

Chapter 2

Even Exponents

In this chapter we consider Catalan's equation $x^p - y^q = 1$ when one of the exponents p and q is even. This reduces to the case when one of p and q is equal to 2, and the other is an odd prime number.

2.1 The Equation $x^p = y^2 + 1$

Six years after Catalan's *note extraite*, the French mathematician Lebesgue [67] made the first step in the long way towards the solution of Catalan's problem. He proved that Catalan's equation $x^p - y^q = 1$ has no solutions with $q = 2$.

Theorem 2.1 (V.A. Lebesgue). *Let $p \geq 3$ be an odd number. Then the equation $x^p = y^2 + 1$ has no solutions in nonzero integers x and y .*

(One may further assume that p is prime, but this is not needed for the proof.)

Proof. If y is odd and x is even, then $y^2 + 1 \equiv 2 \pmod{4}$ and $x^p \equiv 0 \pmod{8}$, a contradiction. Hence y is even and x is odd. Write

$$x^p = (1 + iy)(1 - iy). \quad (2.1)$$

The greatest common divisor of $1 + iy$ and $1 - iy$ (in the ring of Gaussian integers $\mathbb{Z}[i]$) divides the sum $(1 + iy) + (1 - iy) = 2$. Since $1 + y^2$ is odd, the numbers $1 + iy$ and $1 - iy$ are coprime.

Since $\mathbb{Z}[i]$ is a unique factorization ring, every factor in (2.1) is equal to a p th power times a unit of $\mathbb{Z}[i]$; that is,

$$1 + iy = \varepsilon \alpha^p, \quad 1 - iy = \bar{\varepsilon} \bar{\alpha}^p,$$

where $\alpha \in \mathbb{Z}[i]$ and $\varepsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Since p is odd, every unit of $\mathbb{Z}[i]$ is a p th power of another unit. Writing $\varepsilon = \varepsilon_1^p$ and $\beta = \varepsilon_1 \alpha$, we obtain

$$1 + iy = \beta^p, \quad 1 - iy = \bar{\beta}^p.$$

Write $\beta = a + ib$, where $a, b \in \mathbb{Z}$. Since p is odd, the number $2a = \beta + \bar{\beta}$ divides $\beta^p + \bar{\beta}^p = 2$. Hence $a = \pm 1$. Further, $1 + y^2 = (a^2 + b^2)^p = (1 + b^2)^p$ is an odd number, which implies that b is even. It follows that

$$1 + iy = (a + ib)^p \equiv a^p + ipa^{p-1}b \pmod{4},$$

and, in particular, $1 \equiv a^p \pmod{4}$, which rules out the possibility $a = -1$.

Thus, $\beta = 1 + ib$. Comparing the real parts in the equality

$$1 + iy = (1 + ib)^p,$$

we obtain

$$1 = \sum_{k=0}^{(p-1)/2} (-1)^k \binom{p}{2k} b^{2k},$$

which can be rewritten as

$$-\binom{p}{2}b^2 + \sum_{k=2}^{(p-1)/2} (-1)^k \binom{p}{2k} b^{2k} = 0. \quad (2.2)$$

We shall use Lemma A.1 to show that (2.2) is impossible.

For $1 \leq k \leq (p-1)/2$ we have

$$\binom{p}{2k} b^{2k} = \binom{p}{2} b^2 \frac{1}{k(2k-1)} \binom{p-2}{2k-2} b^{2k-2}.$$

Hence

$$\begin{aligned} \text{Ord}_2 \left(\binom{p}{2k} b^{2k} \right) - \text{Ord}_2 \left(\binom{p}{2} b^2 \right) &\geq (2k-2) \text{Ord}_2 b - \text{Ord}_2 k \\ &\geq 2k-2 - \log_2 k. \end{aligned}$$

Since $2k-2 > \log_2 k$ for $k \geq 2$, we have $\text{Ord}_2 \left(\binom{p}{2k} b^{2k} \right) > \text{Ord}_2 \left(\binom{p}{2} b^2 \right)$ for $k = 2, \dots, (p-1)/2$. Now Lemma A.1 implies that the left-hand side of (2.2) cannot vanish. The theorem is proved. \square

2.2 Units of Real Quadratic Rings

This section is auxiliary. In it we recall the structure of the unit group of the ring $\mathbb{Z}[\sqrt{D}]$, where D is a positive integer, which is not a square (we do not assume that D is square-free).

Theorem 2.2. *The multiplicative group $\mathbb{Z}[\sqrt{D}]_+^\times$ of positive units of the ring $\mathbb{Z}[\sqrt{D}]$ is infinite cyclic.*

It follows that the group $\mathbb{Z}[\sqrt{D}]^\times$ of all units of $\mathbb{Z}[\sqrt{D}]$ is ± 1 times an infinite cyclic group.

The ring $\mathbb{Z}[\sqrt{D}]$ is not, in general, the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{D})$. Hence Theorem 2.2 is not a formal consequence of the *Dirichlet unit theorem*, as stated in Appendix A.2. Of course, it may be deduced from the slightly more general *Dirichlet unit theorem for maximal orders*; see [12, Sect. 2.4]. However, we sketch here a short independent proof, for the reader's convenience.

