Some Diophantine equations from finite group theory: $\Phi_m(x) = 2p^n - 1$

Florian Luca (Morelia), Pieter Moree (Bonn)
and Benne de Weger (Eindhoven)

July 20, 2009

Abstract

We show that the equation in the title (with Φ_n the nth cyclotomic polynomial) has no integer solution with $n \geq 1$ in the cases $(m, p) = (15, 41), (15, 5581), (10, 271)$. These equations arise in a recent group theoretical investigation by Z. Akhlaghi, M. Khatami and B. Khosravi.

1 Introduction

In the recent work [1] by Zeinab Akhlaghi, Maryam Khatami and Behrooz Khosravi, some Diophantine equations come up in a group theoretical context. In particular, Zeinab Akhlaghi posed the following problems to us.

- Which primes P of the form $P = 2 \cdot 41^{2a} - 1$ can also be written as $P = \Phi_{15}(q)$, with q a prime power?
- For which primes P of the form $P = 2 \cdot 5581^{2a} - 1$ can an odd power P^b also be written as $P^b = \Phi_{15}(\pm q)$, with q a prime power?
- For which primes P of the form $2 \cdot 271^{2a} - 1$ can an odd power P^b also be written as $P^b = \Phi_{10}(q^2)$, with q a prime power?

Here Φ_m is the mth cyclotomic polynomial. In particular,

$$\begin{aligned} \Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1, \\ \Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1. \end{aligned}$$

Note that $\Phi_{10}(q^2) = \Phi_{20}(q)$.

Typical for Diophantine equations arising in group theory is the occurrence of primes, and so the above present some ‘typical’ examples of equations so arising.

Given a group G, let $\pi(G)$ denote the set of primes q such that G contains an element of order q. Then the prime graph $\Gamma(G)$ of G is defined as the graph G with vertex set $\pi(G)$ in which two distinct primes $q, q' \in \pi(G)$ are adjacent if G contains an element of order qq'. Akhlaghi et al. [1] show, using Theorem 1 below and various already known Diophantine results, that in case p is an odd prime and $k > 1$ is odd, then $\mathrm{PGL}(2, p^k)$ is uniqely characterized by its prime graph, i.e. there is no other group having the same prime graph.

In this paper we will prove the following result, implying the answer "None" to the first problem, and the same for the second and third problem in the case $b = 1$.

Theorem 1. *Let* $(m, p) = (15, 41), (15, 5581),$ *or* $(10, 271)$. *Then the Diophantine equation*

$$\Phi_m(x) + 1 = 2p^n \tag{1}$$

has no integer solutions (n, x) *with* $n \geq 1$.

In the literature, by different methods, some equations of a similar nature have been studied, e.g. the equations $\Phi_m(x) = p^n$ and $\Phi_m(x) = p^n + 1$, with m a prime. The first equation is a special case of the Nagell-Ljunggren equation $(x^m - 1)/(x - 1) = p^n$ and is studied in many papers (for a survey see [2]). For a non-existence result of solutions of the second equation see Le [4].

General results on solutions of equations of the form $f(x) = by^m$ (see the book by Shorey and Tijdeman [7]) imply that for an arbitrary, but fixed $m \geq 3$, equation (1) has finitely many solutions (x, p, n) with $\max\{|x|, p, n\} \leq C$, with C a computable number. Formulated in this generality, C which comes from applying the theory of linear forms in logarithms, will be huge.

In Section 2.1, we give an elementary proof of a lower bound $n \geq 239$, and a related heuristic argument why we do not expect any solutions for these problems. In Section 2.2 we see what information can be obtained by considering (1) modulo a prime number $q \neq p$. As $(x, n) = (0, 0)$ is a solution of (1), we cannot prove Theorem 1 in this way. Nevertheless, some information can be obtained by modular considerations. For the reader only interested in the proof of Theorem 1, this section can be skipped. In Section 3, we use algebraic number theory and a deep result from transcendence theory to deduce an upper bound $n < 2.163 \cdot 10^{27}$ for n satisfying (1). Then in Section 4 the LLL algorithm will be invoked to efficiently reduce this bound to $n \leq 59$. In this way we obtain a rigorous, albeit computational, proof of Theorem 1. We note that our method should work in principle for other equations of the type $f(x) = ap^n$, when f is a fixed polynomial with integral coefficients and at least three distinct roots, $a \geq 1$ is a fixed integer, and p is a fixed prime not dividing the discriminant of f. The nature of our method is algorithmic in the sense that for every single choice of parameters the details of the method have to be worked through separately.

