, *The Problem of Catalan*, Springer, Cham, 2014

[2] J. W. S. Cassels, Wikipedia article, `https://en.wikipedia.org/wiki/J._W._S._Cassels`

[3] J. W. S. Cassels, On the equation $a^x - b^y = 1$, *Amer. J. Math.* **75** (1953), 159–162

[4] J. W. S. Cassels, On the equation $a^x - b^y = 1$. II, *Proc. Cambridge Phil. Soc.* **56** (1960), 97–103; Corrigendum: Ibid, **57** (1961), 187

[5] E. Catalan, Problème 48, *Nouv. Ann. Math.* **1** (1842), 520

[6] E. Catalan, Note extraite d'une lettre adressée à l'éditeur, *J. reine angew. Math.* **27** (1844), 192

[7] E. Z. Chein, A note on the equation $x^2 = y^q + 1$, *Proc. Amer. Math. Soc.* **56** (1976), 83–84

[8] H. Cohen, *Number Theory. Volume I: Tools and Diophantine Equations*, Springer, New York 2007

[9] B. Conrad, An example of descent by Euler, 5 pp., `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/descentbyeuler.pdf`
(visited in December 4, 2025)

[10] P. Erdős, Chao Ko and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford.* Ser. (2) **12** (1961), 313–320

[11] Erdős–Ko–Rado theorem, Wikipedia article, `https://en.wikipedia.org/wiki/Erd%C5%91s%E2%80%93Ko%E2%80%93Rado_theorem`

[12] Euclidean domain, Wikipedia article, `https://en.wikipedia.org/wiki/Euclidean_domain`

[13] Eugène Charles Catalan, Wikipedia article, `https://en.wikipedia.org/wiki/Eug%C3%A8ne_Charles_Catalan`

[14] Leonhard Euler, Wikipedia article, `https://en.wikipedia.org/wiki/Leonhard_Euler`

[15] L. Euler, Theorematum quorundam arithmeticorum demonstrationes, *Comm. Acad. Sci. Petrop.* **10** (1738), 125–146

[16] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* Fourth Edition, Oxford at the Clarendon Press, Oxford 1960

[17] Ke Zhao, Wikipedia article, `https://en.wikipedia.org/wiki/Ke_Zhao`

[18] M. Klazar, O řešení diofantické rovnice $x^2 - y^3 = \pm 1$, *Matematické obzory* **32** (1989), 47–53 (Solving the Diophantine equation $x^2 - y^3 = \pm 1$)

[19] Chao Ko, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, *Sci. Sinica* **14** (1965), 457–460

[20] S. Lang, *Algebra.* Revised Third Edition, Springer-Verlag, New York 2002

[21] V. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, *Nouv. Ann. Math.* **8** (1850), 178–181

[22] Victor Amédée Lebesgue, Mac Tutor article, `https://mathshistory.st-andrews.ac.uk/Biographies/Lebesgue_Victor/`

[23] T. Metsänkylä, Catalan's conjecture: another old Diophantine problem solved, *Bulletin Amer. Math. Soc.* **41** (2003), 43–57

[24] P. Mihăilescu, A class number free criterion for Catalan's conjecture, *J. Number Theory* **99** (2003), 225–231

[25] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. reine angew. Math.* **572** (2004), 167–195

[26] P. Mihăilescu, On the class group of cyclotomic extensions in presence of a solution to Catalan's equation, *J. Number Theory* **118** (2006), 123–144

[27] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York 1969

[28] T. Nagell, Sur l'impossibilité de l'équation indéterminée $z^p + 1 = y^2$, *Norsk. Mat. Forenings Skrifter* **4** (1921), 14 pp.

[29] Ch. Notari, Une résolution élémentaire de l'équation diophantienne $x^3 = y^2 - 1$, *Expositiones Mathematicae* **21** (2003), 279–283

[30] P. Ribenboim, *Catalan's Conjecture. Are 8 and 9 the Only Consecutive Powers?*, Academic Press, Inc., Boston, MA, 1994

[31] K. Rogers, The axioms for Euclidean domains, *Amer. Math. Monthly* **78** (1971), 1127–1128

[32] R. Schoof, *Catalan's Conjecture*, Springer-Verlag London, Ltd., London, 2008

[33] Antoni Wakulicz, Wikipedia article, `https://pl.wikipedia.org/wiki/Antoni_Wakulicz` (in Polish)

[34] A. Wakulicz, On the equation $x^3 + y^3 = 2z^3$, *Colloq. Math.* **5** (1957), 11–15

[35] A. Weil, *Number Theory. An Approach through History: From Hammurapi to Legendre*, Birhkhäuser, Boston 1984