The proof uses the famous *Dirichlet approximation theorem*.

Theorem 2.3 (Dirichlet approximation theorem). *Let α be a real number and $Y > 0$. Then there exist integers x, y such that $0 < y \leq Y$ and $|y\alpha - x| < Y^{-1}$.*

Informally, this means that the rational number x/y is a “good approximation” for α .

Proof. It is well known and simple: on the quotient group \mathbb{R}/\mathbb{Z} consider the images of the real numbers $m\alpha$, where m runs through the integers satisfying $0 \leq m \leq Y$. We obtain $\lfloor Y \rfloor + 1$ points on \mathbb{R}/\mathbb{Z} , which split \mathbb{R}/\mathbb{Z} into $\lfloor Y \rfloor + 1$ disjoint intervals. Since $\lfloor Y \rfloor + 1 > Y$, at least one of these intervals is of length $< Y^{-1}$. This means that there exist integers m_1, m_2 , and x such that $0 \leq m_1 < m_2 \leq Y$ and $|m_2\alpha - m_1\alpha - x| < Y^{-1}$. Putting $y = m_2 - m_1$, we complete the proof. \square

The following consequence is immediate.

Corollary 2.4. *Let α be a real number. Then there exist infinitely many couples $(x, y) \in \mathbb{Z}^2$ with $y > 0$ and $|y\alpha - x| < y^{-1}$.*

We return to the proof of Theorem 2.2. We denote the group $\mathbb{Z}[\sqrt{D}]_+^\times$ of positive units by U . We denote by $\alpha \mapsto \bar{\alpha}$ the nontrivial automorphism of $\mathbb{Z}[\sqrt{D}]$ (that is, $x + y\sqrt{D} \mapsto x - y\sqrt{D}$) and by $\mathcal{N} : \mathbb{Z}[\sqrt{D}] \rightarrow \mathbb{Z}$ the norm map: $\mathcal{N}\alpha = \alpha\bar{\alpha}$.

Proof of Theorem 2.2. First of all, we prove that $U \neq \{1\}$. By the Dirichlet approximation theorem, there exist infinitely many couples of positive integers x and y such that $|x - y\sqrt{D}| \leq y^{-1}$. For any such x and y we have $x \leq y\sqrt{D} + 1$. Hence $\alpha = x + y\sqrt{D}$ satisfies $0 < \alpha \leq 2y\sqrt{D} + 1$ and $|\bar{\alpha}| \leq y^{-1}$, which implies $|\mathcal{N}\alpha| = |\alpha\bar{\alpha}| \leq 2\sqrt{D} + 1$.

We have proved that $\mathbb{Z}[\sqrt{D}]$ contains infinitely many positive elements of norm bounded by $2\sqrt{D} + 1$. Therefore there exists a nonzero $a \in \mathbb{Z}$ such that $\mathbb{Z}[\sqrt{D}]$ contains infinitely many positive elements of norm equal to a . Since there are only

finitely many residue classes mod a , there exist distinct positive $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$ such that $\mathcal{N}\alpha = \mathcal{N}\beta = a$ and $\alpha \equiv \beta \pmod{a}$. Then

$$\alpha\bar{\beta} \equiv \beta\bar{\alpha} \equiv a \equiv 0 \pmod{a}.$$

Put $\eta = \alpha/\beta$. Then $\eta \neq 1$, because α and β are distinct. On the other hand, $\eta = \alpha\bar{\beta}/a \in \mathbb{Z}[\sqrt{D}]$, and, similarly, $\eta^{-1} \in \mathbb{Z}[\sqrt{D}]$. We have found an element $\eta \in U$ distinct from 1. Hence $U \neq \{1\}$.

Next, we prove that U is an infinite cyclic group. The logarithmic map $\log : U \rightarrow \mathbb{R}$ defines an injective homomorphism of U into the additive group of real numbers. Since $U \neq \{1\}$, the image $\log U$ is a nonzero subgroup of \mathbb{R} .

Further, if $\eta \in U$ satisfies $\eta > 1$, then $\eta = x + y\sqrt{D}$ with $x, y > 0$, whence $\eta > \sqrt{D}$. It follows that any positive element of $\log U$ is greater than $\log \sqrt{D}$, which implies that $\log U$ is a discrete subgroup of \mathbb{R} .

Since any nonzero discrete subgroup of \mathbb{R} is infinite cyclic, the theorem follows. \square

The unit $\eta > 1$, generating the group $\mathbb{Z}[\sqrt{D}]_+^\times$, is called the *basic* (or *fundamental*) unit of the ring $\mathbb{Z}[\sqrt{D}]$. Usually, it is not easy to find the basic unit or to decide whether a given unit is basic. In some cases this can be done using the following simple observation.

Proposition 2.5. *Let $\eta = a + b\sqrt{D}$ be the basic unit of $\mathbb{Z}[\sqrt{D}]$, and let $\theta = x + y\sqrt{D}$ be any other unit. Then $b \mid y$.*

Proof. We may assume that $x, y > 0$. Then $\theta = \eta^n$, where n is a positive integer. It follows that $2b\sqrt{D} = \eta - \bar{\eta}$ divides $2y\sqrt{D} = \eta^n - \bar{\eta}^n$, whence the result. \square

The following consequence is immediate.

