16.6 abc conjecture

Definition 16.2. *Let K be an algebraically closed field of characteristic 0 and $f \in K[x]$. The product of distinct irreducible factors of f is called the* radical of the polynomial *f and denoted by $\mathrm{rad}(f)$, while the number of distinct roots of f is denoted by $n_0(f)$, i.e. $n_0(f) = \deg(\mathrm{rad}(f))$.*

The following theorem was proved independently by Stothers (1981) and Mason (1984), and it is often called the *abc theorem for polynomials* ([267, Chapter 4.7]).

Theorem 16.11 (abc theorem for polynomials)**.** *Let K be an algebraically closed field of characteristic 0 and $a, b, c \in K[x]$ non-constant relatively prime polynomials such that*

$$a(x) + b(x) = c(x).$$

Then

$$\max(\deg a, \deg b, \deg c) \leq n_0(abc) - 1.$$

Proof: Let us introduce the notation $f = a/c$, $g = b/c$, so we have $f + g = 1$. By taking derivatives, we obtain $f' + g' = 0$, which we will write in the form

$$\frac{f'}{f} f + \frac{g'}{g} g = 0.$$

From this,

$$\frac{b}{a} = \frac{g}{f} = -\frac{f'/f}{g'/g}.$$

Let

$$a(x) = a_0 \prod_i (x - \alpha_i)^{m_i}, \;\; b(x) = b_0 \prod_j (x - \beta_j)^{n_j}, \;\; c(x) = c_0 \prod_k (x - \gamma_k)^{r_k}.$$

Then

$$\frac{b}{a} = -\frac{f'/f}{g'/g} = -\frac{\sum_i \frac{m_i}{x-\alpha_i} - \sum_k \frac{r_k}{x-\gamma_k}}{\sum_j \frac{n_j}{x-\beta_j} - \sum_k \frac{r_k}{x-\gamma_k}}.$$

Let us denote $N_0(x) = \prod_i (x - \alpha_i) \prod_j (x - \beta_j) \prod_k (x - \gamma_k)$. Then $\deg N_0 = n_0(abc)$ and $\deg N_0 f'/f \leq n_0(abc) - 1$, $\deg N_0 g'/g \leq n_0(abc) - 1$. Since a and b are relatively prime, from

$$\frac{b}{a} = -\frac{N_0 f'/f}{N_0 g'/g},$$

it follows that $\deg a \leq n_0(abc) - 1$ and $\deg b \leq n_0(abc) - 1$ and finally, $\deg c \leq \max(\deg a, \deg b) \leq n_0(abc) - 1$. □

Theorem 16.12 (Fermat's Last Theorem for polynomials)**.** *Let K be an algebraically closed field of characteristic 0 and $a, b, c \in K[x]$ non-constant relatively prime polynomials. If*

$$a(x)^n + b(x)^n = c(x)^n,$$

then $n \leq 2$.

Proof: Let us apply Theorem 16.11 to the polynomials $a(x)^n$, $b(x)^n$ and $c(x)^n$. We obtain

$$n \deg a(x) = \deg a(x)^n \leq \deg a(x) + \deg b(x) + \deg c(x) - 1$$

and the same inequality holds for $n \deg b(x)$ and $n \deg c(x)$. By adding those three inequalities, we obtain

$$n(\deg a + \deg b + \deg c) \leq 3(\deg a + \deg b + \deg x) - 3,$$

which implies that $n \leq 2$. □

Theorem 16.13 (Davenport, 1965)**.** *Let K be an algebraically closed field of characteristic 0 and $f, g \in K[x]$ non-constant relatively prime polynomials. If $f^3 \neq g^2$, then*

$$\deg(f^3 - g^2) \geq \frac{1}{2} \deg f + 1.$$

Proof: Let $h = f^3 - g^2$. The polynomials f^3 and g^2 are relatively prime, so we can apply Theorem 16.11. We obtain

$$\max(\deg h, \deg f^3, \deg g^2) \leq n_0(fgh) - 1 \leq \deg f + \deg g + \deg h - 1.$$

