Finding ABC-triples using Elliptic Curves

Johannes Petrus van der Horst

Thesis advisor: Dr. Bart de Smit

Master thesis, defended on August 27, 2010

Mathematisch instituut, Universiteit Leiden

Abstract

When adding coprime numbers A and B, one could ask how big A, B, and $A+B$ could be compared with the product of the prime numbers dividing these numbers. One can expect that this prime product has about three times as many digits as $A+B$, but with smart choices of A and B this prime product can be *smaller* than $A+B$.

However, the so-called *ABC-conjecture* says that it cannot be much smaller. Several mathematicians have tried to develop algorithms creating infinitely many triples A_n, B_n, and A_n+B_n such that A_n+B_n is large compared to the product of the primes dividing one of the numbers A_n, B_n, and A_n+B_n. And I add a new algorithm to this list of algorithms and use the tool of *elliptic curves*, the zero set of a polynomial equation together with a *group law*, to create my triples.

Table of contents

Chapter 1
Introduction to the ABC-conjecture

The inspiration of my thesis goes back to Diophantus, who proved the following:

Theorem 1.1. (Diophantus) *Let a and b be positive rational numbers such that $a > b$. Then there exist positive rational numbers x and y such that*

$$a^3 - b^3 = x^3 + y^3$$

For example, if one starts with $7 = 2^3 - 1^3$, after some research one finds

$$\left(\frac{4}{3}\right)^3 + \left(\frac{5}{3}\right)^3 = \frac{64+125}{27} = 7$$

The proof of this theorem is very easy after the introduction of the group law on elliptic curves, and will be shown in 3.6. But in the introduction I only tell why this result is interesting for me. For this thesis I was doing some research about the *ABC-conjecture*:

One can start with three positive integers A, B, and C such that $A + B = C$. If A, B, and C have common divisors, we can divide these numbers by their greatest common divisor and get another integer triple A', B' and C' such that A', B' and C' are coprime and $A' + B' = C'$. So we look only at triples A, B, and C such that A, B, and C are coprime.

We define the *radical* $r(n)$ of a number n as the product of all distinct prime numbers dividing n. This makes $r(n)$ being the largest squarefree (not divisible by any square except 1) divisor of n. The *ABC-conjecture* compares $r(ABC)$, which is equal to $r(A) \cdot r(B) \cdot r(C)$ since A, B, and C are coprime, with C as follows:

$$\limsup_{A,B,C>0, C\to\infty, A+B=C, \gcd(A,B,C)=1} \frac{\log C}{\log r(ABC)} = 1$$

In other words, if I make an infinite sequence of coprime positive integer triples A_n, B_n, and C_n such that $A_n + B_n = C_n$ and $C_n \to \infty$ as $n \to \infty$, then the largest limit point of $\frac{\log C_n}{\log r(A_n B_n C_n)}$ is equal to 1. Note that the smallest limit point is at least $\frac{1}{3}$, since $r(ABC) \leqslant ABC < C^3$ for any triple (A, B, C) of coprime positive integers satisfying $A + B = C$. Note also that it is important to require that A, B, and C are coprime. Else one can pick a prime number p dividing ABC and consider the sequence of triples $(A_n, B_n, C_n) = (p^n A, p^n B, p^n C)$ where the radical is constant for each $n \geqslant 0$, but $\log C_n \to \infty$ as $n \to \infty$.

Definition 1.2. *Let (A, B, C) be a triple of positive integers such that $A + B = C$ and with $\gcd(A, B, C) = 1$.*

1. *The* quality *of the triple is defined as $q(A, B, C) = \frac{\log C}{\log r(ABC)}$*
2. *The triple is called an* ABC-triple *if $q(A, B, C) \geqslant 1$*

Note that the only case of equality is $(1, 1, 2)$, since in other triples, at least one of the numbers A and B is divisible by a prime number not dividing C.

It is easy to construct infinitely many ABC-triples. For example, take

$$(A_n, B_n, C_n) = (1, 9^n - 1, 9^n)$$

for any integer $n \geqslant 1$. Then B_n is divisible by $9-1=8$, so

$$\begin{aligned} r(A_nB_nC_n) &\leqslant 1 \cdot \frac{9^n-1}{4} \cdot 3 < \frac{3}{4} \cdot C_n, \\ q(A_n,B_n,C_n) &> \frac{\log C_n}{\log C_n + \log \frac{3}{4}} = 1 + \frac{\log 4 - \log 3}{\log C_n}, \end{aligned}$$

where $\frac{\log 4 - \log 3}{\log C_n} \to 0$ as $n \to \infty$. So one could ask whether such a function $\frac{\log 4 - \log 3}{\log x}$ can be improved to a larger function $f(x)$ such that there are infinitely many ABC-triples (A_n, B_n, C_n) with

$$\forall n \geqslant 1 \colon q(A_n,B_n,C_n) \geqslant 1 + f(C_n)$$

The answer of this question is yes, and there are some such sequences of these triples known. In the following section I give some methods making better functions, but in general these methods gives full control over two out of the three numbers, and only little control over the third one like it is very small for example. In the rest of this thesis, I state my own method, which works differently: It takes equal control of *all three* numbers, in the sense that two of them are cubes, and the third one is the product of a small given number and a cube, and is relatively small. This method uses *Elliptic Curves*, algebraic curves over $\mathbb{Q}$ with a *group law*, which will be introduced in the third section.

Here the theorem from Diophantus comes in. If I begin with an integer d which is the difference between two rational cubes, so $d = a^3 - b^3$, then by Diophantus, there are positive rational numbers x and y such that $x^3 + y^3 = d$. Such a solution (x, y) can be seen as a *point* in the *Elliptic Curve* E: $x^3 + y^3 = d$. It turns out that if E_d has one non-trivial point (a point (x, y) such that $x \cdot y \cdot (x - y) \neq 0$, for example the starting numbers $(a, -b)$), then by using the group law on E one can find many rational points $\{(\frac{p_i}{r_i}, \frac{q_i}{r_i})\}_{i \in I}$ on E. Note that I use that d is an *integer*, so the denominators in both coordinates of each point must be equal. Each such point $(\frac{p_i}{r_i}, \frac{q_i}{r_i})$ gives rise to a *candidate* ABC-triple $(|p_i^3|, |q_i^3|, dr_i^3)$ whose radical is at most $dp_iq_ir_i$. Here I need to take absolute values since one of the coordinates of the point can be negative. If that happens, the number dr_i^3 is not the largest number among them, but then one of the numbers $|p_i^3|$ and $|q_i^3|$ is the sum of the other one and dr_i^3. The radical $dp_iq_ir_i$ is in general larger than $\max(\{|p_i^3|, |q_i^3|, |dr_i^3|\})$, but with smart choices of the points I can make the radical smaller.

Back to the example, I started with $d = 7$ and the initial point $(2, -1)$ on the elliptic curve E_7: $x^3 + y^3 = 7$, and discovered the point $(\frac{4}{3}, \frac{5}{3})$ on E_7. This point gives rise to the equation

$$\left(\frac{4}{3}\right)^3 + \left(\frac{5}{3}\right)^3 = 7.$$

To make this an integer equation I multiply each side with 3^3 to get

$$4^3 + 5^3 = 7 \cdot 3^3 = 189$$

Thus I got the candidate triple $(4^3, 5^3, 7 \cdot 3^3)$. Their radical is equal to $2 \cdot 3 \cdot 5 \cdot 7 = 210 > 189$, so this time the candidate is *not* an ABC-triple. The problem here is that the disturbing factor $d = 7$ is larger than the benefit gain from the fact $4 = 2^2$, and the fact that the numbers $7 \cdot 3^3$, 5^3 and 4^3 are too close to each other. But when running along the elliptic curve $x^3 + y^3 = 7$ one can find rational numbers x and y whose absolute value are very large - so p_i and q_i are very large compared to r_i - making the radical smaller than $\max(|p_i^3|, |q_i^3|)$. In chapter 3 I explain how such points can be discovered. In chapter 4 then I explain how much I can get the quality above 1 this way. Then in chapter 5 I come back to this case and give an ABC-triple right from the point $(2, -1) \in E_7$.

But first I explain some other known methods for finding ABC-triples with a quailty as high as possible.

Chapter 2
Several methods for finding ABC-triples

As seen in the introduction, it is easy to create sequences of infinitely many ABC-triples. Each of such sequences has its own function $f\colon \mathbb{Z}_{>0} \longrightarrow \mathbb{R}_{>0}$ such that the quality of the ABC-triple is at least $1 + f(C)$. More precisely, one creates an infinite sequences of ABC-triples $(A_n,\ B_n,\ C_n)_{n\geqslant 1}$ and defines a function $f\colon \mathbb{Z} \longrightarrow \mathbb{R}$, often also defined over $\mathbb{R}$, such that

$$\forall n \geqslant 1\colon q(A_n, B_n, C_n) \geqslant 1 + f(C_n)$$

Until now, the ABC-conjecture has not been proven or disproved yet - it is a *conjecture* - but if it is true, then a pair of an infinite sequence $(A_n,\ B_n,\ C_n)_{n\geqslant 1}$ and a function $f(x)$ such that $q(A_n, B_n, C_n) \geqslant 1 + f(C_n)$ for all $n \geqslant 1$ only can be constructed if $f(C_n) \to 0$ as $C_n \to \infty$. The ABC-conjecture has some refinements claiming a sharper bound of $f(x)$. One of them is stated by Stewart and Tenenbaum. They created the family of functions

$$f_N(x) = \frac{\sqrt{N}}{\sqrt{(\log x) \cdot \log\log x}}$$

and conjecture that there cannot be created an infinite sequence of ABC-triples $(A_n,\ B_n,\ C_n)$ such that

$$q(A_n, B_n, C_n) \geqslant 1 + f_N(C_n)$$

for $N > 48$. They claim that there does exist an infinite sequence of ABC-triples $(A_n,\ B_n,\ C_n)$ with quality above $1 + f_N(C_n)$ for each $N < 48$, but such a sequence, or a method finding the sequence, has not been discovered yet. The best known methods gives infinitely many ABC-triples $(A_n, B_n, C_n)_{n\geqslant 1}$ with quality larger than a function of the shape

$$f(C_n) = \frac{\text{const.}}{\sqrt{\log C_n} \cdot \log\log C_n}$$

and the *LLL-method* explained later in this section is one of these methods.

We need more properties an ABC-triple (A, B, C) can satisfy:

Definition 2.1. *Let (A, B, C) be an ABC-triple.*

1. *(A, B, C) is a* good ABC-triple *when $q(A, B, C) \geqslant 1.4$.*
2. *The* merit *$m(A, B, C)$ is defined as the largest N such that*

$$q(A, B, C) \geqslant 1 + \frac{\sqrt{N}}{\sqrt{(\log C) \cdot \log\log C}}$$

   hence

$$m(A, B, C) = (q(A, B, C) - 1)^2 \cdot (\log C) \cdot \log\log C.$$

3. *(A, B, C) is called* unbeaten *if there are no triples (A', B', C') with $C' > C$ and*

$$q(A', B', C') \geqslant q(A, B, C).$$

The value of 1.4 given in this defenition is arbitrary - it could have been any value. So in this thesis I use this definition as little as possible. A consequence of the ABC-conjecture is that there are only finitely many good ABC-triples. At the time this thesis is defended, there are 233 known good ABC-triples, and the largest one among them is

$$(2^{37} \cdot 3^{12} \cdot 9109^3,\ 5^{13} \cdot 13^{15} \cdot 2939,\ 7^{23} \cdot 11 \cdot 793345871)$$

with 30 digits. However, it has not been proved yet that there are no more good ABC-triples.

Als long as the ABC-conjecture has not been proven, it theoretically could be possible that for any number $\alpha \in \mathbb{R}$ there are infinitely many ABC-triples $(A_n, B_n, C_n)_{n\geqslant 1}$ with quality larger than α. If that is true, then every ABC-triple (A, B, C) is not unbeaten; there is another ABC-triple (A', B', C') that beats it. So at present, to the question whether an ABC-triple (A, B, C) is unbeaten we can only answer "no" or "we don't know." Of course, from the largest good ABC-triple we don't know whether it is unbeaten as long as we don't know better. There is a list of the smallest 100 ABC-triples for which no one has discovered another ABC-triple which beats them, and this "unbeaten" list can be seen on A). The 'holy grail' of the methods below is to add new ABC-triples to the "unbeaten" list - maybe beating some ABC-triples current on the list.

2.1 Elementary number theory

In the introduction I gave an explicit method constructing infinitely many ABC-triples using nothing more than 'elementary' number theory - number theory not using tools from other courses. A method like this uses a small number A and a large number $C_n = p^n$ with p a (small) prime number not dividing A, and n a (large) integer. Their difference $B_n = C_n - A$ also is a large number, over which we have only little control. For an arbitrary integer n, we in general don't have a better upper bound for $r(B_n)$ than B_n itself. So (A, B_n, C_n) even isn't an ABC-triple. But we can fix a prime number $q \neq p$ and choose n such that q^2 divides B_n. Then

$$r(AB_nC_n) \leqslant A \cdot \frac{B_n}{q} \cdot p$$

which is smaller than C_n if $q > A \cdot p$.

This can be done by finding an integer k such that

$$p^k \equiv A \pmod{q^2}$$

Then any integer $n = k + l \cdot \varphi(q^2)$ will create an ABC-triple (A, B_n, C_n). But here we have to be careful. Such an integer k does not always exist for a given A, p and q. The problem is that p is not necessary a generator of the multiplicative group $(\mathbb{Z}/q^2\mathbb{Z})^*$. But for $A = 1$ it is always possible since 1 is the unit of this group.

The exponent of q occurring in $p^n - A$ can be improved from 2 by a larger integer m. If we create an infinite sequence of ABC-triples (A, B'_n, C'_n) where C'_n is the smallest power of p congruent to $A \bmod q^n$ and $B'_n = C'_n - A$, then

$$C'_n \leqslant p^{\varphi(q^n)} = p^{(q-1)q^{n-1}}.$$

Hence the quality is at least

$$\frac{\log C'_n}{\log r(AB'_nC'_n)} \geqslant \frac{\log C'_n}{\log\left(A \cdot \frac{C'_n}{q^{n-1}} \cdot p\right)} = 1 + \frac{(n-1)\log q - \log A - \log p}{\log C'_n + \log A + \log p - (n-1)\log q}.$$

We can use that $\log A$, $\log p$ and $\log q$ are small fixed constants. We know

$$\begin{aligned} \log\log C'_n &\leqslant \log\left((q-1)q^{n-1}\right) + \log\log p = (n-1)\log q + \log(q-1) + \log\log p, \\ q(A, B_n, C_n) &\geqslant 1 + \frac{\log\log C'_n - \log A - \log p - \log(q-1) - \log\log p}{\log C'_n + \log A + \log p + \log(q-1) - \log\log C'_n}. \end{aligned}$$

As $n \to \infty$, this quality can be approximated by

$$1 + f(C_n) = 1 + \frac{\log\log C_n}{\log C_n}$$

since for n sufficiently large, the denominator is smaller than $\log C_n$ and the numerator is equal to $\log\log C'_n + \delta$ with δ a constant number only depending on A, p, and q, but not on n. This function $f(x) = \frac{\log\log x}{\log x}$ does not depend on the choises of A, p and q, so for each choise of these constants there are infinitely many ABC-triples $(A, B'_n, C'_n)_{n\geqslant 1}$ and a constant $\delta > 0$ such that

$$q(A, B'_n, C'_n) \geqslant 1 + \frac{\log\log C'_n - \delta}{\log C'_n}.$$

The only prerequisite is that A must be in the subgroup of $(\mathbb{Z}/p^m\mathbb{Z})^*$ generated by p for all m.

This method seems not to be optimal compared with the function $\frac{C_0}{\sqrt{\log x}\cdot\log\log x}$, where C_0 is some constant number. But the difference is that the term $\log\log x$ now is in the *numerator* rather than the denominator, so this function can be better for some values for x:

$$(\log\log x)^4 > C_0^2\cdot\log x \Longrightarrow \frac{\log\log x}{\log x} > \frac{C_0}{\sqrt{\log x}\cdot\log\log x}$$

If $C_0 = 1$, then this happens if $x \leqslant 1.626\cdot 10^{2390}$.

Of course we also can try to use several prime numbers $q_1, ..., q_r$ such that B_n is divisible by squares of all these numbers, trying to improve this method. But that is harder to compute and to write down, and falls outside the subject of this thesis.

My own method, the one using elliptic curves, has a similar result, creating infinitely many ABC-triples $(A_n, B_n, C_n)_{n\geqslant 1}$ with quality at least

$$1 + f(x) = 1 + \frac{r\cdot\log\log x - \delta}{\log x}$$

where the constant δ depends on the choice of the elliptic curve. The constant r can be larger than 1 and hence my method using elliptic curves seems to be better than the method above, using only elementary number theory, but my method often has some larger disturbing constant factor δ. But it has another important property: *All the numbers A_n, B_n and C_n are of a special form: Two of them are cubes and the third one is the product of a cube and a small constant.*

2.2 LLL-method

This method picks some distinct prime numbers $p_1, ..., p_n$ with n a positive integer. Then the purpose is to find integers $e_1, ..., e_n \in \mathbb{Z}$ and to define B and C, both integers completely factorized into primes along $p_1, ..., p_n$, such that

$$\frac{C}{B} = \prod_{i=1}^{n} p_i^{e_i}$$

is as close to 1 as possible. Hence C is the product of the prime powers of the shape $p_i^{e_i}$ with $e_i > 0$ and B is the product of prime powers of the shape $p_j^{-e_j}$ with $e_j < 0$. Then we have full control of B and C in the sense that their radical is bounded by a constant number depending only on the set of primes, but no control of $A := C - B$ (it can be an arbitrary number), except that A is relatively a very small number compared with B and C. If A is small enough, then $r(ABC) < C$ and we have an ABC-triple. This is the case when

$$r(BC) \leqslant p_1\cdot\cdots\cdot p_n \leqslant \frac{C}{A}$$

and in general we don't know more than $r(A) \leqslant A$. So we have full control of B and C, but in general we only know $r(A) \leqslant A$. This method is one of the best methods for finding nice ABC-triples:

Theorem 2.2. (Stewart-Tijdeman) *For each $\delta > 0$ there are infinitely many triples $(A_i, B_i, C_i)_{i\geqslant 1}$ with $A_i + B_i = C_i$, $\gcd(A_i, B_i) = 1$ and R_i defined as $r(A_iB_iC_i)$ such that*

$$C_i > \exp\left((4-\delta)\frac{\sqrt{\log R_i}}{\log\log R_i}\right)R_i$$

Since $\log C_i \geqslant \log R_i$, this formula says that the quality $\frac{\log C_i}{\log R_i}$ is larger than

$$\frac{\log R_i}{\log R_i} + \frac{(4-\delta)\sqrt{\log R_i}}{(\log R_i)\log\log R_i} = 1 + \frac{4-\delta}{\sqrt{\log R_i}\cdot\log\log R_i} > 1 + \frac{4-\delta}{\sqrt{\log C_i}\cdot\log\log C_i}$$

The proof of this theorem uses subtle analytic number theory using the *prime number theorem with error terms*: The fact that the n-th prime number is about $n \log n$ with relatively small error term. The details of this proof falls outside this thesis, but can be find in B). Here I only explain how it works.

First of al we must translate the problem above to a "smallest vector problem". Then we need to solve the smallest vector problem and finally we need to translate it back into ABC-triples. The first part, translating the problem above into the shortest vector problem, goes as follows: Let $p_1, ..., p_n$ be (small) prime numbers. Then find (probably negative) integers $e_1, ..., e_n$ such that $p_1^{e_1} \cdot \cdots \cdot p_n^{e_n} \approx 1$. This is equivalent with

$$e_1 \log p_1 + \cdots + e_n \log p_n \approx 0$$

So this has become an *approximate linear dependency problem*: Given real numbers α_1, ..., α_n, find (small) integers e_1, ..., e_n such that $\alpha_1 e_1 + \cdots + \alpha_n e_n$ lie as close to 0 as possible - to make them "nearly linear dependent." This can be solved using *lattices*. Before defining a lattice, first I need some tools:

I. The vector space $\mathbb{R}^n$ is equipped with an *inner product* $\langle , \rangle \colon \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ satisfying the following properties for all $\lambda \in \mathbb{R}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{R}^n$:

1. $\langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z} \rangle = \langle \boldsymbol{x}, \boldsymbol{z} \rangle + \langle \boldsymbol{y} + \boldsymbol{z} \rangle$.
2. $\langle \lambda \boldsymbol{x}, \boldsymbol{y} \rangle = \lambda \langle \boldsymbol{x}, \boldsymbol{y} \rangle$.
3. $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{y}, \boldsymbol{x} \rangle$.
4. $\langle \boldsymbol{x}, \boldsymbol{x} \rangle \geqslant 0$ and equality holds if and only if $\boldsymbol{x} = \boldsymbol{0}$.

II. The inner product as defined above also defines a *norm* and a *distance*

$$\begin{aligned} \|\boldsymbol{x}\| &:= \langle \boldsymbol{x}, \boldsymbol{x} \rangle^{\frac{1}{2}} \\ d(\boldsymbol{x}, \boldsymbol{y}) &:= \|\boldsymbol{x} - \boldsymbol{y}\| \end{aligned}$$

III. The inner product and the norm also can be defined alternatively by a *quadratic form*

$$q \colon \mathbb{R}^n \longrightarrow \mathbb{R}$$

satisfying for all $l \in \mathbb{R}, \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$:

1. $q(\boldsymbol{x} + \boldsymbol{y}) + q(\boldsymbol{x} - \boldsymbol{y}) = 2q(\boldsymbol{x}) + 2q(\boldsymbol{y})$. (*parallelogram law*)
2. $q(l\boldsymbol{x}) = l^2 q(\boldsymbol{x})$.
3. $q(\boldsymbol{x}) = 0 \Longleftrightarrow \boldsymbol{x} = \boldsymbol{0}$.
4. $\{\boldsymbol{x} \in L \colon q(\boldsymbol{x}) \leqslant r\}$ is a finite subset of the lattice L.

Then the norm $\| \cdot \|$ is defined as $\|\boldsymbol{x}\| = \sqrt{q(\boldsymbol{x})}$ and the inner product $\langle , \rangle$ is defined as

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \frac{q(\boldsymbol{x} + \boldsymbol{y}) - q(\boldsymbol{x}) - q(\boldsymbol{y})}{2}.$$

Now I am ready to define a lattice:

Definition 2.3. *Let n be an integer. Then $\mathbb{R}^n$ is a vector space equipped with some quadratic form $q \colon \mathbb{R}^n \longrightarrow \mathbb{R}$ and a* lattice *is a discrete subgroup $L \subset \mathbb{R}^n$ in $\mathbb{R}^n$ with the induced quadratic form. Sometimes the lattice is denoted (L, q).*

The rank *$r(L)$ of the lattice L is defined as the rank of the linear subspace $\mathbb{T}$ of $\mathbb{R}^n$ spanned by the elements of L.*

A lattice $L \subset \mathbb{R}^n$ is said to have full rank *if r(L)=n*

So L can be written as $L = \mathbb{Z}^r, r \leqslant n,$ generated by vectors $\boldsymbol{b_1}, ..., \boldsymbol{b_r}$ where $\boldsymbol{b_1}, ..., \boldsymbol{b_r}$ form a basis of $\mathbb{T}$.

