Mihăilescu

(proof of Catalan's conjecture)

Martin Klazar

(KAM MFF UK Praha)

This is the preliminary version of December 6, 2024 (day 49).

dedicated to my parents Blanka and Jiří

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

See [7].

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 $x^m - y^n = 1$, dans „ laquelle les inconnues sont entières et positives, n'admèt qu'une seule „ solution. "

See [8].

Like FLT, Catalan's conjecture — the only solution of $x^m - y^n = 1$ in integers $x, y > 0$ and $m, n > 1$ is $3^2 - 2^3 = 1$ — was born in 1842 as a theorem. Unlike P. de Fermat, after two years E. Catalan corrected himself and changed it to a conjecture. Written according to [3, pp. 1–2].

The term *Catalan's conjecture*, in contrast to *the Catalan conjecture*, avoids ambiguities. The reader probably knows that the Catalan numbers $\frac{1}{n+1}\binom{2n}{n}$ (see the book [35] on them), where $n = 0, 1, 2, \ldots$, are also named after the Belgian-French mathematician Eugène Ch. Catalan (1814–1894) ([15]). But the Catalan Opening in chess, 1. d4 Nf6 2. c4 e6 3. g3, is named after Catalonia. It was invented by the grandmaster Savielly (Xavier, Ksawery) Tartakower (1887–1956) for the 1929 tournament in Barcelona ([9]).

Introduction

This is the first installment in the Diophantine tetralogy ([36][1])

Mihăilescu–Baker–Siegel–Faltings

I plan and hope to write. In 2004 in [27] P. Mihăilescu affirmatively solved the conjecture posed by E. Catalan in [8] in 1844: The only solution of the equation $x^m - y^n = 1$ in integers x, y, m, n with $x, y > 0$ and $m, n > 1$ is $3^2 - 2^3 = 1$. In this text I *completely* describe Mihăilescu's proof and the whole solution of Catalan's conjecture, including the involved algebraic number theory. I rely on three books on Mihăilescu's theorem (Catalan's conjecture): Ribenboim [31], Schoof [34], and Bilu, Bugeaud and Mignotte [3]. There is a survey by Metsänkylä [26] of Mihăilescu's theorem.

In my text I stress proofs and clarity of presentation. The beauty and sense of mathematics lies in the arguments and proofs by which she justifies her results and theorems. So I make an effort to present also the "standard" material with all details and as clearly as I can. The appendices present in detail and slow pace considerable amounts of standard material in elementary number theory, commutative algebra, and algebraic number theory.

As for the other three parts of the tetralogy, **Baker** will treat the effective solution of Thue equations achieved by A. Baker, and **Siegel**, respectively **Faltings**, will be devoted to the finiteness theorems for integral, respectively rational, points on algebraic curves, that were obtained by C.-L. Siegel, respectively G. Faltings. I am somewhat sentimental about this first part because it gives me the opportunity to present my 1989 solution of the case $x^2 - y^3 = 1$.

Praha and Louny, October 2024 to ?? Martin Klazar

[1] One of the best known tetralogies is Wagner's (commutative) Ring: Das Rheingold, Die Walküre, Siegfried and/und Götterdämmerung.

Notation

$\mathbb{N} = \{1, 2, \dots\}$ are natural numbers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ are nonnegative integers. By $(\mathbb{N}, <)$ we denote the standard well ordering of natural numbers. For $n \in \mathbb{N}$ we set $[n] = \{1, 2, \dots, n\}$; $[0] = \emptyset$. The ordered domain (ring) of integers is denoted by $\mathbb{Z}$. We denote the set of prime numbers by $\mathbb{P}$, thus

$$\mathbb{P} = \{2,\, 3,\, 5,\, 7,\, 11,\, 13,\, 17,\, 19,\, 23,\, 29,\, 31,\, 37,\, \dots\}\,,$$

and primes are denoted by the letters p and q. If $a, b, c \in \mathbb{Z}$ and $a = b \cdot c = bc$, we say that b (and c) divides a, or that b is a divisor of a, or that a is a multiple of b, and write $b \,|\, a$. For $a, b, c \in \mathbb{Z}$ we write $a \equiv b \pmod{c}$ if $a = b + dc$ for some $d \in \mathbb{Z}$. If b does not divide a, we write $\neg(b \,|\, a)$. Two integers are coprime if they are simultaneously divisible only by -1 and 1. For a nonempty set $A \subset \mathbb{Z}$ we write $\mathrm{GCD}(A)$ for the greatest common divisor of the elements in A. If $A = \{m, n\}$, we write just $\mathrm{GCD}(m, n)$. Phrases like "the only solution of $x^2 - y^2 = 1$ is $(\pm 1, 0)$" mean that the only solutions of the equation in $\mathbb{Z}^2$ are $(x, y) = (-1, 0)$ and $(x, y) = (1, 0)$. The symbols $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of fractions, real numbers and complex numbers, respectively.

By $\wedge$, respectively $\vee$, we denote the connective of conjunction ("and"), respectively of disjunction ("or"). For a finite set X we denote by $|X|$ $(\in \mathbb{N}_0)$ the number of its elements. A linear order $(X, \prec)$ on a set X is a binary relation $\prec$ on X such that for every $a, b, c \in X$ we have $\neg(a \prec a)$ (irreflexivity), $a \prec b \wedge b \prec c \Rightarrow a \prec c$ (transitivity) and $a \prec b \vee b \prec a \vee a = b$ (trichotomy). For two sets X, Y we write $f\colon X \to Y$ to say that the set f is a function (map) from X to Y. It means that $f \subset X \times Y = \{(a, b) :\ a \in X, b \in Y\}$ and that for every $a \in X$ there is a unique $b \in Y$ with $(a, b) \in f$, written $f(a) = b$. If $f\colon X \to Y$ and Y has a distinguished "zero" element $0_Y \in Y$, then the support of f refers to the set $S(f) = \{x \in X :\ f(x) \neq 0_Y\}$. Let $f\colon X \to Y$ be a map. For any set Z we define $f[Z] = \{f(a) :\ a \in X \cap Z\}$ and $f^{-1}[Z] = \{x \in X :\ f(x) \in Z\}$. We say that f is injective iff $f(a) = f(b)$ always implies $a = b$. For injective f we define the inverse map $f^{-1}\colon f[X] \to X$ by setting $f^{-1}(b) = a \iff f(a) = b$. We say that f is a bijection iff it is injective and surjective, the latter meaning that $f[X] = Y$. What is the purpose of this terminology in a number-theoretic text? In Theorem C.1.3 we succinctly express the Fundamental Theorem of Arithmetic by the statement that the factorization map $F\colon P \to \mathbb{N}$ is a bijection. The prime factorization of $n \in \mathbb{N}$ is then simply the value $F^{-1}(n)$. We use the same approach more generally for (unique) factorization in monoids and integral domains. We denote the variables of complex functions

$$f\colon M \to \mathbb{C},\ M \subset \mathbb{C}\,,$$

by X, Y, Z, ... and write $f(X)$, $G(Y)$, ...; small letters x, y and z are reserved for integral solutions of Diophantine equations.

The algebraic structures that we use most are rings and fields. A ring $R_{\mathrm{ri}} = (R, 0_R, 1_R, +, \cdot)$ is equipped with commutative and associative binary operations $+$ and $\cdot$ on a nonempty set R that are bound by the distributivity of $\cdot$ to $+$,

have the respective neutral elements 0_R and 1_R, and $+$ has an inverse to every $a \in R$. In Section D.1 we will see that a ring also consists of two monoids bound by the distributive law. A ring is field if $\cdot$ has an inverse to every $a \in R \setminus \{0_R\}$.

Contents

Chapter 1

Outline of Mihăilescu's proof and of this text

Chapter 2

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

Catalan's conjecture (1844), which says that the only solution of the equation $x^m - y^n = 1$ in integers $x, y > 0$ and $m, n > 1$ is $x = n = 3$ & $y = m = 2$, is clearly equivalent to the same claim with the exponents restricted to prime numbers: $m = p$ and $n = q$. This follows from the identity

$$z^{k \cdot l} = \left(z^k\right)^l$$

that is valid for all $z \in \mathbb{C}$ and $k, l \in \mathbb{N}$. Note, however, that

$$(-1)^{2 \cdot \frac{1}{2}} = (-1)^1 = -1 \neq 1 = 1^{\frac{1}{2}} = \left((-1)^2\right)^{\frac{1}{2}}.$$

In this and the next two chapters we treat the cases when $p = 2$ or $q = 2$.

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

Theorem 2.1.1 *For every integer $m \geq 2$, equation $x^m - y^2 = 1$ has only the solution $(\pm 1, 0)$ for even m and $(1, 0)$ for odd m.*

Proof. Let $m = 2m_0 \geq 2$ be even and x, y be integers such that $x^m - y^2 = 1$. Then $(x^{m_0} + y)(x^{m_0} - y) = 1$. Hence $x = \pm 1$ and $y = 0$.

Let $m \geq 3$ be odd and x, y be nonzero integers such that $x^m - y^2 = 1$. We derive a contradiction; so in this case the only integral solution is $(1, 0)$. If y is odd then $x^m = y^2 + 1 \equiv 2$ modulo 4, contradicting that $x^m \equiv 0$ modulo 4. Thus x is odd and y is even, and both are nonzero.

The factorization

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

takes us in the domain $\mathbb{Z}[i]$ of Gaussian integers; see Proposition D.1.16. The numbers $1 + yi$ and $1 - yi$ in it are coprime; see Section D.1 for the divisibility terminology in rings. Indeed, if $\alpha \in \mathbb{Z}[i]$ is their common divisor then α divides their sum 2, and $\alpha\overline{\alpha} \in \mathbb{N}$ divides (in the domain $\mathbb{Z}$) $2^2 = 4$ and their odd

product $1 + y^2 = x^m$. Thus $\alpha\overline{\alpha} = 1$ and $\alpha \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Since $\mathbb{Z}[i]$ is UFD (Proposition D.1.16), part 1 of Proposition D.1.9 gives that for some $\alpha \in \mathbb{Z}[i]$ and $\varepsilon \in \mathbb{Z}[i]^\times$,

$$1 + yi = \varepsilon\alpha^m \text{ and } 1 - yi = \overline{\varepsilon}(\overline{\alpha})^m .$$

Since m is odd, like in the domain $\mathbb{Z}$ every unit in $\mathbb{Z}[i]$ is an m-th power and we can express both numbers more simply as $1+yi = (a+bi)^m$ and $1-yi = (a-bi)^m$ for some $a, b \in \mathbb{Z}$. From (m is odd)

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

we get $a = \pm 1$. We rule out $a = -1$. Since $(1 + b^2)^m = (a^2 + b^2)^m = 1 + y^2$ is odd, the number b is even. From

$$1 + yi = (a + bi)^m = \textstyle\sum_{j=0}^{m} \binom{m}{j} a^{m-j}(bi)^j \equiv a^m + ma^{m-1}bi \pmod 4$$

we get $a^m \equiv 1$ modulo 4, and indeed $a = -1$ is impossible (m is odd).

Hence $a + bi = 1 + bi$, with even and nonzero b (since $y \neq 0$). By comparing the real parts in $1 + yi = (1 + bi)^m$ we get an identity in the domain $\mathbb{Z}$:

$$1 = \textstyle\sum_{j=0}^{(m-1)/2} (-1)^j \binom{m}{2j} b^{2j}, \text{ that is, } -\binom{m}{2}b^2 + \sum_{j=2}^{(m-1)/2} (-1)^j \binom{m}{2j} b^{2j} = 0$$

(for $m = 3$ the last sum is 0). We show that the 2-adic order of $-\binom{m}{2}b^2$ is smaller than all 2-adic orders of summands in the last sum. Corollary C.1.10 then says that the last displayed equality is impossible.

For $m = 3$ it is clear because $\binom{m}{2}b^2 \neq 0$ but the last displayed sum is 0. Let $m \geq 5$, $A = \binom{m}{2}b^2$ and $B_j = \binom{m}{2j}b^{2j}$ for $j = 2, 3, \ldots, \frac{m-1}{2}$. Then

$$B_j = A \cdot \tfrac{1}{j(2j-1)} \binom{m-2}{2j-2} b^{2j-2} = A \cdot C_j .$$

Thus, since b is even, $\mathrm{ord}_2(B_j) - \mathrm{ord}_2(A) = \mathrm{ord}_2(C_j) \geq (2j-2)\mathrm{ord}_2(b) - \mathrm{ord}_2(j) \geq 2j - 2 - \lfloor \log_2 j \rfloor > 0$ for every $j \geq 2$. □

2.2 Remarks

Theorem 2.1.1 is due to V. Lebesgue in [25] in 1850. Here we adapt the proof in [3, pp. 11–12]. Noteworthy features of the proof are the fact that $\mathbb{Z}[i]$ is UFD (Proposition D.1.16) and the local trick for obtaining the final contradiction (Corollary C.1.10).

Chapter 3

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

In this chapter we prove in two ways by elementary means — we work only in the domain $\mathbb{Z}$, almost — that the solutions of $x^2 - y^3 = 1$ are just $(\pm 3, 2)$, $(\pm 1, 0)$ and $(0, -1)$. To solve this Diophantine equation one can go in two ways and start from the factorization $x^2 = (y+1)(y^2 - y + 1)$ or $(x+1)(x-1) = y^3$. In Sections 3.1 and 3.2 we take the former way, and in Section 3.3 the latter.

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

We prove in Theorem 3.1.6 that the only solution of the equation is $(\pm 1, 0)$.

Proposition 3.1.1 *If $x, y, z \in \mathbb{N}_0$ satisfy $x^2 + y^2 = z^2$ and are pairwise coprime then for some $u, v \in \mathbb{N}_0$ we have $z = u^2 + v^2$ and $x = u^2 - v^2$, $y = 2uv$, or $x = 2uv$, $y = u^2 - v^2$.*

Proof. Suppose that x, y, z are as stated. Modulo 4 we see that z and exactly one of x, y, say x, is odd. Then, since $\frac{z-x}{2}$ and $\frac{z+x}{2}$ are coprime, from $\left(\frac{y}{2}\right)^2 = \frac{z-x}{2} \cdot \frac{z+x}{2}$ we get by 1 of Corollary C.1.6 numbers $u, v \in \mathbb{N}_0$ such that $\frac{z-x}{2} = v^2$, $\frac{z+x}{2} = u^2$ and $uv = \frac{y}{2}$. Hence $x = u^2 - v^2$, $y = 2uv$ and $z = u^2 + v^2$. □

Corollary 3.1.2 *If $x, y \in \mathbb{N}_0$ satisfy $2x^2 - y^2 = 1$ then there exist $a, b \in \mathbb{N}_0$ such that $a^2 - 2b^2 = 1$ and $x = a^2 + 2b^2 \pm 2ab$.*

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 3.1.1 there exist $u, v \in \mathbb{N}_0$ such that $x = u^2 + v^2$, $y_0 = 2uv$, $y_0 + 1 = u^2 - v^2$ or $y_0 = u^2 - v^2$, $y_0 + 1 = 2uv$. In the first case $1 = u^2 - v^2 - 2uv = (u - v)^2 - 2v^2$. In the second case $1 = 2uv - u^2 + v^2 = (u + v)^2 - 2u^2$. We set $a = u - v$, $b = v$, respectively $a = u + v$, $b = u$, and get $a, b \in \mathbb{N}_0$ satisfying the two stated relations. □

Proposition 3.1.3 *If $x, y \in \mathbb{Z}$ satisfy $x^4 - 2y^2 = 1$ then $(x, y) = (\pm 1, 0)$.*

Proof. Let x, y be as stated. Then x is odd and $x^2 = 1 + 4k$ for some $k \in \mathbb{N}_0$. From $(x^2 - 1)(x^2 + 1) = 2y^2$ we get $4k(2k + 1) = y^2$. Since $4k$ and $2k + 1$ are coprime, by 1 of Corollary C.1.6 we get $4k = a^2$, $a \in \mathbb{N}_0$. Thus $(x-a)(x+a) = 1$ and $x = \pm 1, y = 0$. □

Proposition 3.1.4 *All solutions of $x^2 - 3y^2 = 1$ are $(\pm x_n, \pm y_n)$ for $n = 0, 1, 2, \ldots,$ where*

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

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

Proof. This is an instance of Theorem C.2.1, the Pell equation $x^2 - 3y^2 = 1$ has the minimum solution $(a, b) = (2, 1)$. □

Proposition 3.1.5 *If (x_n, y_n) $(\in \mathbb{N}_0^2)$ for $n \in \mathbb{N}_0$ are pairs in the previous proposition then for every $n \in \mathbb{N}_0$,*

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

It holds that x_n is odd iff n is even, and that y_n is odd iff n is odd.