Finally, we like to note that we have preferred to give a rather uniform approach here to answering the above problems. For the third problem (in case $b = 1$), however, an easier, but not so instructive, approach is available. Starting point is the realization that $2y^2 - 1 = \Phi_{10}(x)$ is an elliptic curve. On rewriting it as $y_1^2 = 8(\Phi_{10}(x) + 1)$, and invoking e.g. MAGMA it is found that the first curve has only the integral solutions $(x, y) = (-2, \pm 4), (0, \pm 1), (1, \pm 1)$. In particular it follow from this, that (1) has no solutions with $n \geq 1$ in case $(m, p) = (10, 271)$.

2 Elementary considerations

2.1 p-adic considerations

Without loss of generality we may assume that $|x| \geq 2$ and $n \geq 1$. We write $f_m(x) = \Phi_m(x) + 1$ and $d = \deg f_m$ for $m = 10, 15$. Elementary calculus shows that for all x

$$(|x| - 1)^d < \Phi_m(x) < f_m(x) < (|x| + 1)^d. \tag{2}$$

See e.g. [3] for some similar estimates. We start with seeing what information we can derive from studying the p-adic roots of f_m. If (x, n) is a solution of (1), then there is a root

$$\mathbf{x} = \sum_{k=0}^{\infty} a_k p^k \qquad (\text{with } a_k \in \{0, 1, \ldots, p-1\})$$

of f_m in $\mathbb{Q}_p$ such that $x \equiv \mathbf{x} \pmod{p^n}$. Note that if $a_0 \neq 0$ then the p-adic expansion of $-\mathbf{x}$ is

$$-\mathbf{x} = (p - a_0) + \sum_{k=1}^{\infty} (p - 1 - a_k) p^k.$$

Now (2) with $f_m(x) = 2p^n$ implies that

$$|x| < 2^{1/d} p^{n/d} + 1 < 2p^{n/d},$$

and this immediately implies that, in the case $x > 0$

$$a_k = 0 \text{ for all } k \in \mathbb{N} \text{ with } \lfloor (n+1)/d \rfloor + 1 \leq k \leq n-1,$$

and in the case $x < 0$

$$a_k = p-1 \text{ for all } k \in \mathbb{N} \text{ with } \lfloor (n+1)/d \rfloor + 1 \leq k \leq n-1.$$

In other words, the existence of a solution n of (1) implies that of the first n p-adic digits of the root $\mathbf{x}$, the last consecutive $\approx n(1-1/d)$ all have to be equal to 0 or $p-1$, in respectively the cases $x > 0$ and $x < 0$. This seems unlikely to happen, as can easily be verified experimentally for not too large n. It seems not unreasonable to expect that the p-adic digits of the roots $\mathbf{x}$ are uniformly distributed over $\{0, 1, \ldots, p-1\}$, and that these distributions per digit are independent. Then the probability that $n(1-1/d)$ specific consecutive digits are all 0 respectively $p-1$ is $p^{-n(1-1/d)}$, and the expected number of solutions is at most

$$\sum_{n=1}^{\infty} \frac{1}{p^{n(1-1/d)}} = \frac{1}{p^{(1-1/d)}-1} \ll 1.$$

We conclude that if p is large, then likely there are no solutions. If p is small and there is no solution with n small, then very likely there are no solutions at all.

A minor variation of the above argument suggests that in case $d \geq 3$ there are only finitely many solutions (x, p, n) of (1) with $n \geq 2$. As we already remarked in the introduction, this result is known to be true, see [7].

Explicit computation of the p-adic root $\mathbf{x}$ up to some finite precision is a quick way to rule out small values of n. We now give details for the cases that are of interest to us. Note that p-adic roots of polynomials are quite easy to compute by Hensel lifting (i.e. the p-adic version of the Newton-Raphson method).