Definition 2.4. *Let $L \subset \mathbb{R}^n$ be a lattice of full rank. The* determinant *$d(L)$ of L is defined as*

$$d(L) = \lim_{r \to \infty} \frac{\operatorname{vol} B(\sqrt{r})}{\#\{\boldsymbol{x} \in L \colon q(\boldsymbol{x}) \leqslant r\}} = \lim_{r \to \infty} \frac{\operatorname{vol}(\{\boldsymbol{x} \in \mathbb{R}^n \colon \langle \boldsymbol{x}, \boldsymbol{x} \rangle \leqslant r\})}{\#\{\boldsymbol{x} \in L \colon q(\boldsymbol{x}) \leqslant r\}}$$

where the standard volume in $\mathbb{R}^n$ is used, using the standard ball $B(\sqrt{r})$ of radius $\sqrt{r}$. So

$$\operatorname{vol} B(\sqrt{r}) = r^{\frac{n}{2}} \cdot \operatorname{vol} B(1) = r^{\frac{n}{2}} \cdot \frac{\pi^{\frac{n}{2}}}{\left(\frac{n}{2}\right)!}$$

where $0! = 1$, $\left(\frac{1}{2}\right)! = \frac{\sqrt{\pi}}{2}$ and $\left(\frac{n}{2}\right)! = \frac{n}{2} \cdot \left(\frac{n}{2} - 1\right)!$ if $n \geqslant 2$. Note that the determinant of (L, q) also depends on q since the number of elements in the set $\#\{\boldsymbol{x} \in L\colon q(\boldsymbol{x}) \leqslant r\}$ depends on the choice of the quadratic form q. The determinant of L is equal to the volume, depending on q, of the *fundamental domain*

$$F_L := \left\{ \sum_{i=1}^{n} \lambda_i \boldsymbol{b}_i \colon 0 \leqslant \lambda_i < 1 \right\}.$$

where $\boldsymbol{b_1}, ..., \boldsymbol{b_n}$ form a basis of L. That volume is equal to

$$\sqrt{|\det\left((\langle \boldsymbol{b_i}, \boldsymbol{b_j} \rangle)_{1 \leqslant i,j \leqslant n}\right)|}$$

Theorem 2.5. (Minkowski) *Each lattice L of rank n contains a nonzero vector $\boldsymbol{x}$ satisfying*

$$q(\boldsymbol{x}) \leqslant \frac{4}{\pi} \cdot \left(\left(\frac{n}{2}\right)!\right)^{\frac{2}{n}} \cdot d(L)^{\frac{2}{n}} \leqslant n \cdot d(L)^{\frac{2}{n}}$$

Proof. Let

$$\lambda := \lambda(L) = \min\{q(\boldsymbol{x})\colon \boldsymbol{x} \in L, \boldsymbol{x} \neq \boldsymbol{0}\}$$

Then there are no two lattice points $\boldsymbol{x}$,$\boldsymbol{y}$ such that

$$d(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\| \lneqq \frac{\sqrt{\lambda}}{2}$$

Let

$$B' = \{\boldsymbol{z} \in \mathbb{R}^n \colon \langle \boldsymbol{z}, \boldsymbol{z} \rangle < \frac{\lambda}{4}\}$$

the standard ball of diameter $\sqrt{\lambda}$. Then the sets $\boldsymbol{x} + B'$ are pairswise disjoint if $\boldsymbol{x}$ runs through L. But also the sets $\boldsymbol{x} + F_L$ are pairswise disjoint if $\boldsymbol{x}$ runs through L and these sets cover $\mathbb{R}^n$. So

$$\left(\bigcup_{\boldsymbol{x} \in L} \boldsymbol{x} + B'\right) \subset \left(\bigcup_{\boldsymbol{x} \in L} \boldsymbol{x} + F_L\right)$$

hence $\operatorname{vol}(B') \leqslant \operatorname{vol}(F) = d(L)$. Since

$$\operatorname{vol}(B') = \left(\frac{\lambda}{4}\right)^{\frac{n}{2}} \cdot \pi^{\frac{n}{2}} \cdot \left(\left(\frac{n}{2}\right)!\right)^{-1}$$

we get the first inequality

$$\lambda \leqslant \left(\pi^{-\frac{n}{2}} \cdot 4^{\frac{n}{2}} \cdot \left(\frac{n}{2}\right)! \cdot d(L)\right)^{\frac{2}{n}} = \frac{4}{\pi} \cdot \left(\left(\frac{n}{2}\right)!\right)^{\frac{2}{n}} \cdot d(L)^{\frac{2}{n}}$$

The second inequality is true because

$$B(1) \supset \left\{(x_1, ..., x_n) \in \mathbb{R}^n \colon |x_1|, ..., |x_n| \leqslant \frac{1}{\sqrt{n}}\right\}$$

a cube of volume $\left(\frac{2}{\sqrt{n}}\right)^n$. Hence

$$\pi^{\frac{n}{2}} \cdot \left(\left(\frac{n}{2}\right)!\right)^{-1} \geqslant \left(\frac{2}{\sqrt{n}}\right)^n = \left(\frac{4}{n}\right)^{\frac{n}{2}}$$

So we get the second inequality

$$n \geqslant \left(\left(\frac{4}{\pi}\right)^{\frac{n}{2}} \cdot \left(\frac{n}{2}\right)!\right)^{\frac{2}{n}} = \frac{4}{\pi} \cdot \left(\left(\frac{n}{2}\right)!\right)^{\frac{2}{n}}$$

□

Remark 2.6. Stirling proved in 1730 that $\frac{4}{\pi} \cdot \left(\left(\frac{n}{2}\right)!\right)^{\frac{2}{n}} = \frac{2+\mathcal{O}(1)}{e\pi} \cdot n$ as $n \to \infty$. A proof using only elementary calculus is published by Keith Conrad, see C).

Now we are able to translate the approximate linear dependency problem into a shortest vector problem: If we begin with the $\mathbb{Q}$-linearly independent numbers α_1, ..., α_n and want to find 'small' integers $x_1, ..., x_n$ such that $x_1\alpha_1 + \cdots + x_n\alpha_n \approx 0$, one can create the lattice $L = \mathbb{Z}^n$ with

$$q_N(x_1, ..., x_n) = \left(\sum_{i=1}^{n} x_i^2\right) + N\left(\sum_{i=1}^{n} x_i\alpha_i\right)^2$$

where N is a sufficiently large number.

Lemma 2.7. *The determinant of this lattice is equal to* $d((L, q_N)) = \sqrt{1 + N\sum_{i=1}^{n} \alpha_i^2}$.

The proof of this lemma falls outside my thesis, but can be find in D). With this result and the shortest vector whose existence is proved by Minkowski, one can get the result from Stewart-Tijdeman (Theorem 2.2).

However, the given proof of Minkowski's theorem 2.5 is called *ineffective*: It proves the existence, but doesn't give an algorithm that finds one. Moreover, there is no known algorithm that finds the shortest nonzero vector in a given lattice, which runs in *polynomial time*: For each number M each known algorithm requires (much) more than n^M bit operations as $n \to \infty$, where n is the rank of the lattice. In practice it takes too much time to find the optimal solution, especially when looking at many lattices - or at least many different values for N - so to find at least *approximately good* solutions, one needs an algorithm that doesn't give the optimal solution but a sufficiently good solution in sufficiently few time. And one of such algorithms is called the *LLL algorithm*.

For each lattice L of rank n and with basis $\boldsymbol{b_1}, ..., \boldsymbol{b_n}$ one can define a *flag* $\mathfrak{F} = (L_i)_{i=0}^n$ where

$$\{\mathbf{0}\} = L_0 \subsetneqq L_1 \subsetneqq ... \subsetneqq L_n = L$$

a chain of pure sublattices, where $M \subset L$ is a *pure sublattice* of L if the linear subspace spanned by M does not contain lattice points of L outside M, with for each $i \in \{1, ..., n\}$ the quotient L_i/L_{i-1} being a lattice of rank 1, by defining

$$L_i = \mathbb{Z} \cdot \boldsymbol{b_1} \oplus \cdots \oplus \mathbb{Z} \cdot \boldsymbol{b_i},\ i = 1, ..., n$$

This is a bad flag in general, and the LLL-algorithm finds a better flag by reducing the *size* of the flag. The *size* of the flag is defined by

$$s(\mathfrak{F}) = s(\{L_i\}_{i=0}^n) = \prod_{i=0}^{n} d(L_i)$$

where $d(L_i)$ is the determinant of the sublattice L_i. Define the j-th *successive distance* $l_j(\mathfrak{F})$ of $\mathfrak{F}$ to be $d(L_j)/d(L_{j-1})$ with $l_0(\mathfrak{F}) := 1$, then the size of the flag $\mathfrak{F}$ is equal to

$$s(\mathfrak{F}) = \prod_{i=0}^{n} \prod_{j=0}^{i} l_j(\mathfrak{F})$$

Since the factors with small j occur more often than the factors with large j, a way to reduce the size of a flag is to make the values of $l_j(\mathfrak{F})$ the largest if j is large.

The numbers $d(L_i)$ can be computed through the *Gram Schmidt orthogonalization*: Let $\boldsymbol{b_i^*}$ be the unique vector in $\boldsymbol{b_i} + \sum_{j=1}^{i-1} \mathbb{R} \cdot \boldsymbol{b_j}$ that is orthogonal to $\sum_{j=0}^{i-1} \mathbb{R} \cdot \boldsymbol{b_j}$. Then $\boldsymbol{b_1^*} = \boldsymbol{b_1}$ and inductively

$$\boldsymbol{b_i^*} = \boldsymbol{b_i} - \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{b_i}, \boldsymbol{b_j^*} \rangle}{\langle \boldsymbol{b_j^*}, \boldsymbol{b_j^*} \rangle}$$

So $l_i(\mathfrak{F}) = \|\boldsymbol{b}_i^*\| = \sqrt{q(\boldsymbol{b}_i^*)}$.

Let c be a real number. Then a flag $\mathfrak{F}$ of a lattice L of rank n is called *c-reduced* if

$$\forall j \in \{0, ..., n-1\}: (l_{j+1}(\mathfrak{F}))^2 \geqslant \frac{(l_j(\mathfrak{F}))^2}{c}$$

hence when $c \cdot q(\boldsymbol{b}_{\boldsymbol{j+1}}^*) \geqslant q(\boldsymbol{b}_{\boldsymbol{j}}^*)$ for all j. Such a c-reduced flag exists if $c \geqslant \frac{4}{3}$ and in general such a c-reduced flag does not exist for smaller values of c. If a given flag $\mathfrak{F} = (L_i)_{i=0}^n$ is not c-reduced, then there exists a *pivot*, an index $j \in \{1, ..., n-1\}$ such that

$$c \cdot l_{j+1}(\mathfrak{F})^2 < l_j(\mathfrak{F})^2$$

Then $\mathfrak{F}_j = (L_i/L_{j-1})_{i=j-1}^{j+1}$ is a flag of the rank two lattice L_{i+1}/L_{i-1} which is not c-reduced. We need to find a *size-reduced* basis which give rise to this flag: First take the basis $\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}}, \boldsymbol{b}_{\boldsymbol{j},\boldsymbol{2}}$ of the lattice L_{j+1}/L_{j-1} giving rise to this flag. Then we have a unique vector $\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}$ such that $\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}} - \boldsymbol{b}^*_{\boldsymbol{j},\boldsymbol{2}}$ belongs to the *fundamental domain* $\{\lambda \boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}} : -\frac{1}{2} < \lambda \leqslant \frac{1}{2}\}$ of L_j/L_{j-1}. Then the basis $\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}}, \boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}$ is size-reduced, and $\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}} = \boldsymbol{b}^*_{\boldsymbol{j},\boldsymbol{2}} + \mu \boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}}$ with $|\mu| \leqslant \frac{1}{2}$. So

$$q(\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}) = q(\boldsymbol{b}^*_{\boldsymbol{j},\boldsymbol{2}}) + \mu^2 q(\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}}) \leqslant \left(\frac{l_2(\mathfrak{F}_j)^2}{l_1(\mathfrak{F})^2} + \frac{1}{4}\right) q(\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}}) < \left(\frac{1}{c} + \frac{1}{4}\right) q(\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}})$$

where the latter inequality comes from the assumption that $\mathfrak{F}$ is not c-reduced. So if $c \geqslant \frac{4}{3}$, we have $q(\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}) < q(\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}})$ and have a flag $\mathfrak{F}'_j$ corresponding to the basis $\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}, \boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}}$ which is of smaller size than $\mathfrak{F}_j$ is. Since this doesn't influence $L_i(\mathfrak{F})$ outside the pivot j, we also have a flag $\mathfrak{F}'$ of smaller size than the flag $\mathfrak{F}$, where $\mathfrak{F}' = (L'_i)_{i=0}^n$ with $L'_i = L_i$ if $i \neq j$, and

$$L'_j = L_{j-1} \oplus \mathbb{Z} \cdot \boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}} = \mathbb{Z} \cdot \boldsymbol{b}_{\boldsymbol{1}} \oplus \cdots \oplus \mathbb{Z} \cdot \boldsymbol{b}_{\boldsymbol{i-1}} \oplus \mathbb{Z} \cdot \boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}$$

If we have a strict inequality $c < \frac{4}{3}$, let's say $c = \frac{4}{3} + \varepsilon$ for some $\varepsilon > 0$ the size of the new flag is reduced by a factor at least

$$\left(\frac{1}{c} + \frac{1}{4}\right)^{-1} = \left(\frac{3}{4+3\varepsilon} + \frac{1}{4}\right)^{-1} = \left(\frac{12+4+3\varepsilon}{4(4+3\varepsilon)}\right)^{-1} = \frac{16+12\varepsilon}{16+3\varepsilon} = 1 + \frac{9\varepsilon}{16+3\varepsilon} > 1$$

Since every lattice has only finitely many flags of size smaller than a given number, we find in polynomial time a flag what is c-reduced when $c > \frac{4}{3}$. However, if $c = \frac{4}{3}$, this algorithm is not guaranteed to work in polynomial time. In practice it is mostly used with $c = 2$.

Note that when we take $c < \frac{4}{3}$, we still have $q(\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}) < \left(\frac{1}{c} + \frac{1}{4}\right) q(\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}})$, but then $\frac{1}{c} + \frac{1}{4} < 1$, so we don't necessary have $q(\boldsymbol{b}'_{\boldsymbol{j},\boldsymbol{2}}) < q(\boldsymbol{b}_{\boldsymbol{j},\boldsymbol{1}})$. So this method doesn't necessary increase the flag each time, and when it doesn't, we can repeat the process using the same indices. So the algorithm doesn't always end, and that is why we need to have the lower bound $c \geqslant \frac{4}{3}$ to guarantee that there exist a c-reduced flag.

The next step is to find a short vector from the c-reduced flag. From our final c-reduced flag $\mathfrak{F}_{\text{final}} = (L_i)_{i=0}^n$, we have a size-reduced basis $\boldsymbol{b}_{\boldsymbol{1}}, ..., \boldsymbol{b}_{\boldsymbol{n}}$ of L such that $L_i = \mathbb{Z} \cdot \boldsymbol{b}_{\boldsymbol{1}} \oplus \cdots \oplus \mathbb{Z} \cdot \boldsymbol{b}_{\boldsymbol{i}}$ for $i = 1, ..., n$. Let $\boldsymbol{y}$ be an optimal solution of the shortest vector problem. Then there is some index i, $1 \leqslant i \leqslant n$ such that $\boldsymbol{y} \in L_i$ but $\boldsymbol{y} \notin L_{i-1}$. Then $l_i(\mathfrak{F}_{\text{final}}) = q(\boldsymbol{y})$ and by the fact that $\mathfrak{F}_{\text{final}}$ is c-reduced, $q(\boldsymbol{b}_{\boldsymbol{1}}) \leqslant c^{i-1} \boldsymbol{q}(\boldsymbol{y})$. Since $i \leqslant n$,

$$q(\boldsymbol{b}_{\boldsymbol{1}}) \leqslant c^{n-1} \min\{q(\boldsymbol{x}) : \boldsymbol{x} \in L - \{\boldsymbol{0}\}\} \leqslant c^{\frac{n-1}{2}} d(L)^{\frac{2}{n}}$$

where the latter inequality comes from Minkowski's theorem 2.5. To find the optimal solution $\boldsymbol{y}$, one needs to check $q(\boldsymbol{x})$ for each $\boldsymbol{x}$ of the form

$$\boldsymbol{x} = \sum_{i=1}^n r_i \boldsymbol{b}_{\boldsymbol{i}}, |r_i| \leqslant c^{\frac{n-1}{2}} \left(\frac{3c}{4}\right)^{n-i}, 1 \leqslant i \leqslant n$$

The number of vectors in this "box" is very high, of the form

$$\text{const}_1^{1+2+\cdots+n} \cdot \text{const}_2^{\frac{n(n-1)}{2}} = \mathcal{O}(e^{n^2})$$

so it takes very much time to check all vectors when n grows large. So often one is satisfied with just taking $\boldsymbol{b_1}$ as solution.

With the algorithm described above, H.E. Reijngoud showed in her Bachelor Thesis (see E), written in Dutch) that one cannot get a better lower bound for the quality than $1 + \frac{\log\log C}{\log C}$. However, when n is small enough, one can find optimal solutions, and this method has lead to new ABC-triples in the "unbeaten" list.

2.3 Transfer method

Another method creating infinitely many ABC-triples is to create new ABC-triples from old ones. A simple way is the following: Suppose we have an ABC-triple $(A,\ B,\ C)$ with quality equal to $1+q>1$ and suppose $B>A$. Since $A+B=C$, one can multiply C with $(B-A)$ getting

$$C(B-A)=B^2-A^2$$

Then we have a new ABC-triple $(A^2, C(B-A), B^2)$ with quality

$$q(A^2, C(B-A), B^2)=\frac{\log B^2}{\log r(A^2\cdot C(B-A)\cdot B^2)}$$

Here we already have the factors A, B and C and the only new factor is $(B-A)$. Hence the quality is

$$\begin{aligned}
\frac{\log B^2}{\log r(ABC(B-A))} &> \frac{\log\left(C(B-A)\right)}{\log r(ABC)\cdot\log r(B-A)} \\
&> \frac{\log C+\log(B-A)}{\log r(ABC)+\log(B-A)} \\
&> \frac{\log C+\log C}{\log r(ABC)+\log C} \\
&= \left(\frac{\log r(ABC)}{2\log C}+\frac{\log C}{2\log C}\right)^{-1} \\
&= \left(\frac{1}{2(1+q)}+\frac{1}{2}\right)^{-1} \\
&= 1+\frac{q}{2+q}
\end{aligned}$$

Also the largest number B^2 is larger than $\frac{1}{4}\,C^2$, so the triple nearly doubles in size. So one can ask how slow the quality decreases each step and can try to find a function $f(C)$ such that

$$q(A_n, B_n, C_n)\geqslant 1+f(C_n)$$

where for all $i\geqslant 2$: $B_i>A_i$, $C_i=B_{i-1}^2$,

$$B_i=\max\left(A_{i-1}^2, C_{i-1}(B_{i-1}-A_{i-1})\right)$$

and $A_i=C_i-B_i$. Here we have a not so good function: The larger n is, the smaller A_n is relative to B_n and C_n since both B_n^2 and A_n^2 are involved, and then we have

$$\frac{f(C_{n+1})}{f(C_n)}>\frac{\left(\frac{q}{2+q}\right)}{q}=\frac{1}{2+q}\to\frac{1}{2}$$

as $q\to 0$. We also have

$$\frac{\log C_{n+1}}{\log C_n}\geqslant\frac{2\log C_n-\log 4}{\log C_n}\to 2$$

as $n\to\infty$. Hence $f(C_n)\cdot\log C_n$ is approximately constant, and we have a function of the shape $f(C)=\frac{\text{const.}}{\log C}$, a function worse than other discovered functions.

But there are many other polynomial *transfers* of such a triple. The transfer above takes the polynomial equation $A^2+(A+B)(B-A)=B^2$. When we only look at the polynomial itself and compare the degree of the radical with the degree of the largest polynomial, we see that the radical is equal to $A\cdot B\cdot(A+B)\cdot(B-A)$, of degree 4, while the largest polynomial (hence all the three polynomials since they are homogenious) has degree 2. So this is a "sharp" triple in the sense of the results below. To prove these results, define $\deg(f)$ as being the degree of a polynomial f and define $r(f)$ as being the radical of f. I use the following facts for f, g, h coprime polynomials with $f+g=h$:

Fact 1. $\deg(\gcd(f,f'))=\deg(f)-\deg(\mathrm{rad}(f))$

Fact 2. $f'g-fg'=f'h-fh'\neq 0$ if f, g and h are not all three constant.

Fact 2 is true because $f'+g'=h'$ and therefore

$$f'g-fg'=f'(h-f)-f(h'-f')=f'h-fh'$$

It is nonzero because otherwise $f'g=fg'\neq 0$, and since f and g are relative prime, g must divide g'. This is unless f and g are both constants, but then h is constant too. Note that if $\frac{f}{g}$ is constant, but f and g are not constant, then f and g are not coprime.

Theorem 2.8. (Mason-Stothers) *Let $f,g,h\in\mathbb{C}[X]$. Then*

$$\max\{\deg(f),\deg(g),\deg(h)\}\leqslant\deg(r(fgh))-1$$

Proof. We observe that $\gcd(f,f')$ and $\gcd(g,g')$ divide the left hand side of fact 2, and that $\gcd(h,h')$ divides the right hand side of fact 2. Since both sides are equal and $\gcd(f,f')$, $\gcd(g,g')$ and $\gcd(h,h')$ are coprime (they divide f, g resp. h), we conclude that

$$\frac{f'g-fg'}{(\gcd(f,f'))(\gcd(g,g'))(\gcd(h,h'))}\in\mathbb{C}[X]$$

So

$$\deg(\gcd(f,f'))+\deg(\gcd(g,g'))+\deg(\gcd(h,h'))\leqslant\deg(f'g-fg')=\deg(f)+\deg(g)-1$$

and by fact 1 on f, g and h, applied to the equation above, we get

$$\deg(h)\leqslant\deg(r(f))+\deg(r(g))+\deg(r(h))-1=\deg(r(fgh))-1$$

since f, g and h are coprime. Applying fact 2 to g and f yields $g'h-gh'\neq 0$ and we can use the above argument for f and g to get the same inequality for $\deg(f)$ and $\deg(g)$. □

In fact Stothers discovered the theorem in 1981, Mason rediscovered it in 1983, and the version above of the proof is given by Noah in 1998, as stated in F).

Corollary 2.9. *Let f, g and h be coprime homogenious polynomials of degree d in variables x and y such that $f+g=h$. Then $r(fgh)$ has degree at least $d+2$.*

Proof. $r(fgh)$ is a product of linear factors over $\mathbb{C}$. By change of variables one can set one of these linear factors to be y, and make the equation inhomogenious over one variable by setting $y=1$. This lowers the degree of the radical by 1 while keeping

$$\max\{\deg(f),\deg(g),\deg(h)\}=d$$

(only one of them has a factor y since they are coprime.) By the Mason-Stothers theorem

$$d=\max\{\deg(f),\deg(g),\deg(h)\}\leqslant\deg(r(fgh))-1$$

hence

$$\deg(r(fgh))\geqslant d+1$$

In the original equation, the factor y is added in the radical, making the degree of the radical at least $d+2$. □

A special family of polynomial triples is of the shape

$$(A+B)^n = A^k\left(\sum_{i=0}^{n-k}\binom{n}{i}A^{n-k-i}B^i\right)+B^{n-k+1}\left(\sum_{i=0}^{k-1}\binom{n}{i}A^iB^{k-1-i}\right), n\geqslant 2, i\leqslant k<n$$

where we have the degree 1 factors A, B and $A+B$, and split up the *binomium of Newton* into a part of degree $n-k$ and a part of degree $k-1$. The radical of their product is of degree

$$1+1+1+(n-k)+(k-1)=n+2$$

so it is a sharp triple. Starting with an initial ABC-triple $(A,\ B,\ A+B)$ of integers, one constructs another ABC-triple

$$\left(A^k\left(\sum_{i=0}^{n-k}\binom{n}{i}A^{n-k-i}B^i\right), B^{n-k-1}\left(\sum_{i=0}^{k-1}\binom{n}{i}A^iB^{k-1-i}\right), (A+B)^n\right)$$

whose radical is at most

$$r(A\cdot B\cdot(A+B))\cdot\left(\sum_{i=0}^{n-k}\binom{n}{i}A^{n-k-i}B^i\right)\cdot\left(\sum_{i=0}^{k-1}\binom{n}{i}A^iB^{k-1-i}\right)$$

where $r(A\cdot B\cdot(A+B))<A+B$ and the product of the other two factors is of degree $n-1$ in terms of A and B, but it can be larger than $(A+B)^{n-1}$.