Proof. Indeed, $x_{2n} + y_{2n}\sqrt{3}$ equals (recall that $x_n^2 - 3y_n^2 = 1$)

$$\left(2 + \sqrt{3}\right)^{2n} = \left(x_n + y_n\sqrt{3}\right)^2 = x_n^2 + 3y_n^2 + 2x_n y_n\sqrt{3} = 2x_n^2 - 1 + 2x_n y_n\sqrt{3}$$

and $x_{2n+1} + y_{2n+1}\sqrt{3} = (2 + \sqrt{3})(x_n^2 + 3y_n^2 + 2x_n y_n\sqrt{3})$ equals

$$2x_n^2 + 6x_n y_n + 6y_n^2 + (x_n^2 + 4x_n y_n + 3y_n^2)\sqrt{3} .$$

Now $2x_n^2 + 6x_n y_n + 6y_n^2 = x_n^2 + 6x_n y_n + 9y_n^2 + 1 = (y_n + x_n + 2y_n)^2 + 1 = (y_n + y_{n+1})^2 + 1$ and $x_n^2 + 4x_n y_n + 3y_n^2 = (x_n + 2y_n)^2 - y_n^2 = y_{n+1}^2 - y_n^2$. The last claim easily follows from these relations by induction on n. □

We prove the main result of this section.

Theorem 3.1.6 *If $x, y \in \mathbb{Z}$ satisfy $x^4 - 3y^2 = 1$ then $(x, y) = (\pm 1, 0)$.*

Proof. We need to solve $x_n = m^2$ for $n, m \in \mathbb{N}_0$ where x_n are as in Proposition 3.1.4. If $n = 2n_0 + 1$ is odd then Proposition 3.1.5 gives $(m - y_{n_0} - y_{n_0+1})(m + y_{n_0} + y_{n_0+1}) = 1$. Thus $m = \pm 1$ and $y_{n_0} + y_{n_0+1} = 0$. But this is impossible because always $y_{n_0} + y_{n_0+1} > 0$.

Let $n = 2n_0$ be even. Then Proposition 3.1.5 gives $2x_{n_0}^2 - 1 = x_{2n_0} = x_n = m^2$ and $2x_{n_0}^2 - m^2 = 1$. Modulo 4 we see that x_{n_0} is odd. Proposition 3.1.5 gives $x_{n_0} = x_{2n_1} = 2x_{n_1}^2 - 1$. Corollary 3.1.2 shows that there are $a, b \in \mathbb{N}_0$ such that $a^2 - 2b^2 = 1$ and

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

Hence $x_{n_1}^2 = a(a \pm b)$. Since a, b are coprime, so are $a, a \pm b$, and by 1 of Corollary C.1.6 the number a is a square. By Proposition 3.1.3 we have $a = 1$. Thus $b = 0$, $x_n = x_{n_0} = 1$ and $x = \pm 1, y = 0$. □

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

Starting from $x^2 = (y+1)(y^2 - y + 1)$ and using the previous theorem, in the next theorem we find all solutions of $x^2 - y^3 = 1$. In Theorem 3.2.2, which can be proven by the same method, we mention without proof solutions of some more Diophantine equations similar to $x^2 - y^3 = 1$.

Theorem 3.2.1 *The only solutions of* $x^2 - y^3 = 1$ *are* $(\pm 3, 2)$, $(\pm 1, 0)$ *and* $(0, -1)$.

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

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

Note that $y^2 - y + 1 \geq 0$, hence $y + 1 \geq 0$, and that $\mathrm{GCD}(y+1, y^2 - y + 1) = 1$ or 3. In the former case we have by 1 of Corollary C.1.6 that $y+1$ and $y^2 - y + 1$ are squares. Thus $4y^2 - 4y + 4 = (2a)^2$ for $a \in \mathbb{N}_0$, $3 = (2a - 2y + 1)(2a + 2y - 1)$ and $(a, y) = (\pm 1, 1)$ or $(\pm 1, 0)$. For $y = 1$ the number $y + 1$ is not a square and for $y = 0$ we get the trivial solution $(\pm 1, 0)$.

Let $\mathrm{GCD}(y+1, y^2 - y + 1) = 3$. By 1 of Corollary C.1.7 there are $a, b \in \mathbb{N}_0$ such that $3a^2 = y + 1$ and $3b^2 = y^2 - y + 1$. 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 $(X, Y, a) = (2, -1, 0)$ solves this system. We get $y = -1$ and the trivial solution $(0, -1)$.

We can assume that $Y \in \mathbb{N}_0$. We look for an $n \in \mathbb{N}_0$ such that $Y = y_n = 2a^2 - 1$, where $a \in \mathbb{N}_0$ and x_n, y_n are as in Proposition 3.1.4. Since y_n is odd, so is n. By Proposition 3.1.5 we have for some $m \in \mathbb{N}_0$ that

$$\begin{aligned} 2a^2 - 1 &= y_n = y_{2m+1} = y_{m+1}^2 - y_m^2 = (x_m + 2y_m)^2 - y_m^2 \\ &= x_m^2 + 4y_m y_m + 3y_m^2 = 2x_m^2 + 4x_m y_m - 1 \\ &= 2x_m(x_m + 2y_m) - 1 = 2x_m y_{m+1} - 1\,. \end{aligned}$$

Thus

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

We have $\mathrm{GCD}(x_m, y_{m+1}) = \mathrm{GCD}(x_m, x_m + 2y_m) = 1$ or 2. If $\mathrm{GCD}(x_m, y_{m+1}) = 1$ then by 1 of Corollary C.1.6 the number x_m is a square. Theorem 3.1.6 gives $x_m = 1$. Thus $m = 0$, $n = 1$, $y_n = Y = 1$ and $y = 2$. We get the nontrivial solution $(\pm 3, 2)$.

Finally, it remains to treat the case $\mathrm{GCD}(x_m, y_{m+1}) = 2$. Part 1 of Corollary C.1.7 shows that $y_{m+1} = 2c^2$ for some $c \in \mathbb{N}_0$. By Proposition 3.1.5 we have for some $k \in \mathbb{N}$ that

$$2c^2 = y_{m+1} = y_{2k} = 2x_k y_k \text{ and } c^2 = x_k y_k \,.$$

Since x_k, y_k are coprime, by 1 of Corollary C.1.6 the number x_k is a square. But by Theorem 3.1.6 this is not possible, the number x_k is never a square for $k \geq 1$. We do not obtain any more solutions of $x^2 - y^3 = 1$ and are done. □

This method also gives the following theorem. See [21] for more details.

Theorem 3.2.2 *The following hold.*

1. *The only solution of $x^2 - y^3 = -1$ is $(0, 1)$.*
2. *The two equations $3x^2 - y^3 = \pm 1$ have no solution with $x \neq 0$.*
3. *For every $k \in \mathbb{N}$ and choice of the sign the equation $x^2 - y^3 = \pm 3^{3k}$ has effectively finitely many solutions.*

In part 3 we say that an algorithm can be given that for every k and every choice of the sign finds all (finitely many) solutions of the equation.

3.3 Equation $x^3 + y^3 = 2z^3$

In this section we again determine all solutions of $x^2 - y^3 = 1$, but now we start from the factorization $(x+1)(x-1) = y^3$. We first reduce $x^2 - y^3 = 1$ to $x^3 - 2y^3 = \pm 1$. These equations are actually equivalent, and to explain how we introduce the following notation. If $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is an integral polynomial in n variables, then

$$S(f) = \{\overline{a} \in \mathbb{Z}^n : \ f(\overline{a}) = 0\}$$

denotes the set of solutions of the Diophantine equation $f(\overline{x}) = 0$. If $X \subset \mathbb{Z}^n$ and $i \in [n]$, then

$$X_i = \{x \in \mathbb{Z} : \ \exists\, \overline{a} \in \mathbb{Z}^n : \ a_i = x \wedge \overline{a} \in X\}$$

denotes the projection of X on the i-th coordinate. For $n = 2$ we use the convention that x denotes the coordinate x_1, and y the coordinate x_2.

Proposition 3.3.1 *Let $S(x^3 - 2y^3 \pm 1) = S(x^3 - 2y^3 + 1) \cup S(x^3 - 2y^3 - 1)$. Then two inclusions hold, $S(x^2 - y^3 - 1)_1$ is a subset of*

$$\{0\} \cup \{2x^3 + 1 : \ x \in S(x^3 - 2y^3 \pm 1)_1\} \cup \{2x^3 - 1 : \ x \in S(x^3 - 2y^3 \pm 1)_1\}\,,$$

and $S(x^3 - 2y^3 \pm 1)_1$ of

$$\{x : \ 2x^3 + 1 \in S(x^2 - y^3 - 1)_1\} \cup \{x : \ 2x^3 - 1 \in S(x^2 - y^3 - 1)_1\}\,.$$

Thus given $S(x^3 - 2y^3 \pm 1)$, we can determine $S(x^2 - y^3 - 1)$, and vice versa.

Proof. Given $S(x^3 - 2y^3 \pm 1)$, we solve $x^2 - y^3 = 1$. Let x, y be integers such that $x^2 - y^3 = 1$. In $(x+1)(x-1) = y^3$ we have $\mathrm{GCD}(x+1, x-1) = 1$ or 2. In the former case, 2 of Corollary C.1.6 gives $x + 1 = a^3$ and $x - 1 = b^3$, with $a, b \in \mathbb{Z}$. Thus $2 = a^3 - b^3 = (a-b)(a^2 + ab + b^2)$. Hence $(a, b) = (1, -1)$ and $x = 0$. If $\mathrm{GCD}(x+1, x-1) = 2$ then with $x - 1 = 2x_0$ and $y = 2y_0$, where $x_0, y_0 \in \mathbb{Z}$, we get $(x_0 + 1)x_0 = 2y_0^3$. Now $x_0 + 1, x_0$ are coprime and by 2 of Corollary C.1.8 there are $u, v \in \mathbb{Z}$ such that $x_0 + 1 = u^3$, $x_0 = 2v^3$ or $x_0 + 1 = 2v^3$, $x_0 = u^3$. Subtracting we get $u^3 - 2v^3 = \pm 1$. So $x = 2x_0 + 1 = 2u^3 \pm 1$ and $(u, v) \in S(x^3 - 2y^3 \pm 1)$. We get the first inclusion.

Given $S(x^2 - y^3 - 1)$, we solve equations $x^3 - 2y^3 = \pm 1$. Let x, y be integers such that $x^3 - 2y^3 = 1$. Then with $u = 2x^3 - 1 = 4y^3 + 1$ we have $u^2 - 1 = (u+1)(u-1) = (2xy)^3$. Thus $(u, 2xy) \in S(x^2 - y^3 - 1)$. If $x, y \in \mathbb{Z}$ satisfy $x^3 - 2y^3 = -1$, we set $v = 2x^3 + 1 = 4y^3 - 1$ and again get $v^2 - 1 = (2xy)^3$. Thus $(v, 2xy) \in S(x^2 - y^3 - 1)$. We get the second inclusion. □

The almost perfect symmetry between both reductions is remarkable. So if we prove that

$$S(x^3 - 2y^3 \pm 1) = \{(1,1),\ (-1,0),\ (1,0),\ (-1,-1)\}$$

then $S(x^3 - 2y^3 \pm 1)_1 = \{-1, 1\}$, and we get by the first reduction that

$$S(x^2 - y^3 - 1)_1 \subset \{0\} \cup \{2x^3 + 1 :\ x \in \{-1,\ 1\}\} \cup \{2x^3 - 1 :\ x \in \{-1,\ 1\}\}$$

which is $\{0, -1, 3, -3, 1\}$. Hence we again get

$$S(x^2 - y^3 - 1) = \{(0,-1),\ (-1,0),\ (3,2),\ (-3,2),\ (1,0)\}\,.$$

We solve $x^3 - 2y^3 = \pm 1$ by solving the next more general Diophantine equation.

Theorem 3.3.2 *Equation $x^3 + y^3 = 2z^3$ has no solution with $x \neq y$ and $z \neq 0$.*

Indeed, then $x^3 + (\pm 1)^3 = 2y^3$ may have a solution only if $x = \pm 1$ or $y = 0$, which gives the above solution set $S(x^3 - 2y^3 \pm 1)$. We prove Theorem 3.3.2 by reducing $x^3 + y^3 = 2z^3$ to another Diophantine equation, and then by solving that equation.

Proposition 3.3.3 *If equation $x^3 + y^3 = 2z^3$ has a solution with $x \neq y$ and $z \neq 0$, then equation $27d^4 + 9a^2d^2 + a^4 = l^2$ has a solution with $dal \neq 0$.*

Proof. Suppose that $x, y, z \in \mathbb{Z}$ are such that $x^3 + y^3 = 2z^3$, $x \neq y$ and $z \neq 0$. It follows that $xyz \neq 0$. Canceling out common factors we may assume that x, y are coprime and odd. Then $u = \frac{x+y}{2}$ and $v = \frac{x-y}{2}$ are coprime integers,

$$u(u^2 + 3v^2) = z^3 \ \text{ and } \ uvz \neq 0\,.$$

The case $\neg(3 \mid u)$. Then $u, u^2 + 3v^2$ are coprime and 2 of Corollary C.1.6 gives that $u = z_1^3$ and $u^2 + 3v^2 = z_2^3$ for coprime $z_1, z_2 \in \mathbb{Z}$. Thus

$$z_2^3 - z_1^6 = 3v^2 \ \text{ and } \ (z_2 - z_1^2) \cdot ((z_2 - z_1^2)^2 + 3z_2 z_1^2) = 3v^2\,.$$

We set $k = z_2 - z_1^2$. Then k, z_1 are coprime and $k(k^2+3kz_1^2+3z_1^4) = 3v^2$. Hence $k = 3k_1$, $v = 3v_1$ for some $k_1, v_1 \in \mathbb{Z}$ and $k_1(3k_1^2 + 3k_1z_1^2 + z_1^4) = 3v_1^2$. Since $z_2^3 - z_1^6 = 3v^2$ and z_1, z_2 are coprime, $\neg(3 \,|\, z_1)$. So $k_1 = 3k_2$ with $k_2 \in \mathbb{Z}$ and

$$k_2 \cdot (27k_2^2 + 9k_2z_1^2 + z_1^4) = v_1^2$$

where k_2, z_1 are coprime. The above definitions give that $z_2, k, k_2 \geq 0$. Since the last two displayed factors are coprime, 1 of Corollary C.1.6 gives $k_3, l \in \mathbb{N}_0$ such that $k_2 = k_3^2$ and

$$27k_3^4 + 9k_3^2z_1^2 + z_1^4 = l^2 \,.$$

Since $k_3z_1l \neq 0$ ($uv \neq 0$), we are done.

The case $3 \,|\, u$. Then $\neg(3 \,|\, v)$ and for some $u_1, z_1 \in \mathbb{Z}$ we have $u = 3u_1$, $z = 3z_1$ and $27u_1^3 + 9u_1v^2 = 27z_1^3$. Thus $u_1 = 3u_2$ with $u_2 \in \mathbb{Z}$ and

$$u_2(27u_2^2 + v^2) = z_1^3 \,.$$

Since u_2, v are coprime, 2 of Corollary C.1.6 gives coprime numbers $a, b \in \mathbb{Z}$ such that $u_2 = a^3$ and $27u_2^2 + v^2 = b^3$. Hence

$$27a^6 + v^2 = b^3 \,.$$

We set $k = b - 3a^2$. Then

$$v^2 = k(k^2 + 9a^2k + 27a^4) \,.$$

Since $k \geq 0$ and k, a are coprime, 1 of Corollary C.1.6 gives numbers $k_1, l \in \mathbb{N}_0$ such that $k = k_1^2$ and $k^2 + 9a^2k + 27a^4 = l^2$. Hence

$$27a^4 + 9a^2k_1^2 + k_1^4 = l^2 \,.$$

Since $ak_1l \neq 0$ ($uv \neq 0$), we are done in this case too. □

We prove the main result of this section.

Theorem 3.3.4 *Equation* $27d^4 + 9a^2d^2 + a^4 = l^2$ *has no solution with* $dal \neq 0$.