Hence,

$$\deg f^3 = 3 \deg f \leq \deg f + \deg g + \deg h - 1,$$
$$\deg g^2 = 2 \deg g \leq \deg f + \deg g + \deg h - 1,$$

so by adding these two inequalities, we obtain $\deg f \leq 2 \deg h - 2$ and $\deg h \geq \frac{1}{2} \deg f + 1$. □

We may ask whether there are polynomials, say with $\deg f = 2\delta$, $\deg g = 3\delta$, for which in the inequality from Theorem 16.13 the equality holds. Zannier [423] proved the existence of such polynomials over $\mathbb{C}$ for any positive integer δ (see also [2]). On the other hand, for polynomials over $\mathbb{Q}$, the existence of such polynomials is known only for $\delta = 1, 2, 3, 4, 5$. The examples

for $\delta = 5$ were found by Birch, Chowla, Hall and Schinzel [46] and Elkies [171]. This is the example from [46]:

$$f(x) = \frac{x}{9}(x^9 + 6x^6 + 15x^3 + 12),$$
$$g(x) = \frac{1}{54}(2x^{15} + 18x^{12} + 72x^9 + 144x^6 + 135x^3 + 27),$$
$$f^3(x) - g^2(x) = -\frac{1}{108}(3x^6 + 14x^3 + 27).$$

In [124], for any even positive integer δ, polynomials $f, g \in \mathbb{Z}[x]$ such that $\deg f = 2\delta$, $\deg g = 3\delta$ and $\deg(f^3 - g^2) = \delta + 5$ were constructed. Similar results on the more general problem, where $f^3 - g^2$ is replaced by $f^n - g^m$ for coprime integers $n > m \geq 2$, can be found in [2, 41].

In mathematics, there are often analogies between the ring of integers $\mathbb{Z}$ and the ring of polynomials, for instance, $\mathbb{C}[x]$. We saw some of those analogies in Chapter 11. Sometimes, those analogies do not hold literally, but they need some modifications. So, we can ask whether the abc-theorem 16.11, which we proved for polynomials, holds in some form also for the integers. That question led to the famous abc conjecture. It was formulated by Masser (1985) and Oesterlé (1988).

Let us denote by $\mathrm{rad}(m)$ the *radical* of the positive integer m, which is defined as the product of all primes that divide m. Therefore,

$$\mathrm{rad}(m) = \prod_{p|m} p.$$

It is also defined that $\mathrm{rad}(1) = 1$.

Conjecture 16.1 (abc conjecture)**.** *For any $\varepsilon > 0$, there is a constant $C(\varepsilon)$ such that all triples (a, b, c) of relatively prime positive integers with*

$$a + b = c$$

satisfy

$$c < C(\varepsilon)\,\mathrm{rad}(abc)^{1+\varepsilon}. \tag{16.16}$$

A direct analogy with Theorem 16.11 would suggest a stronger inequality than the one in (16.16), namely $c < \mathrm{rad}(abc)$, but such a stronger inequality is not valid, which is demonstrated by the following example.

Example 16.7. Let us take $a = 1$, $b = 2^{6m} - 1$, $c = 2^{6m}$. Then it clearly holds that $a + b = c$ and that $\gcd(a, b, c) = 1$. The number b is divisible by $2^6 - 1 = 63 = 9 \cdot 7$, so we have

$$\begin{aligned}\operatorname{rad}(abc) &= \operatorname{rad}(a)\operatorname{rad}(b)\operatorname{rad}(c) = 2\operatorname{rad}(b) = 2\operatorname{rad}\left(9 \cdot \frac{b}{9}\right) \leq 2 \cdot 3\operatorname{rad}\left(\frac{b}{9}\right) \\ &\leq 2 \cdot 3 \cdot \frac{b}{9} = \frac{2}{3}b < \frac{2}{3}c. \end{aligned}$$ ♢