In the case $p = 41$ there is one 41-adic root of f_{15}. Its sequence of 41-adic digits is

8, 18, 3, 17, 9, 14, 12, 38, 31, 35, 19, 25, 19, 38, 25, 24, 1, 18, 25, 10, 14, 29, 31, 18, 36, 2, 24, ...

The smallest k such that $a_k = 0$ or 40 is $k = 53$. Hence a solution of (1) implies $k \geq 53$, which in turn implies $\lfloor (n+1)/8 \rfloor + 1 \geq 53$, so $n \geq 415$.

Two remarks are in place. Firstly, we did not even bother to use consecutive zeros, we used only one. Indeed, $a_{54} = 15$, so we could sharpen our result easily. But we have to stop somewhere, and the result $n \geq 415$ is sufficient for the moment. And secondly, it should be noted that the complexity of this method is exponential, as to compute the nth p-adic digit we have to compute with numbers of the size p^n. This makes this method unrealistic for values of n that become larger than a few thousand.

In the case $p = 5581$ there are two 5581-adic roots of f_{15}. Their sequences of 5581-adic digits are

$$\begin{gathered}257,\ 64,\ 5438,\ 1453,\ 629,\ 833,\ 3090,\ 5096,\ 4809,\ 1493,\ 4462,\ 1922,\\ 4807,\ 782,\ 3819,\ 2190,\ 99,\ 2554,\ 3603,\ 4471,\ 1034,\ 1407,\ 3688,\ \ldots\end{gathered}$$

and

$$\begin{gathered}4477,\ 3993,\ 3590,\ 3157,\ 3667,\ 3404,\ 2233,\ 3440,\ 3784,\ 2333,\ 900,\\ 2522,\ 184,\ 1707,\ 5103,\ 2005,\ 5325,\ 1780,\ 4765,\ 2645,\ 3577,\ \ldots\end{gathered}$$

In both cases we computed up to $k = 502$ and did not encounter a 0 or a 5580. As above it follows that $n \geq 4015$.

In the case $p = 271$ there is one 271-adic root of f_{10}. Its sequence of 271-adic digits is

$$\begin{gathered}241,\ 8,\ 147,\ 250,\ 135,\ 263,\ 1,\ 126,\ 89,\ 262,\ 149,\ 20,\ 147,\ 78,\\ 220,\ 219,\ 176,\ 148,\ 206,\ 255,\ 38,\ 115,\ 186,\ 178,\ 235,\ \ldots\end{gathered}$$

The smallest k such that $a_k = 0$ or $a_k = 270$ is $k = 61$. Hence a solution of (1) implies $k \geq 61$, which in turn implies $\lfloor (n+1)/4 \rfloor + 1 \geq 61$, so $n \geq 239$.

Using the above results we infer that on heuristic grounds with probability at most 10^{-1000} equation (1) has a non-trivial solution. Since in mathematics one has to prove assertions beyond 'unreasonable doubt', we cannont conclude our paper at this point.

2.2 Modular considerations

Given a Diophantine equation one of the standard considerations is to reduce the equation modulo a prime number q. It is then a finite problem to find all solutions. If there are no solutions, then the original equation has no solutions. Since we have a solution with $x = 0$ and $n = 0$ of equation (1), it is impossible to prove Theorem 1 by this approach. Nevertheless, let us see what this line of argumentation gives in case $(m, p) = (15, 5581)$. Naturally we have to consider the value set of the cyclotomic polynomials $\Phi_m(x)$. These consist of the values modulo q assumed by $\Phi_m(x)$. Its cardinality we denote by $V_q(\Phi_m)$. More generally, given a polynomial f, by $V_q(f)$ let us denote the number of distinct values assumed by f modulo q. The number $V_q(f)$ is determined by the Galois group G of $f(x)-t$ over $\mathbb{F}_q(t)$ (the arithmetic monodromy group) and over $\bar{\mathbb{F}}_q(t)$ (the geometric monodromy group). In the generic case that both groups equal S_m, the mth symmetric group, one has

