and $n = 3$ (Mignotte, 2006). Those improvements are important in solving parametric families of Diophantine equations because they usually lead to the conclusion that for large values of parameters we have only "trivial" solutions and leave a relatively small number of concrete equations which need to be additionally examined. If we have just one concrete equation, then the Baker-Wüstholz theorem (and even the initial Baker's result from 1967), combined with the reduction methods which we will discuss in the following sections, is usually sufficient.

Apart from the already mentioned book [22], there are also books [27, 62, 177, 365, 413] and lecture notes [71, 181, 282] devoted to the linear forms in logarithms and their applications.

14.4 Baker-Davenport reduction

We have already mentioned that many problems on Diophantine equations can be transformed into inequalities for linear forms in logarithms of algebraic numbers. Those inequalities usually have the form

$$|n_1 \ln \alpha_1 + \cdots + n_k \ln \alpha_k| < c_1 e^{-c_2 N},$$

where $n_1, \ldots, n_k \in \mathbb{Z}$, $N = \max(|n_1|, \ldots, |n_k|)$, and c_1, c_2 are positive constants. Then we can apply results from the previous section (e.g. the Baker-Wüstholz theorem). In this manner, an inequality of the form

$$c_3 \ln N > c_2 N - \ln c_1,$$

is obtained, from which it follows that $N \leq N_0$, where N_0 is an explicit constant (usually quite large, e.g. 10^{20} or 10^{100}). Since N_0 is usually too large (except when $k = 2$) to check all possible remaining cases, we encounter the question if that bound can be decreased. The answer is affirmative. Namely, two algorithms are known which (if certain technical conditions are satisfied) replace the bound $N \leq N_0$ by a new bound $N \leq N_1$, where $N_1 \approx \ln N_0$.

In this and the following section, we will describe those two methods. The first one is the so-called *Baker-Davenport reduction*. It was introduced by Baker and Davenport in the paper [25] from 1969, in which they solved the problem which emerged in a discussion during a conference in Oberwolfach in March 1968. The problem is connected to the so-called Diophantine m-tuples, i.e. the sets of positive integers such that the product of any two of its distinct elements, increased by 1, is a perfect square. The most famous

Diophantine quadruple is $\{1, 3, 8, 120\}$, found by Fermat. At the mentioned conference, J. H. van Lint presented his results concerning the question of whether it is possible to extend Fermat's set to a quintuple with the same property. More precisely, if d is a positive integer such that $\{1, 3, 8, d\}$ is a Diophantine quadruple, does d have to be equal to 120? The problem was raised by Martin Gardner in his Scientific American column in March 1967 (see [191, Chapter 15, Problem 9]).

By applying Baker's theory of linear forms in logarithms and the newly introduced reduction method, Baker and Davenport completely solved that problem. Harold Davenport (1907 – 1969) was an English mathematician, and the doctoral supervisor of Alan Baker. Their result was later generalized in several directions, which we will discuss in detail in Chapter 14.6, devoted to Diophantine m-tuples.

We will now demonstrate how the Baker-Wüstholz theorem (or another result of a similar kind) can be applied to the problem of the extension of Fermat's set.

Let d be a positive integer such that

$$1 \cdot d + 1 = x^2, \quad 3 \cdot d + 1 = y^2, \quad 8 \cdot d + 1 = z^2.$$

Then

$$y^2 - 3x^2 = -2, \tag{14.25}$$

$$z^2 - 8x^2 = -7, \tag{14.26}$$

so we obtained a system of Pellian equations with a common unknown x. The fundamental solutions of the associated Pell's equations are $2 + \sqrt{3}$ and $3 + \sqrt{8}$, respectively. Now, it is easy to see that all solutions of equation (14.25) are given by

$$y + x\sqrt{3} = \pm(1 \pm \sqrt{3})(2 + \sqrt{3})^n, \tag{14.27}$$

and all solutions of equation (14.26) by

$$z + x\sqrt{8} = \pm(1 \pm \sqrt{8})(3 + \sqrt{8})^m. \tag{14.28}$$

We can assume that x is positive. By keeping in mind that $(1-\sqrt{3})(2+\sqrt{3}) = -(1 + \sqrt{3})$, we can omit the signs $-$ in (14.27) (the class is ambiguous), so we obtain the following exponential equation