For example, one starts with $1+8=9$ and takes $n=3$ and $k=2$, hence looks at

$$(1+8)^3=1^2(1\cdot 1^1\cdot 8^0+3\cdot 1^0\cdot 8^1)+8^2(1\cdot 1^0\cdot 8^1+3\cdot 1^1\cdot 8^0)$$

Their radical is equal to $r(1\cdot 8\cdot 9)\cdot r(25)\cdot r(11)$, but here

$$25\cdot 11=275>(8+1)^{3-1}=81$$

Fortunately, $r(25)=5$, so the radical of $(1\cdot 8\cdot 9)\cdot 25\cdot 11$ is equal to $6\cdot 5\cdot 11=330<729$, so we have created a new ABC-triple

$$(25,704,729)=(5^2,2^6\cdot 11,3^6)$$

this way. But such 'luck' of finding a factor what is not squarefree easily can be forced to happen. If we keep $k=2$, one gets one of the factors being equal to $B^{n-1}(B+nA)$ for any n, so one can try to find an n such that $\frac{B+nA}{r(B+nA)}$ is as large as possible, relative to n.

But even when such a trick succeeds, we get a computation like at the beginning of this section: The size of the triple is increased by a factor n, while the quality minus 1 is decreased by a factor n. So we get the same: A function of the shape $f(C)=1+\frac{\text{const.}}{\log C}$.

Some research is fixed to get the odds for a lucky square factor dividing one of the polynomial factors as high as possible. One can try this by getting as many different factors as possible. So one can try to find sharp polynomial factors which completely can be factored into *linear* polynomials, polynomials of degree 1. Examples of these polynomial transfers already are given above, with a degree 4 and a degree 6 example added:

$$\begin{aligned}
A^2+(B-A)(A+B) &= B^2\\
A^2(A+3B)+B^2(3A+B) &= (A+B)^3\\
A^3(A+2B)+(A+B)^3(B-A) &= B^3(2A+B)\\
27(A+B)^5(B-A)+A^3(3A+5B)^2(3A+2B) &= B^3(5A+3B)^2(2A+3B)
\end{aligned}$$

These examples generates a whole family of such polynomial triples since we can take any multiple of A and any multiple of B. There also are some essential different triples, but there are no such triples known of degree other than 2, 3, 4 or 6. These triples are constructed by Mentien, de Smit and Taelman.

Theoretically using such transfers one doesn't get better functions than $f(C) = 1 + \frac{\text{const.}}{\log C}$, but in practice, when finding squares dividing one of these factors, or when starting with a very good ABC-triple, one can find new good ABC-triples.

Such transfer methods also can be useful when one finds some interesting approximate relation between two numbers of A, B and $C = A + B$. For example, when one finds an ABC-triple (A, B, C) satisfying $B - A = 1$, the ABC-triple $(A^2, (B-A)(B+A), B^2)$ has radical $r(A \cdot B \cdot (A+B)) \cdot r(B-A)$ where $r(B-A) = 1$. So the quality becomes

$$\frac{\log(B^2)}{\log r(A \cdot B \cdot (A+B))} \approx 2q(A, B, A+B)$$

Yes, this way the quality nearly *doubles*, so triples (A, B, C) with $B - A$ very small are expected to be very rare (else the ABC-conjecture seems to be false.) Something similar can be done when $B \approx 2A$. Then $C \approx 3A$, and we get by applying the degree 3 transfer to C and $-A$:

$$C^2(C-3A) + A^2(3C-A) = (C-A)^3 = B^3$$

with factors A, B, C, the very small factor $C - 3A$ and the other factor $3C - A$. Suppose we have $C - 3A = 1$. Then

$$q(C^2(C-3A), A^2(3C-A), B^3) = \frac{3\log B}{\log r(A \cdot B \cdot C \cdot (3C-A))} = \frac{\log(\text{degree } 3)}{\log((\text{degree } 1) \cdot (\text{degree } 1))} \approx \frac{3}{2}$$

Such tricks can be done with many approximate relations, creating high quality triples. However, much of the new discovered ABC-triples are of the shape $B \approx C$ and A very small, in particular when using elementary number theory or the LLL method.

Another way to increase the expected quality is to find a prime factor which will occur often in the factorisation. For example, when we have an ABC-triple (A, B, C) with C an odd number, then $A \cdot B$ is even and we can use the transfer

$$((A-B)^2, 4AB, (A+B)^2)$$

Since $A + B$ is odd, $4AB$ and $(A+B)^2$ are coprime and the necessary factor 2 is involved in the term $4AB$. So compared to the transfer $(A^2, (A+B)(B-A), B^2)$ the radical is the same, but the advantage is that the largest number now is $(A+B)^2$ rather than B^2. Such transfers uses scalar multiplication of a polynomial (like AB) with a scalar number (like 4). But most transfers uses few scalars.

As seen until now, most relatively good ABC-triples (A, B, C) have a very small number A and two approximately equal numbers B and C. This can motivate one to transfer using polynomials of only *one* variable. The small number A will be seen as a *constant number*, and the large number B will be the variable. For example, if $A = 1$, one can transfer the initial ABC-triple $(1, B, B+1)$ into the new triple $(1, B^3, B^3+1)$. Here

$$\begin{aligned} B^3+1 &= (B+1) \cdot (B^2-B+1) \\ r(1 \cdot B^3 \cdot (B^3+1)) &= r(1 \cdot B \cdot (B+1)) \cdot r(B^2-B+1) < (B+1) r(B^2-B+1) < B^3+1 \end{aligned}$$

So $(1, B^3, B^3+1)$ is a new ABC-triple whose quality minus 1 approximately decreases by a factor 3 while the size of the largest number increases by a factor 3. So again such transfers create infinite sequences of ABC-triples (A_n, B_n, C_n) with

$$q(A_n, B_n, C_n) \geqslant 1 + \frac{\text{const.}}{\log C_n}$$

Something similar is true when $A > 1$. Then just take the triple

$$(A^3, B^3, (B+A) \cdot (B^2 - A \cdot B + A^2))$$

with the same effects.

When looking at the radical of the polynomial rather than the number one finds that the radical of the product is

$$r(1 \cdot B^3 \cdot (B+1) \cdot (B^2-B+1)) = B \cdot (B+1) \cdot (B^2-B+1)$$

of degree 4. This is one larger than the degree of the largest polynomial, and also this cannot be improved (by corollary 2.9) unless all the three polynomials are constant.

So also here it doesn't give better ABC-triples in general than the methods creating new ABC-triples. So the transfer method can be used best when starting with an ABC-triple with a very high merit. Then the new ABC-triple discovered by a transfer also may have a relatively high merit, and sometimes it can appear on the "unbeaten" list of A).

2.4 Some other methods

There are many other methods trying to find new good or unbeaten ABC-triples. In this subsection I give an overview of some of these methods and some interesting results for them.

2.4.1 Continued Fractions

One can try to approximate an irrational number by rational numbers in the following way: Let α be an (irrational) number. Then find the unique integer n_0 such that $\alpha - n_0 =: \alpha_1 \in [0, 1)$. Then $\frac{1}{\alpha_1}$ is another number above 1 and we can repeat the process, finding the unique number n_1 such that $\frac{1}{\alpha_1} - n_1 =: \alpha_2 \in [0, 1)$ etc. This creates a sequence $(n_0, n_1, n_2, ...)$ such that

$$\alpha = n_0 + \cfrac{1}{n_1 + \cfrac{1}{n_2 + \cfrac{1}{\ddots}}}$$

This chain of unit fractions is infinite if and only if α is irrational.

At any index i we can stop repeating the process and take

$$(n_0, n_1, ..., n_{i-1}) := n_0 + \cfrac{1}{n_1 + \cfrac{1}{\ddots + \cfrac{1}{n_{i-1}}}}$$

as rational approximation of the initial number α. Denote this approximation $\frac{x_i}{y_i}$ with x_i and y_i coprime integers with $y_i > 0$. This is called the *continued fraction algorithm* to find coprime integers x_i, y_i with $y_i > 0$ such that $|\alpha - \frac{x_i}{y_i}| \leqslant \frac{1}{n_i y_i^2} \leqslant \frac{1}{y_i^2}$. For the purpose of finding nice ABC-triples using continued fractions this is most interesting when we have discovered a large value for n_i and choose to stop at i.

For example, one can start with

$$\alpha = \sqrt[5]{109} = 2.555555397...$$

so $n_0 = 2$. Then $\frac{1}{\alpha_1} = 1.800000515...$ making $n_1 = 1$. This gives $\frac{1}{\alpha_2} = 1.249999196...$ so $n_2 = 1$. This makes $\frac{1}{\alpha_3} = 4.000012864...$ with $n_3 = 4$. Now the large number appears:

$$\frac{1}{\alpha_4} = 77733.379227053...$$

giving $n_4 = 77733$. This extremely large number compared to the others makes us stop by n_4 giving as approximation

$$\alpha \approx 2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{4}}} = \frac{23}{9}.$$

So $109 = \alpha^5 \approx \left(\frac{23}{9}\right)^5$, or in integer terms, $9^5 \cdot 109 \approx 23^5$. And indeed, their difference is equal to 2. So we have an ABC-triple $(2, 3^{10} \cdot 109, 23^5)$ whose quality

$$q(2, 3^{10} \cdot 109, 23^5) = \frac{\log(23^5)}{\log(2 \cdot 3 \cdot 109 \cdot 23)} = 1.629911694...$$

is the highest quality discovered until now, thanks to Reyssal.

However, this was one "lucky shot" since we early got the large number $n_4 = 77733$, but in general the result will be much worse. To explain why, I start with an arbitrary number $\sqrt[p]{q}$. If one finds coprime integers x, y such that $|\sqrt[p]{q} - \frac{x}{y}| \leqslant \frac{1}{ny^2}$ for a certain number, one is interested in the consequence for the quality of the triple (BIG, qy^p, x^p), where "BIG" is a number, relatively small compared to the other two numbers, which we don't have control over. I call this number "BIG" since this number is in general too large to determine its radical exactly and will be much larger than qxy. For computing the size of BIG, one uses the fact that if $|1-\alpha| \leqslant \varepsilon$, then $|1^p - \alpha^p|$ is approximately as small as, or smaller than $p\varepsilon$. Here $\alpha = \frac{y\sqrt[p]{q}}{x}$, hence $|\frac{qy^p}{x^p} - 1|$ is as most as large as approximately $\frac{p}{nxy}$. So at worst BIG $\approx \frac{x^{p-1}}{ny}$. This makes the quality of (BIG, qy^p, x^p) to be at least approximately

$$\frac{\log \max\{x^p, qy^p\}}{\log\left(\frac{x^{p-1}}{ny} \cdot qxy\right)} \geqslant \frac{\log x^p}{\log(\frac{qx^p}{n})}.$$

Hence the triple isn't guaranteed to be an ABC-triple unless $n > q$. Often we have no expectation that an $n = n_i \geqslant 3$ can be discovered from $\sqrt[p]{q}$, so the value $n_4 = 77733$ from $\alpha = \sqrt[5]{109}$ really is a lucky shot. Note that for any

$$\alpha \neq \frac{1+\sqrt{5}}{2} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\ddots}}}$$

there is an index i such that $n_i \geqslant 2$.

One may ask whether we cannot get better than $|\alpha - \frac{x}{y}| \leqslant \frac{1}{ny^2}$ and get something like $|\alpha - \frac{x}{y}| \leqslant \frac{\text{const.}}{y^{2+\delta}}$ for some $\delta > 0$. The answer is known for algebraic numbers α, in particular for α of the shape $\alpha = \sqrt[p]{q}$.

Theorem 2.10. (Roth) *Let α be an algebraic number. Then the inequality $|\alpha - \frac{x}{y}| \leqslant \frac{C}{|y|^{2+\delta}}$ has only finitely many solutions $(x, y) \in \mathbb{Z}^2, \gcd(x, y) = 1$ for any $C, \delta > 0$.*

The proof of this theorem falls outside this thesis. But Granville and Langevin discovered that the ABC-conjecture implies Roth's theorem. If Roth's theorem is false for some $\sqrt[p]{q}$, then one finds infinitely many ABC-triples whose quality goes to $\frac{\log x^p}{\log x^{p-\delta}} = 1 + \frac{\delta}{p-\delta}$, so that would disprove the ABC-conjecture. A consequence is that for better results one must use *transcedental* numbers. So one can try $\alpha = \frac{\log p}{\log q}$. Then if $\frac{x}{y}$ is a good approximation, one can try (BIG, p^y, q^x) as a triple. However, this already can be done by trying LLL on p and q with the same results, since LLL on 2-dimensional lattices can give an optimal solution in only a little time.

2.4.2 2-Dimensional lattices

There also is another way to find ABC-triples out of 2-dimensional lattices, first published by Tim Dokchitser G). This goes as follows: Start with three pairwise coprime integers a, b and c such that each of these numbers are close to each other and have small radicals. Then one can create a sublattice $L \subset \mathbb{Z}^3$ satisfying

$$L = \{(x, y, z) \in \mathbb{Z}^3 : ax + by + cz = 0\}.$$

This is a two-dimensional lattice and one can find small nonzero vectors $(x, y, z) \in L$. Then consider the candidate ABC-triple (A, B, C) where $C = \max\{|ax|, |by|, |cz|\}$ and A, B the other two numbers among them.

A method to find short vectors is to check all numbers

$$\{ax + by + cz : 0 \leqslant x, y, z \leqslant N\}$$

and check whether there are different triples (x_1, y_1, z_1) and (x_2, y_2, z_2) such that

$$ax_1 + by_1 + cz_1 = ax_2 + by_2 + cz_2$$

and take as vector $(x_1 - x_2, y_1 - y_2, z_1 - z_2)$. This is time-consuming since we need

$$N \geqslant 1 + \sqrt{3 \cdot \max(a,b,c)}$$

and get a list of at least $\left(1 + \sqrt{3 \cdot \max(a,b,c)}\right)^3$ numbers, to guarantee that we find two times the same value for $ax + by + cz$ and hence a vector of this lattice. If we take $N = \sqrt{3 \cdot \max(a,b,c)}^3$, then the list contains $3\sqrt{3} \cdot (\max(a,b,c))^{\frac{3}{2}}$ numbers, while these numbers run through $0, ..., 3 \cdot \sqrt{3 \cdot \max(a,b,c)} \cdot \max(a,b,c)$, so theoretically it is possible that all these numbers are different. Since the size of the list grows faster than the largest possible number of that list, the given lower bound for N is required. However, this method does search for a large number of ABC-triples and can find all good ABC-triples below a given value in not too much time. Now all good ABC-triples (A, B, C) with $C \leqslant 10^{20}$ are known.

Another method to find small vectors (x, y, z) is the earlier described LLL-algorithm. To be able to apply LLL to this problem, we first need to know more properties of the lattice L, in particular a basis and the determinant.

A basis can be constructed as follows: Start with a linear subspace $\mathbb{T}$ of the linear subspace of $\mathbb{R}^3$ spanned by L, for example with the subspace $z = 0$, and find point of $\mathbb{T} \cap L$. For example $(b, -a, 0) \in \mathbb{T} \cap L$. This point generates the sublattice $\mathbb{T} \cap L$ since a and b are coprime. Then find integers m, n such that $(m, n, 1) \in L$ is a lattice point of minimal distance from $\mathbb{T}$. Such a point $(m, n, 1)$ exists since x and y are coprime, hence there exists integers u and v such that $m + n = ua + vb = -1$. Then $(uc) \cdot a + (vc) \cdot b + 1 \cdot c = 0$, hence $(uc, vc, 1) \in L$.

The next step is to compute the determinant of L, what can be done using what is described in section 2.2. So the square of the determinant is equal to

$$\begin{aligned}
& \langle (b,-a,0),(b,-a,0)\rangle \cdot \langle (uc,vc,1),(uc,vc,1)\rangle - \langle (b,-a,0),(uc,vc,1)\rangle^2 \\
= \;& (a^2+b^2)(u^2c^2+v^2c^2+1) - (ubc-vac)^2 \\
= \;& a^2+b^2+u^2a^2c^2+u^2b^2c^2+v^2a^2c^2+v^2b^2c^2-u^2b^2c^2+2uvabc^2-v^2a^2c^2 \\
= \;& a^2+b^2+u^2a^2c^2+2uvabc^2+v^2b^2c^2 \\
= \;& a^2+b^2+(uac+vbc)^2 \\
= \;& a^2+b^2+(ua+vb)c^2 \\
= \;& a^2+b^2+c^2
\end{aligned}$$

So by theorem 2.5, L contains a nonzero point (x, y, z) such that

$$x^2 + y^2 + z^2 \leqslant \frac{4}{\pi} \cdot \left(\left(\frac{2}{2}\right)!\right)^{\frac{2}{2}} \cdot \sqrt{a^2+b^2+c^2}^{\frac{2}{2}} = \frac{4}{\pi}\sqrt{a^2+b^2+c^2}.$$

When a, b and c are approximate equal, the theoretical result from LLL and Minkowski is worse than the theoretical result from searching all 2-dimensional lattice points in the box, since that way guarantees a vector (x, y, z) such that

$$x^2 + y^2 + z^2 \leqslant 3 \cdot \left(1 + \sqrt{3 \cdot \max(a,b,c)}\right)^2$$

because then $\sqrt{a^2+b^2+c^2} \approx \sqrt{3} \cdot \max(a, b, c)$. But LLL will be applied on a 2-dimensional lattice, so in this case also one can find the shortest vector using LLL.

2.4.3 *p*-adic LLL

This method goes similar as the LLL-method from section 2.2, but now we use different absolute values. Let p be a prime number. Then one can define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by $|x|_p = p^{-n}$ where $x = p^n \cdot \frac{a}{b}$ where a, b integers not divisible by p. If we add $|0|_p = 0$ this becomes an *absolute value* satisfying the three axioms:

1. $|x|_p \geqslant 0$. Equality holds if and only if $x = 0$.
2. $|x \cdot y|_p = |x|_p \cdot |y|_p$ for any $x, y \in \mathbb{Q}$.

3. $|x+y|_p \leqslant |x|_p + |y|_p$ for any $x, y \in \mathbb{Q}$ (triangular law)

For p-adic absolute values, the triangular law can be improved by the *ultrametric property*

$$|x+y|_p \leqslant \max\{|x|_p, |y|_p\}$$

for any $x, y \in \mathbb{Q}$. The ultrametric property makes this absolute value *non-Archimedian* while the standard absolute value $|\cdot|_\infty$ not satisfying the ultrametic property is called *Archimedian*. Note that for any nonzero number $x \in \mathbb{Q}$ we have

$$|x|_\infty \cdot \prod_{p\,\text{prime}} |x|_p = 1$$

since for $x = (-1)^{e_0} p_1^{e_1} \cdots p_n^{e_n}$, $|x|_{p_i} = p_i^{-e_i}$ and $|x|_q = 1$ for any prime number $q \notin \{p_1, ..., p_n\}$.

Also with p-adic LLL one tries to find $B = p_1^{e_1} \cdots p_m^{e_m}$ and $C = p_{m+1}^{e_{m+1}} \cdots p_n^{e_n}$ such that for a given prime number p one has $|C-B|_p = p^{-N}$ with N a sufficiently large number. In other words, try to find two numbers B and C such that their difference is divisible by a large factor of p. Then $r((C-B)\cdot B \cdot C)$ is small because of the factor p occuring often in the number $C-B$ and $r(B)$ and $r(C)$ are constants.

2.4.4 Sort method from Jarek Wrobleski

The most succesful known method is from Jarek Wrobleski, who discovered 81 of the first 100 ABC-triples from the unbeaten list from now. He hasn't published much of his tool, so we can only guess what he is doing, but we guess he finds them on the following way:

Start with some numbers $(x_i)_{i\in I}$, all rational and nearly equal to 1, and with small radical. From this list of numbers one can try to create a new list of rational numbers $(y_j)_{j\in J}$ by multiplying some numbers from list I, to make the numbers y_j much closer to 1 than the numbers x_i are. This way he creates exactly the same kind of ABC-triple as the LLL-method does, but it probably works more efficiently. However, for the large numbers the merit shrinks to values around 13, suggesting there are still better ABC-triples waiting to be discovered.

Chapter 3
A short introduction to Elliptic Curves

My own method is another form of lattice theory, but of a different kind using *Elliptic Curves*. Before I can explain how it exactly works, I will introduce Elliptic Curves first. Since a complete introduction can be very large and is taught during any course of Elliptic Curves, I only give the important definitions and some important results.

At first I need to say what an Elliptic Curve is. An *elliptic curve* over a field k is a smooth 1-dimensional projective algebraic variety over k with *genus* 1, with a given rational point, and what is irreducible as a variety. In this introduction I will explain what this means. When $k = \mathbb{C}$, topologically it looks like a real *torus*, or the product set of two real circles, on which a point is specified. This sounds 2-dimensional, but the torus is a one-dimensional object when one views it as a variety over $\mathbb{C}$, the field of complex numbers. Since it is one-dimensional, it actually is a *curve* rather than a surface. The presence of the rational point means that there must exist at least one given point with coordinats in the field the curve is defined in. The reason such curves are *elliptic* is that they originally are used to compute arc lengths of ellipses. This is done by integrating functions of the shape $\frac{\mathrm{dt}}{\sqrt{(a-t^2)(b-t^2)}}$. These functions have 4 singularities, namely $\pm\sqrt{a}$ and $\pm\sqrt{b}$, but integrating over a path containing two of these singularities gives 0 again. Furthermore, taking the square root is two-valued. So the original curve $y^2 = (a - x^2)(b - x^2)$ over $\mathbb{C}$ looks like two complex planes with a point ∞ added, connected to each other by two *wormholes*. Since the comples plane with ∞ looks like a sphere, the whole construction is topologically equal with a sphere with one handle, or a torus. That makes it a *Riemann Surface*, a complex curve without singularities, and its *genus* is equal to the number of handles it has. Since topologically a torus looks like a sphere with one handle, the genus of such a curve is equal to 1. But such curves does contain points at infinity, so is not sufficient to consider the affine space; we need to consider an elliptic curve as a subset of the *projective space*. However, the part at infinity mostly is restricted to one point, so often we look at the affine part.

Another way to describe a torus is as $\mathbb{C}$ modulo a 2-dimensional *lattice* L. In this way, the torus becomes a quotient variety and you can still *add* two elements from $\mathbb{C}/L$ - it also is a quotient *group*. The given rational point there becomes the *zero element* of that curve.

On an elliptic curve E, seen as a Riemann surface, one can do complex analysis. On a Riemann surface, there is a *function field* $\mathbb{C}(E)$ defined as the field of $\mathbb{C}$-valued functions which are regular on E with the exception of at most finitely many points, on which such a function has a *pole* of finite order. There also are *divisors* on E: Formal sums $\sum_{P\in E} n_P \cdot P$ for which n_P is 0 for all but finitely many points P. For each $f \in \mathbb{C}(E)$ and each P we can define the *order* $\mathrm{ord}_f(P)$ of f at P. If f is regular and nonzero at P the order is 0. If $f(P) = 0$, then the order of f is the order of the zero at P. If f is singular at P, then the order of f at P is minus the order of the *pole* of f at P, hence minus the order of the zero of $\frac{1}{f}$ at P. Then for each function $f \in \mathbb{C}(E)$ there is an associated divisor

$$D(f) := \sum_{P\in E} \mathrm{ord}_f(P) \cdot P.$$

Note that for all $f \in \mathbb{C}(E)$, we have $\sum_{P\in E} \mathrm{ord}_f(P) = 0$. From algebraic geometry there is a theorem, which tells that the set of functions on $\mathbb{C}(E)$ on which the singularities have given bounds is a *vector space*, and which tells the dimension of that vector space, depending on the genus of E. But I already know the genus is 1 since E is an Elliptic Curve.

Theorem 3.1. (Riemann-Roch for elliptic curves) *Let $D = \sum_{P\in E} n_P \cdot P$ be a divisor and $n = \sum_{P\in E} n_P$. Then the dimension of the vector space*

$$L(D) = \{0\} \cup \{ f \in \mathbb{C}(E) : \forall P \in E : \operatorname{ord}_f(P) + n_P \geqslant 0\}$$

is equal to

- *0 if $n < 0$,*
- *0 or 1 if $n = 0$,*
- *n if $n > 0$.*

The first part of the theorem is clear. The second and third part follows from the general Riemann-Roch theorem and the fact that the genus of any elliptic curve is equal to 1. The proof for general Riemann-Roch can be read in H). The constant functions clearly are defined over $\mathbb{C}/L$. Then Riemann-Roch says that there are no functions with just one simple zero and one simple pole, but there are functions with a double pole in some point and which is regular everywhere else.