$$V_q(f) = \Big(\sum_{k=1}^{m} \frac{(-1)^{k-1}}{k!}\Big)q + O(\sqrt{q}).$$

In case f satisfies the Morse condition, both groups equal S_m. For example, if m is a prime and $q \nmid m(m-1)$, then $\Phi_m(x)$ over $\mathbb{F}_q$ is Morse, and hence both Galois groups are equal to S_m. For m composite, it seems more complicated to calculate these groups. In case $m = 15$ this was kindly done for us by Nick Alexander using the SAGE package Singular, with as outcome that both Galois groups equal S_8 and hence we infer that $V_q(\Phi_{15}) = cq + O(\sqrt{q})$, where

$$c = \frac{3641}{5760} \approx 0.632118\cdots \text{ and } 1 - \frac{1}{e} \approx 0.632120\cdots$$

We raise as a problem computing $V_q(\Phi_m)$ for arbitrary m.

Now let us consider $\langle 5581\rangle$ modulo q. Its cardinality is obviously $r_q := \mathrm{ord}_q(5581)$, where $\mathrm{ord}_q(a)$ denotes the multiplicative order modulo q of a and is equal to the smallest $k \geq 1$ such that $a^k \equiv 1 (\mathrm{mod}\ q)$, where we assume that $q \nmid a$. Now if an element g_1 of $2\langle 5581\rangle$ is not in the value set of $\Phi_{15} + 1$, then we conclude that $n \not\equiv \alpha (\mathrm{mod}\ r_q)$, where α is such that $g_1 \equiv 2 \cdot 5581^{\alpha} (\mathrm{mod}\ q)$. We expect to exclude about $r_q(1-c) \approx r_q/e$ classes mod r_q in this way, which fits well with numerical experiments. In case 5581 is a primitive root modulo q, one excludes $q(1-c) + O(\sqrt{q})$ residue classes modulo $q-1$ for n in this way. On taking $q = 7$ one finds that $3|n$. On taking $q = 37$ one infers that $n \equiv 0 (\mathrm{mod}\ 4)$ or $n \equiv 1 (\mathrm{mod}\ 4)$. On taking $q = 337$ one then concludes that $4|n$. Thus, using modular arguments we conclude that for an integer solution of (1) in case $(m,p) = (15, 5581)$, we have $12|n$. Indeed, if for more general (m,p) a result of the form $n_1|n$ (with n_1 depending on the choice of m and p) can be established by modular arguments, then heuristics suggest that n_1 must be really small.

3 Finding an upper bound

We start with giving some data on relevant algebraic number fields. Then we derive from equation (1) an S-unit inequality, to which we apply transcendence theory to find an explicit upper bound for n.

3.1 Field data

We have

$$\begin{aligned} f_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 2, \\ f_{10}(x) &= x^4 - x^3 + x^2 - x + 2, \end{aligned}$$

and we write equation (1) as

$$f_m(x) = 2p^n, \tag{3}$$

where $(m,p) = (15,41), (15,5581), (10,271)$. For brevity we will refer to these cases as the cases $p = 41, 5581, 271$ or $m = 15, 10$. In Section 2.1, we have seen that $n \geq 239$, and we may assume that $|x| \geq 2$.

The polynomials f_m are irreducible and have no real roots. We label the roots as follows:

root	f_{15}	f_{10}
$\alpha^{(1)}$	$1.0757\ldots{+}0.4498\ldots i$	$0.9734\ldots{+}0.7873\ldots i$
$\alpha^{(2)}$	$0.6243\ldots{+}0.8958\ldots i$	$-0.4734\ldots{+}1.0255\ldots i$
$\alpha^{(3)}$	$-0.1701\ldots{+}1.0292\ldots i$	
$\alpha^{(4)}$	$-1.0299\ldots{+}0.2698\ldots i$	
	$\alpha^{(j)} = \overline{\alpha}^{(j-4)}$ for $j = 5,6,7,8$	$\alpha^{(j)} = \overline{\alpha}^{(j-2)}$ for $j = 3,4$
$\max \lvert\alpha^{(j)}\rvert <$	1.167	1.252

We write $\mathbb{K}_m$ for the field $\mathbb{Q}(\alpha)$ where α is a root of $f_m(x) = 0$, so that $d = \deg f_m = [\mathbb{K}_m : \mathbb{Q}]$, i.e. $d = 8$ for $m = 15$ and $d = 4$ for $m = 10$.