Proof. We assume that $d, a, l \in \mathbb{N}$ are such that $27d^4 + 9a^2d^2 + a^4 = l^2$ and obtain a contradiction. First we show that if we take a triple d, a, l with minimum a then $\neg(3 \,|\, a)$. Suppose not, that is, $a = 3a_1$ with $a_1 \in \mathbb{Z}$. Then $l = 3l_1$ with $l_1 \in \mathbb{Z}$, and $3d^4 + 9a_1^2d^2 + 9a_1^4 = l_1^2$. Thus $l_1 = 3l_2$ with $l_2 \in \mathbb{Z}$, and $d^4 + 3a_1^2d^2 + 3a_1^4 = 3l_2^2$. Thus $d = 3d_1$ with $d_1 \in \mathbb{Z}$, and $27d_1^4 + 9a_1^2d_1^2 + a_1^4 = l_2^2$; we got the triple d_1, a_1, l_2 with $a_1 < a$.

So we assume that $d, a, l \in \mathbb{N}$ are such that $27d^4 + 9a^2d^2 + a^4 = l^2$ and $\neg(3 \,|\, a)$, and obtain a contradiction. By canceling common factors we get that d, a, l are pairwise coprime. The pair $(x, y) = (\frac{d^2}{l}, \frac{a^2}{l})$ solves equation

$$27x^2 + 9xy + y^2 = 1 \,.$$

By Proposition C.2.2, all *rational* solutions $(x, y) \in \mathbb{Q}^2$ of this equation, with the exception of $(0, 1)$, are given by the formulas

$$x = \tfrac{2m+9}{m^2+9m+27} \text{ and } y = \tfrac{m^2-27}{m^2+9m+27} \text{ for } m \in \mathbb{Q}\,.$$

Since $y = \frac{a^2}{l} > 0$, we can exclude $m = 0$. Thus for $m = \frac{p}{q}$ with coprime $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ we have $pq \neq 0$ and

$$\tfrac{d^2}{l} = \tfrac{2pq+9q^2}{p^2+9pq+27q^2} \text{ and } \tfrac{a^2}{l} = \tfrac{p^2-27q^2}{p^2+9pq+27q^2}\,.$$

Since d^2, l, a^2 are pairwise coprime, we get that

$$\mathrm{GCD}(2pq + 9q^2,\, p^2 + 9pq + 27q^2) = \mathrm{GCD}(p^2 - 27q^2,\, p^2 + 9pq + 27q^2) = \delta\,.$$

Let $p = 3^s p_1$ where $s \in \mathbb{N}_0$, $p_1 \in \mathbb{Z}$ and $\neg(3 \,|\, p_1)$. We show that the case $s \geq 1$ is impossible. □

3.4 Remarks

The Diophantine equation $x^2 - y^3 = 1$ was first solved by Euler in 1748. See [3] and [31] for more information on its history. In this chapter we described the solution this author gave in [21] in 1989. In 2003 Notari [30] published a similar solution, based on properties of solutions of the same Pell equation $x^2 - 3y^2 = 1$. As explained in [21] (but this is well known), the Diophantine equations $x^2 - y^3 = 1$ and $x^3 - 2y^3 = \pm 1$ can be reduced one to the other. So the somewhat forgotten article [37] of Wakulicz ([31, 34, 3] do not mention it) on the equation $x^3 + y^3 = 2z^3$ provides another solution of $x^2 - y^3 = 1$. Wakulicz proved in an elementary way that the only integral solutions of $x^3 + y^3 = 2z^3$ are the trivial ones with $x = y$ or $xyz = 0$. For more high-tech proof see Cohen [11, Chapter 6.4.5].

Proposition 3.1.1 is a standard result on Pythagorean triples $(x, y, z) \in \mathbb{N}_0^3$, $x^2 + y^2 = z^2$, for which we refer in [21] to ... . Corollary 3.1.2 is an original result of [21]. Proposition 3.1.3 is a standard result for which we refer in [21] to ... . Proposition 3.1.4 is an instance of the standard Theorem C.2.1 on the Pell equation; in [21] we refer for theory of the Pell equation to ... . Proposition 3.1.5 is an original result of [21]. The proof of Theorem 3.1.6 is an original result of [21]. The proof of Theorem 3.2.1 is an original result of [21]. The proof of Theorem 3.2.2 is an original result of [21].

Chapter 4

Equation $x^2 - y^q = 1$ for $q \geq 5$

Combining two congruences in Propositions 4.1.2 and 4.1.4, we prove in Theorem 4.1.5 that for every prime $q \geq 5$ the only solutions of equation $x^2 - y^q = 1$ are $(\pm 1, 0)$ and $(0, -1)$.

4.1 Equation $x^2 - y^q = 1$ for $q \geq 5$

Lemma 4.1.1 *Let q be a prime number and $a, b \in \mathbb{Z}$, $a \neq b$, be coprime. Then*

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

divides q.

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

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

Thus $d \,|\, q b^{q-1}$. Since a, b are coprime, so are $b, a-b$ and by Corollary C.1.5 the number d divides q. □

Proposition 4.1.2 *If $q \geq 3$ is a prime number and nonzero $x, y \in \mathbb{Z}^*$ satisfy $x^2 - y^q = 1$, then $2 \,|\, y$ and $q \,|\, x$.*

Proof. We may assume that $x, y \in \mathbb{N}$. We begin with a simple proof that y is even. Using Corollary C.1.6 we see that in $(x+1)(x-1) = y^q$ the two factors cannot be coprime because the only two q-th powers differing by 2 are -1 and 1, hence $x = 0$ but this was excluded. Since $\mathrm{GCD}(x+1, x-1) = 1$ or 2, we conclude that y is even.

It is harder to prove that q divides x. We assume that $\neg(q \,|\, x)$ and obtain a contradiction. By Lemma 4.1.1, 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. Both factors are nonnegative and by Corollary C.1.6 they are squares. So $y+1=u^2$ for $u\in\mathbb{N}_0$. The equalities

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

show that $(x,y^{(q-1)/2})$ and $(u,1)$ are solutions of the equation $X^2-yY^2=1$. Since $y=u^2-1\geq 3$ and is not a square, $X^2-yY^2=1$ is a Pell equation. It is clear that $(u,1)\in\mathbb{N}^2$ is its minimum solution. By Theorem C.2.1 there is an $m\in\mathbb{N}_0$ such that in the domain $\mathbb{Z}[\sqrt{y}]$ we have equality

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

So $m\in\mathbb{N}$ and in $\mathbb{Z}[\sqrt{y}]$ we have 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, so u is odd and m is even. In $\mathbb{Z}[\sqrt{y}]$ we therefore have equality

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

and 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 $y=0$, which contradicts $y\in\mathbb{N}$. □

Lemma 4.1.3 *Let $q\in\mathbb{N}$ with $q\geq 3$ be odd and $x,y\in\mathbb{Z}^*$ be nonzero such that $x^2-y^q=1$. Then, replacing x with $-x$ if necessary, for some coprime $a,b\in\mathbb{Z}$ with odd b we have*

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

Proof. In the factorization $(x-1)(x+1)=y^q$ the two factors are coprime or their GCD is 2. From the previous proof we know that the former case is impossible, and so $\mathrm{GCD}(x-1,x+1)=2$, x is odd, y is even and $2^q\mid(x-1)(x+1)$. Changing the sign of x if necessary, we may assume that $x\equiv 1\pmod 4$. Then $\frac{x+1}{2}$ is odd and using Corollary C.1.7 we get the required numbers a and b. □

Proposition 4.1.4 *If $q\geq 5$ is prime and $x,y\in\mathbb{Z}^*$ are nonzero integers such that $x^2-y^q=1$ then $x\equiv\pm 3\pmod{q}$.*

Proof. Suppose that q is as stated and that the numbers $x,y\in\mathbb{Z}^*$ satisfy $x^2-y^q=1$. Changing the sign of x if necessary, by the previous lemma 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 $b^{2q}-(2a)^q$ equals

$$\left(\tfrac{x+1}{2}\right)^2-2(x-1)=\left(\tfrac{x-3}{2}\right)^2, \text{ and } (b^2-2a)\cdot\left(\tfrac{b^{2q}-(2a)^q}{b^2-2a}\right)=\left(\tfrac{x-3}{2}\right)^2.$$

The numbers $2a, b^2$ are coprime and by Lemma 4.1.1 the GCD of the last two factors divides q.

We show that 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 and obtain a contradiction. So we assume that $b^2 - 2a, \frac{b^{2q}-(2a)^q}{b^2-2a}$ are coprime. Since $b^{2q} - (2a)^q \geq 0$ (it is a square), also $b^2 - 2a \geq 0$ and by Corollary C.1.6 there is a $c \in \mathbb{N}_0$ 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,

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

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 bound $|x| \geq 2^{q-1}|a|^q - 1 \geq 15$. Hence also $|a| < |b|$ and we have a contradiction. □

Theorem 4.1.5 *Equation $x^2 - y^q = 1$, where $q \geq 5$ is a prime number, has no nonzero solution $x, y \in \mathbb{Z}^*$.*

Proof. Suppose that q is as stated and $x, y \in \mathbb{Z}^*$ satisfy $x^2 - y^q = 1$. By Proposition 4.1.2 we have $x \equiv 0 \pmod q$, but also $x \equiv \pm 3 \pmod q$ by Proposition 4.1.4. For $q > 3$ these congruences are contradictory. □

4.2 Remarks

Theorem 4.1.5 was first proven by Chao Ko in [23] in 1965. His proof is reproduced on [28, pp. 302–304] of the book of L. J. Mordell. Proposition 4.1.2 is due to T. Nagel in [29] in 1921. Proposition 4.1.4 is due to E. Z. Chein in [10] in 1976. By it E. Z. Chein gave in [10] a simpler proof of Chao Ko's theorem. We reproduce and streamline the proof in [34, pp. 13–16], and consult also [3, pp. 15–18]. The history of solving the Diophantine equation $x^2 - y^q = 1$ is surveyed in [3, Section 2.3.3].

Say to an extremal combinatorialist slowly and clearly "ko, ko, ko, . . . " and you should get the reply: The Erdős–**Ko**–Rado theorem! The second author is indeed Chao Ko (or Ke Zhao) (1910–2002); the other two are Paul Erdős (1913–1996) and Richard Rado (1906–1989). We give this theorem, proven in [13], and its proof, taken from [1], below. The article [13] with 715 citations in *Mathematical Reviews* in November 2024 belongs to the most cited articles in pure mathematics. Endlichkeitssätze [16] of G. Faltings have 623 citations, the solution [27] of Catalan's conjecture by P. Mihăilescu has 173 citations and the article [10] of E. Z. Chein has 2 citations.

A set X (of sets) is an *intersecting set system* if for every $A, B \in X$ we have $A \cap B \neq \emptyset$. For any set X and $k \in \mathbb{N}_0$ we define

$$\tbinom{X}{k} = \{Y : \, Y \subset X \wedge |Y| = k\} \,.$$

Theorem 4.2.1 (Erdős–Ko–Rado) *Let $k, n \in \mathbb{N}$ be such that $n \geq 2k$. Then every intersecting set system $X \subset \binom{[n]}{k}$ has $|X| \leq \binom{n-1}{k-1}$ elements. This bound is tight.*

Proof.

□

Chapter 5

The relations of Cassels

We want to show, and eventually we prove it, that for no primes $p, q \in \mathbb{P} \setminus \{2\}$ there are nonzero integers $x, y \in \mathbb{Z}^*$ such that $x^p - y^q = 1$. Clearly, $p = q$ is impossible. If (x, y, p, q) is a nonzero solution, then so is $(-x, -y, q, p)$. Thus we may assume that $p > q$. In this chapter we prove the property of the hypothetical nonzero solution $x, y \in \mathbb{Z}^*$ of the equation

$$x^p - y^q = 1 \text{ where } p > q > 2 \text{ are primes},$$

obtained by John W. S. Cassels (1922–2015): p divides y and q divides x. In particular, $|y| \geq q$ and $|x| \geq p$, but in Section 5.3 we deduce much stronger lower bounds ... but bounds on what? On the size of the hypothetical (nonzero) solution of the displayed Catalan's equation. But we eventually prove that this solution does not exist! Starting from such a solution, in the next chapter we begin a long journey. On the end of it there will be a shining supernova, or if you want a black hole, of a contradiction.

5.1 The relation $q \mid x$

The next lemma is proven as Lemma B.1.2 in Section B.1.

Lemma 5.1.1 *Let u be a real number. Then the following hold.*

1. *If $u \geq 1$ then $f(x) = \left(u^x + 1\right)^{1/x} \colon (0, +\infty) \to (0, +\infty)$ decreases.*
2. *If $u > 1$ then $f(x) = \left(u^x - 1\right)^{1/x} \colon (0, +\infty) \to (0, +\infty)$ increases.*

Now we prove the easier of the two divisibilities due to J. W. S. Cassels.

Theorem 5.1.2 *If $p > q > 2$ are primes and $x, y \in \mathbb{Z}^*$ satisfy $x^p - y^q = 1$ then $q \mid x$.*

Proof. Suppose that p, q, x and y are as stated and that $\neg(q \mid x)$. Then by Lemma 4.1.1 the two factors in $(y+1) \cdot \frac{y^q+1}{y+1} = x^p$ are coprime. By Corollary C.1.6 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.

We set

$$g(X) = X^p - (b^p-1)^q, \ X \in \mathbb{R}\,,$$

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

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

and

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

because, since $q < p$, by part 2 of Lemma 5.1.1 it holds that

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

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,

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

(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 5.1.1 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 have a contradiction and deduce that $q \mid x$. □

Thus $|x| \geq q$, but in the next section we need a stronger lower bound on x. In its proof in the next proposition we use two lemmas.

Lemma 5.1.3 *Let $q \in \mathbb{N}$ and $y \in \mathbb{Z}$. If $q > 2$ is odd, and $y \equiv -1 \pmod q$ then $\frac{y^q+1}{y+1}$ is q both modulo q^2 and $y+1$.*

Proof. This follows from

$$\tfrac{y^q+1}{y+1} = \tfrac{(y+1-1)^q+1}{y+1} = \textstyle\sum_{j=1}^{q-1}\binom{q}{j}(y+1)^{j-1}(-1)^{q-j}\,.$$

Modulo q^2 this is $q(-1)^{q-1} + \binom{q}{2}(y+1) \equiv q$. □

Lemma 5.1.4 *Let $q \in \mathbb{N}$ and $y \in \mathbb{Z}$. If $q > 2$ and is odd, and $y \equiv -1 \pmod{q}$ then $\frac{y^q+1}{y+1} \equiv q \pmod{q^2}$.*

Proposition 5.1.5 *If $p > q > 2$ are primes and $x, y \in \mathbb{Z}^*$ satisfy $x^p - y^q = 1$ then $|x| \geq q + q^{p-1}$.*

Proof. Suppose that p, q, x and y are as stated. From the proof of Theorem 5.1.2 we know that both factors in $(y+1) \cdot \frac{y^q+1}{y+1} = x^p$ are divisible by q. By Lemma **??** we have $\frac{y^q+1}{y+1} \equiv q \pmod{q^2}$, hence $\neg\big(q^2 \mid \frac{y^q+1}{y+1}\big)$. Since the GCD of both factors is q, Corollary C.1.7 gives

$$y + 1 = q^{p-1}b^p \text{ and } \tfrac{y^q+1}{y+1} = qu^p \text{ for } b, u \in \mathbb{Z}\,.$$

□

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

Recall from Section B.2 that for $m \in \mathbb{N}$, a point $a \in I$, an open interval $I \subset \mathbb{R}$ and an m times differentiable function $f\colon I \to \mathbb{R}$, we denote by

$$T_a^m(f) = T_a^m(f(X)) = T_a^m(f)(X) = \textstyle\sum_{j=0}^m \frac{1}{j!} f^j(a)(X-a)^j \quad (\in \mathbb{R}[X])$$

the Taylor polynomial of f with order m and center a. In this section we consider for odd integers $p > q \geq 3$, for $m \in \mathbb{N}$, $I = \mathbb{R}$ and $a = 0$ the polynomial $T_0^m(F)$ for the function

$$F(X) = F_{p,q}(X) = \big((1+X)^p - X^p\big)^{1/q}\,.$$

This is possible because $(1+X)^p - X^p > 0$ for every $X \in \mathbb{R}$. The following first lemma is proven as Corollary B.2.2 in Section B.2.