Example 16.8. Let $n \geq 0$ be an integer. Let us take $a_n = 1$, $b_n = 3^{2^n} - 1$, $c_n = 3^{2^n}$. Then $a_n + b_n = c_n$ and $\gcd(a_n, b_n, c_n) = 1$. From Euler's theorem, it follows that $3^{2^n} \equiv 1 \pmod{2^{n+1}}$, so b_n is divisible by 2^{n+1} and we get

$$\operatorname{rad}(a_n b_n c_n) = 3\operatorname{rad}(b_n) \leq 3 \cdot 2 \cdot \frac{3^{2^n} - 1}{2^{n+1}} < \frac{3}{2^n} c_n.$$

Hence, $c_n > \frac{2^n}{3}\operatorname{rad}(a_n b_n c_b)$, so there is no constant $C(0)$ such that $c_n < C(0)\operatorname{rad}(a_n b_n c_n)$, which shows that a modification of (16.16) is not possible simply by adding a multiplicative constant, which explains the appearance of $1 + \varepsilon$ in the formulation of the abc conjecture. ♢

Many significant consequences (and some equivalent formulations) of the abc conjecture are known (see [52, Chapter 12], [238] and [268]). We list only a few which are mentioned in this book:

- Roth's theorem on approximation of algebraic numbers,
- Faltings's theorem on rational points on curves of genus ≥ 2,
- the asymptotic version of Fermat's Last Theorem,
- Hall's conjecture on integer points on the Mordell curve (an analogue of Davenport's theorem 16.13),
- Szpiro's conjecture which related the discriminant and conductor of an elliptic curve;
- for a given integer a, the Diophantine equation $n! + a = k^2$ only has finitely many solutions,
- the size of sets of positive integers such that the product of their any two distinct elements increased by 1 is a non-trivial power of a positive integer is bounded by an absolute value.

The connection between the abc conjecture and elliptic curves comes through a construction which was proposed by Hellegouarch and Frey, and was used in proving Fermat's Last Theorem. To each triple of relatively prime integers a, b, c, such that $a + b = c$, we can assign the elliptic curve

$$y^2 = x(x - a)(x + b).$$

It can be shown that the conductor of this elliptic curve is equal to $N = 2^{f_2} \prod_{p|abc,\, p\neq 2} p$, where the exponent f_2 depends on the type of reduction at $p = 2$. One of the forms of Szpiro's conjecture states that for any $\varepsilon > 0$ there is a constant $K(\varepsilon)$ such that

$$\max(\Delta, |c_4|^3) \leq K(\varepsilon) N^{6+\varepsilon},$$

where $\Delta = 16(abc)^2$ is the discriminant and $c_4 = 16(a^2+ab+b^2)$ the quantity defined in Chapter 15.2. The proof of equivalence of the abc conjecture and this form of Szpiro's conjecture can be found in [52, Chapter 12.5].

16.7 Diophantine m-tuples and elliptic curves

We will now describe connections between rational Diophantine m-tuples and elliptic curves. Let $\{a, b, c\}$ be a rational Diophantine triple, i.e.

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2$$

for nonnegative rational numbers r, s, t. In order to extend this triple to a rational Diophantine quadruple, we need to find a rational number x such that $ax+1$, $bx+1$ and $cx+1$ are squares of rational numbers. By multiplying these three conditions, we obtain a single condition

$$y^2 = (ax + 1)(bx + 1)(cx + 1),$$

which is the equation of an elliptic curve. We will explain below which points on the curve satisfy the initial system of three equations and give extensions to rational Diophantine quadruples.

Let us denote the curve $y^2 = (ax+1)(bx+1)(cx+1)$ by $\mathcal{E}$. We say that $\mathcal{E}$ is *induced by the Diophantine triple* $\{a, b, c\}$. On the curve $\mathcal{E}$, we have three obvious rational points of order 2, namely $A = (-1/a, 0)$, $B = (-1/b, 0)$, $C = (-1/c, 0)$. We also have two other obvious rational points

$$P = (0, 1), \quad S = (1/abc, rst/abc). \tag{16.17}$$