We need a lot of data on these fields. We used Pari [6] to obtain the data given below.

The discriminants of $\mathbb{K}_{15}, \mathbb{K}_{10}$ are respectively $682862912 = 2^6 {\cdot} 83 {\cdot} 128551$ and $1396 = 2^2 \cdot 349$. In both cases α generates a power integral basis. Fundamental units are:

$$\begin{aligned} \text{for } m = 15: \quad & \beta_1 = \alpha^7 + \alpha^4 + \alpha^2 + \alpha - 1, \\ & \beta_2 = \alpha^6 - \alpha^5 + \alpha^4 + \alpha - 1, \\ & \beta_3 = \alpha^2 - \alpha + 1, \\ \text{for } m = 10: \quad & \beta_1 = \alpha^3 - \alpha^2 + 1. \end{aligned}$$

The regulators are $4.2219\ldots, 1.1840\ldots$ respectively. The class groups of both fields is trivial.

The prime decomposition of 2 is

$$\begin{array}{ll} \text{for } m = 15: & 2 = \alpha(\alpha+1)^4(\alpha^3-\alpha^2+1)\beta_1^{-2}\beta_2, \\ \text{for } m = 10: & 2 = -\alpha(\alpha-1)^3\beta_1^{-1}. \end{array}$$

Thus the prime ideals of norm 2 are $(\alpha), (\alpha+1)$ when $m = 15$, and $(\alpha), (\alpha-1)$ when $m = 10$.

The prime decomposition of p in the field $\mathbb{K}_m$ is as follows:
for $p = 41$: $41 = \gamma_1\gamma_2$, where

$$\begin{array}{ll} \gamma_1 = -\alpha^7+\alpha^6+\alpha^5-2\alpha^4+\alpha^3+\alpha^2-\alpha+1, & N(\gamma_1) = 41, \\ \gamma_2 = -4\alpha^7+13\alpha^6-19\alpha^5+8\alpha^4-14\alpha^3+7\alpha^2+15\alpha+1, & N(\gamma_2) = 41^7, \end{array}$$

for $p = 5581$: $5581 = \gamma_1\gamma_2\gamma_3\gamma_4$, where

$$\begin{array}{ll} \gamma_1 = \alpha^6-\alpha^5-2\alpha+1, & N(\gamma_1) = 5581, \\ \gamma_2 = 2\alpha^5+\alpha^2+\alpha+1, & N(\gamma_2) = 5581, \\ \gamma_3 = -3\alpha^7-\alpha^6+7\alpha^5-4\alpha^4-5\alpha^3+7\alpha^2+\alpha+1, & N(\gamma_3) = 5581^2, \\ \gamma_4 = 85\alpha^7-41\alpha^6-112\alpha^5+55\alpha^4-21\alpha^3+ & \\ \qquad\qquad\qquad\qquad +134\alpha^2+92\alpha-135, & N(\gamma_4) = 5581^4, \end{array}$$

for $p = 271$: $271 = \gamma_1\gamma_2$, where

$$\begin{array}{ll} \gamma_1 = -2\alpha^3+4\alpha^2-4\alpha+3, & N(\gamma_1) = 271, \\ \gamma_2 = -18\alpha^3+16\alpha^2+44\alpha+53, & N(\gamma_2) = 271^3. \end{array}$$

3.2 Deriving an S-unit inequality

If x is an integer satisfying (3), then it follows that in $\mathcal{O}_{\mathbb{K}}$ we have

$$(x-\alpha)z = 2p^n$$

for a $z \in \mathcal{O}_{\mathbb{K}}$. Thus, we can write (taking $\gamma_3 = \gamma_4 = 1$ in the cases $p = 41, 271$)

$$x-\alpha = \delta\gamma_1^{n_1}\gamma_2^{n_2}\gamma_3^{n_3}\gamma_4^{n_4}\beta, \qquad z = (2/\delta)\gamma_1^{n-n_1}\gamma_2^{n-n_2}\gamma_3^{n-n_3}\gamma_4^{n-n_4}\beta^{-1},$$