Corollary 2.6. *Assume that $D = a^2 \pm 1$, where a is a positive integer (satisfying $a > 1$ if $D = a^2 - 1$). Then $a + \sqrt{D}$ is a basic unit of $\mathbb{Z}[\sqrt{D}]$.*

It is worth mentioning that Corollary 2.6 is the simplest particular case of the famous theorem of Størmer (1897).

Theorem 2.7 (Størmer). *Let $a + b\sqrt{D}$ be a unit of $\mathbb{Z}[\sqrt{D}]$ such that $a, b > 0$ and every prime divisor of b divides D . Then it is a basic unit.*

We do not prove this theorem since we do not need it. An interested reader can find the proof in Ribenboim's book [117, Sect. A.4].

To conclude, let us mention that the results of this section are often interpreted in terms of the ‘‘Pell Diophantine equation’’ $x^2 - Dy^2 = \pm 1$.

2.3 The Equation $x^2 - y^q = 1$ with $q \geq 5$

The equation $x^2 - y^q = 1$ with an odd (prime) exponent q is much more difficult than $x^p - y^2 = 1$. The case $q = 3$ was settled already by Euler, but, in spite of some partial results, the general case remained open until 1965, when the Chinese mathematician Ko Chao¹ proved [55, 56] that, for a prime $q \geq 5$, the equation $x^2 - y^q = 1$ has no solutions in positive integers x and y .

In 1976 Chein [23] discovered another proof, simpler than Ko Chao's and based on a totally different idea. Chein's proof is reproduced below (with some changes). Ko Chao's proof can be found in Mordell's book [96, Sect. 30].

Both the arguments of Ko Chao and Chein work for a prime $q \geq 5$ and do not extend to $q = 3$. This case is solved in Sect. 2.5 by a totally different argument.

Most of the known proofs of the theorem of Ko Chao rely on a result of Nagell about the arithmetical structure of the solutions of the equation $x^2 - y^q = 1$. We prove this theorem in Sect. 2.3.1. The theorem of Ko Chao will be proved (following Chein) in Sect. 2.3.2. In Sect. 2.3.3 we briefly describe the history of the equation.

2.3.1 Nagell's Theorem

We start with an elementary lemma, which will be used in the next chapter as well.

Lemma 2.8. *Let A and B be distinct coprime rational integers and p a prime number.*

1. *If p divides one of the numbers $(A^p - B^p)/(A - B)$ and $A - B$, then it divides the other as well.*
2. *Put $d = \gcd((A^p - B^p)/(A - B), A - B)$. Then $d \in \{1, p\}$.*
3. *If $p > 2$ and $d = p$, then $\text{Ord}_p((A^p - B^p)/(A - B)) = 1$.*

Proof. All the three statements easily follow from the identity

$$\frac{A^p - B^p}{A - B} = \frac{((A - B) + B)^p - B^p}{A - B} = \sum_{k=1}^p \binom{p}{k} (A - B)^{k-1} B^{p-k}. \quad (2.3)$$

Rewriting it as

$$\frac{A^p - B^p}{A - B} = \sum_{k=1}^{p-1} \binom{p}{k} (A - B)^{k-1} B^{p-k} + (A - B)^{p-1},$$

we obtain $(A^p - B^p)/(A - B) \equiv (A - B)^{p-1} \pmod{p}$, which proves part (1).

¹Sometimes spelled as Ko Zhao.

Rewriting (2.3) as

$$\frac{A^p - B^p}{A - B} = pB^{p-1} + (A - B) \sum_{k=2}^p \binom{p}{k} (A - B)^{k-2} B^{p-k}, \quad (2.4)$$

we observe that d divides pB^{p-1} . Since A and B are coprime, d and B are coprime as well, and we conclude that $d \mid p$, which proves part (2).

Finally, if $d = p$ then p divides $A - B$ and does not divide B . Rewriting (2.3) as

$$\frac{A^p - B^p}{A - B} = pB^{p-1} + (A - B) \left(\sum_{k=2}^{p-1} \binom{p}{k} (A - B)^{k-2} B^{p-k} + (A - B)^{p-2} \right),$$

we obtain $(A^p - B^p)/(A - B) \equiv pB^{p-1} \pmod{p^2}$, which proves part (3). \square

Next, we establish the following preliminary result, due to Nagell [100].

Theorem 2.9 (Nagell). *Let x, y be positive integers and q an odd prime number satisfying $x^2 - y^q = 1$. Then $2 \mid y$ and $q \mid x$.*

Proof. Write $(x - 1)(x + 1) = y^q$. The greatest common divisor of $x - 1$ and $x + 1$ divides 2. If y is odd then they are coprime; hence both are q th powers: $x - 1 = a^q$ and $x + 1 = b^q$. We obtain $b^q - a^q = 2$, which is impossible. This proves that $2 \mid y$.