Lemma 5.2.1 *If $F_{p,q}(X)$ is as above and $m < p$ then*

$$T_0^m(F_{p,q}(X)) = T_0^m((1+X)^{p/q}) = \textstyle\sum_{j=0}^m \binom{p/q}{j} X^j\,.$$

The second lemma is proven as Lemma B.1.4 in Section B.1.

Lemma 5.2.2 *Suppose that $F_{p,q}(X)$ is as above and $m = \lfloor p/q \rfloor + 1$. Then for every $X \in (-1, 1)$,*

$$|F_{p.q}(X) - T_0^m(F_{p,q}(X))| \leq (1 - |X|)^{-2} \cdot |X|^{m+1}\,.$$

The third lemma is proven as Corollary C.1.13 in Section C.1. Recall that for $k \in \mathbb{N}$,

$$\tbinom{X}{k} = \tfrac{1}{k!} X(X-1)\ldots(X-k+1)$$

and that $\binom{X}{0} = 1$.

Lemma 5.2.3 *Suppose that q is a prime, $a \in \mathbb{Z}$ is not divisible by q and $k \in \mathbb{N}_0$. Then there exists a number $b \in \mathbb{Z}$ not divisible by q such that*

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

Finally, recall the classical bound on the p-adic order of factorial which is proven as Proposition C.1.11 in Section C.1.

Lemma 5.2.4 *If q is a prime and $m \in \mathbb{N}_0$ then*

$$\mathrm{ord}_q(m!) \le \frac{m}{q-1}\,.$$

With the help of the four lemmas and the previous section we prove the main result of this chapter.

Theorem 5.2.5 *If $p > q > 2$ are primes and $x, y \in \mathbb{Z}^*$ satisfy $x^p - y^q = 1$ then $p \,|\, y$.*

Proof. Let p, q, x and y be as stated and let $\neg(p \,|\, x)$. By Lemma 4.1.1 the two factors in $(x-1)\cdot\frac{x^p-1}{x-1} = y^q$ are coprime; we obtain a contradiction. By Corollary C.1.6 we have $x - 1 = a^q$ with $a \in \mathbb{Z}$. Clearly $a \neq 0$. Thus $y^q = (a^q+1)^p - 1$ and with $F_{p,q}(X)$ as above 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

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

Using Lemmas 5.2.1 and 5.2.3 and the inequality $mq - p \ge 0$ (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 5.2.3 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 5.1.2, $a \neq 0, \pm 1$ and $|a| \ge 2$. We can use Lemma 5.2.2 with $X = 1/a^q$ and get the bound

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

By Proposition 5.1.5, $|x| \geq q^{p-1} + q$. Thus

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

If the exponent is negative, we are done. And indeed, by Lemma 5.2.4, the inequality $m < \frac{p}{q} + 1$ and since $p \geq 5$ and $q \geq 3$, it is negative:

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

□

5.3 Lower bounds on x and y

5.4 Remarks

Theorem 5.1.2 is due to J. W. S. Cassels in [5] in 1953. We followed the proof in [34, pp. 33–34], [34, Exercise 6.1] and fixed in it some errors. Theorem 5.2.5 is due to J. W. S. Cassels in [6] in 1960. We followed the proof in [34, pp. 35–37], [34, Exercise 5.7].

Chapter 6

The obstruction group

Chapter 7

Mihăilescu IV

In this chapter we prove the next theorem.

7.1 Equation $x^p - y^q = 1$ for $p \leq 5$ or $q \leq 5$

Theorem 7.1.1 (Mihăilescu IV) *Equation $x^p - y^q = 1$ has no nonzero solution $x, y \in \mathbb{Z}^*$ if p and q are odd primes such that $p \leq 5$ or $q \leq 5$.*

7.2 Remarks

Appendix A

Some set theory

A.1 Axioms of ZFC

A *poset* (partially ordered set) $X_{\rm po} = (X, \prec)$ is a transitive and irreflexive binary relation $\prec$ ($\subset X \times X$) on a set X, cf. the definition of linear orders in Notation. Instead of writing $(a, b) \in \prec$, we write $a \prec b$. The notation $a \preceq b$ means that $a \prec b$ or $a = b$. Let $Y \subset X$. We say that $b \in X$ is an *upper bound* of Y (in $X_{\rm po}$), if $y \preceq b$ for every $y \in Y$. We say that Y is a *chain* (in $X_{\rm po}$) if $(Y, \prec)$ is a linear order. An element $a \in X$ is *maximal* (in $X_{\rm po}$) if there is no $b \in X$ such that $a \prec b$.

Axiom A.1.1 (Zorn's lemma) *Suppose that $X_{\rm po} = (X, \prec)$ is a poset such that every chain in it has an upper bound. Then for every $a \in X$ there is a maximal element $b \in X$ such that $a \preceq b$.*

A.2 Remarks

Appendix B

Mathematical analysis

In this appendix we collect and, more importantly, prove several analytical results that we used in the previous pages in the described solution of Catalan's conjecture.

B.1 Sums, inequalities and bounds

Proposition B.1.1 *If $m \in \mathbb{N}_0$ and $X \in (-1,1)$ then*

$$\textstyle\sum_{n=m}^{\infty} X^{-n} = \frac{X^{-m}}{1-X}\,.$$

Proof. Let m and X be as stated. Then for $n \in \mathbb{N}$ with $n \geq m$ we have $X^m + X^{m+1} + \cdots + X^n = \frac{X^m}{1-X}(1 - X^{n-m+1}) \to \frac{X^m}{1-X}$ as $n \to \infty$. □

Lemma B.1.2 *Let u be a real number. Then the following hold.*

1. *If $u \geq 1$ then $f(X) = \big(u^X + 1\big)^{1/X} : (0,+\infty) \to (0,+\infty)$ decreases.*
2. *If $u > 1$ then $f(X) = \big(u^X - 1\big)^{1/X} : (0,+\infty) \to (0,+\infty)$ 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 $Xu^X \log u = u^X \log(u^X) > (u^X-1)\log(u^X-1)$. □

Lemma B.1.3 *If $p > 1$, $X \in (-1,1)$ and ξ are real numbers such that ξ lies between $(1+X)^p - X^p$ and $(1+X)^p$, then $|\xi| \geq (1-|X|)^p$*

Proof.

□

For odd integers $p > q > 2$ and $X \in \mathbb{R}$ let

$$F_{p,q}(X) = \big((X+1)^p - X^p\big)^{1/q}\,.$$

Lemma B.1.4 *Suppose that $F(X) = F_{p,q}(X)$ is as above and $m = \lfloor p/q \rfloor + 1$. Then for every $X \in (-1,1)$,*

$$|F(X) - T_0^m(F)(X)| \le (1-|X|)^{-2} \cdot |X|^{m+1}\,.$$

Proof. We bound the terms $A = A(X)$ and $B = B(X)$ in

$$|F(X) - T_0^m(F)(X)| \le |F(X) - (1+X)^{p/q}| + |(1+X)^{p/q} - T_0^m(F)(X)| = A + B\,.$$

We estimate $|A|$ by applying Lagrange's mean value theorem to the function $f(Y) = Y^{1/q}$ and the interval spanned by the numbers $(1+X)^p - X^p$ and $(1+X)^p$. Thus with some number ξ lying between them we have by Lemma B.1.3 and by the inequality $p(1-\frac{1}{q}) > 2$ that

$$|A| \le \tfrac{1}{q}|X|^p|\xi|^{1/q-1} \le \tfrac{1}{q}|X|^p(1-|X|)^{p(1/q-1)} \le \tfrac{1}{q}|X|^p(1-|X|)^{-2}\,.$$

□

B.2 Power series

Let $n \in \mathbb{N}$, $a \in I \subset \mathbb{R}$ where I is an open interval and let $f\colon I \to \mathbb{R}$ have at every $X \in I$ finite n-th derivative $f^{(n)}(X) \in \mathbb{R}$. Then

$$T_a^n(f(X)) = T_a^n(f)(X) = \sum_{j=0}^{n} \frac{1}{j!} f^{(j)}(a)(X-a)^j \quad (\in \mathbb{R}[X])$$

is the *Taylor polynomial of f with order n and center a.*

Proposition B.2.1 *In this situation $T_a^n(f)(X)$ is a unique polynomial $p(X)$ in $\mathbb{R}[X]$ with degree at most n such that*

$$f(X) = p(X) + o\big((X-a)^n\big) \quad (X \to a)\,.$$

Proof.

□

Corollary B.2.2 *If $F(X) = F_{p,q}(X)$ is as before Lemma B.1.4 and $m \in \mathbb{N}$ satisfies $m < p$ then*

$$T_0^m(F(X)) = T_0^m((1+X)^{p/q}) = \textstyle\sum_{j=0}^{m} \binom{p/q}{j} X^j\,.$$

Proof. In view of the previous proposition, to prove the first equality it suffices to show that $F(X) - (1+X)^{p/q} = o(X^m)$ as $X \to 0$. This is true because $F(X) - (1+X)^{p/q}$ equals

$$\begin{aligned}\big((1+X)^p - X^p\big)^{1/q} - (1+X)^{p/q} &= (1+X)^{p/q}\big(\big(1 - \tfrac{X^p}{(1+X)^p}\big)^{1/q} - 1\big)\\ &= (1+O(X))\cdot((1+O(X^p)) - 1)\\ &= O(X^p) = o(X^m)\,.\end{aligned}$$

The second equality is immediate from the definition of Taylor polynomials,

$$\tfrac{1}{j!}\big((1+X)^{p/q}\big)^{(j)}(0) = \tbinom{p/q}{j}(1+X)^{p/q-j+1}(0) = \tbinom{p/q}{j}\,.$$

□

B.3 Remarks

Appendix C

Elementary number theory

In this appendix we collect and, more importantly, prove several results in elementary number theory that were used in the solution of Catalan's conjecture in the first part of the book.

Section C.1 concerns prime numbers. Theorem C.1.2 demonstrates in three ways the infinitude of their set $\mathbb{P}$. Theorem C.1.3, the *Fundamental Theorem of Arithmetic* (FTA), establishes uniqueness of prime factorizations of natural numbers. Corollaries C.1.5– C.1.8 of FTA are main tools in elementary solution of Diophantine equation and we use them repeatedly in Chapter 3. In Chapter 2 we apply Corollary C.1.10 on the p-adic order whose properties are established in Proposition C.1.9. Propositions C.1.11 and C.1.12 and their Corollary C.1.13 on $\mathrm{ord}_p(n)$ are used in Chapter 5.

In Section C.2 we discuss some Diophantine equations. Theorem C.2.1 expresses all integral solutions of any Pell equation in terms of the minimum solution. Proposition C.2.2 describes all rational solutions of $\alpha x^2 + \beta xy + y^2 = 1$, under a condition on $\alpha, \beta \in \mathbb{Q}$. We need these results in Chapters 3 and 4.

C.1 Prime numbers

Recall that $p \in \mathbb{N}$ is a prime number, briefly a prime, if $p > 1$ and for $m, n \in \mathbb{N}$ the equality $p = mn$ holds only if $\{m, n\} = \{1, p\}$; the number p is then multiplicatively indecomposable, irreducible. The set of primes is denoted by $\mathbb{P}$, so that $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$, and primes themselves are denoted by the letters p and q. We say that $p \in \mathbb{P}$ is a *prime divisor* of $n \in \mathbb{N}$ if $p \,|\, n$. We begin with a simple but important lemma.

Lemma C.1.1 *An integer $n \in \mathbb{Z}$ has a prime divisor iff $n \neq -1, 1$.*

Proof. The numbers ± 1 clearly have no prime divisor. Every prime is a prime divisor of 0. Let $n \neq 0, \pm 1$ be an integer and $M = \{m \in \mathbb{N} : \ m > 1 \wedge m \,|\, n\}$. Then $M \neq \emptyset$ because $|n| \in M$ and $\min(M)$ is a prime divisor of n. □

Theorem C.1.2 *The set of prime numbers $\mathbb{P}$ is infinite.*

Proof. We give three proofs. Many more can be found in the literature and on the Internet.

First version of Euclid's proof. The world with only finitely many primes is contradictory because it contains an integer $m \geq 2$ with no prime divisor, in contradiction with Lemma C.1.1. We assume that $\mathbb{P}$ is finite. $\mathbb{P} \neq \emptyset$ because $2 \in \mathbb{P}$. The number $m = 1 + \prod_{p \in \mathbb{P}} p$ (≥ 3) exists due to finiteness and nonemptiness of $\mathbb{P}$. It has no prime divisor: if $p \in \mathbb{P}$ and $p \,|\, m$ then $p \,|\, 1$ which is impossible.

Second version of Euclid's proof. Positively taken, the previous proof gives a recipe for obtaining for any finite set of primes X a prime $q \notin X$. If $X = \emptyset$, we take $q = 2$. For $X \neq \emptyset$ we take the above number $m = 1 + \prod_{p \in X} p$ and set q to be any prime divisor of it, for example the one described in the proof of Lemma C.1.1. Then $q \notin X$, for else $q \,|\, 1$. Hence $\mathbb{P}$ is infinite.

The proof of Cass and Wildenberg. It is not as well known as Euclid's proof(s), which is a pity. A set $X \subset \mathbb{Z}$ is *periodic* if for some $a \in \mathbb{N}$ we have $X = a + X$ ($= \{a + x : \ x \in X\}$). It is easy to see that (i) no nonempty finite set is periodic and that (ii) every (infinite) arithmetic progression $a + d\mathbb{Z} = \{a + dx : \ x \in \mathbb{Z}\}$, $a \in \mathbb{Z}$ and $d \in \mathbb{N}$, is periodic. Periodic sets are closed (iii) to complements to $\mathbb{Z}$ and (iv) to finite unions. Due to Lemma C.1.1 we have the equality

$$\mathbb{Z} \setminus \{-1, \, 1\} = \bigcup_{p \in \mathbb{P}} (0 + p\mathbb{Z}) \, .$$

If $\mathbb{P}$ is finite, it is contradictory. By (i) and (iii) the left-hand side is not periodic. By (ii) and (iv) the right-hand side is periodic. □

We view the maps $f \colon \mathbb{P} \to \mathbb{N}_0$ with finite supports as finite multisets of primes. We denote the set of these maps by P. Let $f \in P$ and $p \in \mathbb{P}$. Recall that $S(f)$ ($\subset \mathbb{P}$) is the support of f. We call the value $f(p)$ ($\in \mathbb{N}_0$) the *multiplicity* of p in f. We define the *factorization map* $F \colon P \to \mathbb{N}$ by

$$F(f) = \prod_{p \in \mathbb{P}} p^{f(p)} \quad \big(= \prod_{p \in \mathbb{P}, f(p) > 0} p^{f(p)} \big) \, .$$

To be precise, if $2 = p_1 < p_2 < \dots$ is the sequence of all primes then we define the value $F(f) \in \mathbb{N}_0$ as the limit

$$F(f) = \lim_{n \to \infty} \prod_{i=1}^{n} p^{f(p_i)}$$

of the eventually constant sequence of partial products. If $f \in P$ and $F(f) = n$, we say that f is a *prime factorization* of n. We prove the *Fundamental Theorem of Arithmetic* (FTA).

Theorem C.1.3 (FTA) *The factorization map $F \colon P \to \mathbb{N}$ is a bijection.*

We preface its proof with a lemma.

Lemma C.1.4 1. *Every $n \in \mathbb{N}$ has a prime factorization $f \colon \mathbb{P} \to \mathbb{N}_0$.* 2. *If $n \in \mathbb{N}$ and $p \,|\, n$ then n has a prime factorization f such that $p \in S(f)$.*

Proof. 1. This is actually the surjection part of Theorem C.1.3. We prove by induction on $n \in \mathbb{N}$ that there is a map $f\colon \mathbb{P} \to \mathbb{N}_0$ with finite support such that $F(f) = n$. For $n = 1$ we take for f simply the constantly 0 function. Suppose that $n > 1$ and that every $m < n$ has a prime factorization. Using Lemma C.1.1 we write n as $n = pm$ where p is a prime and $m \in \mathbb{N}$ is smaller than n. Let f be a prime factorization of m. Then the map $g\colon \mathbb{P} \to \mathbb{N}_0$ with the same values as f, except for $g(p) = f(p) + 1$, is a prime factorization of n.