where $\delta \mid 2$ and β is a unit. Taking norms we find

$$2p^n = N(x-\alpha) = N(\delta)p^{c_1n_1+c_2n_2+c_3n_3+c_4n_4},$$

where $(c_1, c_2, c_3, c_4) = (1, 7, 0, 0), (1, 1, 2, 4), (1, 3, 0, 0)$ for respectively $p = 41, 5581, 271$. It follows that $N(\delta) = 2$, and $n = c_1 n_1 + c_2 n_2 + c_3 n_3 + c_4 n_4$.

First observe that $0 < n_i < n$ is impossible. Indeed, for if not, then there exists $k \in \{1, 2, 3, 4\}$ such that $\gamma_k \neq 1$ divides both $x - \alpha$ and z. Observe that if $\alpha = \alpha^{(i)}$, then $z = \prod_{j \neq i}(x - \alpha^{(j)})$. Thus, if $\mathfrak{p}$ is some prime ideal of $\mathcal{O}_{\overline{\mathbb{K}}}$ dividing γ_k, then $\mathfrak{p}$ divides both $x - \alpha^{(i)}$ and $x - \alpha^{(j)}$ for some $j \neq i$. In particular, $\mathfrak{p}$ divides $\alpha^{(i)} - \alpha^{(j)}$, and thus also $\Delta(f_m)$. Since this last number is an integer and $\mathfrak{p}$ has norm a power of p in $\overline{\mathbb{K}}_m$, it would follow that p divides $\Delta(f_m)$, which is not the case. Thus, the only possibilities are $n_i \in \{0, n\}$ for all i. The equation $n = c_1 n_1 + c_2 n_2 + c_3 n_3 + c_4 n_4$ now has only the solutions $(n_1, n_2) = (n, 0)$ in the cases $p = 41, 271$, and $(n_1, n_2, n_3, n_4) = (n, 0, 0, 0), (0, n, 0, 0)$ in the case $p = 5581$.

We get the following equations:

$$\begin{array}{llll} p = 41: & x - \alpha = \pm\delta\gamma^n\beta_1^{m_1}\beta_2^{m_2}\beta_3^{m_3}, & \delta = \alpha, \alpha + 1, & \gamma = \gamma_1, \\ p = 5581: & x - \alpha = \pm\delta\gamma^n\beta_1^{m_1}\beta_2^{m_2}\beta_3^{m_3}, & \delta = \alpha, \alpha + 1, & \gamma = \gamma_1, \gamma_2, \\ p = 271: & x - \alpha = \pm\delta\gamma^n\beta_1^{m_1}, & \delta = \alpha, \alpha - 1, & \gamma = \gamma_1. \end{array} \tag{4}$$

Now we could proceed by conjugating equation (4) and eliminating x to get a unit equation. However, this resulting unit equation will live in the field $\mathbb{Q}[\alpha, \overline{\alpha}]$, which is of degree $d(d-1)$, because the Galois group of $f_m(x)$ over $\mathbb{Q}$ is S_d. Since estimates for linear forms in logarithms are quite sensitive to the degree, we will continue to work in $\mathbb{K}_m$. We proceed as follows. For convenience in the cases $p = 41, 271$ we put $\beta_2 = \beta_3 = 1$ and $m_2 = m_3 = 0$. We have from (4) that

$$z = \frac{2p^n}{x - \alpha} = \pm\left(\frac{2}{\delta}\right)\left(\frac{p}{\gamma}\right)^n \beta_1^{-m_1}\beta_2^{-m_2}\beta_3^{-m_3}. \tag{5}$$

Putting $y = x - \alpha$, Taylor's formula yields $z = \sum_{i=1}^{d} \frac{f_m^{(i)}(\alpha)}{i!} y^{i-1}$, hence

$$\left| z - y^{d-1} \right| = \left| \sum_{i=1}^{d-1} \frac{f_m^{(i)}(\alpha)}{i!} y^{i-1} \right|.$$