Further, write

$$\frac{y^q + 1}{y + 1} (y + 1) = x^2.$$

By Lemma 2.8, the greatest common divisor of the factors in the left-hand side is either 1 or q . If x is not divisible by q then the factors are coprime, which means that each of them is a complete square. Thus, there exist positive integers a and b such that

$$y + 1 = a^2, \quad \frac{y^q + 1}{y + 1} = b^2, \quad x = ab.$$

On the other hand, equality $x^2 - y^q = 1$ means that $x + y^{(q-1)/2} \sqrt{y}$ is a unit of the ring $\mathbb{Z}[\sqrt{y}]$, and Corollary 2.6 implies that $a + \sqrt{y}$ is the basic unit of this ring. Hence there exists a positive integer n such that

$$x + y^{(q-1)/2} \sqrt{y} = (a + \sqrt{y})^n. \quad (2.5)$$

We want to show that this is impossible.

First of all, let us prove that n is even. Expanding $(a + \sqrt{y})^n$ by the binomial formula, and reducing mod y , we find

$$(a + \sqrt{y})^n \equiv a^n + na^{n-1}\sqrt{y} \pmod{y}$$

in the ring $\mathbb{Z}[\sqrt{y}]$. Combining this with (2.5), we obtain

$$na^{n-1} \equiv y^{(q-1)/2} \equiv 0 \pmod{y}.$$

Since y is even and a is odd, this implies that n is even.

Next, reducing (2.5) mod a and using the congruences

$$x = ab \equiv 0 \pmod{a}, \quad y = a^2 - 1 \equiv -1 \pmod{a},$$

we obtain

$$(-1)^{(q-1)/2} \sqrt{y} \equiv (-1)^{n/2} \pmod{a},$$

which means that a divides one of the numbers $1 \pm \sqrt{y}$ in the ring $\mathbb{Z}[\sqrt{y}]$. Since $a > 1$, this is impossible. The theorem is proved. \square

We learned this argument from Hendrik Lenstra (private communication). It was also independently discovered by Nesterenko and Zudilin [106]. Nagell himself used the Theorem of Størmer (see Theorem 2.7) to show that both units $a + \sqrt{y}$ and $x + y^{(q-1)/2} \sqrt{y}$ should be basic, which is a contradiction.

2.3.2 Chein's Proof of the Theorem of Ko Chao

Now we are ready to prove the theorem of Ko Chao.

Theorem 2.10 (Ko Chao). *The equation $x^2 - y^q = 1$ has no solutions in positive integers x, y and prime $q \geq 5$.*

Proof (Chein). Theorem 2.9 implies that x is odd. Assume that $x \equiv 3 \pmod{4}$. Equality $(x-1)(x+1) = y^q$ implies that there exist positive integers a and b such that

$$x+1 = 2^{q-1}a^q, \quad x-1 = 2b^q.$$

Notice that $a^q = (b^q + 1)/2^{q-2} < b^q$, which implies $a < b$.

We have

$$(b^2 + 2a) \frac{b^{2q} + (2a)^q}{b^2 + 2a} = b^{2q} + (2a)^q = \left(\frac{x-1}{2}\right)^2 + 2(x+1) = \left(\frac{x+3}{2}\right)^2. \quad (2.6)$$

We again invoke Theorem 2.9, this time the statement $q \mid x$. Since $q > 3$, this implies that the right-hand side of (2.6) is not divisible by q . Now Lemma 2.8 yields that the factors on the left-hand side are coprime. Hence they are complete squares.

Since $b^2 + 2a$ is a complete square, we have $2a \geq (b+1)^2 - b^2 = 2b+1$, which contradicts the previously established inequality $a < b$.

If $x \equiv 1 \pmod{4}$ then $x-1 = 2^{q-1}a^q$ and $x+1 = 2b^q$. We obtain

$$b^{2q} - (2a)^q = \left(\frac{x-3}{2} \right)^2,$$

and the rest of the argument is the same. \square

2.3.3 Some Historical Remarks

Here we give some historical and bibliographical remarks on the equation

$$x^2 - y^q = 1 \tag{2.7}$$

with $q \geq 5$.

Before Ko Chao, the problem attracted many mathematicians. In 1921 Nagell [100] observed that a theorem of Lebesgue [66] asserting that the equation $x^5 + y^5 = 8z^5$ has no solutions implies that $x^2 - y^5 = 1$ has no solutions.

In the same article Nagell [100] presented several conditions involving the congruence class of q modulo 16 and the arithmetic of the number field $\mathbb{Q}(\sqrt{-q})$ under which the equation has no solution. In particular, he proved that there are no solutions with $q \leq 101$, except maybe with $q = 31, 59, 73, 83$ or 89 . In 1934, he [103] improved upon the latter result, by showing that there is no solution if $q \not\equiv 1 \pmod{8}$. Thus, below 101 only 73 and 89 remained untreated.

In 1932, Selberg [126] solved completely the Diophantine equation $x^4 - y^q = 1$, answering a question posed by Nagell [98] in 1919.

In 1940, Obláth [108, 109] showed that (2.7) has no solution except, possibly, when

$$2^{q-1} \equiv 1 \pmod{q^2}, \quad 3^{q-1} \equiv 1 \pmod{q^2}. \tag{2.8}$$

His starting point was the key observation that it is sufficient to solve the equation $2^{q-2}a^q - b^q = \pm 1$, as it is clear from the proof of Theorem 2.10. Then, he combined the results of Lubelski [75] on the Diophantine equation $x^q + y^q = cz^q$ with Theorem 2.9 to get (2.8).