2. Let $n \in \mathbb{N}$ and $p \in \mathbb{P}$ be as stated, so that $n = pm$ with $m \in \mathbb{N}$. We use part 1 and take a prime factorization g of m. We define a map $f\colon \mathbb{P} \to \mathbb{N}_0$ by giving it the values of g, except for $f(p) = g(p) + 1$. Then $f \in P$, $f(p) > 0$ and $F(f) = pF(g) = pm = n$. □

Proof of Theorem C.1.3. In part 1 of Lemma C.1.4 we proved that F is surjective and it remains to show that it is injective; this is the main claim of FTA. For contrary let $n \in \mathbb{N}$ be minimum such that there are $f, g \in P$ with $f \neq g$ and $F(f) = F(g) = n$. Clearly, $\sum_{p\in\mathbb{P}} f(p) \geq 2$, $\sum_{p\in\mathbb{P}} g(p) \geq 2$ and $S(f) \cap S(g) = \emptyset$ (else for some p the number $\frac{n}{p}$ would contradict the choice of n). Thus if $p = \min(S(f))$ and $q = \min(S(g))$, then $p \neq q$. It follows that $m = n - pq > 0$, $m \in \mathbb{N}$ and $m < n$. Let h be the unique prime factorization of m. Since p and q divide n, they divide m. Part 2 of Lemma C.1.4 gives that $p, q \in S(h)$. Thus $pq \,|\, m$ and $pq \,|\, n$. Then $\frac{n}{p} < n$ and $q \,|\, \frac{n}{p}$. We set $f_0 \in P$ to be equal to f, except for $f_0(p) = f(p) - 1$. Then $F(f_0) = \frac{n}{p}$ and f_0 is the unique prime factorization of $\frac{n}{p}$. Part 2 of Lemma C.1.4 gives that $q \in S(f_0)$. Since $f(q) = f_0(q)$, we have the contradiction that $q \in S(f) \cap S(g)$. □

Thus for every $n \in \mathbb{N}$ we can correctly denote its unique prime factorization by $F^{-1}(n)$, and n has the unique expression as the product

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} ,$$

where $k \in \mathbb{N}_0$, $p_1 < p_2 < \dots < p_k$ are primes and $a_i = F^{-1}(n)(p_i) \in \mathbb{N}$ are their multiplicities. For $n = 1$ we have $k = 0$ and define this product as 1.

FTA has several corollaries which in elementary number theory, especially in elementary solutions of Diophantine equations, are used all the time. Recall that $m, n \in \mathbb{Z}$ are coprime if their common divisors are only -1 and 1. If $m, n \neq 0$ then by Theorem C.1.3 m and n are coprime iff $F^{-1}(|m|)$ and $F^{-1}(|n|)$ have disjoint supports.

Corollary C.1.5 *Let $a, b, c \in \mathbb{Z}$. If the number a divides the product bc and a, b are coprime, then a divides c.*

Proof. If $bc = 0$ then $b = 0$ or $c = 0$. In the former case $a = \pm 1$ and divides c. In the latter case a divides c because 0 is divisible by every number. We suppose that $b, c \neq 0$, hence $a \neq 0$, and consider the prime factorizations $f = F^{-1}(|a|)$, $g = F^{-1}(|b|)$, $h = F^{-1}(|c|)$ and $j = F^{-1}(|bc|)$. By Theorem C.1.3, for every p we have $g(p) + h(p) = j(p)$. By the assumption $S(f) \cap S(g) = \emptyset$ and for every p

we have $f(p) \le j(p)$. Thus for every p it holds that $f(p) \le h(p)$. It means that $a \mid c$. □

For $x, y \in \mathbb{Z}$ we write $x \sim y$ iff $x = y$ or $x = -y$. It is an equivalence relation.

Corollary C.1.6 *Let $k \in \mathbb{N}$ with $k \ge 2$, $x, y, z \in \mathbb{Z}$ with $xy \sim z^k$ and x, y be coprime. Then there exist $x_0, y_0 \in \mathbb{Z}$ such that $x \sim x_0^k$ and $y \sim y_0^k$. For odd k the last two $\sim$s may be replaced by $=$s.*

Proof. For $xyz = 0$ it holds because then $\{x, y\} = \{0, \pm 1\}$ are $\pm$ k-th powers. We assume that $x, y, z \neq 0$ and consider the prime factorizations $f = F^{-1}(|x|)$, $g = F^{-1}(|y|)$ and $h = F^{-1}(|xy|)$. Since $|x| \cdot |y| = |z|^k$, Theorem C.1.3 implies that for every p we have $f(p) + g(p) = k \cdot h(p)$. Since $S(f) \cap S(g) = \emptyset$, one of the last two summands is always zero. Hence for every p both $f(p)$ and $g(p)$ is divisible by k, both $|x|$ and $|y|$ is a k-th power and the result follows. For odd k the k-th powers absorb the sign $-$ as $-1 = (-1)^k$. □

Note that for even $k \ge 2$ the $\sim$s in general cannot be removed. For example, $(-1)(-1) = 1^2$ with coprime $-1, -1$ gives only $-1 \sim (\pm 1)^2$.

Corollary C.1.7 *Let p be a prime, $k \in \mathbb{N}$ with $k \ge 2$, $x, y, z \in \mathbb{Z}$ with $xy \sim z^k$ and let $\mathrm{GCD}(x, y) = p$. Then there exist coprime $x_0, y_0 \in \mathbb{Z}$ such that $x \sim p x_0^k$, $y \sim p^{k-1} y_0^k$ or $x \sim p^{k-1} x_0^k$, $y \sim p y_0^k$. For odd k we have instead of the last four $\sim$s equalities.*

Proof. For $xyz = 0$ it holds because then $\{x, y\} = \{0, \pm p\}$. We assume that $x, y, z \neq 0$ and consider the prime factorizations $f = F^{-1}(|x|)$, $g = F^{-1}(|y|)$ and $h = F^{-1}(|xy|)$. As in the previous proof we deduce that for every $q \neq p$ both $f(q)$ and $g(q)$ is divisible by k. Also, $f(q) \cdot g(q) = 0$. Since $f(p) + g(p) = h(p)$ is divisible by k, $f(p) \cdot g(p) > 0$ and one of $f(p)$ and $g(p)$ is 1, we deduce that

$$\{f(p),\, g(p)\} = \{1,\, k - 1 + rk\} \text{ with } r \in \mathbb{N}_0\,.$$

The result follows. Minuses are absorbed by odd powers as before. □

Note that for $k = 2$ the two possibilities for x and y coincide.

We leave the proof of the fourth corollary to the interested reader.

Corollary C.1.8 *Let p be a prime, $k \in \mathbb{N}$ with $k \ge 2$, $x, y, z \in \mathbb{Z}$ with $xy \sim p z^k$ and let x, y be coprime. Then there exist coprime $x_0, y_0 \in \mathbb{Z}$ such that $x \sim p x_0^k$, $y \sim y_0^k$ or $x \sim x_0^k$, $y \sim p y_0^k$. For odd k we have instead of the last four $\sim$s equalities.*

In Section D.1 we generalize these corollaries to monoids and domains.

For any prime p and nonzero $a \in \mathbb{Z}$ we define $\mathrm{ord}_p(a) \in \mathbb{N}_0$ as the maximum $k \in \mathbb{N}_0$ such that $p^k \mid a$. Thus $\mathrm{ord}_p(a) = F^{-1}(|a|)(p)$. We extend ord_p to $\mathbb{Q}$. For any nonzero fraction $\frac{a}{b}$ we set $\mathrm{ord}_p(\frac{a}{b}) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. We define

$\mathrm{ord}_p(0) = +\infty$. It is easy to see that $\mathrm{ord}_p(\frac{a}{b})$ does not depend on the concrete representation of the fraction $\frac{a}{b}$. We extend addition of integers to $\mathbb{Z}^\infty = \mathbb{Z} \cup \{+\infty\}$ by setting $a + (+\infty) = (+\infty) + a = +\infty$ for every $a \in \mathbb{Z}^\infty$. As for the comparison, $a < +\infty$ for every $a \in \mathbb{Z}$. The map $\mathrm{ord}_p \colon \mathbb{Q} \to \mathbb{Z}^\infty$ has the following properties.

Proposition C.1.9 *Let p be a prime number and $\alpha, \beta \in \mathbb{Q}$.*

1. *It holds that* $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$.
2. *We have* $\mathrm{ord}_p(\alpha + \beta) \geq \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta))$, *and if* $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$ *then the equality holds.*
3. *More generally, for every fractions α_1, α_2, …, α_n where $n \geq 2$ we have*

$$\mathrm{ord}_p\big(\textstyle\sum_{i=1}^n \alpha_i\big) \geq \min(\alpha_1, \alpha_2, \ldots, \alpha_n)\,,$$

and if the minimum is attained uniquely then the equality holds.

Proof. 1. If $\alpha\beta = 0$ then it holds because we have $+\infty$ on both sides. If $\alpha\beta \neq 0$ then with $\alpha = \frac{a}{b}$ and $\beta = \frac{c}{d}$ we have by Theorem C.1.3 for every p that

$$\begin{aligned}\mathrm{ord}_p(\alpha\beta) \;&=\; \mathrm{ord}_p(ac) - \mathrm{ord}_p(bd) = \mathrm{ord}_p(a) + \mathrm{ord}_p(c) - \\ &\quad - \mathrm{ord}_p(b) - \mathrm{ord}_p(d) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) + \\ &\quad + \mathrm{ord}_p(c) - \mathrm{ord}_p(d) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)\,.\end{aligned}$$

2. Let $\alpha = \frac{a}{b}$ and $\beta = \frac{c}{d}$. Multiplying

$$\alpha + \beta = \tfrac{ad+bc}{bd} = \tfrac{a}{b} + \tfrac{c}{d}$$

by bd ($\neq 0$) and using part 1 we see that we may assume that $\alpha, \beta \in \mathbb{Z}$. Then it is easy to check part 2 if $\alpha\beta = 0$. Let $\alpha\beta \neq 0$ and $\alpha = p^r\alpha_0$, $\beta = p^s\beta_0$ with $r = \mathrm{ord}_p(\alpha)$, $s = \mathrm{ord}_p(\beta)$ ($\in \mathbb{N}_0$) and nonzero $\alpha_0, \beta_0 \in \mathbb{Z}$ not divisible by p. We may assume that $r \leq s$ and get

$$\alpha + \beta = p^r(\alpha_0 + p^{s-r}\beta_0) =: p^r c,\ c \in \mathbb{Z}\,.$$

By part 1 we have $\mathrm{ord}_p(\alpha + \beta) = r + \mathrm{ord}_p(c) \geq r = \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta))$. If $r < s$ then c is not divisible by p, thus $\mathrm{ord}_p(c) = 0$ and $\mathrm{ord}_p(\alpha + \beta) = r = \min(\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta))$.

3. We proceed by induction on n. For $n = 2$ this is part 2. For $n > 2$ we get by induction, denoting $S = \sum_{i=1}^n \alpha_i$ and $T = \sum_{i=1}^{n-1} \alpha_i$, that $\mathrm{ord}_p(S)$ is

$$\begin{aligned}\mathrm{ord}_p(T + \alpha_n) &\overset{(1)}{\geq} \min(\mathrm{ord}_p(T), \mathrm{ord}_p(a_n)) \\ &\overset{(2)}{\geq} \min\big(\min(\mathrm{ord}_p(a_1), \ldots, \mathrm{ord}_p(a_{n-1})), \mathrm{ord}_p(a_n)\big) \\ &= \min(\mathrm{ord}_p(a_1), \ldots, \mathrm{ord}_p(a_n))\,.\end{aligned}$$

If $\min(\mathrm{ord}_p(\alpha_i) :\ i \in [n])$ is attained uniquely for $i = n$, then

$$\mathrm{ord}_p(\alpha_n) < \min(\mathrm{ord}_p(a_1), \ldots, \mathrm{ord}_p(a_{n-1})) \leq \mathrm{ord}_p(T)$$

and inequalities (1) and (2) become equalities. If that minimum is attained uniquely for an $i \in [n-1]$, then by induction

$$\mathrm{ord}_p(T) = \min(\mathrm{ord}_p(a_1),\ \ldots,\ \mathrm{ord}_p(a_{n-1})) < \mathrm{ord}_p(\alpha_n)$$

and inequalities (1) and (2) again become equalities. □

Corollary C.1.10 *Let $n \in \mathbb{N}$, p be a prime number and for $i \in [n]$ we have fractions $\alpha_i \in \mathbb{Q}$. Suppose that*

$$\forall\, i \in [n-1] :\ \mathrm{ord}_p(\alpha_i) > \mathrm{ord}_p(\alpha_n)\,,$$

where for $n = 1$ we interpret it as $+\infty > \mathrm{ord}_p(\alpha_n)$. Then $\sum_{i=1}^n \alpha_i \neq 0$.

Proof. Let $n = 1$. Then $+\infty > \mathrm{ord}_p(\alpha_n)$ gives $\sum_{i=1}^n \alpha_i = \alpha_n \neq 0$. Let $n \geq 2$. By the assumption, $+\infty > \mathrm{ord}_p(\alpha_n)$. By property 3 in the previous proposition, $\mathrm{ord}_p\big(\sum_{i=1}^n \alpha_i\big) = \mathrm{ord}_p(\alpha_n)$. Thus $+\infty > \mathrm{ord}_p(\sum_{i=1}^n \alpha_i)$ and $\sum_{i=1}^n \alpha_i \neq 0$. □

Proposition C.1.11 *If p is a prime and $m \in \mathbb{N}_0$ then*

$$\mathrm{ord}_p(m!) = \textstyle\sum_{k=1}^{\infty} \big\lfloor \frac{m}{p^k} \big\rfloor \leq \frac{m}{p-1}\,.$$

Proof. For $m = 0$ this holds trivially, and we assume that $m \in \mathbb{N}$. The first equality displayed then follows by double counting the pairs

$$A = \{(k,\, n) \in \mathbb{N}^2 :\ p^k \,|\, n \wedge n \leq m\}\,.$$

Then $|A| = \sum_{k=1}^{\infty} \lfloor \frac{m}{p^k} \rfloor$ by grouping the pairs according to k, but on the other hand $|A| = \sum_{n=1}^{m} \mathrm{ord}_p(n) = \mathrm{ord}_p(m!)$ by grouping the pairs according to n and using part 1 of Proposition C.1.9. The inequality displayed follows from the sum of geometric series

$$\textstyle\sum_{k=1}^{\infty} \frac{1}{p^k} = \sum_{k=1}^{\infty} p^{-k} = \frac{1/p}{1-1/p} = \frac{1}{p-1}\,,$$

see Proposition B.1.1. □

This formula for the p-adic order of factorial is due to A.-M. Legendre. We need a generalization of it.