Let us now make some estimates. Observe that the lower bound $n \geq 239$ from Section 2.1 is amply sufficient to guarantee $p^n > (2 \cdot 10^{10})^d$. Then (2) implies

$$|y| = |x - \alpha| \geq |x| - |\alpha| > f_m(x)^{1/d} - 1 - |\alpha| > 2^{1/d} p^{n/d} - 2.252 > C_1 p^{n/d}, \tag{6}$$

where $C_1 = 1.090$ when $m = 15$ and $C_1 = 1.189$ when $m = 10$. Hence, $|y| > 2 \cdot 10^{10}$. We now compute upper bounds for $\dfrac{|f_m^{(i)}(\alpha)|}{i!}$, getting

i	1	2	3	4	5	6	7
$\lvert f_{15}^{(i)}(\alpha)\rvert/i! <$	16.40	56.37	109.6	126.7	90.07	39.00	9.489
$\lvert f_{10}^{(i)}(\alpha)\rvert/i! <$	6.977	9.261	5.021				

so that

$$\left|z - y^{d-1}\right| < |y|^{d-2} \sum_{i=1}^{d-1} \frac{f^{(i)}}{i!} \frac{1}{|y|^{d-1-i}} < C_2 |y|^{d-2},$$

where $C_2 = 9.490$ for $m = 15$ and $C_2 = 5.022$ for $m = 10$, because $|y| > 2 \cdot 10^{10}$. Thus,

$$\left|1 - \frac{z}{y^{d-1}}\right| < \frac{C_2}{|y|} < \frac{C_3}{p^{\frac{n}{d}}}, \tag{7}$$

where $C_3 > \dfrac{C_2}{C_1}$, so $C_3 = 8.706$ for $m = 15$ and $C_3 = 4.223$ for $m = 10$. Using equations (4), (5) and (7), we get the S-unit inequality we want:

$$\left|1 - \left(\frac{2}{\delta^d}\right)\left(\frac{p}{\gamma^d}\right)^n \beta_1^{-8m_1}\beta_2^{-8m_2}\beta_3^{-8m_3}\right| < \frac{C_3}{p^{n/d}}. \tag{8}$$

3.3 Applying transcendence theory

We shall apply a linear form in logarithms to bound the expression on the left of inequality (8) from below. We first check that it is not zero. If it were, then since it comes from rewriting the left hand side of inequality (7), we would get that $z = y^{d-1}$. Since $yz = 2p^n$, we get that $y^d = 2p^n$, which violates the prime decomposition of 2 in $\mathbb{K}_m$.

Next, we need to bound m_1, m_2 and m_3 in terms of n. Since $p^{n/d} > 2 \cdot 10^{10}$, it follows from (2) that

$$|y| = |x - \alpha| \le |x| + |\alpha| < f_m(x)^{1/d} + 1 + |\alpha| < 2^{1/d} p^{n/d} + 2.252 < C_4 p^{n/d}, \tag{9}$$

where $C_4 = 1.091$ for $m = 15$ and $C_4 = 1.190$ for $m = 10$. Now we take absolute values of the conjugates of equation (4), and rewrite them as

$$\frac{\left|x - \alpha^{(i)}\right|}{\left|\delta^{(i)}\right| \left|\gamma_1^{(i)}\right|^n} = \left|\beta_1^{(i)}\right|^{m_1} \left|\beta_2^{(i)}\right|^{m_2} \left|\beta_3^{(i)}\right|^{m_3}. \tag{10}$$

We computed:

$$\begin{aligned}
\text{for } p = 41: &\quad 0.2714 < |\delta^{(i)}| < 2.124, \quad 0.5676 < |\gamma^{(i)}| < 5.349,\\
\text{for } p = 5581: &\quad 0.2714 < |\delta^{(i)}| < 2.124, \quad 1.522 < |\gamma^{(i)}| < 5.531,\\
\text{for } p = 271: &\quad 0.7877 < |\delta^{(i)}| < 1.796, \quad 2.253 < |\gamma^{(i)}| < 7.307,
\end{aligned}$$