The abovementioned work of Lubelski generalizes the famous results of Wieferich [138] and Mirimanoff [95] on the Fermat equation $x^q + y^q + z^q = 0$. Wieferich showed that if the latter equation has a solution with q not dividing xyz (the “first case” of the Fermat theorem), then $2^{q-1} \equiv 1 \pmod{q^2}$, and Mirimanoff

showed that $3^{q-1} \equiv 1 \pmod{q^2}$. Wieferich-type conditions systematically occur in Catalan's problem; see Sects. 6.2 and 6.5.

Obláth [110] combined his conditions with Nagell's results to show that there is no solution with $q < 25000$.

In 1961, Inkeri and Hyryö [52] improved upon Nagell's Theorem 2.9: they showed that existence of a nontrivial solution of (2.7) implies that $q^2 \mid x$ and $q^3 \mid (y - 1)$. Using this result, they proved that there is no nontrivial solutions with $q < 100000$.

Equation $x^2 - y^q = 1$ continued to attract researchers even after the work of Ko Chao. We have already seen Chein's contribution. In 2004 Mignotte [88] suggested yet another proof of the theorem of Ko Chao. He adapted the classical argument of Kummer to show that (2.7) has no solution when $q \geq 5$ is a regular² prime.

The first irregular primes congruent to 1 modulo 8 are 233 and 257. This gives a weaker result than Obláth's; however, modern sharp estimates [65] for binary logarithmic forms imply that (2.7) is impossible for $q > 200$. This gives an alternative proof of Ko Chao's theorem.

One can also apply a deep theorem of Ribet [118] on the Diophantine equation $a^p + 2^\alpha b^p + c^p = 0$ which implies that (2.7) has no nontrivial solutions. This is not the easiest way to prove Ko Chao's theorem, since Ribet's work uses the advanced machinery of Galois representations.

We are left with the equation $x^2 - y^3 = 1$. It will be solved in Sect. 2.5, after some preparation in Sect. 2.4.

2.4 The Cubic Field $\mathbb{Q}(\sqrt[3]{2})$

In this auxiliary section we determine the ring of integers \mathcal{O}_K and the group of units $\mathcal{U}_K = \mathcal{O}_K^\times$ of the cubic field $K = \mathbb{Q}(\sqrt[3]{2})$. We shall use this in Sect. 2.5.

Everywhere throughout this section we use the notation

$$\pi = 1 + \sqrt[3]{2}, \quad \eta = \sqrt[3]{2} - 1.$$

Notice that η is a unit of K .

We start from a simple observation.

Proposition 2.11. *The principal ideal (π) is a prime ideal of K . It satisfies $(\pi)^3 = (3)$.*

Proof. One verifies that $3 = \pi^3 \eta$. Since η is a unit, this implies that $(3) = (\pi)^3$. Since a rational prime number cannot split in K into more than 3 primes, the ideal (π) is prime. \square

²An odd prime number ℓ is *regular* if it does not divide the class number of the ℓ th cyclotomic field and *irregular* if it does.

In the sequel, we write Ord_π instead of $\text{Ord}_{(\pi)}$.

Proposition 2.12. *The ring of integers \mathcal{O}_K is $\mathbb{Z}[\sqrt[3]{2}]$.*

Proof. Denote by \mathcal{D} the discriminant of K and put $d = [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]]$. Then $\mathcal{D}d^2$ is the discriminant of the ring $\mathbb{Z}[\sqrt[3]{2}]$. Since the conjugates of $\sqrt[3]{2}$ are $\xi\sqrt[3]{2}$ and $\xi^2\sqrt[3]{2}$, where $\xi = (-1 + \sqrt{-3})/2$ is a primitive cubic root of unity, we have

$$\mathcal{D}d^2 = \left(\det \left[\left(\xi^k \sqrt[3]{2} \right)^\ell \right]_{0 \leq k, \ell \leq 2} \right)^2 = -2^2 \cdot 3^3.$$

It follows that $d \mid 6$. If d is even, then \mathcal{D} is odd, which is impossible because 2 ramifies in K . Thus, d divides 3.

Since $\mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z}[\pi]$, every $\alpha \in \mathcal{O}_K$ can be written as $\alpha = a_0 + a_1\pi + a_2\pi^2$, where $a_0, a_1, a_2 \in \frac{1}{3}\mathbb{Z}$. If we show that

$$\text{Ord}_3(a_k) \geq 0 \quad (k = 0, 1, 2), \quad (2.9)$$

it would follow that $\alpha \in \mathbb{Z}[\pi]$, proving the proposition.