Proposition C.1.12 *Let p be a prime, $m \in \mathbb{N}$ and $M = \prod_{j=1}^{m}(a + jd)$, where $a, d \in \mathbb{Z}$ and $\neg(p \,|\, d)$. For $k \in \mathbb{N}$ we denote by $r(k) \in \{0, 1, \ldots, m-1\}$ the remainder obtained when m is divided by p^k, so that $r(k) = m - p^m \lfloor \frac{m}{p^k} \rfloor$, and set $\varepsilon(k) = |\{j \in [r(k)] :\ p^k \,|\, (a + jq)\}|$. Then $\varepsilon(k) \in \{0, 1\}$ for every k and*

$$\mathrm{ord}_p(M) = \textstyle\sum_{k=1}^{\infty} \big(\big\lfloor \frac{m}{p^k} \big\rfloor + \varepsilon(k)\big)\,.$$

Proof. For $k \in \mathbb{N}$ let $s(k) = |\{j \in [m] : \ p^k \,|\, (a + jd)\}|$. The argument in the previous proof shows that $\mathrm{ord}_p(M) = \sum_{k=1}^{\infty} s(k)$. We show that $s(k) = \left\lfloor \frac{m}{p^k} \right\rfloor + \varepsilon(k)$. For $j, j' \in [m]$ if $a + jd \equiv a + j'd$ modulo p^k, then $(j - j')d \equiv 0$ and $j \equiv j'$. So if $I \subset [m]$ is an interval of numbers with length $|I| \leq p^k$ then for every residue r modulo p^k there is at most one $j \in I$ such that $a + jd \equiv r$, and if $|I| = p^k$ then there is exactly one such $j \in I$. Hence the partition $[m] = J \cup I_1 \cup \cdots \cup I_l$ into intervals $J < I_1 < \cdots < I_l$ with $|J| = r(k)$ and $|I_i| = p^k$, thus $l = \left\lfloor \frac{m}{p^k} \right\rfloor$, shows that $s(k) = l + \varepsilon(k)$ and that $\varepsilon(k) \in \{0, 1\}$. □

Corollary C.1.13 *Suppose that q is a prime, $a \in \mathbb{Z}$ is not divisible by q and $k \in \mathbb{N}_0$. Then there exists a number $b \in \mathbb{Z}$ not divisible by q such that*

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

Proof. For $k = 0$ it trivially holds, as $\binom{a/q}{0} = 1$, and we assume that $k \in \mathbb{N}$. Then

$$\textstyle\binom{a/q}{k} = \frac{1}{k!} \cdot \frac{1}{q^k} \cdot \prod_{j=1}^{k} (a + q - jq) \,.$$

Let $M = \prod_{j=1}^{k} (a + q - jq)$. Then $\mathrm{ord}_q\big(\binom{a/q}{k}\big) = \mathrm{ord}_q\big(\frac{1}{k!} \cdot \frac{1}{q^k}\big) = -k - \mathrm{ord}_q(k!)$ as $\mathrm{ord}_q(M) = 0$, and for every $p \neq q$ we have by Propositions C.1.11 and C.1.12 that $\mathrm{ord}_p\big(\binom{a/q}{k}\big) = \mathrm{ord}_p(M) - \mathrm{ord}_p(k!) \geq 0$. □

C.2 Diophantine equations

A *Pell equation* is any Diophantine equation $x^2 - dy^2 = 1$ with unknowns x, y and parameter $d \in \mathbb{N}$ that is not a square. If d is a square then it is easy to show that there is only the trivial solutions $(\pm 1, 0)$. Every Pell equation has infinitely many (integral) solutions. In Chapters 3 and 4 we rely on the important property of the solution set that it is generated by the *minimum (nontrivial) solution*. This is the solution $(a, b) \in \mathbb{N}^2$ such that there is no solution $(a', b') \in \mathbb{N}^2$ with $a' < a$. Every Pell equation has a unique minimum solution. Already for moderately sized d the minimum solution can be quite large, but on the other hand it is often easy to find. In Chapter 3, for $x^2 - 3y^2 = 1$ it is $(a, b) = (2, 1)$. In Chapter 4, for $x^2 - (c^2 - 1)y^2 = 1$, $c \in \mathbb{N}$ with $c \geq 2$, it is $(a, b) = (c, 1)$.

We express generation of solutions of $x^2 - dy^2 = 1$ by an equality in the integral domain $(\mathbb{Z}[\sqrt{d}], 0, 1, +, \cdot)$, where

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

It is a subring of the field $\mathbb{R}$, hence a domain. The *conjugation map* is the automorphism $a + b\sqrt{d} \mapsto a - b\sqrt{d}$.

Theorem C.2.1 *Let $(a, b) \in \mathbb{N}^2$ be the minimum solution of the Pell equation $x^2 - dy^2 = 1$. Then the set of integral solutions has the form*

$$\{(\pm x_n, \pm y_n) \in \mathbb{Z}^2 : \ n \in \mathbb{N}_0\},$$

where

$$x_n + y_n\sqrt{d} = \left(a + b\sqrt{d}\right)^n \ \ (\in \mathbb{Z}[\sqrt{d}]).$$

The sequences (x_n) in $\mathbb{N}$ and (y_n) in $\mathbb{N}_0$, $n \in \mathbb{N}_0$, satisfy two recurrences, with the initial conditions $x_0 = 1$, $y_0 = 0$, $x_1 = a$ and $y_1 = b$.
1. $x_{n+1} = ax_n + dby_n$ and $y_{n+1} = bx_n + ay_n$.
2. $x_{n+2} = 2ax_{n+1} + (b^2d - a^2)x_n$ and $y_{n+2} = 2ay_{n+1} + (b^2d - a^2)y_n$.

Proof. Let a, b, x_n and y_n be as stated. The conjugation map gives that also $x_n - y_n\sqrt{d} = (a - b\sqrt{d})^n$. Hence $x_n^2 - y_n^2 d = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d})$ equals

$$(a + b\sqrt{d})^n(a - b\sqrt{d})^n = (a^2 - b^2d)^n = 1^n = 1$$

and $(x_n, y_n) \in \mathbb{N}_0^2$ is a solution. Let $(e, f) \in \mathbb{N}_0^2$ with $e \in \mathbb{N}$ be an arbitrary nonnegative solution. Since $1 = x_0 < x_1 < \ldots$, we have a unique $n \in \mathbb{N}_0$ such that $x_n \le e < x_{n+1}$. Then also $y_n \le f < y_{n+1}$ and $(a + b\sqrt{d})^n \le e + f\sqrt{d} < (a + b\sqrt{d})^{n+1}$. We set

$$g + h\sqrt{d} = \tfrac{e+f\sqrt{d}}{(a+b\sqrt{d})^n} = (e + f\sqrt{d})(a - b\sqrt{d})^n \ \ (\in \mathbb{Z}[\sqrt{d}]).$$

It follows that $(g, h) \in \mathbb{Z}^2$ is a solution. From $1 \le g + h\sqrt{d} < a + b\sqrt{d}$ we get $1 \le g < a$ and $0 \le h < b$. By the minimality of (a, b) we have $g = 1$ and $h = 0$. Hence $e = x_n$, $f = y_n$ and we see that $(\pm x_n, \pm y_n)$, $n \in \mathbb{N}_0$, exhaust all integral solutions of $x^2 - dy^2 = 1$. Let $\alpha = a + b\sqrt{d}$. The two recurrences follow from the respective identities $\alpha^{n+1} = (a + b\sqrt{d}) \cdot \alpha^n$ and $\alpha^2 = 2a \cdot \alpha + b^2d - a^2$. □

The description of the generation of the set of solutions of $x^2 - dy^2 = 1$ by the minimum solution could be completely coached in $\mathbb{Z}$ in terms of recurrences, but the description in $\mathbb{Z}[\sqrt{d}]$ is easy to manipulate algebraically.

We describe all rational solutions of a family of quadratic equations with two unknowns and rational coefficients.

Proposition C.2.2 *Let $\alpha, \beta \in \mathbb{Q}$ be such that $\beta^2 - 4\alpha$ is not a square in $\mathbb{Q}$, in particular α, β are not both zero. Then all solutions $(x, y) \in \mathbb{Q}^2$ of equation $\alpha x^2 + \beta xy + y^2 = 1$, except $(0, 1)$, are given by the formulas*

$$x = \tfrac{\beta+2m}{\alpha+\beta m+m^2} \ \text{ and } \ y = \tfrac{m^2-\alpha}{\alpha+\beta m+m^2} \ \text{ for } \ m \in \mathbb{Q}.$$

Proof. We substitute for y in the left-hand side of $\alpha x^2 + \beta xy + y^2 - 1 = 0$ the polynomial $mx - 1$ $(\in \mathbb{Q}[m, x])$:

$$\alpha x^2 + \beta x(mx - 1) + (mx - 1)^2 - 1 = (\alpha + \beta m + m^2)x^2 - (\beta + 2m)x = 0.$$

Thus $x = 0$ or $x = \frac{\beta+2m}{\alpha+\beta m+m^2}$. With the latter value we have $y = mx - 1 = \frac{m^2-\alpha}{\alpha+\beta m+m^2}$. By the assumption the denominator $\alpha + \beta m + m^2 \neq 0$ for every $m \in \mathbb{Q}$. Since for every $x, y \in \mathbb{Q}$, $x \neq 0$, there is an $m \in \mathbb{Q}$ such that $y = mx - 1$, the result follows. □

C.3 Remarks

The original proof of Euclid of Theorem C.1.2 appears, in a form, in Proposition 20 in Book IX of his *Elements*. The two Euclid's proofs here are inspired by Euclid's proof in [12]. The third proof of Theorem C.1.2 is due to D. Cass and G. Wildenberg in [4]. It combinatorially simplifies H. Fürstenberg's topological proof [18] (of infinitude of $\mathbb{P}$). On my visit on October 30, 2024, the Wikipedia page [19] still did not mention the Cass–Wildenberg proof. The proof of uniqueness of prime factorizations in Theorem C.1.3 is taken from [20, Chapter II.2.11] of the classical textbook authored by G. H. Hardy (1877–1947) and E. M. Wright (1906–2005). In [20, Notes to Chapter II] they attribute it to several authors: F. A. Lindemann in 1933, H. Davenport (date not given), E. Zermelo in 1934 and H. Hasse in 1928. The first mentioned person is not Ferdinand von Lindemann (1852–1939) who was the first to prove the transcendence of π, but Frederick Alexander Lindemann (1886–1957), "a British physicist who was the prime scientific adviser to Winston Churchill in World War II (...) [and] pressed the case for the strategic area bombing of cities." ([17], see also [32]).

Appendix D

Unique factorization

This appendix is devoted to generalizations of the Fundamental Theorem of Arithmetic (Theorem C.1.3) about unique expressions of natural numbers in products of primes. In Definition D.1.1 we introduce unique factorization of elements in monoids. In Definition D.1.8 we introduce somewhat non-standardly standard unique factorization domains (UFD). Definition D.1.10 introduces Euclidean domains. The main result is Theorem D.1.11 that every Euclidean domain is UFD. In Proposition D.1.16 we establish via this theorem unique factorization in the domain $\mathbb{Z}[i]_{\mathrm{do}}$, which we used in the proof of Theorem 2.1.1. Proposition D.1.17 demonstrates failure of unique factorization of elements in the domain $\mathbb{Z}[\sqrt{-5}]_{\mathrm{do}}$.

In the transitional Section D.2 about principal ideal domains (PID) we present the well known condition on ideals in the domain ensuring unique factorization of elements (Theorem D.2.6). Section D.3 is devoted to proving existence and uniqueness of primary decompositions of ideals in noetherian rings (Theorem D.3.1), here the operation on ideals is their intersection $\cap$. These two sections were not used in the first part of our book, and we include them from aesthetic reasons. On the other hand quite important in algebraic number theory is unique factorization of ideals in products of prime ideals in Dedekind domains (Theorem D.4.1) in Section D.4.

D.1 Euclidean domains

Unique factorization monoids

We begin by describing unique factorization in *monoids*. These are algebraic structures $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ such that M is a nonempty set endowed with a commutative and associative (binary) operation $\cdot$ with the neutral element 1_M ($\in M$). For $a \in M$ and $k \in \mathbb{N}$ we define $a^k = a \cdot a \cdot \ldots \cdot a$, with k factors a (and any bracketing); we set $a^0 = 1_M$. The product $a \cdot b$ is abbreviated by ab.

An element $a \in M$ is *invertible* if there is a $b \in M$ such that $ab = 1_M$. We denote the set of invertibles in M_{mo} by $M^\times$. Clearly, $1_M \in M^\times$ and $(M^\times, 1_M, \cdot)$

is an Abelian group. If $M^\times = M$, we call the whole M_{mo} an *Abelian group*. If $a, b, c \in M$ satisfy $a = bc$, we say that b *divides* a, or that b is a *divisor* of a, or that a is a *multiple of* b (in M_{mo}) and write $b \,|\, a$. If two elements $a, b \in M$ can be divided simultaneously only by invertibles, we say that a and b are *coprime* (in M_{mo}). An element $a \in M$ is *irreducible* iff $a \in M \setminus M^\times$ and $a = bc$ with $b, c \in M$ holds only if b or c is invertible. We denote the set of irreducible elements in M_{mo} by M^{ir}.

For $a, b \in M$ we write $a \sim b$ if $a = bc$ for a $c \in M^\times$. It is easy to see that $\sim$ is an equivalence relation. We denote the equivalence class of $a \in M$ by $[a]_\sim$. Thus $[1_M]_\sim = M^\times$. We define the *associated monoid* of $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ to be the monoid

$$M^{\mathrm{as}}_{\mathrm{mo}} = (M/\!\sim,\, [1_M]_\sim,\, \cdot)\,,$$

with the multiplication $\cdot$ defined via representatives: $[a]_\sim \cdot [b]_\sim = [a \cdot b]_\sim$. We prove correctness of this definition. Let $a \sim a'$ and $b \sim b'$, so that $a = a'c$ and $b = b'd$ with $c, d \in M^\times$. Then $ab = a'b'(cd)$ with $cd \in M^\times$ and $ab \sim a'b'$. It follows that $(M/\!\sim)^\times = \{[1_M]_\sim\}$ and $(M/\!\sim)^{\mathrm{ir}} = \{[a]_\sim :\ a \in M^{\mathrm{ir}}\}$. In $M^{\mathrm{as}}_{\mathrm{mo}}$, an element $A \in M/\!\sim$ is irreducible iff $A \neq [1_M]_\sim$ and $A = B \cdot C$ with $B, C \in M/\!\sim$ holds only for $\{B, C\} = \{[1_M]_\sim, A\}$.

Let $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ be a monoid with $M^{\mathrm{ir}} \neq \emptyset$. We again consider maps

$$f\colon (M/\!\sim)^{\mathrm{ir}} \to \mathbb{N}_0$$

with finite supports and denote their set by Q. Recall that $S(f)$ is the support of f and that $f(P)$ $(\in \mathbb{N}_0)$ is the multiplicity of P $(\in (M/\!\sim)^{\mathrm{ir}})$ in f. We view the elements of Q as finite multisets of irreducibles in $M^{\mathrm{as}}_{\mathrm{mo}}$. The map $F\colon Q \to N$,

$$F(f) = \textstyle\prod_{P \in (M/\sim)^{\mathrm{ir}}} P^{f(P)}$$

(this is effectively a finite product), is the *factorization map* (of M_{mo}). For $a \in M$, if $F(f) = [a]_\sim$ then f is the *prime factorization of* a.

Definition D.1.1 (UFM) *Let $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ be a monoid. We say that M_{mo} is a unique factorization monoid, abbreviated* UFM*, if $M^{\mathrm{ir}} \neq \emptyset$ and the factorization map $F\colon Q \to M/\!\sim$ is a bijection.*

If $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ is UFM and $a \in M$ then the unique prime factorization of a is $F^{-1}([a]_\sim)$ $(: (M/\!\sim)^{\mathrm{ir}} \to \mathbb{N}_0)$.

Proposition D.1.2 *The monoid of natural numbers $N_1 = (\mathbb{N}, 1, \cdot)$ is isomorphic to its associated monoid. The associated monoid of the monoid of nonzero integers $Z_{1,0} = (\mathbb{Z} \setminus \{0\}, 1, \cdot)$ is (isomorphic to) N_1.*

Proof. The first claim follows from the fact that $\mathbb{N}^\times = \{1\}$. As for the second claim, $(\mathbb{Z} \setminus \{0\})^\times = \{-1, 1\}$ and the the map

$$\mathbb{N} \ni n \mapsto \pm n = \{-n, n\} \in (\mathbb{Z} \setminus \{0\})/\!\sim$$

is an isomorphism from N_1 to $Z^{\mathrm{as}}_{1,0}$. □

In this terminology Theorem C.1.3 takes the following form.

Corollary D.1.3 *Both N_1 and $Z_{1,0}$ are* UFM.

Proof. This follows from Theorem C.1.3 and Proposition D.1.2. □

The following UFM is much simpler.

Proposition D.1.4 *The unary natural numbers $N_0 = (\mathbb{N}_0, 0, +)$ is* UFM.

Proof. Like for N_1 we have $\mathbb{N}_0^\times = \{0\}$ and N_0^{as} is N_0. But now $\mathbb{N}_0^{\mathrm{ir}} = \{1\}$. For every $n \in \mathbb{N}$ the expression $n = 1 + 1 + \cdots + 1$ with n summands is the unique irreducible factorization of n; the unique irreducible factorization of the number 0 is the empty sum, more precisely, the map $f\colon \{\{1\}\} \to \mathbb{N}_0$ with the value $f(\{1\}) = 0$. □

The monoid $(\mathbb{Z}, 1, \cdot)$ is not UFM because F is not surjective, $[0]_\sim = \{0\}$ is not in the image of the factorization map. The monoid $(\mathbb{Z}, 0, +)$ is not UFM because it is an Abelian group and has no irreducible element. We give as an example irreducible factorizations $f = F^{-1}([12]_\sim)$ of the number 12 in the monoids N_1, $Z_{1,0}$ and N_0. In N_1 it has the nonzero values $f(\{2\}) = 2$ and $f(\{3\}) = 1$, in $Z_{1,0}$ these are $f(\{-2, 2\}) = 2$ and $f(\{-3, 3\}) = 1$, and in N_0 it is just $f(\{1\}) = 12$.