One of these functions is the *Weierstrass-$\wp$-function*

$$\wp = \wp_L : z + L \longmapsto \frac{1}{z^2} + \sum_{w\in L-\{0\}} \left(\frac{1}{(w-z)^2} - \frac{1}{w^2} \right).$$

This function is regular except on the point $z = 0$. Elsewhere

$$\frac{1}{(w-z)^2} - \frac{1}{w^2} = \frac{z(2w+z)}{w^2(w-z)^2}$$

is of degree -3 in w. So this series converges over $x \in L - \{0\}$ for any $z \in \mathbb{C}$, but the term $\frac{1}{z^2}$ makes 0 a pole of order 2. The Weierstrass-$\wp$-function also has a derivative

$$\wp'(z) = -2 \sum_{w\in L} \frac{1}{(z-w)^3}$$

which is regular everywhere except an order 3 pole at $z = 0$. The function with a degree 4 pole is $\wp(z)^2$, an order 5 pole is provided by $\wp(z) \cdot \wp'(z)$, but for the order 6 pole there are two possibilities, namely $\wp(z)^3$ and $\wp'(z)^2$. Since by Riemann-Roch the vector space of functions with a pole at order at most 6 at $z = 0$ and regular everywhere has dimension 6, and the dimension is reduced to 5 when we only allow order $\leqslant 5$ poles, there must be a *linear relation* between $\wp(z)^3$, $\wp'(z)^2$, 1, $\wp(z)$, $\wp'(z)$, $\wp(z)^2$, and $\wp(z)\wp'(z)$. And indeed, we have

$$\wp'(z)^2 = 4\wp(z)^3 + g_2\wp(z) + g_3$$

where g_2 and g_3 are constants depending only on the lattice L. If we multiply the equation with a factor 16 and put $y = 4\wp'(z)$ and $x = 4\wp(z)$, we get the elliptic curve in *Weierstrass form*

$$y^2 = x^3 + ax + b$$

with a and b some constant numbers. Also it is always possible to go back from a smooth elliptic curve in Weierstrass form into some lattice, where *smooth* means that the discriminant $g_2^3 - 27g_3^2$ is nonzero. The proof of this result is given in I), page 25.

Theorem 3.2. (Uniformization Theorem) *Given $g_2, g_3 \in \mathbb{C}$ such that $g_2^3 \neq 27g_3^2$, there exists a lattice $L \subset \mathbb{C}$ of rank 2 such that $g_2(L) = g_2$ and $g_3(L) = g_3$. Here $g_2(L) = 60 \sum_{z\in L, z\neq 0} z^{-4}$ and $g_3(L) = 140 \sum_{z\in L, z\neq 0} z^{-6}$.*

In this thesis, I only use fields with characteristic 0 - either $\mathbb{Q}$ or $\mathbb{R}$ and sometimes $\mathbb{C}$. That means that any elliptic curve used in this thesis can be written in Weierstrass form. In fact the form $y^2 = x^3 + a \cdot x + b$ is called the *short Weierstrass form* and there also exists a (long) Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

In characteristic $\neq 2$ we can get rid of a_1 and a_3 by taking $y' = y + \frac{a_1x + a_3}{2}$. Then in characteristic $\neq 3$ one can get rid of a_2 by taking $x' = x + \frac{a_2}{3}$. When looking over $\mathbb{R}$, the curve topologically either looks like one circle, or it looks like two circles.

It also is possible for the family of elliptic curves of the form $x^3 + y^3 = dz^3$ to transform it into Weierstrass form. When taking $x = u + v$ and $y = u - v$ this equation becomes

$$(u+v)^3 + (u-v)^3 = 2u^3 + 6uv^2 = dz^3$$

To get this in short Weierstrass form, one sets the curve in affine coordinats by taking $u = 1$ and gets

$$6v^2 = dz^3 - 2 \Leftrightarrow (6^2 dv)^2 = (6dz)^3 - 432d^2.$$

So taking

$$X = \frac{12dz}{x+y}, Y = \frac{36d(x-y)}{x+y}$$

one gets $Y^2 = X^3 - 432d^2$. Conversely one has

$$x = \frac{36d + Y}{6X}, y = \frac{36d - Y}{6X}$$

to go back to $x^3 + y^3 = d$.

3.1 The group law

Let L again be a lattice in $\mathbb{C}$, and $E(\mathbb{C})$ be the elliptic curve associated with L. Then the map

$$\mathbb{C}/L \to E(\mathbb{C}), z + L \mapsto (\wp(z) : \wp'(z) : 1)$$

is an isomorphism of Riemann surfaces. One also wants this isomorphism to be a *group isomorphism* and then needs to define a *group law* directly described in terms of E: $y^2 = x^3 + ax + b$. This is possible and one can do it by looking again at divisors. Suppose we have a line in $\mathbb{A}^2(\mathbb{C})$, the affine complex plane. Then that line is given by a linear equation

$$lx + my + n = 0$$

Since $x = \wp(z)$ and $y = \wp'(z)$, we have a function

$$l\wp(z) + m\wp'(z) + n \in \mathbb{C}(E)$$

This function is regular everywhere on E with the exception of a pole of order 3 in $z = 0$. So the divisor of such a function is of the form $1 \cdot P + 1 \cdot Q + 1 \cdot R - 3 \cdot 0_E$, where P, Q, R are not necessary distinct points on E where the function $lx + my + n$ has a zero, and where 0_E is defined to be the image of $0 + L$ under the isomorphism described above. This point 0_E turns out to be the *zero point* under the group law on E.

Lemma 3.3. *Let f be a meromorphic function on $\mathbb{C}/L$. Then*

$$\sum_{z \in \mathbb{C}/L} z \cdot \mathrm{ord}_f(z) = 0 \in \mathbb{C}/L$$

Proof. (sketch) This expression is equal to $\int_{\partial(F)} z\frac{f'(z)}{f(z)}\mathrm{d}z$, where F is a fundamental domain of L such that its boundary $\partial(F)$ does not contain zeroes or poles of $f(z)$. When computing the integral over this path, one finds that

$$\int_{\partial(F)} z\frac{f'(z)}{f(z)}\mathrm{d}z \in L$$

hence is equal to $0 \in \mathbb{C}/L$. The details of this computation is given in any course of Elliptic Curves, for example on I), pages 13-14. □

As a consequence, if the points P, Q and R are collinear, there is a function $f \in \mathbb{C}(E)$ with associated divisor $D(f) = P + Q + R - 3 \cdot 0_E$ and we can describe the group law as

$$P + Q + R = 0_E.$$

When one takes $Q = 0_E$, the equation becomes $P + 0_E + (-P) = 0_E$, so P and $-P$ are collinear with 0_E. So the group law can be interpreted geometrically as follows: To determine $P + Q$, draw the line through P and Q. Then there is a third point R intersecting this line, and we have $P + Q = -R$. To determine $P + P$, we just take the tangent line at P, that intersects P with multiplicaty 2, or 3 if P is an inflection point.

But if one has an equation $y^2 = x^3 + ax + b$ defining the curve E, the group law also can be computed algebraically: First of all, the point 0_E is the 'point at infinity'

$$(\wp(0)\colon \wp'(0)\colon 1) = (0\colon 1\colon 0)$$

where "infinity" is in the sense of the affine plane $z = 1$. These coordinates $(0\colon 1\colon 0)$ follows from the fact that $\wp(0)$ is of order -2 and $\wp'(0)$ is of order -3. Then let $(x_1, y_1) \neq (x_2, y_2)$ be two distinct points on the curve E. The line through these points is given by

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

if $x_1 \neq x_2$. If so, this is equivalent to

$$y = \frac{y_2 - y_1}{x_2 - x_1}x + (y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1)$$

To find the third intersection point we substitute this equation in the equation of E and get

$$\left(\frac{y_2 - y_1}{x_2 - x_1}x + y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1\right)^2 = x^3 + ax + b$$

To solve this equation we put all terms on one side getting

$$x^3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 x^2 + \ldots = 0$$

where we already have two solutions x_1 and x_2 from our initial points. So it suffices to look at the coefficient of x^2:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

For the y-coordinate we just use the line equation:

$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2\right) + y_1 - \frac{y_2 - y_1}{x_2 - x_1}x_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \frac{y_2 - y_1}{x_2 - x_1}(-2x_1 - x_2) + y_1$$

But that is just the intersection point. To finish the computation, we have to take the third intersection point of the line through (x_3, y_3) and 0_E, and get

$$(x_1, y_1) + (x_2, y_2) = (x_3, -y_3) = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \frac{y_2 - y_1}{x_2 - x_1}(-2x_1 - x_2) + y_1\right)$$

If $x_1 = x_2$, then the line through these points is vertical, so the third intersection point of the line is 0_E. The "line through 0_E and 0_E" is the tangent line at 0_E, so is the line at infinity, hence the "third" intersection point also is 0_E. So $(x_1, y_1) + (x_1, y_2) = 0_E$ if $y_1 \neq y_2$.

We also need to determine $P + P$, hence to compute $(x_1, y_1) + (x_1, y_1)$. The formula above doesn't work, but instead we need the tangent line at (x_1, y_1). Since $y = \pm\sqrt{x^3 + a \cdot x + b}$, the derivative is

$$\pm\frac{3x^2 + a}{2\sqrt{x^3 + a \cdot x + b}} = \frac{3x^2 + a}{2y}$$

so the tangent line is given by

$$y - y_1 = \frac{3x_1^2 + a}{2y_1}(x - x_1)$$

and is vertical if $y_1 = 0$. In that case, $(x_1, y_1) + (x_1, y_1) = 0_E$. If $y_1 \neq 0$, the line equation is equivalent with

$$y = \frac{3x_1^2 + a}{2y_1}x + \left(y_1 - \frac{3x_1^2 + a}{2y_1}x_1\right)$$

and this equation can be filled in the curve equation:

$$x^3+\left(\frac{3x_1^2+a}{2y_1}\right)^2x^2+\ldots=0$$

with a known double root x_1. Hence the third root is

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1$$

and the corresponding y_3 is equal to

$$\frac{3x_1^2+a}{2y_1}\left(\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1\right)+y_1-\frac{3x_1^2+a}{2y_1}x_1.$$

This completes the proof of the *duplication formula*:

$$(x_1,y_1)+(x_1,y_1)=\left(\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1,\left(\frac{3x_1^2+a}{2y_1}\right)^3-3\frac{3x_1^2+a}{2y_1}x_1+y_1\right)$$

So now we have an algebraic expression for the group law. Note that this expression is a rational formula in terms of x_1, y_1, x_2, y_2, so when these coordinates and the coefficients a and b are defined over some other field (with characteristic $\neq 2$), this group law stays intact. In particular, the set $E(\mathbb{Q})$ of points in $E(\mathbb{C})$ of rational coordinates is closed under the group law.

For any elliptic curve E, we can pick any point $P\in E$ and then define a group law such that P is the zero element of the group, that looks like the group law described above. Suppose we take the group law with another zero point $P_0\in E$, then the group law on E with respect to P can be described in terms of the group law w.r.t. P_0. Namely, suppose Q, R and S are collinear, and let S_0 be the third point intersecting E and the line through S and P_0. Then $Q+_{P_0}R=S_0$, where "$+_{P_0}$" means adding w.r.t. P_0. If we add Q and R w.r.t. P, then their sum (w.r.t. P) is the third point S_P intersecting the line through P and S. But we also can write S as being the third intersection point of E and the line through P and S_P, and write $S_0=S_P+_{P_0}P$. Hence

$$S_P=Q+_PR=S_0-_{P_0}P=Q+_{P_0}R-_{P_0}P$$

or in other words, to add Q and R w.r.t. P, you can add them w.r.t. P_0 and then substract P w.r.t. P_0 from it. In the world of $\mathbb{C}/L$ this is much easier: Suppose we choose z as zero element rather than 0. If we compute $x+y$ w.r.t. this zero element, actually we first substract z from both elements, then add them as usual, and finally add z to the outcome. In formula

$$x+_zy=(x-_0z)+_0(y-_0z)+_0z=x+_0y-_0z.$$

This gives rise to another (formal) definition of an Elliptic Curve:

Definition 3.4. *An* Elliptic Curve over a field k *is a smooth nonempty projective curve E=E(k) of genus* 1 *together with a given zero point* $P\in E$*, and what is irreducible as a variety.*

As seen above, there is a natural group law on E such that the given rational point P is the zero element of this group. Then there is a isomorphism (of algebraic curves preserving the group law) between this curve E and a curve E' in Weierstrass form. When looking at this natural group law, one can see that the group is abelian.

Theorem 3.5. (Mordell-Weil) *Let E be an elliptic curve with rational point 0_E and suppose 0_E is defined over $\mathbb{Q}$. Then the group of points in E defined over $\mathbb{Q}$ is finitely generated.*

The proof of this theorem is too complicated to put in this thesis, but can be found in J) part VIII (p 189-240). It uses the *height* of points on $E/\mathbb{Q}$, what will be introduced in the next section. A consequence of the Mordell-Weil theorem is that as a group, $E(\mathbb{Q})\cong\mathbb{T}\oplus\mathbb{Z}^r$ where $\mathbb{T}$ is the (finite) *torsion subgroup* of elements of finite order, and $r\in\mathbb{Z}_{\geqslant 0}$ is the *rank* of $E(\mathbb{Q})$.

If we go back to the curve

$$E\colon x^3+y^3=d\cong C\colon Y^2=X^3-432d^2$$

over $\mathbb{R}$ it looks like one circle. Over $\mathbb{Q}$ it is a subgroup, and if the rank of it is at least 1, the subset is *dense*: In every open subset of the real curve there are rational points. This is easy to see in the world of $\mathbb{C}/L$ on where the real subset behaves like a circle. Then the rational subset is generated by one or more points, and running this over the circle clearly gives a dense subset on the circle. This motivates to write down an isomorphism sending a point on E (or on C) to $\mathbb{R}/\mathbb{Z}$ preserving the group law.

If that is possible, one can think of the following method to find ABC-triples: Start with a number d which is the sum of two (possible negative) integer cubes. This sum gives rise to a point on E. If that point is not a torsion point, it generates a subgroup of $E(\mathbb{Q})$ isomorphic to $\mathbb{Z}$, and topologically one can get as close to the zero point $0_E = (-1:1:0)$ as one wants. A point $P = (\frac{p}{r}:\frac{q}{r}:1)$ close to 0_E gives rise to the equation $p^3+q^3 = dr^3$ with $pq<0$ while r is small compared to $|p|$ and $|q|$. We can assume without loss of generality that $|p|>|q|$, hence get the candidate ABC-triple (q^3, dr^3, p^3). The quality of the triple (q^3, dr^3, p^3) is at least

$$\frac{\log(p^3)}{\log r\,(dp^3q^3r^3)} \geqslant \frac{3\log p}{\log(dpqr)}$$

This is larger than 1 if $p>dr$, and after enough research such points $(p:q:r)$ can be discovered, just by repeatedly adding the initial starting point to itself. Another way to achieve this is by associating a real number α to the initial point. Then one tries to find integers m, n such that $n\alpha \approx m$ and for each irrational $\alpha \in [0,1)$ it is possible to find m, n such that $|m\alpha - n| \leqslant \frac{1}{|n|}$. So it is a good question to ask that given $|m\alpha - n| < \varepsilon$, what do we know about the associated $\frac{q}{r}$? To answer this question, the following result is useful:

Theorem 3.6. *Let $d>0$ and $E_d\colon x^3+y^3=d$ be an elliptic curve over $\mathbb{R}$. Then the homeomorphism (of Euclidean topological spaces)*

$$\varphi_d\colon E_d \longrightarrow \mathbb{R}/\mathbb{Z}, (x,y) \longmapsto \frac{\int_{-\infty}^{x} \frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}}{\int_{-\infty}^{+\infty} \frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}} + \mathbb{Z}$$

preserves the group law.

Proof. We need to prove that $\omega = \frac{\mathrm{d}x}{3y^2} = \frac{\mathrm{d}y}{3x^2}$ is an invariant differential on E_d. Hence let $Q \in E_d$ and define

$$\tau_Q\colon E_d \longrightarrow E_d, P \longmapsto P+Q$$

be the "translation-by-Q-map." Then to prove: $\tau_Q^*\omega = \omega$, where τ_Q^* is the automorphism induced by τ_Q on $\mathbb{C}(E_d)$, the function field of rational functions defined over the algebraic closure of $\mathbb{R}$. This automorphism is defined by

$$(P \longmapsto f(P)) \longmapsto (P \longmapsto f(P+Q)).$$

Since ω can be written as a formal expression $g(t)\mathrm{d}t$ for some variable t, this $\tau_Q^*\omega$ is well defined as $(\tau_Q^*(g))(t)\mathrm{d}t$.

Since E_d is a curve, the set of differential forms on E_d is a one-dimensional vectorspace over $\mathbb{C}(E_d)$, so there is a function $a_Q \in \mathbb{C}(E_d)^*$ such that $\tau_Q^*\omega = a_Q\omega$. Their associated divisors satisfy

$$D(a_Q) = D(\tau_Q^*\omega) - D(\omega) = \tau_Q^*D(\omega) - D(\omega)$$

where $D(\omega) = D(g(t)\mathrm{d}t) = D(g(t)) = \sum_{P\in E_d} \mathrm{ord}_P(g)$ and $\tau_Q^*D(\omega) = \sum_{P\in E_d} \mathrm{ord}_{P+Q}(g)$. Now $\tau_Q^*D(\omega) - D(\omega)$ is equal to 0 because of the following:

Let $P=(x_0,y_0)\in E_d$. Then

$$\omega = \frac{\mathrm{d}(x-x_0)}{3y^2} = -\frac{\mathrm{d}(y-y_0)}{3x^2}.$$

Since E_d is smooth, $P \in E_d$ cannot be a pole. We have a bijection

$$E_d(\mathbb{R}) \longrightarrow \mathbb{P}^1(\mathbb{R}), (x:y:1) \longmapsto (x:1),$$

so $\mathrm{ord}_P(x-x_0) = 1$ if $P \neq 0_{E_d}$ and $y(P) \neq 0$. In the case $y(P)=0$ we have $\mathrm{ord}_P(x-x_0)=3$, but then the denominator has a zero of order 2 in P. In either case,

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(x-x_0) - \mathrm{ord}_P(3x^2) - 1 = 0.$$

If $P = 0_{E_d}$, then let t be an uniformizer at 0_{E_d}. Since

$$\begin{gathered}\mathrm{ord}_{0_{E_d}}(x) = \mathrm{ord}_{0_{E_d}}(y) = 3,\\ x = t^{-3}f, y = t^{-3}g\end{gathered}$$

for some f, g regular at 0_{E_d}. Now

$$\omega = \frac{\mathrm{d}x}{3y^2} = \left(\frac{-3t^{-4}f + t^{-3}f'}{3t^{-6}g^2}\right)\mathrm{d}t = \frac{t^3f' - 3t^2f}{3g^2}.$$

But f' is the derivative of a rational function hence regular at 0_{E_d}, so the function $\frac{t^3f' - 3t^2f}{3g^2}$ is regular and does not vanish at 0_E, so $\mathrm{ord}_{0_{E_d}}(\omega) = 0$.

So a_Q neither has zeroes nor has poles, hence is constant and can be seen as a complex number. Consider the map

$$E_d \longrightarrow \mathbb{P}^1, Q \longmapsto (a_Q \colon 1)$$

what is rational from E_d to $\mathbb{P}^1$ since a_Q can be expressed as a rational function of $x(Q)$ and $y(Q)$. But it is not surjective since both $(1\colon 0)$ and $(0\colon 1)$ aren't in the image of this map. By algebraic geometry, a morphism between curves either is surjective, or is constant. So in this case it is constant. So

$$\forall Q \in E_d \colon a_Q = a_{0_{E_d}}$$

but $\tau_{0_{E_d}}$ is the identity on E_d hence $a_Q = 1$. □

Remark 3.7. These integrals - called *elliptic logarithms* - are not exactly computable. But for the purpose of finding approximate linear dependencies between such numbers it suffices to get a good numerical approximation. There are several ways to get good numerical approximations to these numbers. An algorithm which *doubles* the accuracy of the approximation on each iteration uses the *Arithmetic-Geometric Mean*, see K).

Now it has become easy to proof theorem 1.1.

Corollary 3.8. (theorem of Diophantus) *The difference between two positive integer cubes also is the sum of two positive rational cubes.*

Proof. Let $a^3 - b^3 = d$ where $a > b > 0 < d$ all integers. Then $P = (a, -b)$ is on the curve

$$E_d \colon x^3 + y^3 = d.$$

Since the point $\left(\sqrt[3]{d}, 0\right)$ is an inflection point, by theorem 3.6, $\varphi_d\Big(\left(\sqrt[3]{d}, 0\right)\Big) = \frac{2}{3}$, so since the y-coordinate of P is negative, $\varphi_d(P) \in \left(\frac{2}{3}, 1\right)$. Hence there is some multiple $m \in \mathbb{Z}$ such that

$$\varphi_d(m * P) \in \left(\frac{1}{3}, \frac{2}{3}\right)$$

and the point $m * P$ has positive rational coordinates. □

Remark 3.9. This theorem also holds when starting with $d = a^3 + b^3$ unless $ab(a - b) = 0$. In all other cases, the discovered point $(a, -b)$ resp. (a, b) are points of infinite order. The proof of this claim is an exercise in a course of Elliptic Curves, and it is for example written as exercise in L).

When we start with an initial point $P = (a \colon b \colon 1)$ on E_d, the quest for finding nice ABC-triples now restricts to associate a real number $\alpha_P \in \mathbb{R}/\mathbb{Z}$ to P and find integers m, n such that $|m\alpha_P - n|$ becomes very small. Since this also is a numerical approximation, it suffices to give a numerical approximation of α_P. But what does it mean for ABC-triples when we already know that $|m\alpha_P - n| < \varepsilon$?