Observe that $\text{Ord}_\pi(a_k\pi^k) \equiv k \pmod{3}$. It follows that the numbers

$$\text{Ord}_\pi(a_k\pi^k) \quad (k = 0, 1, 2)$$

are pairwise distinct. Lemma A.1 implies that

$$\text{Ord}_\pi(\alpha) = \min_{0 \leq k \leq 2} \text{Ord}_\pi(a_k\pi^k).$$

But $\text{Ord}_\pi(\alpha) \geq 0$, because α is an algebraic integer. Hence $\text{Ord}_\pi(a_k\pi^k) \geq 0$ for $k = 0, 1, 2$, which is only possible if $\text{Ord}_3(a_k) \geq 0$ for all k . This proves (2.9) and the proposition. \square

Proposition 2.13. *The unit group \mathcal{U}_K is generated by -1 and η .*

Proof. The field K has a real embedding and a pair of complex conjugate embeddings. We identify K with its real embedding and denote the complex embeddings by σ and $\bar{\sigma}$, so that

$$|\sigma(\eta)|^2 = \eta^{-1} = 1 + \sqrt[3]{2} + \sqrt[3]{4}.$$

The Dirichlet unit theorem (Appendix A.2) implies that the rank of the unit group is 1. Also, since K has a real embedding, it cannot contain roots of unity other than ± 1 . Thus, \mathcal{U}_K is generated by -1 and a unit θ , where we may assume that

$$0 < \theta < 1. \quad (2.10)$$

Then $\eta = \theta^m$, where $m \geq 1$. This implies the inequality

$$|\sigma(\theta)| = |\bar{\sigma}(\theta)| \leq |\sigma(\eta)| = \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right)^{1/2} < 2. \quad (2.11)$$

Proposition 2.12 implies that $\theta = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$, where $a_0, a_1, a_2 \in \mathbb{Z}$. We have

$$a_k = \frac{1}{3} \text{Tr} \left(\theta \left(\sqrt[3]{2} \right)^{-k} \right) \quad (k = 0, 1, 2),$$

where $\text{Tr} : K \rightarrow \mathbb{Q}$ is the trace map. Using inequalities (2.10) and (2.11), we obtain $|a_0|, |a_1|, |a_2| \leq 5/3$. Thus, $a_0, a_1, a_2 \in \{0, \pm 1\}$. Also, $a_0 \neq 0$, since otherwise θ is not a unit.

Among the 18 remaining possibilities, only ± 1 , $\pm \eta$, and $\pm \eta^{-1}$ are units. Among the latter, only η belongs to the interval $(0, 1)$. Thus, $\theta = \eta$. \square

Remark 2.14. The following more refined argument shows that $a_2 = 0$ (which means that only six possibilities are to be verified instead of 18). Assume that η is not a fundamental unit. Then $\eta = \theta^m$ with $m \geq 2$. This implies, instead of (2.11), the inequality

$$|\sigma(\theta)| = |\bar{\sigma}(\theta)| \leq |\sigma(\eta)|^{1/2} = \left(1 + \sqrt[3]{2} + \sqrt[3]{4}\right)^{1/4} < 1.5.$$

Hence

$$|a_2| = \frac{1}{3} \left| \text{Tr} \left(\theta \left(\sqrt[3]{4} \right)^{-1} \right) \right| \leq 0.9,$$

that is, $a_2 = 0$.

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

This equation has a long history. Already Fermat stated (as usual, without a proof) that it has no solutions in positive integers except the obvious $3^2 - 2^3 = 1$. Euler [31] was the first to prove this. This proof, quite involved, is reproduced in Ribenboim's book [117, Sect. A.2].

Theorem 2.15 (Euler). *The only solution of the equation $x^2 - y^3 = 1$ in nonzero integers x, y is $(\pm 3)^2 - 2^3 = 1$.*

Actually, Euler proved much more: *the equation $x^2 - y^3 = 1$ has no solutions in rational numbers x, y other than $(\pm 1, 0)$, $(0, -1)$ and $(\pm 3, 2)$* . A reader familiar with the notion of elliptic curve can express this as *the elliptic curve $x^2 - y^3 = 1$ has rank 0 and torsion 6 over \mathbb{Q}* .

Later Euler [32, Vol. 2, Article 247] and Legendre [68, pp. 406–409] used an “infinite descent” argument to prove the following theorem.

Theorem 2.16 (Euler, Legendre). *The equation $u^3 + 1 = 2v^3$ has no solutions in integers u, v with $v \neq 0, 1$.*

Theorem 2.15 is an easy consequence of Theorem 2.16.

Proof of Theorem 2.15 (Assuming Theorem 2.16). Rewrite our equation as $(x - 1)(x + 1) = y^3$. If x is even then the factors on the left are coprime. Hence they are complete cubes, which is impossible, because two cubes cannot differ by 2.

Now assume that x is odd. Then y is even, and, replacing x by $-x$, we may assume that $x \equiv 3 \pmod{4}$. Rewrite the equation as

$$\frac{x-1}{2} \frac{x+1}{4} = \left(\frac{y}{2}\right)^3.$$

The factors on the left are coprime rational integers, hence both cubes: $x - 1 = 2u^3$ and $x + 1 = 4v^3$, where u and v are nonzero integers. We obtain $u^3 + 1 = 2v^3$, whence $v = 0$ or 1 by Theorem 2.16. It follows that $x = -1$ or $x = 3$, which proves Theorem 2.15. \square

Here again, both Euler and Legendre proved much more: *the equation $u^3 + 1 = 2v^3$ has no nontrivial solutions in $u, v \in \mathbb{Q}$ (and even in $u, v \in \mathbb{Q}(\sqrt{3})$)*. This also implies the “rational” version of Theorem 2.15 mentioned above.