$$\frac{(1 + \sqrt{3})(2 + \sqrt{3})^n - (1 - \sqrt{3})(2 - \sqrt{3})^n}{2\sqrt{3}}$$
$$= \frac{(2\sqrt{2} \pm 1)(3 + 2\sqrt{2})^m + (2\sqrt{2} \mp 1)(3 - 2\sqrt{2})^m}{4\sqrt{2}}, \tag{14.29}$$

i.e. an equation of the form $v_n = w_m^{+,-}$, where (v_n), $(w_m^{+,-})$ are binary recurrence sequences. We have $v_0 = w_0^{+,-} = 1$, which gives $d = 0$ (trivial solution) and $v_2 = w_2^- = 11$, which gives $d = 11^2 - 1 = 120$. We want to prove that there are no other solutions.

It is easy to see that for $n > 2$ we have $w_n^{+,-} > v_n$, which implies that $m < n$.

Lemma 14.7. *Let $m, n > 2$ be positive integers which satisfy* (14.29). *Then*

$$0 < |\Lambda| < 7.3 \cdot (2+\sqrt{3})^{-2n}, \tag{14.30}$$

where

$$\Lambda = n\ln(2+\sqrt{3}) - m\ln(3+2\sqrt{2}) + \ln\left(\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}\right).$$

Proof: It is clear that

$$v_n > \frac{(1+\sqrt{3})(2+\sqrt{3})^n}{2\sqrt{3}}, \quad w_m^{+,-} < \frac{(2\sqrt{2}+1)(3+2\sqrt{2})^m}{2\sqrt{2}},$$

so from $v_n = w_m^{+,-}$, it follows that

$$(3-2\sqrt{2})^m < \frac{(2\sqrt{2}+1)\sqrt{3}}{(\sqrt{3}+1)\sqrt{2}}(2-\sqrt{3})^n < 1.7163(2-\sqrt{3})^n.$$

Now, from (14.29), by dividing by $\frac{2\sqrt{2}\pm 1}{2\sqrt{2}} \cdot (3+2\sqrt{2})^m$, we obtain

$$\begin{aligned}
&\left|\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} - 1\right| \\
&\quad \le \frac{2\sqrt{2}+1}{2\sqrt{2}-1} \cdot (3-2\sqrt{2})^{2m} + \frac{2\sqrt{2}(\sqrt{3}-1)}{\sqrt{3}(2\sqrt{2}-1)}(2-\sqrt{3})^n(3-2\sqrt{2})^m \\
&\quad < 7.29(2-\sqrt{3})^{2n}.
\end{aligned}$$

We will use the following simple fact: if $a \in \langle 0, 1\rangle$ and $0 < |X| < a$, then

$$|\ln(X+1)| < \frac{-\ln(1-a)}{a} \cdot |X|. \tag{14.31}$$

Indeed,

$$|\ln(X+1)| = \left|\sum_{i=1}^{\infty} \frac{(-1)^{i-1}X^i}{i}\right| < |X| \cdot \sum_{i=1}^{\infty} \frac{a^{i-1}}{i} = |X| \cdot \frac{-\ln(1-a)}{a}.$$

By applying inequality (14.31) to $X = \frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)} \cdot \frac{(2+\sqrt{3})^n}{(3+2\sqrt{2})^m} - 1$ and $a = 0.0027$ ($\approx 7.29 \cdot (2-\sqrt{3})^6$), we obtain the required inequality

$$|\Lambda| < 7.3 \cdot (2-\sqrt{3})^{2n}.$$

It remains to prove that $|\Lambda| > 0$. Indeed, if $\Lambda = 0$, then, by squaring, we would obtain that

$$16(2+\sqrt{3})^{2n+1} = 3(9 \pm 4\sqrt{2})(3+2\sqrt{2})^{2m},$$

which is a contradiction (because the equality of the form $a+b\sqrt{3} = c+d\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$ is possible only if $b = d = 0$). □