To answer that question one needs to know what a small distance to 0 means for the value $\frac{x(m*P)}{z(m*P)}$. So one is interested in $\varphi_d^{-1}(\varepsilon)$. We already have the map σ_d from

$$C_d \colon Y^2Z = X^3 - 432d^2Z^3$$

to E_d defined by

$$(X:Y:Z)\longmapsto(36dZ+Y:36dZ-Y:X)$$

and for L_d the lattice associated with C_d by the Uniformization Theorem the Weierstrass map

$$\wp: z+L_d\longmapsto(\wp(z):\wp'(z):1)$$

but it is in general not true that $1\in L_d$. However, for this particular family of elliptic curves the lattice has a real period denoted α_d and we need a map $\cdot\,\alpha_d$ from $\mathbb{R}/\mathbb{Z}$ to $\mathbb{R}/\alpha_d\mathbb{Z}$ that multiplies every element with α_d. The image of the Weierstrass map $\wp$ is an elliptic curve of the shape

$$C_d': y^2z=4x^3+g_2xz^2+g_3z^3$$

and we need to multiply x and y by 4 to go to

$$C_d: y^2z=x^3+4g_2xz^2+16g_3z^3$$

where $g_2=0$ and $g_3=-27d^2$. So we have the following homeomorphisms preserving the group law:

$$\begin{array}{rccl}
\cdot\,\alpha_d: & \mathbb{R}/\mathbb{Z}\longrightarrow\mathbb{R}/\alpha_d\mathbb{Z} & x\longmapsto\alpha_d x\\
\wp_{L_d}|_{\mathbb{R}}: & \mathbb{R}/\alpha_d\mathbb{Z}\longrightarrow C_d' & z\longmapsto(\wp_{L_d}(z):\wp'_{L_d}(z):1)\\
\cdot\,4: & C_d'\longrightarrow C_d & (x:y:z)\longmapsto(4x:4y:z)\\
\sigma_d: & C_d\longrightarrow E_d & (X:Y:Z)\longmapsto(36dZ+Y:36dZ-Y:6X)\\
\varphi_d: & E_d\longrightarrow\mathbb{R}/\mathbb{Z} & (x:y:z)\longmapsto\dfrac{\int_{-\infty}^{\frac{x}{z}}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}}{\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}}+\mathbb{Z}
\end{array}$$

and $\varphi_d\circ\sigma_d\circ\cdot\,4\circ\wp_{L_d}\circ\cdot\,\alpha_d$ is the identity on $\mathbb{R}/\mathbb{Z}$. Note that in the definition of φ_d, if $z=0$, the term $\frac{x}{z}$ is ∞ and the integral becomes $1+\mathbb{Z}=0+\mathbb{Z}$, so it indeed maps 0_{E_d} to $0+\mathbb{Z}$. So for any $\varepsilon\in\mathbb{R}/\mathbb{Z}$,

$$\varphi_d^{-1}(\varepsilon)=(\sigma_d\circ\cdot\,4\circ\wp_{L_d}\circ\alpha_d)(\varepsilon).$$

It is clear that $\varphi_d^{-1}(z)$ is singular at $z=0$ since $\varphi_d(\infty)=0$, so we need the Laurent series of $\varphi_d^{-1}(z)$ around $z=0$. To determine this, first note that for $z\in\mathbb{R}/\alpha_d\mathbb{Z}$ we have

$$z\longmapsto(\wp(z):\wp'(z):1)\longmapsto(4\wp(z):4\wp'(z):1)\longmapsto(36d+4\wp'(z):36d-4\wp'(z):24\wp(z)).$$

In affine coordinates the latter image becomes

$$\left(\frac{9d+\wp'(z)}{6\wp(z)},\frac{9d-\wp'(z)}{6\wp(z)}\right)$$

Since $\frac{9d}{6\wp(z)}$ is regular at $z=0$, $\frac{9d+\wp'(z)}{6\wp(z)}$ has a simple pole at $z=0$ with residue $\frac{-2}{6}=-\frac{1}{3}$. Hence $\varphi_d^{-1}(z)$ has a simple pole at $z=0$ with residue $-\frac{1}{3\alpha_d}$. This proves

Lemma 3.10. *For all $P\in E_d$, integers $m,n\in\mathbb{Z}$, real $\varepsilon>0$ and $\varphi_d(P)=\alpha_{d,P}$ there is a $\delta>0$ only depending on ε and going to 0 if $\varepsilon\to 0$ such that*

$$|m\alpha_{d,P}-n|<\varepsilon\Longrightarrow\left|\frac{x(m*P)}{z(m*P)}\right|\geqslant\frac{1}{3\alpha_d\varepsilon}-\delta_1$$

The error term δ_1 is needed since $\frac{9d+\wp'(z)}{6\wp(z)}$ is not exactly equal to $-\frac{1}{3(\alpha_d z)}$. In fact, it is equal to

$$-\frac{1}{3}(\alpha_d z)^{-1}+2(\alpha_d z)^3+\cdots$$

It is possible to tell more about α_d:

Proposition 3.11. $\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}=3\alpha_d=3\sqrt[3]{\frac{2}{d}}\alpha_2$.

Proof. To prove the first equality, one computes

$$\varphi_d\left(\left(\sqrt[3]{\frac{d}{2}}\colon\sqrt[3]{\frac{d}{2}}\colon 1\right)\right)=\frac{1}{2}$$

in an alternative way. The easy way is to use that the point $\left(\sqrt[3]{\frac{d}{2}}\colon\sqrt[3]{\frac{d}{2}}\colon 1\right)$ is the point of order 2 at E_d, so the integral must be equal to $\frac{1}{2}$. But it is also possible to compute the integral by computing its *derivative* at the same point. Multiplied with the derivative of φ_d^{-1} at $\frac{1}{2}$ it must be equal to 1 since the composition of these inverse functions is the identity. Clearly

$$\varphi_d'\left(\left(\sqrt[3]{\frac{d}{2}}\colon\sqrt[3]{\frac{d}{2}}\colon 1\right)\right)=\frac{1}{\sqrt[3]{d-\sqrt[3]{\frac{d}{2}^3}^2}}=\frac{\left(\frac{2}{d}\right)^{\frac{2}{3}}}{\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}}$$

On the other side, the derivative of the affine x-coordinate of $\sigma_d\circ\cdot 4\circ\wp_{L_d}\circ\alpha_d$ is equal to

$$\alpha_d\cdot\left(\frac{9d+\wp'(\alpha_d z)}{6\wp(\alpha_d z)}\right)'=\frac{\wp(\alpha_d z)\wp''(\alpha_d z)-(\wp'(\alpha_d z))^2-9d\wp'(\alpha_d z)}{6(\wp(\alpha_d z))^2}\alpha_d$$

Now from the theory of elliptic curves with in this case $g_2=0$:

$$\begin{aligned}\wp''(\alpha_d z) &= -6\sum_{w\in L_d}\frac{1}{(z-w)^4}=6\wp(\alpha_d z)^2-\frac{1}{2}g_2=6\wp(\alpha_d z)^2,\\ \left(\varphi_d^{-1}\right)'\left(\frac{1}{2}\right) &= \frac{6(\wp(\frac{\alpha_d}{2}))^3-(\wp'(\frac{\alpha_d}{2}))^2-9d\wp'(\frac{\alpha_d}{2})}{6(\wp(\frac{\alpha_d}{2}))^2}\alpha_d.\end{aligned}$$

For a specific computation, a numerical example is needed, and for this proof first take $d=2$:

Then the order 2 point is $(1\colon 1\colon 1)$, so

$$\varphi_2'((1\colon 1\colon 1))=\frac{1}{\int_{-\infty}^{\infty}\frac{dt}{\sqrt[3]{2-t^3}^2}}$$

On the other side, $(\wp(\frac{\alpha_2}{2})\colon\wp'(\frac{\alpha_2}{2})\colon 1)$ is the order 2 point from the curve

$$C_2'\colon y^2z=4x^3-27\cdot 2^2z^3$$

hence satisfies $y=0, 4x^3=108$, so is the point $(3\colon 0\colon 1)$. This makes $\wp(\frac{\alpha_2}{2})=3$, $\wp'(\frac{\alpha_2}{2})=0$. So

$$\begin{aligned}\frac{6(\wp(\frac{\alpha_2}{2}))^3-(\wp'(\frac{\alpha_2}{2}))^2-9d\wp'(\frac{\alpha_{d2}}{2})}{6(\wp(\frac{\alpha_2}{2}))^2}\alpha_2 &= \wp\Big(\frac{\alpha_2}{2}\Big)\alpha_2=3\alpha_2,\\ 3\alpha_2\cdot\frac{1}{\int_{-\infty}^{\infty}\frac{dt}{\sqrt[3]{2-t^3}^2}} &= 1\end{aligned}$$

making the equality true for $d=2$.

For d arbitrary the order 2 point on the curve $C_d'\colon y^2z=4x^3-27d^2z^3$ is $\left(3\sqrt[3]{\left(\frac{d}{2}\right)^2}\colon 0\colon 1\right)$ hence

$$(\varphi_d^{-1})'\left(\frac{1}{2}\right)=\alpha_d\cdot 3\sqrt[3]{\left(\frac{d}{2}\right)^2}$$

On the other hand

$$\begin{aligned}\varphi_d'\left(\left(\sqrt[3]{\frac{d}{2}}\colon\sqrt[3]{\frac{d}{2}}\colon 1\right)\right) &= \frac{\left(\frac{2}{d}\right)^{\frac{2}{3}}}{\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}},\\ 3\alpha_d\left(\frac{d}{2}\right)^{\frac{2}{3}}\cdot\frac{\left(\frac{2}{d}\right)^{\frac{2}{3}}}{\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}} &= \frac{3\alpha_d}{\int_{-\infty}^{\infty}\frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}}=1\end{aligned}$$

which implies the first equality. To finish the proof it suffices to determine $\int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}$ knowing $\int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{2-t^3}^2} = 3\alpha_2$:

$$\begin{aligned}
\int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2} &= \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{\left(2-\frac{2t^3}{d}\right)\left(\frac{d}{2}\right)}^2} \\
&= \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\left(\frac{d}{2}\right)^{\frac{2}{3}} \cdot \sqrt[3]{2-\left(\sqrt[3]{\frac{2}{d}}t\right)^3}^2} \\
&= \int_{-\infty}^{\infty} \frac{\left(\frac{2}{d}\right)^{\frac{2}{3}}\mathrm{d}t}{\sqrt[3]{2-\left(\left(\frac{2}{d}\right)^{\frac{1}{3}}t\right)^3}^2} \\
&= \left(\frac{2}{d}\right)^{\frac{1}{3}} \int_{-\infty}^{\infty} \frac{\mathrm{d}\left(\left(\frac{2}{d}\right)^{\frac{1}{3}}t\right)}{\sqrt[3]{2-\left(\left(\frac{2}{d}\right)^{\frac{1}{3}}t\right)^3}^2} \\
&= \left(\frac{2}{d}\right)^{\frac{1}{3}} \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{2-t^3}^2}
\end{aligned}$$

So $1 = \frac{3\alpha_d}{\int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{d-t^3}^2}} = \frac{3\alpha_d}{\left(\frac{2}{d}\right)^{\frac{1}{3}} \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{2-t^3}^2}} = \frac{3\alpha_2}{\int_{-\infty}^{\infty} \frac{\mathrm{d}t}{\sqrt[3]{2-t^3}^2}}$ hence $\alpha_d = \sqrt[3]{\frac{2}{d}}\alpha_2$. □

Hence the real period of the lattice associated with E_d is equal to $\int_{-\infty}^{\infty} \frac{\mathrm{d}t}{3\sqrt[3]{d-t^3}^2}$ and is $\sqrt[3]{d}$ as small as the real period of the lattice associated with E_1. From numerical analysis

$$\alpha_2 = 1.40218...$$

Remark 3.12. (link with ABC-triples) If we have a point "close to 0" the claim in lemma 3.10 tells what one can expect for the quality of the candidate ABC-triple associated with the said point. Suppose we have an elliptic curve E_d: $x^3 + y^3 = dz^3$ and a point $P \in E_d$. We run through the set $\{P, 2*P, 3*P, ...\}$ to find integers $m > 0$ such that $m*P$ lies close to 0_{E_d}. Suppose $m*P = (p_m\colon q_m\colon r_m)$. Then $p_m^3 + q_m^3 = dr_m^3$ and $\max(|p_m|, |q_m|)$ is large compared with dr_m. To be precise,

$$\forall \delta > 0\colon \exists M \in \mathbb{R}_{>0}\colon \forall m > M\colon \left(|m\alpha_P - n| < \frac{1}{a|n|} \right) \Longrightarrow \left(\frac{\max(|p_m|, |q_m|)}{dr_m} \geqslant \frac{a|n|}{3\alpha_d}(1-\delta) \right)$$

The left hand side can be achieved for example by creating the continued fraction (see subsection 2.4.1) associated with $\alpha_P = \varphi_d(P)$ where a is sufficiently small. Also LLL will work finding m, n (and determining a) and is very useful when starting with more than one point P, if E_d has rank higher than 1. In that case, linear combinations of generating points with small coefficients can come much closer to 0_{E_d}. See chapter 4 for details.

The only question left is how large $\log C = \log(\max(|p|, |q|)^3)$ grows when m, n grows. The answer to this question is described in the following section.

3.2 Heights of a point

Let E be an elliptic curve over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$ be written as $P = (x\colon y\colon z)$. The *(absolute) height* $H(P)$ of P has two equivalent definitions:

1. $H(P) = \max(|x'|, |y'|, |z'|)$ where $(x'\colon y'\colon z')$ are coordinates chosen such that $x', y', z' \in \mathbb{Z}$ with $\gcd(x', y', z') = 1$.

2. $H(P) = \max(|x|_\infty, |y|_\infty, |z|_\infty) \cdot \prod_{p\,\text{prime}} \max(|x|_p, |y|_p, |z|_p)$.

The first definition only works for integer coordinates on P, while the second definition works for any choice of coordinates $(x\colon y\colon z)$ in $\mathbb{P}^2(\mathbb{Q})$ and even is independent of the field k over which $E \ni P$ is defined over, as long as k is a finite field extension of $\mathbb{Q}$. But if $k \neq \mathbb{Q}$ the absolute values are defined over prime elements of $\mathcal{O}_k$, the ring of integers over k, multiplicities must be counted and the (positive real) $[k\colon \mathbb{Q}]$-th root must be taken. Also the absolute value $|\cdot|_\infty$ has extensions in $k \supset \mathbb{Q}$, depending on the chosen embedding $k \hookrightarrow \mathbb{C}$.

All I write in this section holds for E defined over an algebraic number field, and the details of it can be found in several books introducing elliptic curves, for example in J) part VIII chapters 5, 6 and 9 (p 205-220, 227-233). But for now I restrict only to $\mathbb{Q}$.

A *morphism of degree d* over $\mathbb{Q}$ is a map

$$f\colon \mathbb{P}^m(\mathbb{Q}) \longrightarrow \mathbb{P}^n(\mathbb{Q}), P \longmapsto (f_0(P)\colon \ldots\colon f_n(P))$$

where $f_0(P), \ldots, f_n(P) \in \mathbb{Q}[X_0, \ldots, X_m]$ are homogeneous of degree d with no common zero except $(0, \ldots, 0)$ in the algebraic closure of $\mathbb{Q}$.

Theorem 3.13. *Let $f\colon \mathbb{P}^m(\mathbb{Q}) \longrightarrow \mathbb{P}^n(\mathbb{Q})$ be a morphism of degree d, then there are constants C_1 and C_2 such that*

$$\forall P \in \mathbb{P}^m(\mathbb{Q})\colon C_1 H(P)^d \leqslant H(F(P)) \leqslant C_2 H(P)^d$$

For example, take

$$\sigma_d\colon C_d \longrightarrow E_d, (X\colon Y\colon Z) \longmapsto (36dZ + Y\colon 36dZ - Y\colon 6X)$$

For each d this is a morphism of degree 1, so there are constants M and N such that for all points $P \in C_d$ we have $M \cdot H(P) \leqslant H(\sigma_d(P)) \leqslant N \cdot H(P)$. Likewise

$$\sigma_d^{-1}\colon (x\colon y\colon z) \longmapsto (12d \cdot z\colon 36d(x-y)\colon x+y)$$

is of degree 1. So analysis about the heights of points on E_d is nearly equivalent with analysis on the corresponding points of C_d.

Proof. (upper bound)

Write $P = (x_0\colon \ldots\colon x_m), F = (f_0\colon \ldots\colon f_n)$, and let $|\cdot|$ be any absolute value defined over $\mathbb{Q}$, so it is either the standard absoulte value $\max(x, -x)$ or a p-adic absolute value $p^{-v_p(x)}$. Let

$$\begin{aligned} |P| &= \max_{0 \leqslant i \leqslant m} |x_i|, \\ |F(P)| &= \max_{0 \leqslant j \leqslant n} |f_j(P)|, \\ |F| &= \max\{|a|\colon a \text{ is a coefficient of some } f_j\}, \\ H(F) &:= |F|_\infty \cdot \prod_{p\,\text{prime}} |F|_p. \end{aligned}$$

Let $\varepsilon(|\cdot|)$ be 1 if $|\cdot| = |\cdot|_\infty$ and $\varepsilon(|\cdot|_p) = 0$ for all prime numbers p. Then for all $t_1, \ldots, t_r \in \mathbb{Q}$,

$$|t_1 + \cdots + t_r| \leqslant r^{\varepsilon(|\cdot|)} \max(|t_1|, \ldots, |t_r|).$$

For an absolute value $|\cdot|$ we have

$$|f_i(P)| \leqslant C_1^{\varepsilon(|\cdot|)} |F| \cdot |P|^d$$

where C_1 is the number of terms in f_i, being at most the number of monomials of degree d in $m+1$ variables. Running through $0 \leqslant i \leqslant n$ we get

$$|F(P) \leqslant C_1^{\varepsilon(|\cdot|)} |F| \cdot |P|^d$$

Multiply over all absolute values defined over $\mathbb{Q}$ gives the upper bound

$$H(F(P)) \leqslant C_1 H(F) H(P)^d$$

(lower bound)

By the Nullstellensatz M), the ideal generated by $f_0, ..., f_n$ in $\mathbb{Q}[X_0, ..., X_m]$ contains some power of X_i for each $i \in \{0, ..., m\}$ since $f_0, ..., f_n$ have a common zero only at $(0, ..., 0)$. So there is an integer $e > 0$ such that

$$X_i^e = \sum_{j=0}^{m} g_{i,j} f_j$$

for some polynomials $g_{i,j}$. Since we can discard all terms which are not homogeneous of degree e we can assume each $g_{i,j}$ is homogeneous of degree $e - d$. Define $|G| = \max\{|b|: b \text{ is a coefficient of some } g_{i,j}\}$ for each absolute value $|\cdot|$ and

$$H(G) := |G|_\infty \cdot \prod_{p \,\text{prime}} |G|_p.$$

Recall $P = (x_0 : ... : x_m)$. The equations for X_i^e imply that for all i:

$$|x_i|^e = |x_i^e| = \left| \sum_{j=0}^{n} g_{i,j}(P) f_j(P) \right| \leqslant C_2^{\varepsilon(|\cdot|)} \max\{|g_{i,j}(P)|: 0 \leqslant j \leqslant n\} |f_j(P)|$$

Maximize over i:

$$|P|^e \leqslant C_2^{\varepsilon(|\cdot|)} \max\{|g_{i,j}(P)|: 0 \leqslant i \leqslant m, 0 \leqslant j \leqslant n\} |F(P)|$$

Each $g_{i,j}$ has degree $e - d$ hence by the triangle inequality

$$|g_{i,j}(P)| \leqslant C_3^{\varepsilon(|\cdot|)} |G| |P|^{e-d}$$

Now substitute the triangular inequality in the upper bound for $|P|^e$ and multiply by $|P|^{d-e}$ to get

$$|P|^d \leqslant C_4^{\varepsilon(|\cdot|)} |G| |F(P)|$$

Multiply over all absolute values to get the desired lower bound. □

Definition 3.14. *For the rest of this section I need the following definitions:*

i. (big-$\mathcal{O}$-notation) $f(x) = g(x) + \mathcal{O}(1) \iff \exists C_1, C_2 \in \mathbb{R}, \forall x: C_1 \leqslant f(x) - g(x) \leqslant C_2$.

ii. Let E be an elliptic curve defined over $\mathbb{Q}$ and $f: E \longrightarrow \mathbb{C}$ be a function in $\mathbb{C}(E)$. Then define a function also denoted f as $f: E \longrightarrow \mathbb{P}^1$, $P \longmapsto (f(P) : 1)$ if f is regular at P and $f(P) = (1 : 0)$ if P is a pole of f.

iii. (absolute logarithmic height) The absolute algorithmic height *is defined as $h: \mathbb{P}^n \longrightarrow \mathbb{R}$, $h(P) = \log H(P) \geqslant 0$ where the inequality comes from the fact that $H(P) \geqslant 1$ for all P.*

iv. The height on E relative to f *is defined as the function $h_f: E \longrightarrow \mathbb{R}, h_f(P) = h(f(P))$.*

Note that the set $\{Q \in E: H_f(P) \leqslant C\}$ is finite for any non-constant function f and for any constant C. This is true since f gives a finite-to-one map of this set to $\{Q \in \mathbb{P}^1(\mathbb{Q}): H(Q) \in e^C\}$ and that set is finite since points in $\mathbb{P}^1(\mathbb{Q})$ are given by coordinates $(a : b)$ with $a, b \in \mathbb{Z}$ coprime. Then $H((a : b)) = \max(|a|, |b|)$. But this claim also holds for any $\mathbb{P}^m(k)$.

Theorem 3.15. *Let E be an elliptic curve defined over $\mathbb{Q}$ and $f \in \mathbb{Q}(E)$ be an even function (i.e. $f \circ \cdot(-1) = f$). Then for all points $P, Q \in E$:*

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + \mathcal{O}(1)$$

The constants implied by $\mathcal{O}(1)$ depend on E and f, but not on P and Q.

Proof. Suppose E is in short Weierstrass form $E: y^2 = x^3 + ax + b$ and start with the function

$$x: (a : b : 1) \longmapsto a.$$

Then $h_x(0_E) = 0$, $h_x(-P) = h_x(P)$, so the result holds if $0_E \in \{P, Q\}$. If $P = Q = (x_1, y_1)$ we use the duplication formula to get

$$x(P + Q) = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1,$$

a degree 4 equation. So

$$\begin{aligned} h_x(2P) - 4h_x(P) &= \log(\max(|(3x_1^2+a)^2 - 8x_1y_1^2|, 4y_1^2)) - 4\log x_1 \\ &= \log(\max(|(3x_1^2+a)^2 - 8x_1(x_1^3+a\cdot x_1+b)|, 4(x_1^3 - a\cdot x_1+b))) - 4\log x_1 \\ &= \log(\max(x_1^4+\mathcal{O}(x_1^2), 4\mathcal{O}(x_1^3))) - 4\log x_1 = \mathcal{O}(1). \end{aligned}$$

So the claim also holds for $0_E \in \{P+Q, P-Q\}$.

For $P \neq Q$, write $x(P) = (x_1\colon 1)$, $x(Q) = (x_2\colon 1)$, $x(P+Q) = (x_3\colon 1)$ and $x(P-Q) = (x_4\colon 1)$. Note that $x_1 \neq x_2$ since otherwise $P = \pm Q$. By the addition formula

$$\begin{aligned} x_3 &= \left(\frac{y(Q)-y(P)}{x_2-x_1}\right)^2 - x_1 - x_2, \\ x_4 &= \left(\frac{y(Q)+y(P)}{x_2-x_1}\right)^2 - x_1 - x_2. \end{aligned}$$

The purpose of the next computation is to express $x_3 + x_4$ and x_3x_4 in terms of $x_1 + x_2$ and x_1x_2:

$$\begin{aligned} x_3+x_4 &= \frac{(y(Q)+y(P))^2 + (y(Q)-y(P))^2}{(x_2-x_1)^2} - 2(x_1+x_2) \\ &= \frac{2y(P)^2 + 2y(Q)^2 - 2(x_1+x_2)(x_2-x_1)^2}{(x_2-x_1)^2} \\ &= \frac{2x_1^3 + 2a\,x_1 + 2b + 2x_2^3 + 2a\,x_2 + 2b - 2(x_1^3 - x_1^2x_2 - x_1x_2^2 + x_2^3)}{(x_1+x_2)^2 - 4x_1x_2} \\ &= \frac{2x_1x_2(x_1+x_2) + 2a(x_1+x_2) + 4b}{(x_1+x_2)^2 - 4x_1x_2} \\ &= \frac{2(x_1+x_2)(a+x_1x_2) + 4b}{(x_1+x_2)^2 - 4x_1x_2} \end{aligned}$$

and

$$\begin{aligned} x_3x_4 &= \left(\frac{(y(Q)+y(P))^2}{(x_2-x_1)^2} - x_1 - x_2\right)\left(\frac{(y(Q)-y(P))^2}{(x_2-x_1)^2} - x_1 - x_2\right) \\ &= \frac{(y(Q)^2-y(P)^2)^2}{(x_2-x_1)^4} - (x_1+x_2)\cdot\frac{2(y(P)^2+y(Q)^2)}{(x_2-x_1)^2} + (x_1+x_2)^2 \\ &= \frac{(x_2^3 + a\,x_2 + b - x_1^3 - a\,x_1 - b)^2}{(x_2-x_1)^4} \\ &\qquad - 2\frac{(x_1+x_2)(x_1^3+x_2^3+a(x_1+x_2)+2b)}{(x_2-x_1)^2} + \frac{(x_1+x_2)^2(x_2-x_1)^2}{(x_2-x_1)^2} \\ &= \frac{((x_2-x_1)(x_1^2+x_1x_2+x_2^2+a))^2}{(x_2-x_1)^4} \\ &\qquad + \frac{-2(x_1^4+x_1^3x_2+x_1x_2^3+x_2^4+a(x_1+x_2)^2+2b(x_1+x_2)) + (x_2^2-x_1^2)^2}{(x_2-x_1)^2} \\ &= \frac{x_1^4+2x_1^3x_2+3x_1^2x_2^2+2x_1x_2^2+x_2^4+2a\,x_1^2+2a\,x_1x_2+2a\,x_2^2+a^2}{(x_2-x_1)^2} \\ &\qquad + \frac{-x_1^4-2x_1^3x_2-2x_1^2x_2^2-2x_1x_2^3-x_2^4-2a(x_1+x_2)^2-4b(x_1+x_2)}{(x_2-x_1)^2} \\ &= \frac{x_1^2x_2^2 + 2a(x_1^2+x_1x_2+x_2^2-x_1^2-2x_1x_2-x_2^2) + a^2 - 4b(x_1+x_2)}{(x_1+x_2)^2 - 4x_1x_2} \\ &= \frac{(x_1x_2)^2 - 2a\,x_1x_2 + a^2 - 4b(x_1+x_2)}{(x_1+x_2)^2 - 4x_1x_2} \\ &= \frac{(x_1x_2-a)^2 - 4b(x_1+x_2)}{(x_1+x_2)^2 - 4x_1x_2}. \end{aligned}$$

With these expressions we can define a map

$$(1\colon x_1+x_2\colon x_1x_2) \longmapsto (1\colon x_3+x_4\colon x_3x_4)$$

as follows: Define

$$g\colon \mathbb{P}^2 \longrightarrow \mathbb{P}^2, (t\colon u\colon v) \longmapsto (u^2 - 4tv\colon 2u(at+v) + 4bt^2\colon (v-at)^2 - 4btu)$$

For $t=1, u=x_1+x_2, v=x_1x_2$ this gives

$$((x_1+x_2)^2 - 4x_1x_2\colon 2(x_1+x_2)(a+x_1x_2) + 4b\colon (x_1x_2-a)^2 - 4b(x_1+x_2))$$

where the first coordinate is the denomerator of both expressions of x_3 and x_4, the second coordinate is the numerator of the expression of x_3 and the third coordinate is the numerator of the expression of x_4.