In 1922, Nagell [101, Sect. 10] suggested an alternative proof of Euler’s theorem; see also [102].

Here we give a different proof, due to McCallum [80]. McCallum’s argument is more transparent than the proofs of Euler, Euler-Legendre, and Nagell, but it does not extend to rational solutions.

(Recently Notari [107] suggested yet another proof, which is totally elementary and, like McCallum’s proof, works only for integer solutions.)

Denote by K the cubic field $\mathbb{Q}(\sqrt[3]{2})$. Recall that $\eta = \sqrt[3]{2} - 1$ generates the group of positive units of K .

Notice that integers u, v satisfy $u^3 + 1 = 2v^3$ if and only if $v\sqrt[3]{2} - u$ is a positive unit of the field K . Hence Theorem 2.16 is equivalent to the following statement.

Theorem 2.17. *The field K has no positive units of the form $a_0 + a_1\sqrt[3]{2}$ (with $a_0, a_1 \in \mathbb{Z}$) other than 1 and η .*

Theorem 2.17 is a particular case of the famous result of Delaunay [27]: *given a cube-free integer d , the ring $\mathbb{Z}[\sqrt[3]{d}]$ has at most one nontrivial positive unit of the form $a_0 + a_1\sqrt[3]{d}$; if such a unit exists, then it generates the group of positive units*. Skolem [130, pp. 114–120] gave another proof of the first part of Delaunay’s theorem using his local method. See also [96, Theorems 23.5 and 24.5]. The proof of McCallum, reproduced below in Sect. 2.5.2, can be viewed as a simplified version of Skolem’s local argument for $d = 2$.

For the proof, we need a preparatory statement on the p -adic convergence of binomial series.

2.5.1 Binomial Series

In this subsection K is an arbitrary number field, not just $\mathbb{Q}(\sqrt[3]{2})$.

If α is a complex number with $|\alpha| < 1$ then the binomial series $\sum_{k=0}^{\infty} \binom{n}{k} \alpha^k$ converges to $(1 + \alpha)^n$. We need the \mathfrak{p} -adic generalization of this: if $\text{Ord}_{\mathfrak{p}}(\alpha) > 0$ then the series $\sum_{k=0}^{\infty} \binom{n}{k} \alpha^k$ “ \mathfrak{p} -adically converges” to $(1 + \alpha)^n$.

Thus, let \mathfrak{p} be a prime ideal of the field K , and let $\mathcal{O}_{\mathfrak{p}}$ be the local ring of \mathfrak{p} :

$$\mathcal{O}_{\mathfrak{p}} = \{\alpha \in K : \text{Ord}_{\mathfrak{p}}(\alpha) \geq 0\}.$$

Given $\alpha, \beta \in \mathcal{O}_{\mathfrak{p}}$, we say that $\alpha \equiv \beta \pmod{\mathfrak{p}^N}$ if $\text{Ord}_{\mathfrak{p}}(\beta - \alpha) \geq N$.

Proposition 2.18. *Let n be an integer, N a nonnegative integer, and \mathfrak{p} a prime ideal of a number field K . Then for any $\alpha \in K$ with $\text{Ord}_{\mathfrak{p}}(\alpha) > 0$ we have*

$$\sum_{k=0}^N \binom{n}{k} \alpha^k \equiv (1 + \alpha)^n \pmod{\mathfrak{p}^{N+1}}.$$

Proof. If $n \geq 0$ then the assertion is an obvious consequence of the binomial formula. Now assume that $n < 0$, and write $n = -m - 1$ with $m \geq 0$. It will be convenient to replace α by $-\alpha$. Since $(-1)^k \binom{-m-1}{k} = \binom{m+k}{m}$, we have to prove that

$$\sum_{k=0}^N \binom{m+k}{m} \alpha^k \equiv (1 - \alpha)^{-m-1} \pmod{\mathfrak{p}^{N+1}}. \quad (2.12)$$

Deriving m times the identity

$$(1 - t)^{-1} - \sum_{k=0}^{m+N} t^k = t^{m+N+1} (1 - t)^{-1},$$

and dividing by $m!$, we obtain the identity

$$(1 - t)^{-m-1} - \sum_{k=0}^N \binom{m+k}{m} t^k = t^{N+1} P(t) (1 - t)^{-m-1}, \quad (2.13)$$

where $P(t)$ is a polynomial, depending on m and N . Notice that

$$t^{N+1} P(t) = 1 - (1 - t)^{m+1} \sum_{k=0}^N \binom{m+k}{m} t^k \in \mathbb{Z}[t],$$

which implies that $P(t) \in \mathbb{Z}[t]$. Hence

$$\text{Ord}_p(\alpha^{N+1} P(\alpha)(1-\alpha)^{-m-1}) \geq (N+1)\text{Ord}_p(\alpha) \geq N+1,$$

and (2.12) follows upon substituting $t = \alpha$ in (2.13). \square

2.5.2 Proof of Theorem 2.17

Now we are ready to prove Theorem 2.17. We again use the notation $K = \mathbb{Q}[\sqrt[3]{2}]$, $\eta = \sqrt[3]{2} - 1$, and $\pi = \sqrt[3]{2} + 1$ from Sect. 2.4.