Now everything is ready to apply the Baker-Wüstholz theorem to the form Λ from Lemma 14.7. We have $\alpha_1 = 2+\sqrt{3}$, $\alpha_2 = 3+2\sqrt{2}$, $\alpha_3 = \frac{2(4\pm\sqrt{2})(3+\sqrt{3})}{21}$, $b_1 = n$, $b_2 = -m$, $b_3 = 1$, $d = 4$ (since $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$). The corresponding minimal polynomials over $\mathbb{Z}$ are

$$\begin{aligned} P_{\alpha_1}(x) &= x^2 - 4x + 1, \\ P_{\alpha_2}(x) &= x^2 - 6x + 1, \\ P_{\alpha_3}(x) &= 441x^4 - 2016x^3 + 2880x^2 - 1536x + 256, \end{aligned}$$

so the heights are $h(\alpha_1) = \frac{1}{2}\ln(2+\sqrt{3}) \approx 0.6585$, $h(\alpha_2) = \frac{1}{2}\ln(3+2\sqrt{2}) \approx 0.8814$, $h(\alpha_3) = \frac{1}{4}\ln\left(441 \cdot \frac{2(4+\sqrt{2})(3+\sqrt{3})}{21} \cdot \frac{2(4-\sqrt{2})(3+\sqrt{3})}{21}\right) \approx 1.7836$. Hence, the Baker-Wüstholz theorem gives us

$$\ln(|\Lambda|) \geq -18 \cdot 4! \cdot 3^4 \cdot (32 \cdot 4)^5 \cdot \ln 24 \cdot 0.6585 \cdot 0.8814 \cdot 1.7836 \ln n \geq -3.96 \cdot 10^{15} \ln n.$$

If we compare this with (14.30), we obtain the inequality

$$3.96 \cdot 10^{15} \ln n > 2.63n - 1.99,$$

which implies that $n < 6 \cdot 10^{16}$.

The following lemma from [157] represents a variant of Baker-Davenport reduction (see also [190]).

Lemma 14.8. *Let κ be a real number and N a positive integer. Let $\frac{p}{q}$ be a convergent in the continued fraction expansion of κ such that $q > 6N$ and let μ, A, B be real numbers such that $A > 0$ and $B > 1$. Let $\varepsilon = \|\mu q\| - N \cdot \|\kappa q\|$, where $\| \ \|$ denotes the distance to the nearest integer. If $\varepsilon > 0$, then the inequality*

$$0 < n\kappa - m + \mu < A \cdot B^{-n}$$

has no solution in positive integers m and n such that

$$\frac{\ln(\frac{Aq}{\varepsilon})}{\ln B} \leq n \leq N.$$

Proof: Assume that $1 \leq n \leq N$. Then we have

$$n(\kappa q - p) + np - mq + \mu q < qAB^{-n}.$$

This gives

$$qAB^{-n} > |\mu q - (mq - np)| - n\|\kappa q\| \geq \|\mu q\| - N\|\kappa q\| = \varepsilon,$$

which implies that

$$n < \frac{\ln(\frac{Aq}{\varepsilon})}{\ln B}.$$ □

Remark 14.2. The condition $q > 6N$ in the lemma is somewhat arbitrary. Namely, on the one hand, we want to ensure that the condition $\varepsilon > 0$ will hold, and on the other hand, we want for q to be as small as possible. From the properties of the convergents of the continued fractions, we know that $\|\kappa q\| < \frac{1}{q}$, while for $\|\mu q\|$ we generally only know that it is $\leq \frac{1}{2}$. Therefore, it is reasonable to take at least $q > 2N$, and $q > 6N$ is experimentally confirmed as a good choice.