Let

$$G\colon E\times E \longrightarrow E\times E, (P,Q) \longmapsto (P+Q, P-Q)$$

and let $\sigma\colon E\times E \longrightarrow \mathbb{P}^2$ be the composition of the following:

$$\begin{aligned} E\times E &\longrightarrow \mathbb{P}^1\times\mathbb{P}^1 \quad & (P,Q) &\longrightarrow (x(P), x(Q)) \\ \mathbb{P}^1\times\mathbb{P}^1 &\longrightarrow \mathbb{P}^2 \quad & ((\alpha_1\colon\beta_1),(\alpha_2,\beta_2)) &\longmapsto (\beta_1\beta_2\colon \alpha_1\beta_2+\alpha_2\beta_1\colon \alpha_1\alpha_2) \end{aligned}$$

Then $g\circ\sigma = \sigma\circ G$. We need g to be a morphism (of degree 2.) To prove it, it suffices to prove that the polynomials

$$\begin{gathered} u^2 - 4tv \\ 2u(at+v) + 4bt^2 \\ (v-at)^2 - 4btu \end{gathered}$$

do not have common zeroes (t,u,v) except $(0,0,0)$. So suppose there is a common zero (t,u,v). If $t=0$, then

$$\begin{aligned} u^2 - 4tv &= u^2 = 0, \\ (v-at)^2 - 4btu &= v^2 = 0, \end{aligned}$$

hence $(t,u,v) = (0,0,0)$. If $t\neq 0$, define $x = \frac{u}{2t}$. Then

$$u^2 - 4tv = 0 \Longleftrightarrow \frac{u^2}{4t^2} = \frac{v}{t} \Longleftrightarrow x^2 = \frac{v}{t}.$$

If so, write the other two polynomials in terms of x after dividing them by t^2:

$$\begin{aligned} \psi(x) &= \frac{2u}{t}(a+\frac{v}{t}) + 4b = 4x(a+x^2) + 4b = 4x^3 + 4ax + 4b = 0 \\ \phi(x) &= (\frac{v}{t} - a)^2 - 4b\frac{u}{t} = (x^2-a)^2 - 8bx = x^4 - 2ax^2 - 8bx + a^2 = 0 \end{aligned}$$

So the duplication formula reads

$$2*(x,y) = (\frac{3x^2+a}{2y})^2 - 2x = \frac{9x^4+6ax+a^2-2x(4x^3+4ax+4b)}{4x^3+4ax+4b} = \frac{x^4-2ax^2-8bx+a^2}{4x^3+4ax+4b} = \frac{\phi(x)}{\psi(x)}.$$

Hence if x is the x-coordinate of a point $P_0\in E$, then $\frac{\phi(x)}{\psi(x)} = x(2*P_0)$. But $\psi(x) = 4y^2$ hence it is only zero at order 2 points. These zeroes are simple since E is regular everywhere while $\frac{\phi(x)}{\psi(x)}$ has a pole in these points: $2*P_0 = 0_E$. Hence $\phi(x)\neq 0$ at these points. So $\psi(x)$ and $\phi(x)$ has no common zeroes, hence g is a morphism.

Now to prove

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + \mathcal{O}(1),$$

use theorem 3.13 and that g is a morphism:

$$h(\sigma(P+Q,P-Q)) = h(\sigma\circ G(P,Q)) = h(g\circ\sigma(P,Q)) = 2h(\sigma(P,Q)) + \mathcal{O}(1)$$

since g is a morphism of degree 2. To determine $h(\sigma(P+Q))$ let again $x(P)=x_1$ and $x(Q)=x_2$. Then

$$h(\sigma(P,Q)) = h((1\colon x_1+x_2\colon x_1x_2))$$

and clearly this is equal to

$$h((x_1:1))+h((x_2:1))+\mathcal{O}(1)=h_x(P)+h_x(Q)+\mathcal{O}(1)$$

since we only look over the field $\mathbb{Q}$. The same holds for $(P+Q,P-Q)$. So

$$\begin{aligned} & h_x(P+Q)+h_x(P-Q)-2h_x(P)-2h_x(Q) \\ = \; & h(\sigma(P+Q,P-Q))+\mathcal{O}(1)-2h(\sigma(P,Q))-\mathcal{O}(1) \\ = \; & 2h(\sigma(P,Q))+\mathcal{O}(1)+\mathcal{O}(1)-2h(\sigma(P,Q))-\mathcal{O}(1) \\ = \; & \mathcal{O}(1) \end{aligned}$$

To finish the proof take f an arbitrary even function. The subfield in $\mathbb{Q}(E)$ of even functions is exactly $\mathbb{Q}(x)$, so we have a rational function $\rho:\mathbb{P}^1\longrightarrow\mathbb{P}^1$ satisfying $\rho\circ x=f$ so

$$\begin{aligned} \deg(f) &= \deg(x)\deg(\rho)=2\deg(\rho), \\ h_f &= h_x\circ\rho=(\deg(\rho))h_x+\mathcal{O}(1)=\frac{1}{2}\deg(f)h_x+\mathcal{O}(1) \end{aligned}$$

since x is a function of degree 2. □

Remark 3.16. Now the goal nearly is reached: If the term $\mathcal{O}(1)$ can be removed, it has become a quadratic form and the height has become a *norm* on the *lattice* of points on E. So then LLL can be used to find points close to 0_E with height as low as possible. This can be done when taking limits of the logarithmic height. Before defining it, I first need some other results.

Note that the elliptic curves I look at are of the form $x^3+y^3=d$, not in Weierstrass form. But the degree 1 isomorphism σ_d transforms the corresponding elliptic curve in Weierstrass form into this form and back, so this theorem also holds for elliptic curves in this form.

These results also holds for odd functions f since f^2 is even, so $h_{f^2}=2h_f$.

Corollary 3.17. *Let E be an elliptic curve (in Weierstrass form) and $f\in\mathbb{Q}(E)$ even.*

a) For all $Q\in E$ we have

$$\forall P\in E: h_f(P+Q)\leqslant 2h_f(P)+\mathcal{O}(1).$$

Here $\mathcal{O}(1)$ depends on E, f and Q.

b) We have for all $m\in\mathbb{Z}$ and $P\in E$:

$$h_f(m*P)=m^2h_f(P)+\mathcal{O}(1)$$

where $\mathcal{O}(1)$ depends on e, f and m but not on P.

Proof. *a)* Theorem 3.15 reads

$$h_f(P+Q)+h_f(P-Q)=2h_f(P)+2h_f(Q)+\mathcal{O}(1).$$

But here $2h_f(Q)$ is a constant number and $h_f(P-Q)\geqslant 0$, getting the inequality.

b) The corollary is trivial for $m=0,1$. The case $m=2$ follows immediately from the proof of theorem 3.15. Assume the claim is true for $m=0,\,1,\,\ldots,\,n$. To check the claim for $m=n+1$ replace (P,Q) by $(m*P,P)$. By theorem 17 we have

$$\begin{aligned} h_f((n+1)*P) &= h_f(n*P+P) \\ &= 2h_f(n*P)+2h_f(P)-h_f((n-1)*P)+\mathcal{O}(1) \\ &= h_f(P)(2n^2+2-(n-1)^2)+\mathcal{O}(1)=(n+1)^2h_f(P)+\mathcal{O}(1) \end{aligned}$$

□

Proposition 3.18. (Tate) *Let E be an elliptic curve defined over $\mathbb{Q}$ and $P\in E$. Let $f\in\mathbb{Q}(E)$ nonzero and even. Then*

$$\frac{1}{\deg f}\lim_{n\to\infty}4^{-n}h_f(2^n*P)$$

exists and is independent of f.

Proof. For the existence of the limit, it suffices to prove that

$$\left\{\frac{1}{\deg f}4^{-n}h_f(2^n*P)\right\}_{n=0}^{\infty}$$

is a Cauchy sequence. That is, that for all $\varepsilon>0$ there is an integer M such that for all $m,n>M$:

$$\left|\frac{1}{\deg f}4^{-m}h_f(2^m*P)-\frac{1}{\deg f}4^{-n}h_f(2^n*P)\right|_{\infty}<\varepsilon$$

By corollary 3.17 b there is a constant $C>0$ such that for all $Q\in E$:

$$|h_f(2*Q)--4h_f(Q)|\leqslant C$$

Let $m,n>0$ be integers. Then

$$\begin{aligned}|4^{-n}h_f(2^n*P)-4^{-m}h_f(2^m*P)| &= \left|\sum_{k=m}^{n-1}4^{-(k+1)}h_f(2^{n+1}*P)-4^{-n}h_f(2^n*P)\right|\\ &\leqslant \sum_{k=m}^{n-1}4^{-(n+1)}|h_f(2^{n+1}*P)-4h_f(2^n*P)|\\ &\leqslant \sum_{k=m}^{n-1}4^{-(n+1)}C\leqslant\frac{C}{4^{m+1}}\end{aligned}$$

For the independence of the choice of the function f take another non-constant even function $g\in\mathbb{Q}(E)$. Then

$$\begin{aligned}(\deg g)h_f-(\deg f)h_g &= (\deg g)(\frac{1}{2}(\deg f)h_x+\mathcal{O}(1))-(\deg f)(\frac{1}{2}(\deg g)h_x+\mathcal{O}(1))\\ &= \frac{1}{2}(\deg f)(\deg g)h_x(1-1)+\mathcal{O}(1)(\deg g-\deg f)=\mathcal{O}(1)\end{aligned}$$

So for all $n\geqslant 0$:

$$(\deg g)4^{-n}h_f(2^n*P)-(\deg f)4^{-n}h_g(2^n*P)=4^{-n}\mathcal{O}(1)$$

Taking the limit over n gives

$$\begin{aligned}&\lim_{n\to\infty}\left(\frac{1}{\deg f}4^{-n}h_f(2^n*P)-\frac{1}{\deg g}4^{-n}h_g(2^n*P)\right)\\ =\ &\frac{1}{(\deg f)(\deg g)}\lim_{n\to\infty}\left((\deg g)4^{-n}h_f(2^n*P)-(\deg f)4^{-n}h_g(2^n*P)\right)=0\end{aligned}$$

So the limit does not depend on the choice of the function f. □

Now it is time to give a height giving rise to quadratic forms:

Definition 3.19. *The* canonical height *on an elliptic curve $E(\mathbb{Q})$, denoted $\hat{h}$ or $\hat{h}_E$ is the function*

$$\hat{h}\colon E\longrightarrow\mathbb{R},P\longmapsto\frac{1}{\deg f}\lim_{n\to\infty}4^{-n}h_f(2^n*P)$$

for any non-constant even function $f\in\mathbb{Q}(E)$.

Theorem 3.20. (Neron-Tate) *Let $\hat{h}$ be the canonical height on $E(\mathbb{Q})$:*

a) $\forall P,Q\in E$: $\hat{h}(P+Q)+\hat{h}(P-Q)=2\,\hat{h}(P)+2\,\hat{h}(Q)$ *(parallelogram law)*

b) $\forall P\in E,m\in\mathbb{Z}$: $\hat{h}(m*P)=m^2\,\hat{h}(P)$

c) $\hat{h}$ *is even and we have a bilinear pairing*

$$\langle,\rangle\colon E\times E\longrightarrow\mathbb{R},\langle P,Q\rangle=\frac{\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)}{2}$$

This pairing is called the Neron-Tate pairing.

d) Let $P \in E$. Then $\hat{h}(P) \geqslant 0$ and equality holds if and only if there is an integer $n > 0$ such that $n * P = 0_E$ (iff P is a torsion point.)

e) Let $f \in \mathbb{Q}(E)$ be an even function. Then $(\deg f)\,\hat{h} = h_f + \mathcal{O}(1)$.

Proof. *e)* In the proof of proposition 3.18 there is a constant C depending on f such that for all $n \geqslant m \geqslant 0$:

$$|4^{-n} h_f(2^n * P) - 4^{-m} h_f(2^m * P)| \leqslant \frac{C}{4^{m+1}}$$

Let $m = 0$ and $n \to \infty$. Then we get

$$|(\deg f)\,\hat{h}(P) - h_f(P)| \leqslant \frac{C}{4} = \mathcal{O}(1)$$

a)

$$\begin{aligned} & \hat{h}(P+Q) + \hat{h}(P-Q) - 2\,\hat{h}(P) - 2\,\hat{h}(Q) \\ = & \lim_{n\to\infty} \frac{1}{(\deg f)4^n} \Big(h_f(2^n * (P+Q)) + h_f(2^n * (P-Q)) - 2h_f(2^n * P) - 2h_f(2^n * Q) \Big) \\ = & \lim_{n\to\infty} \frac{1}{(\deg f)4^n} \mathcal{O}(1) = 0 \end{aligned}$$

b) Same argument as in *a)* with $\hat{h}(m * P) - m^2\,\hat{h}(P)$, or use *a)* using induction on m as in the proof of corollary 3.17 b.

c) From linear algebra, a function satisfying the parallelogram law (proved in *a)*) is quadratic.

d) Inequality: $h_f(P) \geqslant 0$ for all f and for all P, so the limit cannot be negative.

Equivalence: If P is a torsion point, there is some $n > 0$ such that $n * P = 0_E$. Since by *b)*

$$0 = \hat{h}(n * P) = n^2\,\hat{h}(P)$$

we have $\hat{h}(P) = 0$. If $\hat{h}(P) = 0$ for some $P \in E$, then for all

$$n > 0\colon\ \hat{h}(n * P) = n^2\,\hat{h}(P) = 0$$

Now consider the set $\{0_E, P, 2 * P, 3 * P, ...\}$. If P is not a torsion point, this set is infinite while by *e)* there is a $C > 0$ such that

$$h_f(n * P) = |(\deg f)\,\hat{h}(n * P) - h_f(n * P)| \leqslant C$$

But $\{Q \in E(\mathbb{Q})\colon h_f(Q) \leqslant C\}$ is a finite set hence P has finite order. □

Remark 3.21. Part e) of the theorem imply that there is some number $\delta_2 > 0$ such that for all $P \in E$ we have

$$|\,\hat{h}(P) - h(P)| \leqslant \delta_2.$$

This bound δ_2 is called the *Cremona-Prickett-Siksek height bound*. In the case of other number fields rather than $\mathbb{Q}$ this bound is caled the *Silvermann-height-bound*. Here I denote this bound δ_2 since in my main theorem I both use this δ_2 and another bound δ_1 from lemma 3.10.

Actual the Neron-Tate pairing has two different definitions. The definition I gave in the theorem is the easiest for computations, since then $\langle P, P\rangle = \hat{h}(P)$, but it often is defined without dividing by 2. For example, Silvermann defines the pairing in his book J) page 233, as

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

But for concrete computations it is better to define the Neron-Tate pairing as in the theorem above, because we can use the *Elliptic Regulator matrix*

$$M = (\langle P_i, P_j\rangle)_{1 \leqslant i,j \leqslant r}$$

where E has rank r and generator points $P_1, ..., P_r$. With this matrix M and a linear combination of points $a_1 * P_1 + \cdots + a_r * P_r$ we can define the vector $\boldsymbol{a} = (a_1, ..., a_r)$ such that

$$\hat{h}(a_1 * P_1 + \cdots + a_r * P_r) = \boldsymbol{a} M \boldsymbol{a}^\top.$$

So using M we can do linear algebra on points on E using only the standard quadratic form while still computing canonical heights. The determinant of M is called the *elliptic regulator*, denoted $R = R(E_d/\mathbb{Q})$.

Now I can give an answer to the question how large $\log C = \log(\max(|p|, |q|)^3)$ grows when m, n grows, where now

$$m * P = (p\colon q\colon r), |m \cdot \varphi_d(P) - n| \leqslant \frac{1}{a \cdot |n|}$$

for some $a, n \in \mathbb{Z}_{>0}$ and

$$(A, B, C) = (dr^3, \min(|p|^3, |q|^3), \max(|p|^3, |q|^3))$$

an ABC-triple created from the elliptic curve $E_d\colon x^3 + y^3 = d$. We know $\hat{h}(m * P) = m^2 \hat{h}(P)$, so $H((p\colon q\colon r)) \approx (H(P))^{m^2}$. This makes an expected quality of

$$\frac{\log C}{\log r(ABC)} \approx \frac{3\log p}{3\log p - \log \frac{\alpha_d}{3a \cdot |n|} + \text{const.}} \approx \frac{3C_1 m^2}{3C_1 m^2 - \log(C_2 \cdot m^2) + C_3} \approx 1 + \frac{\text{const.} \cdot \log\log C}{\log C}$$

The details of this approximations and the constants are the main result and come in the following chapter.

Chapter 4
The Main Result

Now I have introduced all I need to prove the main result for finding ABC-triples using elliptic curves. Recall that I define an elliptic curve E_d: $x^3 + y^3 = d$ and find points $P_1, ..., P_r$ for some $r \geqslant 0$ such that $E_d(\mathbb{Q})/(E_d(\mathbb{Q})_{\text{tor}})$ is generated by $P_1, ..., P_r$. Then I can approximate 0_{E_d} by a linear combination of $P_1, ..., P_r$ and denote the point given by this linear combination by Q. In section 3.1 I explained the relation of the distance between Q and 0_{E_d} and the quotient of the coordinates of Q. In section 3.2 I explained the relation of the coefficients of the linear combination $a_1 * P_1 + \cdots + a_r * P_r$ and the size of the coordinates of Q. And in this chapter I will explain how one can find Q using what I told in section 2.2. But first I explain what one can expect of the quality one can get for ABC-triples discovered this way.

4.1 The Main Theorem

Theorem 4.1. (Main Theorem of this thesis) *Let $d > 0$ be an integer such that the elliptic curve E_d: $x^3 + y^3 = d \cdot z^3$ has $r \geqslant 1$ linearly independent points $P_1, ..., P_r$. Then there is a constant number $C > 0$ depending only on d and the choice of the set of points $P_1, ..., P_r$, such that there are infinitely many triples $(p_n, q_n, r_n) \in \mathbb{Z}^3$, $n \geqslant 0$, of coprime positive integers, such that*

$$(p_n : q_n : r_n) \in E_d$$

and the associated ABC-triples $(A_n, B_n, C_n) = (dr_n^3, -p_n^3, q_n^3)$, $n \geqslant 0$, satisfy

$$q(A_n, B_n, C_n) > 1 + \frac{r \log\log C_n - C}{2 \log C_n}$$

Proof. Associate $\alpha_{d,1}, ..., \alpha_{d,r} \in \mathbb{R}/\mathbb{Z}$ to the points $P_1, ..., P_r$ as in theorem 3.6 and take a lift of them into $\mathbb{R}$, also denoted $\alpha_{d,1}$, ..., $\alpha_{d,r}$. Then find approximate linear dependencies of 1 and these numbers, using a quadratic form involving the canonical height as in theorem 3.20 c).

We then need to define for any $N > 0$ the lattice $L_N = \{(a_0, ..., a_r) : a_0, ..., a_r \in \mathbb{Z}\}$ with quadratic form

$$q_N((a_0, ..., a_r)) = \hat{h}(a_1 * P_1 + \cdots + a_r * P_r) + N \cdot (a_0 + a_1\alpha_{d,1} + \cdots + a_r\alpha_{d,r})^2.$$

The determinant of L_N is equal to the determinant of the matrix

$$\begin{pmatrix} 0 & ... & 0 & \sqrt{N} \\ \langle P_1, P_1 \rangle & ... & \langle P_1, P_r \rangle & \sqrt{N}\alpha_{d,1} \\ \vdots & & \vdots & \vdots \\ \langle P_r, P_1 \rangle & ... & \langle P_r, P_r \rangle & \sqrt{N}\alpha_{d,r} \end{pmatrix}$$

hence is equal to $R\sqrt{N}$. Here $R = (\det((\langle P_i, P_j \rangle)_{1 \leqslant i,j \leqslant r})$ is the elliptic regulator of E_d when r is the actual rank of E_d and when $P_1, ..., P_r$ is a set of generators of the group $E_d(\mathbb{Q})/(E_d(\mathbb{Q})_{\text{tor}})$.

So by Minkowski's theorem (see 2.5) L has a nonzero vector $\boldsymbol{x}$ with

$$q(\boldsymbol{x}) \leqslant (r+1)\cdot d(L)^{\frac{2}{r+1}} = (r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}.$$

Such an $\boldsymbol{x} = (a_0, ..., a_r)$ satisfies two inequalities:

$$\begin{aligned} \hat{h}(a_1 * P_1 + \cdots + a_r * P_r) &\leqslant (r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}, \\ N\cdot(a_0 + a_1\alpha_{d,1} + \cdots + a_r\alpha_{d,r})^2 &\leqslant (r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}. \end{aligned}$$

The next step is to translate this result to the quality of such a candidate ABC-triple associated with the shortest vector $\boldsymbol{x}$. The upper bound on $\hat{h}(a_1 * P_1 + \cdots + a_r * P_r)$ combined with theorem 3.20 e) says that the point $(p_0 \colon q_0 \colon r_0)$ associated with an optimal solution $\boldsymbol{x} \in L$ satisfies

$$\log(\max(|p_0^3|, |q_0^3|)) \leqslant 3h(a_1 * P_1 + \cdots + a_r * P_r) \leqslant 3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}} + \delta_2,$$

where I take the logarithmic height (see definition 3.14 iii) and δ_2 is the Cremona-Prickett-Siksek height bound, depending only on E_d.