Let $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ be UFM and $a, b \in M$. It follows that a, b are coprime iff $S(f) \cap S(g) = \emptyset$ where $f = F^{-1}([a]_\sim)$ and $g = F^{-1}([b]_\sim)$. The *greatest common divisor* of a, b is

$$\mathrm{GCD}(a,\, b) = \textstyle\prod_{P \in (M/\sim)^{\mathrm{ir}}} P^{\min(f(P),\, g(P))} \quad (\in M/\sim)\,.$$

We abuse notation in the standard way and write $\mathrm{GCD}(a, b) = c$ rather than $\mathrm{GCD}(a, b) = [c]_\sim$. Thus in $Z_{1,0}$ we write $\mathrm{GCD}(4, 6) = 2$, and not $\mathrm{GCD}(4, 6) = \{-2, 2\}$.

We leave the proof of the following UFM version of Corollaries C.1.5–C.1.8 to the interested reader.

Proposition D.1.5 *Let $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ be* UFM*, $a, b, c, d \in M$ and $k \geq 2$ be an integer. Then the following hold.*

1. *If $a \,|\, bc$ and a, b are coprime then $a \,|\, c$.*
2. *If a, b are coprime and $ab \sim c^k$, then there exist $a_0, b_0 \in M$ such that $a \sim a_0^k$ and $b \sim b_0^k$.*
3. *If $c \in M^{\mathrm{ir}}$, $\mathrm{GCD}(a, b) = c$ and $ab \sim d^k$, then there exist coprime a_0, b_0 in M such that $a \sim ca_0^k$, $b \sim c^{k-1}b_0^k$ or $a \sim c^{k-1}a_0^k$, $b \sim cb_0^k$.*
4. *If a, b are coprime, $c \in M^{\mathrm{ir}}$ and $ab \sim cd^k$, then there exist coprime a_0, b_0 in M such that $a \sim ca_0^k$, $b \sim b_0^k$ or $a \sim a_0^k$, $b \sim cb_0^k$.*

Note that in part 3 for $k = 2$ the two cases coincide.

Unique factorization domains

A *ring* is an algebraic structure

$$R_{\mathrm{ri}} = (R,\, 0_R,\, 1_R,\, +,\, \cdot)$$

such that $0_R \neq 1_R$, $(R, 0_R, +)$ is an Abelian group, $R_{\mathrm{mo}} = (R, 1_R, \cdot)$ is a monoid and $\cdot$ is distributive to $+$. We usually work in the multiplicative monoid R_{mo}. Its invertibles $R^\times$ are in the ring context called *units* of R_{ri}. Divisibility, irreducibles and coprimality in R_{ri} are similarly understood to take place in R_{mo}. We extend the congruence notation from $\mathbb{Z}$ to any ring R_{ri}. If $a, b, c \in R$ then we write $a \equiv b \pmod{c}$ iff there is a $d \in R$ such that $a - b = c \cdot d = cd$, i.e., $a = b + cd$.

R_{ri} is an *(integral) domain* R_{do} if the set $R^* = R \setminus \{0_R\}$ is closed to $\cdot$. Then

$$R_{\neq 0} = (R^*,\, 1_R,\, \cdot)$$

is a monoid and $R^\times \subset R^*$. If $R_{\neq 0}$ is an Abelian group then R_{ri} is a field. A monoid $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ is *cancellative* if for every $a, b, c \in M$ the equality $ac = bc$ implies that $a = b$. In the following proof we employ besides $\cdot$ the other ring operation $+$ and the distributive law.

Proposition D.1.6 *In every domain R_{do} the monoid $R_{\neq 0}$ is cancellative.*

Proof. Suppose that $R_{\mathrm{ri}} = (R, 0_R, 1_R, +, \cdot)$ is an integral domain, $a, b, c \in R^*$ and $ac = bc$. Then $(a - b)c = 0_R$ and, since $c \neq 0_R$, we have that $a - b = 0_R$ and $a = b$. □

We need this result in the proof of Theorem D.1.11. Thus $N_1 = (\mathbb{N}, 1, \cdot)$ is a cancellative monoid because it is a submonoid of the monoid $Z_{1,0} = \mathbb{Z}_{\neq 0}$ and $\mathbb{Z}$ is an integral domain. The monoid $N_0 = (\mathbb{N}_0, 0, +)$ is also cancellative because it is a submonoid of the Abelian group $(\mathbb{Z}, 0, +)$ and every Abelian group is cancellative because all elements in it are invertible.

Proposition D.1.7 *Suppose that $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ is a cancellative monoid and $a, b \in M$. Then $a \sim b$ iff $a \mid b \wedge b \mid a$.*

Proof. If $a \sim b$ then $a = bc$ for a $c \in R^\times$, and so also $ac^{-1} = b$ and $a \mid b \wedge b \mid a$. If $a \mid b \wedge b \mid a$ then $a = bc$ and $b = ad$ for $c, d \in R$. Thus $a1_M = a(dc)$ and since M_{mo} is cancellative, $1_M = dc$. Hence $c, d \in R^\times$ and $a \sim b$. □

In this approach the definition of UFM takes the following form.

Definition D.1.8 (UFD) *An integral domain R_{do} is a unique factorization domain, abbreviated* UFD*, if the monoid $R_{\neq 0}$ is* UFM *by* Definition D.1.1.

We have the following UFD version of Corollaries C.1.5–C.1.8.

Proposition D.1.9 *Let $R_{\mathrm{do}} = (R, 0_R, 1_R, +, \cdot)$ be* UFD*, $a, b, c, d \in R$ and $k \geq 2$ be an integer. Then the following hold.*

1. *If $a \,|\, bc$ and a, b are coprime then $a \,|\, c$.*
2. *If a, b are coprime and $ab \sim c^k$ then there exist $a_0, b_0 \in R$ such that $a \sim a_0^k$ and $b \sim b_0^k$.*
3. *If c is irreducible, $\mathrm{GCD}(a, b) = c$ and $ab \sim d^k$, then there exist coprime $a_0, b_0 \in R$ such that $a \sim ca_0^k$, $b \sim c^{k-1}b_0^k$ or $a \sim c^{k-1}a_0^k$, $b \sim cb_0^k$.*
4. *If a, b are coprime, c is irreducible and $ab \sim cd^k$, then there exist coprime $a_0, b_0 \in R$ such that $a \sim ca_0^k$, $b \sim b_0^k$ or $a \sim a_0^k$, $b \sim cb_0^k$.*

Proof. If the elements involved are non-zero, it is just an instance of Proposition D.1.5. Zero elements in parts 1–3 were handled for $R_{\mathrm{do}} = \mathbb{Z}$ in the proofs of Corollaries C.1.5–C.1.7, and the general case is similar. Suppose that in part 4 we have $d = 0_R$. Then $\{a, b\} = \{0_R, \alpha\}$ with $\alpha \in R^\times$, Let $a = 0_R$. Then the claim holds with $a = 0_R = c \cdot 0_R^k$ and $b = \alpha \sim 1_R^k$. □

Again, in part 2 for $k = 2$ the two cases are identical.

A *well ordering* $(X, \prec)$ is a linear order $\prec$ on a set X such that every nonempty set $Y \subset X$ has the *minimum element* $m \in Y$, an element such that $m \leq x$ for every $x \in Y$. This minimum is clearly unique.

Definition D.1.10 (Euclidean domain) *A domain $R_{\mathrm{do}} = (R, 0_R, 1_R, +, \cdot)$ is called Euclidean iff there exist a well ordering $(X, \prec)$ and a function $f\colon R^* = R \setminus \{0_R\} \to X$ such that*

$$\forall\, a,\, b \in R,\, b \neq 0_R \;\exists\, c,\, d \in R \left(a = b \cdot c + d \wedge (d = 0_R \vee f(d) \prec f(b))\right).$$

Note that the last disjunction is an exclusive or. If you miss some condition in this definition, see the corresponding remark in Section D.5. For instance, the domain of integers $\mathbb{Z}$ is Euclidean, $(X, \prec)$ is $(\mathbb{N}, <)$ and $f(n) = |n|$. One can often prove that a domain is UFD by using the next classical theorem. Its proof is more complicated than we originally thought. But with the help of [14, 33] we have put it together.

Theorem D.1.11 *Every Euclidean domain is* UFD*.*

Proof. Let $R_{\mathrm{do}} = (R, 0_R, 1_R, +, \cdot)$ be a Euclidean domain with a well ordering $(X, \prec)$ and a map $f\colon R^* \to X$ as in Definition D.1.10. In the first step we prove existence of irreducible factorizations: every element $x \in R^* \setminus R^\times$ is a product of irreducibles. Recall that $x \in R^* \setminus R^\times$ is irreducible iff $x = y \cdot z = yz$ with $y, z \in R^*$ holds only if $y \in R^\times$ or $z \in R^\times$. 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 the value $f(a)$ is $\prec$-minimum among all such values in X. 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 Propositions D.1.6 and D.1.7 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.

In the second step 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 $\langle a, b\rangle$ in R_{ri} generated by the elements a, b. Let $e \in I \setminus \{0_R\}$ have $\prec$-minimum value $f(e)$. Clearly, $I \neq \emptyset$. Note that $I \neq \{0_R\}$ 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 $1_R = ca + db$.

In the third step 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 we have for some $d, e \in R$ equality

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

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

In the final fourth step we prove that in R_{ri} every $a \in R^*$ has only one irreducible factorization. Suppose for the contrary that there are functions $g, h\colon (R^*/\!\sim)^{\mathrm{ir}} \to \mathbb{N}_0$ with finite supports and such that $g \neq h$ but $F(g) = F(h)$. We take a pair of these maps g, h such that in addition the sum of all involved multiplicities

$$\textstyle\sum_P g(P) + \sum_P h(P)\ \ (\in \mathbb{N}_0)$$

is minimum. Then in $R_{\neq 0}$ we have an equality

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$$

where $k, l \in \mathbb{N}$, $p_i, q_i \in R^{\mathrm{ir}}$, and for every $i \in [k]$ and $j \in [l]$ we have $p_i \not\sim q_j$; else $S(g) \cap S(h) \neq \emptyset$ and we could get maps g', h' with $g' \neq h'$, $F(g') = F(h')$ and a smaller sum of multiplicities. But applying repeatedly the third step we see that for every $i \in [k]$ there is a $j \in [l]$ such that $p_i \,|\, q_j$, hence $p_i \sim q_j$. This is a contradiction. □

The existence of irreducible factorizations can often be proven by means of norm maps, which we now introduce; they generalize norm maps of algebraic number theory. An *ordered monoid* is any structure

$$M_{\mathrm{omo}} = (M,\, 1_M,\, \cdot,\, \prec)$$

such that $(M, 1_M, \cdot)$ is a monoid and $\prec$ is a linear order on M satisfying that always for $x, y \in M$ if x divides y then $x \preceq y$. Note that then 1_M is the minimum element of $(M, \prec)$ and $M^\times = \{1_M\}$. Suppose that $(M, 1_M, \cdot)$ is a monoid, $(N, 1_N, \odot, \prec)$ is an ordered cancellative monoid and $f\colon M \to N$ is a homomorphism, which means that always $f(a \cdot b) = f(a) \odot f(b)$. Then $f(1_M) = 1_N$: just cancel $f(1_M)$ on both sides of $f(1_M) \odot f(1_M) = f(1_M) \odot 1_N$. Also, if $a \in M^\times$ then $f(a) = 1_N$ because $f(a) \odot f(a^{-1}) = f(1_M) = 1_N$.

We say that M_{omo} is *well ordered and cancellative*, abbreviated WOCM, if $(M, \prec)$ is a well ordering and the monoid $(M, 1_M, \cdot)$ is cancellative.

Definition D.1.12 (norm maps) *A monoid $(M, 1_M, \cdot)$ is normed iff there exists a homomorphism $f\colon M \to N$ to a* WOCM *$(N, 1_N, \odot, \prec)$, called a norm, such that $M^\times = f^{-1}[\{1_N\}]$. A domain $R_{\text{do}} = (R, 0_R, 1_R, +, \cdot)$ is normed iff the monoid $R_{\neq 0} = (R^*, 1_R, \cdot)$ is normed.*

Corollary D.1.13 *Suppose that $(M, 1_M, \cdot)$ is a normed monoid with a norm $f\colon M \to N$ and that $a, b \in M$. Then the following hold.*

1. *If $f(a) \neq 1_N$ and there is no element $x \in M$ such that $f(x) \mid f(a)$, $f(x) \neq 1_N$ and $f(x) \prec f(a)$, then $a \in M^{\text{ir}}$.*
2. *If $a \sim b$ then $f(a) = f(b)$.*

Proof. 1. Suppose that $f(a)$ satisfies the stated condition. So $a \notin M^\times$ and if $a = xy$ with $x, y \in M$, then $f(x)$ and $f(y)$ divide $f(a)$ and both are $\preceq f(a)$. Not both are 1_N (else $f(a) = 1_N$), say $f(x) \neq 1_N$. Then $f(x) = f(a)$ and by canceling in $f(a) \odot 1_N = f(x) \odot f(y)$ we get that $1_N = f(y)$ and $y \in M^\times$. Thus a is irreducible.

2. If $a \sim b$ then $a = bx$ with $x \in M^\times$. But then $f(a) = f(b) \odot f(x) = f(b) \odot 1_N = f(b)$. □

Proposition D.1.14 *Every normed domain $R_{\text{do}} = (R, 0_R, 1_R, +, \cdot)$ has irreducible factorizations, that is, the factorization map*

$$F\colon Q \to R^*/\!\sim \quad \textit{where } Q = \{f\colon (R^*/\!\sim)^{\text{ir}} \to \mathbb{N}_0 :\ S(f) \textit{ is finite}\}$$

and $F(f) = \prod_{P \in (R^*/\sim)^{\text{ir}}} P^{f(P)}$, is surjective.

Proof. Suppose that $R_{\text{do}} = (R, 0_R, 1_R, +, \cdot)$ is a domain and that $f\colon R^* \to N$ is a norm. It suffices to show that if $A \subset R^* \setminus R^\times$ is the set of elements that are not products of irreducibles, then $A = \emptyset$. Suppose for contrary that $A \neq \emptyset$ and take the $a \in A$ that has the minimum value $f(a) \in N$ with respect to $\prec$. Since a is not irreducible, $a = bc$ for some $b, c \in R^* \setminus R^\times$. Thus $f(b) \preceq f(a)$. If $f(b) = f(a)$ then by cancelling in $f(a) \odot 1_N = f(b) \odot f(c)$ we get that $1_N = f(c)$ and $c \in R^\times$, which is not possible. Hence $f(b), f(c) \prec f(a)$. But b or c is in A and we get a contradiction with the choice of a. □

We stated this result for domains because it is often used for them but it is clear that we do not really need the ring operation + and that we actually proved the following.

Proposition D.1.15 *Every normed monoid* $M_{\mathrm{mo}} = (M, 1_M, \cdot)$ *has irreducible factorizations.*

An important example of a UFD is the domain $\mathbb{Z}[i]_{\mathrm{do}} = (\mathbb{Z}[i], 0, 1, +, \cdot)$ of *Gaussian integers*, where $i \in \mathbb{C}$ is the imaginary unit, satisfying $i^2 = -1$, and

$$\mathbb{Z}[i] = \{a + bi : \ a, b \in \mathbb{Z}\} \ \ (\subset \mathbb{C}) .$$

We used the next result in the proof of Theorem 2.1.1.

Proposition D.1.16 *The domain* $\mathbb{Z}[i]_{\mathrm{do}}$ *has exactly four units* $\{-i, i, -1, 1\}$ *and is* UFD. *The conjugation map* $a+bi = \alpha \mapsto \overline{\alpha} = a-bi$ *is its automorphism.*

Proof. Since the operations in R_{Ga} are restrictions of the operations in the field $\mathbb{C}$, the structure R_{Ga} is a domain. It is easy to check that $\alpha \mapsto \overline{\alpha}$ is an automorphism of this ring. We find its units, let $\alpha = a + bi$ and $\beta = c + di$ in $\mathbb{Z}[i]$ be such that $\alpha\beta = 1$. Then

$$(a^2 + b^2)(c^2 + d^2) = \alpha\overline{\alpha}\beta\overline{\beta} = \alpha\beta\overline{\alpha\beta} = 1\overline{1} = 1^2 = 1 .$$

Thus $a = \pm 1 \wedge b = 0$ or $a = 0 \wedge b = \pm 1$ and $\mathbb{Z}[i]^{\times} = \{-1, 1, -i, i\}$.