Remark 14.3. If the condition $\varepsilon > 0$ is not satisfied, we can try to take the next convergent and check whether the condition will then be satisfied. Even if $\varepsilon < 0$, it is possible to obtain some information on n. Namely, if $r = \lfloor \mu q + \frac{1}{2} \rfloor$, then

$$\begin{aligned} |np - mq + r| &< qAB^{-n} + |\mu q - r| + n|\kappa q - p| \leq qAB^{-n} + \|\mu q\| + N\|\kappa q\| \\ &< qAB^{-n} + \frac{1}{2} + \frac{1}{6}. \end{aligned}$$

If $qAB^{-n} > \frac{1}{3}$, then $n < \frac{\ln(3Aq)}{\ln B}$. If $qAB^{-n} \leq \frac{1}{3}$, then $np - mq + r = 0$, which means that $np \equiv -r \pmod{q}$. This congruence has a unique solution $n \equiv n_0 \pmod{q}$, so from $n \leq N < q$, it follows that $n = n_0$.

Theorem 14.9. *If $\{1, 3, 8, d\}$ is a Diophantine quadruple, then $d = 120$.*

Proof: Let us apply the reduction from Lemma 14.8 to the form Λ from Lemma 14.7 with $N = 6 \cdot 10^{16}$. Here, $\kappa = \frac{\ln(2+\sqrt{3})}{\ln(3+2\sqrt{2})}$, $\mu_{1,2} = \frac{\ln\left(\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}\right)}{\ln(3+2\sqrt{2})}$,

$A = \frac{7.3}{\ln(3+2\sqrt{2})}$, $B = (2+\sqrt{3})^2$. The continued fraction expansion of κ is

$$[0, 1, 2, 1, 20, 1, 5, 3, 8, 5, 1, 2, 1, 1, 1, 1, 4, 3, 3, 3, 1, 6, 3, 1, 2, 22,$$
$$1, 2, 8, 2, 1, 2, 6, 3, 20, 2, 10, 3, \ldots],$$

so the first convergent of κ which satisfies the condition $q > 6N$ is

$$\frac{p}{q} = \frac{742265900639684191}{993522360732597120}.$$

We will see that for μ_1 it will be needed to take the next convergent, so let us first consider what is obtained for μ_2. We have $\|\mu_2 q\| \approx 0.24492$, $\|\kappa q\| \cdot N \approx 0.01878$, so $\varepsilon \approx 0.22614 > 0$. By applying Lemma 14.8, we obtain $n \leq 16$. Now, we can repeat the reduction with $N = 16$. The corresponding convergent is now $\frac{p'}{q'} = \frac{387}{518}$, and the reduction gives $n \leq 3$.

As we already mentioned, by applying Lemma 14.8 for μ_1 and the above p, q, we obtain negative ε ($\|\mu_1 q\| \approx 0.007626$, $\|\kappa q\| \cdot N \approx 0.01878$). Therefore, we take the next convergent

$$\frac{P}{Q} = \frac{2297570640187354392}{3075296607888933649}.$$

We obtain $\|\mu_1 Q\| \approx 0.2989$, $\|\kappa Q\| \cdot N \approx 0.002254$, so the corresponding $\varepsilon \approx 0.29665 > 0$ and we can apply the reduction, which gives $n \leq 17$. If we repeat the reduction for $N = 17$, we again obtain that the corresponding convergent is $\frac{p'}{q'} = \frac{387}{518}$, and the reduction gives $n \leq 4$.

It is easily checked that the equations $v_n = w_m^{+,-}$ do not have solutions for $n = 3$ and $n = 4$. Hence, we finished the proof of the theorem. □

14.5 LLL reduction

We will now show how the LLL algorithm, described in Chapter 8.9, can be applied to Diophantine problems which can be transformed into inequalities for linear forms. Among books dealing with this topic, that we used in this section, we recommend [378] and [416].

Let us consider an inequality of the form

$$|\alpha_0 + x_1\alpha_1 + \cdots + x_n\alpha_n| < c_2 e^{-c_3 X}, \tag{14.32}$$

where α_i are given real or complex numbers, c_2 and c_3 positive real constants, and $X = \max(|x_1|, \ldots, |x_n|)$. We look for solutions of the inequality