The other inequality gives an upper bound on the distance of the resulting point with 0_{E_d}:

$$|a_0 + a_1\alpha_{d,1} + \cdots + a_r\alpha_{d,r}| \leqslant \sqrt{r+1}\cdot R^{\frac{1}{r+1}}N^{\frac{-r}{2r+2}}.$$

This upper bound combined with remark 3.12 tells that

$$\frac{\max(|p_0|, |q_0|)}{r_0} \geqslant \frac{N^{\frac{r}{2r+2}}}{3\alpha_d\sqrt{r+1}\cdot R^{\frac{1}{r+1}}}(1-\delta_1)$$

for some δ_1 with upper bound depending only on P_1, ..., P_r, and where α_d is the same α_d as in proposition 3.11. We always can replace a point by minus the point, reversing p_0 and q_0, to get $|p_0| < |q_0|$. Then

$$\begin{aligned} q(dr_0^3, |p_0|^3, q_0^3) &= \frac{\log(q_0^3)}{\log r(dr_0p_0q_0)} \\ &\geqslant \frac{\log(q_0^3)}{\log\Big(q_0^3\cdot\frac{r(d)r_0}{q_0}\Big)} \\ &= 1 + \frac{\log\Big(\frac{q_0}{r(d)r_0}\Big)}{\log\Big(q_0^3\cdot\frac{r(d)r_0}{q_0}\Big)} \\ &> 1 + \frac{\log\Big(\frac{q_0}{r(d)r_0}\Big)}{\log(q_0^3)} \end{aligned}$$

Now the numerator $\log\Big(\frac{q_0}{r_0}\cdot\frac{1}{r(d)}\Big)$ can be estimated below by

$$\log\left(\frac{N^{\frac{r}{2r+2}}}{3\alpha_d\sqrt{r+1}\cdot R^{\frac{1}{r+1}}}\cdot\frac{1-\delta_1}{r(d)}\right) = \frac{r}{2r+2}\log N - \frac{1}{r+1}\log R - \log\left(\frac{3\alpha_d r(d)\sqrt{r+1}}{1-\delta_1}\right)$$

and the denominator $\log(q_0^3)$ can be estimated above by $3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}} + \delta_2$. So we get

$$1 + \frac{\log\Big(\frac{q_0}{r(d)r_0}\Big)}{\log(q_0^3)} \geqslant \frac{\frac{r}{2r+2}\log N - \frac{1}{r+1}\log R - \log\Big(\frac{3\alpha_d r(d)\sqrt{r+1}}{1-\delta_1}\Big)}{3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}} + \delta_2}.$$

Now I want to express the numerator in terms of log the denominator, so I need to replace the adding with $+\,\delta_2$ by a multiplication with $(1+\delta_3)$ with δ_3 a (not too) small non-increasing number if N increases. This gives, while still not increasing the numerator and not decreasing the denominator,

$$\begin{aligned}
&\frac{\frac{r}{2r+2}\log N-\frac{1}{r+1}\log R-\log\Big(\frac{3\alpha_d r(d)\sqrt{r+1}}{1-\delta_1}\Big)}{3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}+\delta_2}\\
\geqslant\ &\frac{\frac{r}{2r+2}\log N-\frac{1}{r+1}\log R-\log\Big(\frac{3\alpha_d r(d)\sqrt{r+1}}{1-\delta_1}\Big)}{3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}(1+\delta_3)}\\
=\ &\frac{\frac{r}{2}\Big(\log\Big(3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}(1+\delta_3)\Big)\Big)-\log R-\frac{r}{2}\log(3(r+1)(1+\delta_3))-\log\Big(\frac{3\alpha_d r(d)\sqrt{r+1}}{1-\delta_1}\Big)}{3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}(1+\delta_3)}\\
\geqslant\ &\frac{\frac{r}{2}\Big(\log\Big(3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}(1+\delta_3)\Big)\Big)-\delta_4}{3(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}(1+\delta_3)}
\end{aligned}$$

where δ_4 is a real number, not increasing when N increases. In each step of the computations above, the numerator did not increase and the denominator did not decrease, but now we have got a function of the shape $\frac{\frac{r}{2}\log\log x-\delta_4}{\log x}$ where

$$x=\exp\Big(3(r+1)(1+\delta_3)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}\Big).$$

So the quality, which already is at least $1+\frac{\log\left(\frac{q_0}{r(d)r_0}\right)}{\log(q_0^3)}$, also is at least $1+\frac{\frac{r}{2}\log\log x-\delta_4}{\log(q_0^3)}$. Since x is larger than q_0^3, we therefore have

$$q(dr_0^3,p_0^3,q_0^3)\geqslant\frac{\frac{r}{2}\log\log(q_0^3)-\delta_4}{\log(q_0^3)}$$

Now one can define $C=2\delta_4$.

The last step is to create infinitely many such triples $(dr_n^3,|p_n|^3,q_n^3)$ satisfying the claim in the theorem. Start with any value $N_0>0$ and take a triple $(dr_0^3,\,q_0^3,\,p_0^3)$ corresponding to a shortest vector $\boldsymbol{x_0}$. Then let $N_1>N_0$ grow. By Minkowski and the fact that the determinant of L_{N_1} is equal to $R\sqrt{N_1}$, the shortest nonzero vector of L_{N_1}, denoted $\boldsymbol{x_1}$, satisfy

$$q(\boldsymbol{x_1})\leqslant(r+1)(R\sqrt{N_1})^{\frac{2}{r+1}}=(r+1)R^{\frac{2}{r+1}}N_1^{\frac{1}{r+1}}.$$

But if $\boldsymbol{x_1}=\boldsymbol{x_0}$, the value of N_1 cannot grow too large, since $q(\boldsymbol{x_0})$ will grow linear with N_1 and hence will fall outside the upper bound from Minkowski. So the vector $\boldsymbol{x_1}$ gives rise to another ABC-triple $(dr_1^3,|p_1|^3,q_1^3)$. Now there is an $N_2>N_1$ such that $\boldsymbol{x_1}$ is not the shortest nonzero vector of L_{N_2}, so L_{N_2} has another nonzero shortest vector $\boldsymbol{x_2}$, giving rise to another ABC-triple $(dr_2^3,|p_2|^3,q_2^3)$, etcetera. This process can be continued infinitely many times, getting the infinite sequence of ABC-triples satisfying the claim in the theorem. □

Corollary 4.2. *Let d, E_d, r and $P_1,\ldots,P_r$ be as in the main theorem. Then for all $\delta>0$ there are infinitely many ABC-triples $(A_n,B_n,C_n)=(dr_n^3,-p_n^3,q_n^3)$ with $n\geqslant 0$ where $(p_n\colon q_n\colon r_n)\in E_d$ with integer coordinates and $\gcd(p_n,q_n,r_n)=1$ for all $n\geqslant 0$, such that*

$$q(A_n,B_n,C_n)>1+\frac{r\log\log C_n}{2\log C_n}(1-\delta)$$

Proof. For any $\delta > 0$ one has

$$1 + \frac{r \log\log(q_0^3) - C}{2\log(q_0^3)} \geqslant 1 + \frac{r\log\log(q_0^3)}{2\log(q_0^3)}(1-\delta)$$

if q_0 is sufficiently large. □

One also can be interested in the value of q_0 one has to start with to satisfy the claim for a certain δ. To find such a q_0 one has to start with an N_0 such that the inequality above holds, hence such that the disturbing negative number from the proof of the Main Theorem

$$-\delta_4 = -\log R - \frac{r}{2}\log(3(r+1)) + \log(1-\delta_1) - \log(3r(d)\alpha_d\sqrt{r+1}) - \log\Big(1+\delta_3\Big)$$

is absolutely small compared to $3(r+1)R^{\frac{2}{r+1}}N_0^{\frac{1}{r+1}}(1+\delta_3)$. This happens when

$$\frac{r}{2}\log(3(r+1)R^{\frac{2}{r+1}}N_0^{\frac{1}{r+1}}(1+\delta_2)) - \delta_4 > \frac{r}{2}\log(3(r+1)R^{\frac{2}{r+1}}N_0^{\frac{1}{r+1}}(1+\delta_3))(1-\delta).$$

This inequality is equivalent with each of the following inequalities:

$$\begin{aligned}
\left(\frac{r}{2}\log\left(3(r+1)R^{\frac{2}{r+1}}N_0^{\frac{1}{r+1}}\right)\right)\delta &> \delta_4,\\
\log\left(3(r+1)R^{\frac{2}{r+1}}N_0^{\frac{1}{r+1}}\right) &> \frac{2\delta_4}{r\delta},\\
3(r+1)R^{\frac{2}{r+1}}N_0^{\frac{1}{r+1}} &> e^{\frac{2\delta_4}{r\delta}},\\
N_0 &> \frac{e^{\frac{2(r+1)\delta_4}{r\delta}}}{(3(r+1))^{r+1}R^2}\\
&= \frac{\left(R\cdot(3(r+1))^{\frac{r}{2}}\cdot\frac{1+\delta_3}{1-\delta_1}\cdot 3r(d)\alpha_d\sqrt{r+1}\right)^{\frac{2(r+1)}{r\delta}}}{(3(r+1))^{r+1}R^2}\\
&= R^{\frac{2(r+1)-2r\delta}{r\delta}}\left(\frac{1+\delta_3}{1-\delta_1}\cdot\alpha_d r(d)\right)^{\frac{2(r+1)}{r\delta}} 3^{\frac{(r+1)(1-\delta)}{\delta}}(r+1)^{\frac{(r+1)(1+r-r\delta)}{r\delta}}
\end{aligned}$$

After discovering the first vector $\boldsymbol{x_0}$ associated with a chosen N_0 satisfying the inequality above, one can proceed as in the end of the proof of the Main Theorem to find infinitely many such triples.

Remark 4.3. There are several issues to note.

a) One also can be interested in the *merit* (see definition 2.1 part 2) of such a constructed ABC-triple. This merit is equal to

$$\begin{aligned}
m(A_n,B_n,C_n) &= (q(A_n,B_n,C_n)-1)^2\cdot(\log C_n)\cdot\log\log C_n\\
&\geqslant \left(\frac{r\log\log(q_n^3)-C}{2\log(q_n^3)}\right)^2\cdot(\log(q_n^3))\cdot\log\log(q_n^3)\\
&= \frac{(r\log\log(q_n^3)-C)^2\cdot\log\log(q_n^3)}{4\log(q_n^3)}
\end{aligned}$$

Or in terms of N_n (and δ_2) from the theorem, the merit is at least

$$m(A_n,B_n,C_n) \geqslant \frac{(r\left(\log(r+1)+\frac{2\log R+\log N_n}{r+1}+\delta_2\right)-C)^2\cdot\left(\log(r+1)+\frac{2\log R+\log N_n}{r+1}+\delta_2\right)}{4(r+1)R^{\frac{2}{r+1}}N_n^{\frac{1}{r+1}}+\delta_2}$$

b) In practice the rank often is very small. Thanks to Noam D. Elkies and Nicolas F. Rochers there are elliptic curves of this family known of rank up to 11, see N). The following table shows the smallest integer $d>0$ for which the elliptic curve $E_d/\mathbb{Q}$ has rank r for $0\leqslant r\leqslant 11$.

rank	smallest known number d
0	1
1	6
2	19
3	657
4	21.691
5	489.489
6	9.902.503
7	1.144.421.889
8	1.683.200.989.470
9	349.043.376.293.530
10	137.006.962.414.679.910
11	13.293.998.056.584.952.174.157.235

So the smallest number d increases quickly when r grows. We want d to be small, so the higher rank curves seems to be not very helpful for finding nice ABC-triples. In addition, for $r\geqslant 4$ it is very hard to find the generators of a curve E_d with rank r. So in chapter 5 I only take examples with $r\leqslant 3$.

In the proof of the Main Theorem I more or less said how the algorithm to find ABC-triples using Elliptic Curves goes. In the following section I explain the algorithm and say something about its complexity.

4.2 The algorithm

The following algorithm gives infinitely many ABC-triples:

1. Pick a number d and define the elliptic curve

$$E_d\colon x^3+y^3=d\cdot z^3 \longleftrightarrow C_d\colon y^2z=x^3-432d^2z^3$$

(with rational zero points $(1\colon -1\colon 0)$ resp. $(0\colon 1\colon 0)$). Find as many linearly independent points of $E_d(\mathbb{Q})$ as possible, and let r be the number of these generators, the (expected) rank of E_d. Denote these points

$$P_1,\ldots,P_r=(x_1\colon y_1\colon 1),\ldots,(x_r\colon y_r\colon 1).$$

2. Pick a number $N_0>0$ and compute a good approximation of

$$\alpha_d=\int_{-\infty}^{\infty}\frac{dt}{\sqrt[3]{d-t^3}^2}$$

and for each point $P_i, 1\leqslant i\leqslant r$, a good approximation of the associated real number

$$\alpha_{d,i}=\frac{\int_{-\infty}^{x_i}\frac{dt}{\sqrt[3]{d-t^3}^2}}{\alpha_d}.$$

These numbers are irrational and $\mathbb{Q}$-linear independent and lie between 0 and 1. Their precision will depend on N_0. Then find a shortest nonzero vector in the lattice $L_{N_0}=\{(a_0,\ldots,a_r)\colon a_i\in\mathbb{Z}\}$ with quadratic form

$$q\colon (a_0,\ldots,a_r)\longmapsto \hat{h}(a_1*P_1+\cdots+a_r*P_r)+N_0(a_0+a_1\alpha_{d,1}+\cdots+a_r\alpha_{d,r})^2$$

and denote this vector $\boldsymbol{x_0} = (a_0, ..., a_r)$. This can be done using LLL with the matrix

$$M_{N_0} = \begin{pmatrix} 0 & ... & 0 & \sqrt{N_0} \\ \langle P_1, P_1 \rangle & ... & \langle P_1, P_r \rangle & \sqrt{N_0}\alpha_{d,1} \\ \vdots & & \vdots & \vdots \\ \langle P_r, P_1 \rangle & ... & \langle P_r, P_r \rangle & \sqrt{N_0}\alpha_{d,r} \end{pmatrix}$$

with standard quadratic form on the lattice generated by this matrix. Here the inner products $\langle P_i,\ P_j \rangle$ are defined as in theorem 3.20 c. For more precision, multiply this matrix with a large scalar M and round the entries of $M \cdot M_{N_0}$ to make them integers.

3. Compute $a_1 * P_1 + \cdots + a_r * P_r \in E_d$ and express this point in coprime integer coordinats $(X : Y : Z)$. Then $X^3 + Y^3 = d \cdot Z^3$. Here X and Y are coprime, hence we have a candidate ABC-triple (A_0, B_0, C_0). Here C_0 is the largest among $|X^3|, |Y^3|, |dZ^3|$ and A_0 and B_0 are the other two among them.
4. Pick an $N_{i+1} > N_i$, $i \geqslant 0$ such that $\boldsymbol{x_i}$ is not the shortest vector in the lattice $L_{N_{i+1}}$ with quadratic form defined as in step 2 in terms of N_{i+1}, and go to step 2.

Theorem 4.4. *Each iteration of this algorithm needs a number of bit operations less than quadratic in the length of the output. This output length is at most linear in* $N^{\frac{1}{r+1}}$.

Proof. To pick d and to find r linearly independent generator points P_1, ..., P_r can be hard to compute, but the computation time of this is constant, independent of N.

Now pick N. The precision of α_d and $\alpha_{d,i}, 1 \leqslant i \leqslant r$ must be given in at least the number of bits N has. This precision easily can be given when computing α_d and $\alpha_{d,i}$ using 3.7.

Next is to find short nonzero vectors of the lattice $L = \mathbb{Z}^{r+1}$ with quadratic form

$$q((a_0, ..., a_r)) = \hat{h}(a_1 * P_1 + \cdots + a_r * P_r) + N \cdot (a_0 + a_1\alpha_{d,1} + \cdots + a_r\alpha_{d,r})^2$$

using the LLL algorithm, see section 2.2. Now I need to determine the complexity of the LLL algorithm applied to this problem. Choose a number $c > \frac{4}{3}$.

1. Check whether the initial flag is c-reduced: Start with the row vectors of $M \cdot M_N$ as basis. To compute M_{N_0} one needs to compute

$$\langle P_i, P_j \rangle = \frac{\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j)}{2}$$

There are $\frac{1}{2}(r+1)(r+2)$ such computations, but that is a constant number. For one computation one needs to compute the height of some point. This can be done right from the definition 3.19 of the canonical height, and this way each iteration of doubling the point adds two bits to the precision. The number of bits the entries of M_N must be given in must be at least equal to the number of bits N is given in, to make the computations required to find the optimal solution being not corrupted. The hard part of this step is to multiply N with a linear combination of the $\alpha_{d,i}$'s, with running time at most quadratic with $\log N$. With Gram Schmidt orthogonalization one checks whether the lattice given by the row vectors of $M \cdot M_N$ is c-reduced, and that goes linear with $\log N$.

2. Select a pivot and reduce the flag: Selecting a pivot, if any, takes at most $r + 1$ checks. Then changing the basis goes by finding a new vector $\boldsymbol{b'_{j,2}}$ computed using $\frac{\langle \boldsymbol{b_{j,1}}, \boldsymbol{b_{j,2}} \rangle}{\langle \boldsymbol{b_{j,2}}, \boldsymbol{b_{j,2}} \rangle}$, where computing the denominator is easy after computing the numerator, since it is one computation from part 1. One such interation multiplies the size of the flag by a factor at most $\frac{1}{c} + \frac{1}{4} = \frac{4+c}{4c}$, hence the number of iterations needed is logarithmic in the size of the original flag.
3. If we have our c-reduced flag with first basis element $\boldsymbol{b_1}$, the shortest vector is in the box

$$\left\{ \sum_{i=1}^{r+1} r_i \boldsymbol{b_i} : |r_i| \leqslant c^{\frac{r}{2}} \left(\frac{3c}{4} \right)^{r+1-i}, 1 \leqslant i \leqslant r+1 \right\}$$

This box has at most

$$\prod_{i=1}^{r+1}\left(1+2\cdot c^{\frac{r}{2}}\left(\frac{3c}{4}\right)^{r+1-i}\right)<2^{r+1}c^{r^2}$$

elements, where the last inequality is a rough estimate. For each vector $\boldsymbol{x}=(a_0,...,a_r)$ in the box we can just compute $(a_0,...,a_r)\cdot M_N\cdot(a_0,...,a_r)^\top$ and check whether this number is minimal. The running time of one such computation is linear with $\log N$. There are less than $2^{r+1}c^{r^2}$ such computations, a constant number.

After finding the optimal solution $(a_0,...,a_r)$ one needs to compute the coordinates of the point

$$a_1*P_1+\cdots+a_r*P_r$$

with canonical height at most linear with $N^{\frac{1}{r+1}}$. So the size of the output is linear with $N^{\frac{1}{r+1}}$, but the numbers are computed with multiplication of other numbers with size linear with $N^{\frac{1}{r+1}}$. Hence to compute the coordinates one needs a number of bit operations at most quadratic with the length of the output.

If we have the shortest vector, and have computed in the previous step what candidate ABC-triple (A,B,C) is associated with this, the final step is to do trial division on $\sqrt[3]{\frac{A}{d}}$, $\sqrt[3]{B}$ and $\sqrt[3]{C}$ and the computation of each trial has a running time linear with the size of these numbers, hence is at most linear with $N^{\frac{1}{r+1}}$.

So adding all this together the running time is at most quadratic with $N^{\frac{1}{r+1}}$. □

Remark 4.5. The hard part of this algorithm is the multiplication of two large numbers. Intuitively this has complexity quadratic with the size of this numbers, but there are known algorithms which goes much faster than that.

The constant factor $2^{r+1}\cdot c^{r^2}$ can be avoided when one is happy with an approximate optimal solution rather than the optimal solution. But this weakens the estimate of the quality of the discovered candidate ABC-triples compared with the Main Result.

Sometimes one is not interested in an infinite sequence, but only in one or a few ABC-triples. And often one wants N to be chosen in a specific way to satisfy some condition on the resulting ABC-triple. The following problems can occur when d and E_d are given:

Find an ABC-triple (A, B, C) of bounded size: Suppose we want to have $\log C\leqslant Q$. Then use from the proof of the Main Theorem that for any given N,

$$\hat{h}(a_1*P_1+\cdots+a_r*P_r)\leqslant(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}=Q$$

So it often suffices to take $N=\frac{Q^{r+1}}{(r+1)^{r+1}R^2}$, but in rare cases the optimal solution from there gives a larger logarithmic height (due to the error term $\mathcal{O}(1)$.) But in that case, the discovered ABC-triple has a small value for $|a_0+a_1\alpha_{d,1}+\cdots+a_r\alpha_{d,r}|$ and is accidently a nice ABC-triple.

Find an ABC-triple (A, B, C) with a small value for $\frac{A}{C}$: Suppose we want $\frac{A}{C}<\varepsilon$. Then by lemma 3.10, we want $|a_0+a_1\alpha_{d,1}+\cdots+a_r\alpha_{d,r}|<\frac{\varepsilon}{3\alpha_d d}+\mathcal{O}(1)$. During the proof of the Main Theorem we got

$$|a_0+a_1\alpha_{d,1}+\cdots+a_r\alpha_{d,r}|\leqslant\sqrt{r+1}\cdot R^{\frac{1}{r+1}}N^{\frac{-r}{2r+2}}=\frac{\varepsilon}{3\alpha_d d}$$

so it often suffices to take

$$N=(\frac{3\alpha_d d\sqrt{r+1}R^{\frac{1}{r+1}}}{\varepsilon})^{\frac{2r+2}{r}}=\frac{(3\alpha_d d)^{\frac{2r+2}{r}}(r+1)^{\frac{r+1}{r}}R^{\frac{r}{2}}}{\varepsilon^{\frac{2r+2}{r}}}$$

In rare cases the distance can be larger, but then the height is very small, also giving a nice, small ABC-triple.

Find an ABC-triple (A, B, C) with a large merit: To optimize the merit

$$m(A_0,B_0,C_0)\geqslant\frac{(r\log\log(p_0^3)-C)^2\cdot\log\log(p_0^3)}{4\log(p_0^3)}$$

where C is the disturbing factor from the Main Theorem, one takes the derivative of this real-valued function w.r.t. $\log(p_0^3)$ to get

$$\frac{2(r\log\log(p_0^3)-C)(\log\log(p_0^3))+(r\log\log(p_0^3)-C)^2-(r\log\log(p_0^3)-C)^2\cdot\log\log(p_0^3)}{4(\log(p_0^3))^2}$$

and finds a value of $\log(p_0^3)$ such that this function equals 0. Then one recalls that

$$\log(p_0^3)\leqslant(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}+\delta_1$$

and takes $N=2\cdot\frac{(\log(p_0^3))^{r+1}}{(r+1)^{r+1}R^2}$. This factor 2 is required since we have

$$\log(p_0^3)+\frac{3\alpha_d|p_0|}{|r_0|}\leqslant(r+1)R^{\frac{2}{r+1}}N^{\frac{1}{r+1}}+\delta_1$$

and can expect to both terms on the left hand side to have the same size.

4.3 Some other results

The main result is not the only result I got from my method. In this section I give some other results I got in my research.

4.3.1 Expanding the family of elliptic curves

Until now I only looked at elliptic curves of the shape $X^3+Y^3=d\cdot Z^3$, but this family can be expanded to the family of elliptic curves

$$E_{a,b,c}\colon a\cdot X^3+b\cdot Y^3+c\cdot Z^3=0$$

But such a curve is only elliptic over $\mathbb{Q}$ when there is a rational point given. The unique real point with z-coordinate 0, denoted $P_z=(x_0\colon y_0\colon 0)$, is in general not rational anymore since we need the cubic root of some integers. However, some of these elliptic curves have a rational point with nonzero coordinates. If we denote this point P_0, we have from section 3.1:

$$P+_{P_0}Q=P+_{P_z}Q+_{P_z}(-P_0)$$

where " $+_{P_z}$ " means adding with respect to P_z, still possible over $\mathbb{R}$. To show that if such a point P_0 exists, there are more points in $E_{a,b,c}/\mathbb{Q}$, use that P_0 is not an inflection point. So the tangent line on P_0 intersects $E_{a,b,c}$ on another point, say P. Since the coordinates of P_0 are nonzero, we can use affine coordinats and denote $P_0=(x_0,y_0)$. Then the tangent line satisfies

$$y=-\frac{a\cdot x_0^2}{b\cdot y_0^2}x+y_0+\frac{a\cdot x_0^3}{b\cdot y_0^2}$$

To find the intersection point with $E_{a,b,c}$ we need to solve the cubic equation

$$(a-\frac{a^3x_0^6}{b^2y_0^6})x^3+3b(\frac{a^2x_0^4}{b^2y_0^4}(y_0+\frac{a\cdot x_0^3}{b\cdot y_0^2}))x^2+\cdots=0$$

where the coefficients of x^1 and x^0 are not important since we already know that x_0 is a double solution of this equation. So the solution x_1 can be read from the first two coefficients of this equation. By doing the same reversing x and y by all instances we also get y_1:

$$(x_1,y_1)=(2x_0+\frac{3a\cdot x_0^4}{b\cdot y_0^3-a\cdot x_0^3},2y_0+\frac{3b\cdot y_0^4}{a\cdot x_0^3-b\cdot y_0^3})$$

These are rational functions in x_0 and y_0 hence prove that $P=(x_1,\,y_1)\in E_{a,b,c}(\mathbb{Q})$. It is likely that P is of infinite order in $E_{a,b,c}(\mathbb{Q})$, but if we are unlucky, P is a torsion point.