Every element of the field K can be uniquely written as $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$, where $a_0, a_1, a_2 \in \mathbb{Q}$. This defines the \mathbb{Q} -linear “coefficient functions”

$$a_0, a_1, a_2 : K \rightarrow \mathbb{Q}.$$

Since $\pi^3\eta = 3$, we have $\pi^{3m} = 3^m\eta^{-m}$ for any integer m . Hence for any positive integer k the number π^k is divisible by $3^{\lfloor k/3 \rfloor}$ in the ring $\mathbb{Z}[\sqrt[3]{2}]$. It follows that

$$\text{Ord}_3(a_\ell(\pi^k)) \geq \lfloor k/3 \rfloor \quad (\ell = 0, 1, 2), \quad (2.14)$$

for $k \geq 0$, which will be used throughout the proof.

Let θ be a positive unit of K with $a_2(\theta) = 0$. We have to prove that $\theta = 1$ or $\theta = \eta$. Proposition 2.13 implies that $\theta = \eta^n$, where $n \in \mathbb{Z}$. We assume that $n \neq 0, 1$ and obtain a contradiction.

Fix a large positive integer N , to be specified later. Since $\eta = -2 + \pi$, we have $(-2)^{-n}\theta = (1 - \pi/2)^n$. Proposition 2.18 implies that

$$\sum_{k=0}^N \binom{n}{k} \left(-\frac{\pi}{2}\right)^k \equiv (-2)^{-n}\theta \pmod{\pi^{N+1}}. \quad (2.15)$$

Applying the coefficient function a_2 to both sides of (2.15), and using (2.14), we obtain

$$\sum_{k=0}^N \binom{n}{k} \frac{a_2(\pi^k)}{(-2)^k} \equiv (-2)^{-n}a_2(\theta) \pmod{3^{\lfloor (N+1)/3 \rfloor}}. \quad (2.16)$$

Since $a_2(\theta) = 0$, the right-hand side of congruence (2.16) vanishes. Since $a_2(1) = a_2(\pi) = 0$, so do the summands on the left of (2.16), corresponding to $k = 0$ and $k = 1$. Also, for $k \geq 2$, we have

$$\binom{n}{k} = \frac{n(n-1)}{k(k-1)} \binom{n-2}{k-2}.$$

Hence, for $k \geq 2$, the k th summand on the left of (2.16) is equal to $n(n-1)A_k$, where

$$A_k = \frac{1}{k(k-1)(-2)^k} \binom{n-2}{k-2} a_2(\pi^k).$$

Thus, (2.16) can be rewritten as

$$n(n-1)(A_2 + \cdots + A_N) \equiv 0 \pmod{3^{\lfloor (N+1)/3 \rfloor}}.$$

Since n is distinct from 0 and 1, we may choose N so large that

$$\lfloor (N+1)/3 \rfloor > \text{Ord}_3(n(n-1)).$$

We obtain

$$A_2 + \cdots + A_N \equiv 0 \pmod{3}. \quad (2.17)$$

On the other hand, again using (2.14), we find

$$\text{Ord}_3(A_k) \geq \lfloor k/3 \rfloor - \text{Ord}_3(k(k-1)) \geq \lfloor k/3 \rfloor - \log_3 k. \quad (2.18)$$

As one can easily verify, the right-hand side of (2.18) is positive for $k \geq 6$. Hence $\text{Ord}_3(A_k) > 0$ for $k \geq 6$. Also, $\text{Ord}_3(k(k-1)) = 0$ for $k = 5$, which implies that $\text{Ord}_3(A_5) > 0$.

We have proved that $\text{Ord}_3(A_k) > 0$ for $k \geq 5$. Combining this with (2.17), we obtain

$$A_2 + A_3 + A_4 \equiv 0 \pmod{3}.$$

Since $a_2(\pi^2) = 1$, $a_2(\pi^3) = 3$, and $a_2(\pi^4) = 6$, we have

$$A_2 + A_3 + A_4 = \frac{1}{8} - \frac{n-2}{16} + \frac{(n-2)(n-3)}{32} = \frac{n^2 - 7n + 14}{32}.$$

It follows that $n^2 - 7n + 14 \equiv 0 \pmod{3}$, which is impossible for $n \in \mathbb{Z}$. The theorem is proved. \square

Remark 2.19. The Diophantine equation $y^2 - x^3 = k$, where k is a nonzero integer, is usually called *Mordell's equation*. Many results on it can be found in Chap. 26 of Mordell's book [96]. Modern techniques based on logarithmic forms [11] or forms in elliptic logarithms [33] allow one to solve Mordell's equation completely for small values of k , using electronic computations. For instance, this was done for $|k| \leq 10^4$ in [33].

Cloud Computing and ROI

A New Framework for IT Strategy

Mohapatra, S.; Lokhande, L.

2014, XVII, 214 p. 65 illus., 50 illus. in color., Hardcover

ISBN: 978-3-319-08662-0