Using Theorem D.1.11 we show that R_{Ga} is UFD; we define on $\mathbb{Z}[i]^*$ a map f as in Definition D.1.10 and show that R_{Ga} is Euclidean. We take the well ordering $(X, \prec) = (\mathbb{N}, <)$ and the function $f\colon \mathbb{Z}[i]^* \to \mathbb{N}$, given by $f(\alpha) = f(a + bi) = a^2 + b^2 = \alpha\overline{\alpha} =: \|\alpha\|$. Let $\alpha \in \mathbb{Z}[i]$ and $\beta \in \mathbb{Z}[i]^*$ be arbitrary. For $\frac{\alpha}{\beta} = u_0 + u_1 i$ with $u_j \in \mathbb{R}$ let $v_j \in \mathbb{Z}$ be the integer closest to u_j, so that $|u_j - v_j| \leq \frac{1}{2}$. We define

$$\gamma = v_0 + v_1 i \ \text{ and } \ \delta = \alpha - \beta\gamma \ \ (\in \mathbb{Z}[i]) .$$

Then $\alpha = \beta\gamma + \delta$ and

$$f(\delta) = \|\delta\| = \|\beta\| \cdot \left\|\tfrac{\alpha}{\beta} - \gamma\right\| = f(\beta) \cdot ((u_0 - v_0)^2 + (u_1 - v_1)^2) \leq \tfrac{f(\beta)}{2} < f(\beta) .$$

□

We mention a well known example of failure of unique factorization.

Proposition D.1.17 *The domain* $\mathbb{Z}[\sqrt{-5}]_{\mathrm{do}} = (\mathbb{Z}[\sqrt{-5}], 0, 1, +, \cdot)$, *where*

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : \ a, b \in \mathbb{Z}\} \ \ (\subset \mathbb{C}) ,$$

is not UFD. *More precisely, the factorization map* F *for this domain is surjective but not injective.*

Proof. We prove existence of irreducible factorizations by means of Proposition D.1.14; we take the WOCM $(\mathbb{N}, 1, \cdot, <)$ and easily check that the map $\|\cdot\|\colon \mathbb{Z}[\sqrt{-5}]^* \to \mathbb{N}$, given by

$$\|a + b\sqrt{-5}\| = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2\,,$$

is a norm. Crucially, it is clear that $\mathbb{Z}[\sqrt{-5}]^\times = \{-1, 1\} = \|\cdot\|^{-1}[\{1\}]$.

But the factorization map F is not injective. Consider the equality $\alpha\beta = \gamma\delta$, where

$$\alpha \cdot \beta = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 6 = 2 \cdot 3 = \gamma \cdot \delta\,.$$

Now we use Corollary D.1.13. We have $\|\alpha\| = \|\beta\| = 1^2 + 5 \cdot 1^2 = 6$, $\|\gamma\| = 4$ and $\|\delta\| = 9$. No $x \in \mathbb{Z}[\sqrt{-5}]$ has norm $\|x\| = 2$ or 3, and therefore α, β, γ and δ are irreducible. Because

$$\{\|\alpha\|, \|\beta\|\} \cap \{\|\gamma\|, \|\delta\|\} = \emptyset\,,$$

we have $\alpha \not\sim \gamma, \delta$ and $\beta \not\sim \gamma, \delta$. Thus

$$6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 2 \cdot 3$$

gives two different irreducible factorizations of 6 in the domain $\mathbb{Z}[\sqrt{-5}]$. □

D.2 PID

We switch from individual elements in a domain to ideals, although the next theorem is still on UFD. We extend the previous class of domains guaranteed to be UFD, the Euclidean domains, to the larger class of principal ideal domains. Let $R_{\mathrm{ri}} = (R, 0_R, 1_R, +, \cdot)$ be a ring. Recall that $I \subset R$, $I \neq \emptyset$, is an *ideal* (in R_{ri}) if $(I, 0_R, +)$ is an Abelian group, that is $a, b \in I$ always implies $a - b \in I$, and for every $r \in R$ and $a \in I$ also $ra \in I$. Examples of ideals are for any $a \in R$ the sets

$$(a) = \{ra :\ r \in R\}\,.$$

Ideals of this form, generated by a single element, are called *principal*. Two most prominent principal ideals are the *zero ideal* $(0_R) = \{0_R\}$ and the ideal $(1_R) = R$. It is clear that $a \,|\, b$ iff $(b) \subset (a)$.

Lemma D.2.1 *Let $R_{\mathrm{ri}} = (R, 0_R, 1_R, +, \cdot)$ be a ring and I be an ideal in it. Then $I = R$ iff $1_R \in I$.*

Proof. The implication $\Rightarrow$ is trivial. If $1_R \in I$, then for every $r \in R$ we have $r = r1_R \in I$ and $I = R$. □

We restrict to integral domains and introduce PIDs.

Definition D.2.2 (PID) *A domain is a principal ideal domain, abbreviated* PID*, if all ideals in it are principal.*

Proposition D.2.3 *Every Euclidean domain is* PID*.*

Proof. Let $R_{\mathrm{do}} = (R, 0_R, 1_R, +, \cdot)$ be a domain, $(X, \prec)$ be a well ordering, $f\colon R^* \to X$ be as in Definition D.1.10 and $I \subset R$ be a nonzero ideal ((0_R) is principal). We take $a \in I \setminus \{0_R\}$ with the minimum value $f(a)$ and divide any $x \in I$ by a with a remainder: $x = ab + c$, where $b, c \in R$ and $c = 0_R$ or ($c \neq 0_R$ and $f(c) \prec f(a)$). Since $c = x - ba \in I$, the latter case contradicts the minimality of $f(a)$. Hence $I = (a)$. □

Let I be an ideal in a ring R_{ri}. We call it a *prime ideal* iff always the implication holds that $a, b \in R \wedge ab \in I \Rightarrow a$ or b is in I. We call I a *maximal ideal* if $I \neq R$ and there is no ideal J in R_{do} such that $I \subset J$, $I \neq J$ and $J \neq R$.

Proposition D.2.4 *For every ideal I in R_{ri}, $I \neq R$, there exists a maximal ideal J in R_{ri} such that $I \subset J$.*

Proof. Let $\mathcal{I}$ be the set of all ideals in R_{ri} different from R. We consider the poset $\mathcal{I}_{\mathrm{po}} = (\mathcal{I}, \subset)$. Let $I \in \mathcal{I}$. We get the required maximal ideal containing I by Zorn's lemma in Axiom A.1.1, if we prove that every chain in $\mathcal{I}_{\mathrm{po}}$ has an upper bound. Let $\mathcal{J} \subset \mathcal{I}$ be a chain. We claim that $K = \bigcup \mathcal{J}$ lies in $\mathcal{I}$ and is an upper bound of $\mathcal{J}$. The latter is obvious if we prove the former. We show that K is an ideal in R_{ri}. If $a, b \in K$ then $a \in J_1 \in \mathcal{J}$ and $b \in J_2 \in \mathcal{J}$. Since $J_1 \subset J_2$ or $J_2 \subset J_1$, there is an $i \in [2]$ such that $a, b \in J_i$. Hence $a - b \in J_i$ and $a - b \in K$. Similarly, if $r \in R$ and $a \in K$, then $a \in J \in \mathcal{J}$, $ra \in J$ and $ra \in K$. So K is an ideal. It remains to show that $K \neq R$. This is immediate from Lemma D.2.1: $1_R \notin K$ because $1_R \notin J$ for every $J \in \mathcal{J}$. □

Before we get to the main result of this section, we prove an important property of ideals in general rings.

Proposition D.2.5 *Every maximal ideal in a ring is a prime ideal.*

Proof. Suppose that I is a maximal ideal in a ring $R_{\mathrm{ri}} = (R, 0_R, 1_R, +, \cdot)$ and that for some $a, b \in R$ we have $ab \in I$. We consider the set

$$J = \{x + ra : \ x \in I, r \in R\}.$$

It is easy to see that J is an ideal in R_{ri} and that $I \subset J$ (since $x = x + 0_R r$). If $J = I$ then $a = 0_R + 1_R a \in J = I$ and $a \in I$. If $J \neq I$ then by the maximality of I we have $J = R$ and, by Lemma D.2.1, $1_R \in J$. So $1_R = x + ra$ for some $x \in I$ and $r \in R$. Multiplying by b we get that $b = bx + rab \in I$ (since $ab \in I$). So a or b is always in I and I is a prime ideal. □

Theorem D.2.6 *Every* PID *is* UFD*.*

Proof. Let $R_{\mathrm{do}} = (R, 0_R, 1_R, +, \cdot)$ be PID and $a \in R^* = R \setminus \{0_R\}$. We first observe that $a \in R^\times$ (a is a unit) iff the ideal $(a) = R$. Indeed, if $a \in R^\times$ then $ar = 1_R$ for some $r \in R$, $1_R \in (a)$ and trivially $(a) = R$. If $(a) = R$ then trivially $1_R \in (a)$ and $a \,|\, 1_R$, which means that $a \in R^\times$.

It is only a little harder to show that a is irreducible iff the ideal (a) is maximal. Suppose that (a) is maximal and $a = bc$ for $b, c \in R$. By Proposition D.2.5 (a) is a prime ideal and since $bc \in (a)$, it holds that b or c is in (a). Thus a divides b or c. But both b and c divide a and we get (by Proposition D.1.7) that $a \sim b$ or $a \sim c$. Hence a is irreducible. Suppose that (a) is not maximal. Then there is a $b \in R^*$ such that $(a) \subset (b) \subset R$ and both inclusions are strict. Thus $b \,|\, a$, $\neg(a \,|\, b)$ and $b \notin R^\times$ (by the first paragraph). So $a \not\sim b$ (by Proposition D.1.7) and we have a decomposition $a = bc$ with $b, c \notin R^\times$. Hence a is not irreducible.

We show that in R_{do} there does not exist an infinite strictly increasing sequence of ideals $I_1 \subset I_2 \subset \cdots$. If it existed, we know from the proof of Proposition D.2.5 that $J = \bigcup_{n=1}^{\infty}$ is an ideal. But $J = (a)$ for some $a \in R$ and $a \in I_n$ for some n. Thus $J \subset I_n$. Since $I_n \subset J$, we have $I_n = J$. But this contradicts the assumption that $I_n \neq J$. It is easy to see now that every nonempty set of ideals has an $\subset$- maximal element.

We assume that that set $A \subset R^*$ of elements that are not products of irreducibles is nonempty and get a contradiction. Indeed, let (a) be a maximal ideal in the set of ideals $\{(x) : \ x \in A\}$. Since $a \notin R^{\mathrm{ir}}$, we have $a = bc$ with $b, c \notin R^\times$. It follows that $(a) \subset (b)$, $(a) \subset (c)$ and (by Proposition D.1.7) that both inclusions are strict. But b or c is in A and we get a contradiction with the maximality of (a). Thus we have proved that every nonzero element expresses as a product of irreducibles.

To prove uniqueness of these expressions — up to reordering and associates — it suffices to prove for $a, b, c \in R$ the implication $a \in R^{\mathrm{ir}} \wedge a \,|\, bc \Rightarrow a \,|\, b \vee a \,|\, c$. Suppose that a is irreducible and divides bc. Thus $bc \in (a)$. By the second paragraph and Proposition D.2.5, (a) is a prime ideal. Thus b or c is in (a) and a divides b or c. □

Theorem D.2.7 *Let* $\alpha = \frac{1+\sqrt{-19}}{2}$. *The domain*

$$\mathbb{Z}[\alpha]_{\mathrm{do}} = (\mathbb{Z}[\alpha],\, 0,\, 1,\, +,\, \cdot) \quad (\subset \mathbb{C})\,,$$

where $\mathbb{Z}[\alpha] = \{a\alpha + b : \ a, b \in \mathbb{Z}\}$, *is* PID *but not Euclidean.*

Proof.

□

D.3 The Lasker–E. Noether theorem

Theorem D.3.1

Proof.

□

D.4 Dedekind domains

Recall that an integral domain, briefly a domain, is an algebraic structure $R_{\mathrm{do}} = (R, 0_R, 1_R, +, \cdot)$ such that $(R, 0_R, +)$ is an Abelian group, $(R, 1_R, \cdot)$ is a monoid, the distributive law holds, and $R^* = R \setminus \{0_R\}$ is closed to the operation $\cdot$. In the previous section we considered irreducible factorization in the monoids $R_{\neq 0} = (R^*, 1_R, \cdot)$, that is, in the monoid

$$R_{\neq 0}^{\mathrm{as}} = (R^*/\!\sim,\, [1_R]_\sim,\, \cdot)\,.$$

Theorem D.4.1

Proof.

□

D.5 Remarks

Algebra textbooks usually take the function f in Definition D.1.10 of Euclidean domains with the range $(\mathbb{N}, <)$ and require that in addition to the condition of division with a remainder, f satisfies some condition (C) like that for every $a, b \in R^*$ one has $f(a) \preceq f(a \cdot b)$. It is not clear to us what precise effect the relaxation of $(\mathbb{N}, <)$ to any well ordering $(X, \prec)$ has. In the note [33] it is proven that (C) is superfluous, thus we did not include it in Definition D.1.10.

Proposition D.5.1 ([33]) *If in the situation of* Definition D.1.10 *we introduce another function* $g\colon R^* \to X$ *by* ($a \in R^*$)

$$g(a) = \min_{\preceq}(\{f(a \cdot b) :\ b \in R^*\})\,,$$

then g *satisfies the condition in* Definition D.1.10 *and condition* (C).

In the proof of Theorem D.1.11 we took the proof of existence of irreducible factorizations also from [33]. The terminology of "abnormal" numbers used in [33] reveals the inspiration by [20, Chapter II.2.11].

Appendix E

More commutative algebra

E.1 Extensions of rings and fields

For an extension of rings $R \subset S$ (so that R is a subring of S) and any subset $U \subset S$ we define

$$R[U] = \bigcap \{R' : \ R \cup U \subset R' \text{ and } R' \text{ is a subring of } S\} .$$

Theorem E.1.1 *In any extension of rings $R \subset S$ the elements in S integral over R form a subring of S.*

Proof.

□

E.2 Remarks

Appendix F

Algebraic number theory

F.1 Number fields

A *number field* K is any subfield $K \subset \mathbb{C}$ of complex numbers such that the dimension of K as a $\mathbb{Q}$-vector space is finite. We call this dimension the *degree of* K and denote it by $[K : \mathbb{Q}]$ ($\in \mathbb{N}$). A K-*integer* or an *integer of* K is any $\alpha \in K$ that is a root of a monic integral polynomial. By Theorem E.1.1 the set O_K of K-integers is a domain.

F.2 The class group and class number

F.3 Remarks

Appendix G

Cyclotomic fields

Bibliography

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*. Second Edition, Springer, Berlin 2001

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusets 1969

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

[4] D. Cass and G. Wildenberg, Math Bite: A Novel Proof of the Infinitude of Primes, Revisited, *Math. Magazine* **76** (2003), 203

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

[6] 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

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

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

[9] Catalan Opening, Wikipedia article, `https://en.wikipedia.org/wiki/Catalan_Opening`

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

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

[12] K. Devlin, *The millennium problems. The seven greatest unsolved mathematical puzzles of our time*, Basic Books, New York, 2002

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

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

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

[16] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366

[17] Frederick Lindemann, 1st Viscount Cherwell, Wikipedia article, https://en.wikipedia.org/wiki/Frederick_Lindemann,_1st_Viscount_Cherwell

[18] H. Fürstenberg, On the infinitude of primes, *Amer. Math. Monthly* **62** (1955), 353

[19] Furstenberg's proof of the infinitude of primes, Wikipedia article, https://en.wikipedia.org/wiki/Furstenberg%27s_proof_of_the_infinitude_of_primes

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

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

[22] M. Klazar, *Absolutní direktní sčítance v modulech nad Dedekindovými okruhy*, diplomová práce, vedoucí práce: Doc. RNDr. Ladislav Procházka, DrSc., Praha 1989 (Absolute direct sumands in modules over Dedekind rings, Master thesis, supervisor)

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

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

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

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

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

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

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

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

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

[32] A. Roberts, *Churchill: Walking with Destiny*, Viking, 2018

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

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

[35] R. P. Stanley, *Catalan Numbers*, Cambridge University Press, New York, 2015

[36] Tetralogy, Wikipedia article, `https://en.wikipedia.org/wiki/Tetralogy`

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

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