Also in $E_{a,b,c}$ one can try to approximate P_z with a linear combination of generator points $P_1, ..., P_r$ trying to find integers $a_1, ..., a_r$ such that

$$a_1 * P_1 +_{P_0} \cdots +_{P_0} a_r * P_r$$

lie close to P_0. So one can associate α_1, ..., $\alpha_r \in \mathbb{R}/\mathbb{Z}$ to the generating points and associate another $\alpha \in \mathbb{R}/\mathbb{Z}$ to P_z and try to find $a_0, ..., a_r \in \mathbb{Z}$ such that

$$|a_0 + a_1\alpha_1 + \cdots + a_r\alpha_r - \alpha|$$

is as small as possible. This can be done in the same way as done before, but here we use the invariant differential $\omega = \frac{dx}{3b \cdot y^2} = \frac{dy}{3a \cdot x^2}$. So we take the isomorphism

$$\begin{aligned} \varphi\colon E_{a,b,c} &\longrightarrow \mathbb{R}/\mathbb{Z} \\ (x\colon y\colon 1) &\longmapsto \frac{\int_{x_0}^{x} \frac{dt}{\sqrt[3]{b(c-a\cdot t^3)^2}}}{\int_{-\infty}^{\infty} \frac{dt}{\sqrt[3]{b(c-a\cdot t^3)^2}}} \\ P_z &\longmapsto \frac{\int_{x_0}^{\infty} \frac{dt}{\sqrt[3]{b(c-a\cdot t^3)^2}}}{\int_{-\infty}^{\infty} \frac{dt}{\sqrt[3]{b(c-a\cdot t^3)^2}}} \end{aligned}$$

where we now in the numerator have the lower border at x_0 so the integral is negative when $x < x_0$. This isomorphism preserves the group law with respect to P_0.

But surprisingly, proven results for irrational α for this problem are very weak. We only know

Theorem 4.6. *For all $\varepsilon > 0$ and given $\mathbb{Q}$-linear independent reals α, α_1, ..., α_r there is an integer solution $x_1, ..., x_r, y$ such that*

$$|\alpha_1 x_1 + \cdots + \alpha_r x_r + y - \alpha| < \varepsilon$$

This theorem follows immediately from the fact that the set $\{\alpha_1 x_1 + \cdots + \alpha_r x_r \colon x_1, ..., x_r \in \mathbb{Z}\}$ is dense in $\mathbb{R}$. But this isn't very helpful when finding nice ABC-triples. Note that P_z is of infinite order with respect to P_0 if and only if P_0 is of infinite order with respect to P_z.

4.3.2 Approximate other points

Until now we only looked at the possibilities when approximating the point 0_E, but it can be possible to approximate other points. However, also this problem leads to the approximation of a given real number α by a linear combination of given reals $1, \alpha_1, ..., \alpha_r$. But if we approximate a torsion point, hence a rational number α, the theory required for the main result still works. This can be done by finding an approximate linear dependence of α, $\alpha_{d,1}$, ..., $\alpha_{d,r}$ where α is a given rational number rather than 1. If one finds a solution (a_0, a_1, ..., a_r) with a_0 such that $\alpha a_0 \in \mathbb{Z}$, then we have a solution of the original problem. Actually such a solution can be better since the determinant is smaller: It is multiplied with α since for determining the determinant one can start with a map

$$(a_0, a_1, ..., a_r) \longmapsto (\alpha a_0, a_1, ..., a_r)$$

of determinant α. In practice this improvement only works for $\alpha = \frac{1}{3}$ or $\alpha = \frac{1}{2}$.

To see it for the case $\alpha = \frac{1}{3}$ is easy: Then one approximates the point $(0\colon \sqrt[3]{d}\colon 1)$ or $(\sqrt[3]{d}\colon 0\colon 1)$ and this time not the z-coordinate becomes small but either the x-coordinate or the y-coordinate. Since we also can take minus the solution, we can assume without loss of generality that we approximate $(0\colon \sqrt[3]{d}\colon 1)$. Assume we have discovered a solution $(a_0, ..., a_r)$ such that

$$|\frac{a_0}{3} + a_1\alpha_{d,1} + \cdots + a_r\alpha_{d,r}| \leqslant \sqrt{r+1}(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{1}{r+1}} N^{\frac{-r}{2r+2}}$$

Then we are at an affine point (x, y) with

$$|x| = \sqrt{r+1}(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{1}{r+1}} N^{\frac{-r}{2r+2}} (\varphi_d^{-1})'(\frac{1}{3})(1-\delta) = \sqrt{r+1}(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{1}{r+1}} N^{\frac{-r}{2r+2}} 3\alpha_1 \sqrt[3]{d}(1-\delta)$$

where the equality follows from proposition 3.11 and its proof. Note that α_1 is the real period of the elliptic curve $E_1\colon x^3+y^3=1$. We also have

$$\hat{h}(a_1*P_1+\cdots+a_r*P_r)\leqslant(r+1)(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{2}{r+1}}N^{\frac{1}{r+1}}$$

we get an ABC-triple with quality of the form

$$\begin{aligned}
&\frac{\log C}{\log r(A\cdot B\cdot C)}\\
\geqslant\ &\frac{3\hat{h}(a_1*P_1+\cdots+a_r*P_r)}{3\hat{h}(a_1*P_1+\cdots+a_r*P_r)-\log(\frac{1}{\sqrt{r+1}}(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{-1}{r+1}}N^{\frac{r}{2r+2}}\frac{1}{3\alpha_1\sqrt[3]{d}}(1-\delta))+\log d}\\
\geqslant\ &1+\frac{\log(\frac{1}{3\alpha_1\sqrt[3]{d}\sqrt{r+1}}(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{-1}{r+1}}N^{\frac{r}{2r+2}}(1-\delta))}{(r+1)(\frac{1}{3}R(E_d/\mathbb{Q}))^{\frac{2}{r+1}}N^{\frac{1}{r+1}}}\\
\geqslant\ &1+\frac{\frac{r}{2}\log\log C}{\log C}(1-\delta_0)
\end{aligned}$$

where for any $\delta_0>0$ there is an $M>0$ such that all $N>M$ gives an optimal solution $(a_0,...,a_r)$ satisfying the inequality above. So in fact I can try to approximate three points rather than one point.

The case $\alpha=\frac{1}{2}$ works differently. Here we find a point $(x,\,y)$ where $x\approx y\approx\sqrt[3]{\frac{d}{2}}$. This does not necessary give rise to an ABC-triple, but with the aid of a *transfer* (see section 2.3) there may appear a possible nice ABC-triple. The starting triple clearly has $A\approx B$ (since both x and y are positive) so a transfer involving $B-A$ can be useful. To determine $B-A$ it is useful to notice that around the 2-torsion point we have

$$x-\sqrt[3]{\frac{d}{2}}\approx\sqrt[3]{\frac{d}{2}}-y$$

so it suffices to determine $(\varphi_d^{-1})'(\sqrt[3]{\frac{d}{2}})$ what already is determined in proposition 3.11: It is equal to

$$\frac{\int_{-\infty}^{\infty}\frac{dt}{\sqrt[3]{d-t^3}^2}}{(\frac{2}{d})^{\frac{2}{3}}}=3\alpha_d\sqrt[3]{\frac{d}{2}}^2=3\alpha_2\sqrt[3]{\frac{d}{2}}$$

with α_2 being the real period of E_2. So let n be the degree of a sharp transfer polynomial involving $B-A$. Then for all $\delta_1>0$ there is an $M>0$ such that all $M>N$ yield a solution $(a_0,...,a_r)$ satisfying

$$\begin{aligned}
&\frac{\log C}{\log\operatorname{rad}(ABC)}\\
\geqslant\ &\frac{3n\cdot\hat{h}(a_1*P_1+\cdots+a_r*P_r)}{3n\cdot\hat{h}(a_1*P_1+\cdots+a_r*P_r)+\log d-\log\left(\frac{1}{3\sqrt[3]{\frac{d}{2}}\alpha_2\sqrt{r+1}}(\frac{1}{2}R(E_d/\mathbb{Q}))^{\frac{-1}{r+1}}N^{\frac{r}{2r+2}}(1-\delta)\right)}\\
\geqslant\ &1+\frac{\frac{r}{2n}\log\log C}{\log C}(1-\delta_1)
\end{aligned}$$

So this is a weaker result, since we must take $n\geqslant 2$. In section 2.3 there are given transfers involving $B-A$ of degree $n=2$. However, such transfers can make ABC-triples in new special form. If for example the transfer $((A-B)^2,\,4AB,\,(A+B)^2)$ is taken, then $(A-B)^2$ is a small square number, 4AB is 4 times a cube, and $(A+B)^2$ is d^2 times a sixth power.

But there is also the possibility of a *linear* transfer. Since the order 2 point is approximated, if we write the curve in Weierstrass form, the y-coordinate comes close to 0. Recall the isomorphism

$$\sigma_d^{-1}\colon(x\colon y\colon z)\longmapsto(12d\cdot z\colon 36d(x-y)\colon x+y)$$

Then we have got an equality

$$(x+y)(36d(x-y))^2 = (12d\cdot z)^3 - 432d^2(x+y)^3$$

This equality tells that $(12d\cdot z)^3$ is divisible by $x+y$ and indeed by $x^3+y^3 = d\cdot z^3$ we have

$$(12d\cdot z)^3 = 1728d^2(d\cdot z^3) = 1728d^2(x+y)(x^2-x\cdot y+y^2)$$

So after dividing each side by an additional factor $432d^2$ the triple restricts to

$$3(x-y)^2 = 4(x^2-x\cdot y+y^2) - (x+y)^2$$

for some arbitrary selected $x \approx y$. But even when $(x-y)^2 = 1$ the radical of this triple is of degree 3 so the expected quality of such a candidate ABC-triple goes at best to the too low value of $\frac{2}{3}$. But it is a sharp polynomial transfer and can be interesting in de sense of section 2.3.

4.3.3 Fixing coordinates, varying the curve

Another different way to search for ABC-triples is to fix some properties of the coordinates and changing d such that these properties work optimal. The best way to explain this is with an example:

An alternative way to approximate a 3-torsion point is to take $x=1$. Then we have the point

$$P = (1\colon y_0\colon 1) \in E_{y_0^3+1}\colon x^3+y^3 = (y_0^3+1)z^3$$

The larger y_0 is, the closer P is to the 3-torsion point with $x=0$, hence the closer $3*P$ is to $0_{E_{y_0^3+1}}$. By the first part of the proof of proposition 3.11 the distance between $\varphi_d((0\colon \sqrt[3]{d}\colon 1))$ and $\varphi_d((1\colon \sqrt[3]{d-1}\colon 1))$ is approximately equal to

$$\frac{(\frac{1}{\sqrt[3]{d}^2})}{3\alpha_d} = \frac{\sqrt[3]{d}}{3\alpha_1\sqrt[3]{d}^2} = \frac{1}{3\alpha_1\sqrt[3]{d}}$$

hence $|\varphi_d(3*P)| \approx \frac{1}{\alpha_1\sqrt[3]{d}}$. So we can expect $3*P = (x\colon y\colon 1)$ where $|x| \approx \frac{\alpha_1\sqrt[3]{d}}{3\alpha_d} = \frac{\sqrt[3]{d}^2}{3}$. Then we can get an expected quality of at least the shape

$$\frac{\hat{h}(3*P)}{\hat{h}(3*P)+\log d - \log(\frac{\sqrt[3]{d}^2}{3})} \approx \frac{27\log y_0}{28\log y_0} = \frac{27}{28}$$

what seems not good. However, there can be infinitely many y_0 chosen such that $r(y_0^3+1) \leqslant y_0^{\frac{2}{3}}$. For example (see section 2.1) take $y_0 = p^n - 1$ for any $n \geqslant 1$ and prime number p such that p^3+1 is divisible by q^2 with $q > p$. This decreases the radical by a factor y_0 hence pushes the quality just above 1.

Since here we only compute $3*P$ it also is possible to write down the direct formula:

$$3*(1\colon y_0\colon 1) = (y_0^9 - 3y_0^6 - 6y_0^3 - 1\colon -y_0^9 - 6y_0^6 - 3y_0^3 + 1\colon -3y_0^7 - 3y_0^4 - 3y_0)$$

and here one can see directly that the factor y_0 appears in this formula, hence any ABC-triple $(1, y^3, y^3+1)$ can be transferred into a new ABC-triple

$$((y^3+1)(3y^7+3y^4+3y)^3, (y^9-6y^6-3y^3-1)^3, (y^9-3y^6-6y^3-1)^3)$$

and viewing this as polynomials this is a sharp triple in the sense of the theorem from Mason-Stothers: The largest term is of degree 27 and their radical is of degree 28. Substituting $t = y^3$ we get

$$(t(t+1)(3t^2+3t+3)^3, (t^3-6t^2-3t-1)^3, (t^3-3t^2-6t-1)^3)$$

and this also defines a point on a new elliptic curve:

$$(y_0^3 - 3y_0^2 - 6y_0 - 1\colon -y_0^3 - 6y_0^2 - 3y_0 + 1\colon -3y_0^2 - 3y_0 - 3) \in E_{y_0(y_0+1)}\colon x^3+y^3 = y_0(y_0+1)z^3$$

proving the following:

Theorem 4.7. *The rank of the elliptic curve* $E_{d(d+1)}/\mathbb{Q}: x^3+y^3=d(d+1)z^3$ *is nonzero if* $d\geqslant 2$.

Proof. For $d=1$ we get the point $(-9:-9:-9)=(1:1:1)$, the torsion point. For $d\geqslant 2$ there are no torsion points unless $d(d+1)=2x^3$ for some integer x. This is the equation of an Elliptic Curve, so solutions $(x,\, d)$ of this equation are on the Elliptic Curve $(d+\frac{1}{2})^2=2x^3+\frac{1}{4}$. This Elliptic Curve can be transformed linearly into the Elliptic Curve with equation

$$y^2=x'^3+1$$

This curve has rank 0 and the torsion group is of order 6. Each such torsion point $(x',\, y)$ corresponds with a solution $(x,d)=(2x',2y-1)$, where $y\in\{-3,-1,0,1,3\}$. So we only have to look at $y=3$ since in all other cases we don't have $d\geqslant 2$. But when $y=3$, we have $d=5$ and look at the elliptic curve E_{30} whose actual rank is 2.

In all other cases for d, the point $(d^3-3d^2-6d-1:-d^3-6d^2-3d+1:-3d^2-3d-3)$ clearly is of infinite order in $E_{d(d+1)}$, proving that the rank of that curve is at least 1. □

Remark 4.8. Something similar can be done when starting with a point $(-1:\, y_0:\, 1)$ from an ABC-triple $(1,\, y_0^3-1,\, y_0^3)$, and this gives the following results:

$$3*(-1:\, y_0:\, 1)=(y_0^9+3y_0^6-6y_0^3+1:-y_0^9+6y_0^6-3y_0^3-1:3y_0^7-3y_0^4+3y_0)$$
$$(y_0^3+3y_0^2-6y_0+1:-y_0^3+6y_0^2-3y_0-1:3y_0^2-3y_0+3)\in E_{y_0(y_0-1)}: x^3+y^3=y_0(y_0-1)z^3$$

However, when we replace y_0 by y_0+1 in these formula, we get the same results as in the theorem, where each coordinate is multiplied with -1. So this gives no new points on $E_{d(d+1)}$.

The 2-torsion point also can be approximate when varying the elliptic curve:

$$P:=(x_0:\, x_0+1:\, 1)\in E_{x_0^3+(x_0+1)^3}: x^3+y^3=(x_0^3+(x_0+1)^3)z^3$$

Also here we can get close to $0_{E_{x_0^3+(x_0+1)^3}}$: Directly from the duplication formula we get

$$2*P=((x_0+1)(2x_0^3-5(x_0+1)^3):x_0(5x_0^3-2(x_0+1)^3):3x_0^2+3x_0+1)$$

hence a polynomial ABC-triple of degree 12 whose radical is of degree 13. So also this is a sharp transfer from an ABC-triple $(1,x_0,x_0+1)$.

When transferring the initial point $(x:\, x+1:\, 1)$ into Weierstrass form, from the previous trial we got an equation where we fill in x and $x+1$, making it a sharp polynomial equation of one variable:

$$3=4(x^2+x+1)-(2x+1)^2$$

One also could ask whether it is possible to pick another torsion point P_d (with irrational coordinats) such that $n*P_d=0_{E_d}$. Start with $P_1=(x_1:\, y_1:\, 1)$ such that $n*P_1=0_{E_1}$. Then

$$(\sqrt[3]{d}x_1:\sqrt[3]{d}y_1:1)\in E_d$$

of order n. So the x-coordinate and the y-coordinate keep having the same quotient, and $\frac{x_1}{y_1}\notin\mathbb{Q}$. Hence there are infinitely many rationals $p,q\in\mathbb{Z}$ coprime such that

$$|\frac{x_1}{y_1}-\frac{p}{q}|\leqslant\frac{1}{q^2}$$

Now $P=(p:\, q:\, 1)$ is a good approximation of P_d where $d=p^3+q^3$. But the approximation is not good enough:

$$x(n*P_{p^3+q^3})=\mathcal{O}(q^2)\text{ as }q\to\infty$$

hence the disturbing factor p^3+q^3 is of degree 3 while the distance between $n*P_{p^3+q^3}$ and $0_{E_{p^3+q^3}}$ is of degree -2. This has as usual a factor q "too much", but this time we don't have control of the radical of p^3+q^3 since they need to approximate a given number. So this doesn't create nice ABC-triples in general.

Chapter 5
Examples

Recall from the introduction the example

$$7 = 2^3 - 1^3 = \left(\frac{4}{3}\right)^3 + \left(\frac{5}{3}\right)^3$$

So the points $(2:-1:1)$ and $(4:5:3)$ are on the elliptic curve $E_7: x^3+y^3=7z^3$. The real number I associate with $P=(2:-1:1)$ in the sense of theorem 3.6 now is equal to 0.763100196119... and one easily can see that $(4:5:3)=2*P$ is far away from 0_{E_7}. So it doesn't surprise much that the triple $(4^3, 5^3, 7\cdot 3^3)$ is not an ABC-triple. But $4*P=(-1256:1265:183)$ is close to 0_{E_7}. However, $7\cdot 183 = 1281 > 1265$ so at first sight this still doesn't guarantee that we have got an ABC-triple. But $1256 = 2^3\cdot 157$ what makes the quality above 1. Actually,

$$q(7\cdot 183^3, 1256^3, 1265^3) = 1.068879285550...$$

This triple occurs when one chooses $N=10$. So according to the algorithm there will be an $N_1 > N$ such that this triple is not the ABC-triple associated with the shortest vector in the lattice L_{N_1}. In fact $N_1 = 111$ is the smallest integer such that there is a new triple, here associated with $17*P$. The coordinates of this point give rise to an ABC-triple on where each number has at most 169 digits and has a quality of at least 1.001643803949... This is not the best result: When taking $N=500$ one finds that there is an ABC-triple associated with $38*P$ with 842 digits and with quality at least 1.001992020237...

It can be improved when using section 4.3.2. We got $\varphi_7(2*P)\approx\frac{1}{2}$ so we can apply the transfer

$$((A-B)^2, 4AB, (A+B)^2)$$

on $A=5^3$ and $B=4^3$. Since AB is even we don't need to divide by 4 and get

$$q(3721, 32000, 35721) = 1.108428277918...$$

But here $A^3 \approx 2B^3$ so one also could try to apply the transfer above to $2B$. We then lose the profit from $A+B=C=7\cdot 3^3$ but get as reward $A-2B=-3$ having

$$q((5^3-2\cdot 4^3)^2, 4\cdot 5^3\cdot 2\cdot 4^3, (5^3+2\cdot 4^3)^2) = q(9, 64000, 64009)^2 = 1.238644733998...$$

Also 38 is an even number, so we can do the same with $\varphi_7(19*P)\approx\frac{1}{2}$. This way one discovers an ABC-triple with 422 digits each and with quality at least $1.0047u07267854$.

But 7 is not the smallest value for d on which $E_d: x^3+y^3=d\cdot z^3$ has rank $\geqslant 1$. Since we are more interested in $r(d)$ we got as smallest value $r(d)=3$ by taking $d=9$ and define $P=(2:1:1)$. Then $\varphi_9(P) = 0.574182369078...$ hence $54\varphi_9(P)\approx 31$. So by section 4.3.2 it suffices to consider $18*P$. The ABC-triple associated with this point has about 320 digits and a quality of at least 1.009705805844...

We also can look at higher ranks. An interesting case of luck with quadratic divisors comes from the rank 2 curve E_{30}. It has generators $P_1=(163:107:57)$ and $P_2=(289:-19:93)$. So

$$\varphi_{30}(P_1)\approx 0.547976236974..., \varphi_{30}(P_2)\approx 0.679071968111...$$

Note that P_2 itself already generates a nice ABC-triple, since $\varphi_{30}(P_2)\approx\frac{2}{3}$ and one coordinate is equal to 17^2. We already have

$$q(6859, 24130710, 24137569) = 1.347776094029...$$

But $3\varphi_{30}(P_2) = 2.037215904333...$ It creates an ABC-triple of up to 67 digits and with quality of at least 1.029542135303..., a good result compared with the ABC-triple got from $3 * P_1 + 2 * P_2$. Namely, this point creates an ABC-triple of up to 73 digits with quality $\geqslant 1.020554802425...$ but it comes from

$$\varphi_{30}(3 * P_1 + 2 * P_2) = 3.002072647144...$$

more than ten times as close as $3 * P_2$ is to $0_{E_{30}}$.

A more interesting result comes from the rank 3 curve E_{854} with generators $P_1 = (9: 5: 1)$, $P_2 = (685: 291: 74)$ and $P_3 = (29: -11: 3)$ Then using $N = 90000$ one finds

$$\varphi_{854}(-2 * P_1 - 1 * P_2 + 3 * P_3) \approx \frac{1}{2}$$

so the same transfer as above can be applied to the triple created from this point. This creates an ABC-triple of up to 170 digits, and with quality being at least 1.021691571883... When one just takes $-4 * P_1 - 2 * P_2 + 6 * P_3$ one finds an even more interesting ABC-triple with 340 digits and a quality of at least 1.016356735498...

So the method from my thesis does find ABC-triples, but not with very spectacular quality: An ABC-triple with 340 digits already is beaten as long as the quality is below 1.0616...

Bibliography

A) The 'unbeaten' list of ABC-triples as on the site of Dr. Bart de Smit (Universiteit Leiden), http://www.math.leidenuniv.nl/~desmit/abc/index.php?set=1

B) C.L.Stewart & R. Tijdeman, *On the Oesterle-Masser Conjecture*, Monatshefte fur Mathematik, **102** (1986), page 251-257

C) K. Conrad, *Stirling's Formula*, http://www.math.uconn.edu/~kconrad/blurbs/analysis/stirling.pdf

D) H.J. Lenstra JR., *Lattices (part of Algorithmic Number Theory)*, MSRI Publications **44** (2008), http://www.msri.org/communications/books/Book44/files/06hwl.pdf, page 141

E) H.E. Reijngoud, *Kwaliteit van ABC-drietallen*, Universiteit Leiden (2010), http://www.math.leidenuniv.nl/scripties/Reijngoudback.pdf

F) Vishal Lama, *Mason-Stothers theorem and the ABC-conjecture*, Todd and Vishal's blog (2008, 3rd of march), http://topologicalmusings.wordpress.com/2008/03/03/mason-stothers-theorem-and-the-abc-conjecture/

G) Tim Dokchitser, *LLL and ABC*, J. Number Theory 107 **1** (2004), page 161-167

H) M. Kosters, *Mastermath Algebraic Geometry Spring 2009, course by Bas Edixhoven and Lenny Taelman*, www.math.leidenuniv.nl/~astolk/ag/ag-notes.pdf, Universiteit Leiden, page 45

I) P. Stevenhagen, *Elliptic Curves*, http://math.leidenuniv.nl/~rvl/elliptic/2009/ec.pdf, Universiteit Leiden (2008)

J) J.H. Silvermann, *The Arithmetic of Elliptic Curves*, Graduate Text in Mathematics **106** (1986)

K) N.P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts **41**, p 197-202

L) J.W.S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts **22** (1991), p 52-53

M) R. Hartshorne, *Algebraic Geometry*, Graduate Text in Mathematics **52** (1977), `I` theorem 1.3A, page 4.

N) N.D. Elkies & N.F. Rochers, *Elliptic Curves $x^3 + y^3 = k$ of High Rank*, Harvard University, Cambridge (2004) http://arxiv.org/abs/math.NT/0403116