and thus

$$\max\left(\log\frac{p^{1/d}}{\min|\gamma^{(i)}|}, \log\frac{\max|\gamma^{(i)}|}{p^{1/d}}\right) < C_5,$$
$$\max\left(\log\frac{C_4}{\min|\delta^{(i)}|}, \log\frac{\max|\delta^{(i)}|}{C_1}\right) < C_6,$$

where for $p = 41$ we have $C_5 = 1.213, C_6 = 1.392$, for $p = 5581$ we have $C_5 = 0.6584, C_6 = 1.392$, and for $p = 271$ we have $C_5 = 0.5884, C_6 = 0.4126$. It follows from (6) and (9) that

$$\left|\log\left(\frac{|x-\alpha^{(i)}|}{|\delta^{(i)}|\,|\gamma^{(i)}|^n}\right)\right| < C_5 n + C_6.$$

Writing u_i for the logarithm of the left hand side of equations (10), we get that

$$u_i = m_1 \log\left|\beta_1^{(i)}\right| + m_2 \log\left|\beta_2^{(i)}\right| + m_3 \log\left|\beta_3^{(i)}\right| \quad \text{for three conjugates } i, \tag{11}$$

and hence $|u_i| < C_5 n + C_6$ for all i. If $m = 10$ this simply states $\log\left|\beta_1^{(i)}\right| > 1.184$ (this is the regulator of K_{10}), as then $\beta_2 = \beta_3 = 1$, and thus $|m| < (C_5 n + C_6)/1.184$. If $m = 15$, solving the system (11) with Cramer's rule, we get that

$$\max\{|m_1|, |m_2|, |m_3|\} < \frac{3(C_5 n + C_6)R_2}{R_\beta},$$

where R_2 is the maximal absolute value of all the 2×2 minors of the coefficient matrix appearing in formula (11) whose determinant is R_β. The minor largest in absolute value is the $(2,1)$ minor obtained by eliminating the second row and first column, and its value is $R_2 < 2.746$. Putting all this together gives

$$\max\{|m_1|, |m_2|, |m_3|\} < C_7 n + C_8,$$

where $C_7 = 2.369, C_8 = 2.718$ when $p = 41$, $C_7 = 1.286, C_8 = 2.718$ when $p = 5581$, and $C_7 = 0.4970, C_8 = 0.3485$ when $p = 271$.

The next step is to prepare for the application of a deep result from transcendence theory. We return to inequality (8) and rewrite it as

$$\left|1-\prod_{i=1}^{r}\eta_i^{b_i}\right| < \frac{C_3}{p^{n/d}}, \tag{12}$$

where $r = 5$ when $m = 15$ and $r = 3$ if $m = 10$, and

$$\eta_1 = \frac{2}{\delta^d}, \quad \eta_2 = \frac{p}{\gamma^d}, \quad \eta_3 = \beta_1, \quad \eta_4 = \beta_2, \quad \eta_5 = \beta_3,$$

and $b_1 = 1, b_2 = n, b_3 = -dm_1, b_4 = -dm_2, b_5 = -dm_3$ are integers satisfying

$$B = \max|b_i| < d(C_7 n + C_8).$$

Recall that for an algebraic number η having

$$a_0\prod_{i=1}^{d}(X-\eta^{(i)})$$

as minimal polynomial over the integers, the logarithmic height is defined as

$$h(\eta) = \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d}\log\max\left\{\left|\eta^{(i)}\right|, 1\right\}\right).$$

With this notation, Matveev [5] proved the following deep theorem.

Theorem 2. *Let $\mathbb{K}$ be a field of degree D, $\eta_1, \ldots, \eta_k$ be nonzero elements of $\mathbb{K}$, and $b_1, \ldots, b_k$ integers. Put*

$$B = \max\{|b_1|, \ldots, |b_k|\}$$

and

$$\Lambda = 1 - \prod_{i=1}^{k}\eta_i^{b_i}.$$

Let $A_1, \ldots, A_k$ be real numbers such that

$$A_j \geq \max\{Dh(\eta_j), |\log\eta_j|, 0.16\}, \qquad j = 1, \ldots, k.$$

Then, assuming that $\Lambda \neq 0$, we have

$$\log|\Lambda| > -3\cdot 30^{k+4}(k+1)^{5.5}D^2(1+\log D)(1+\log(kB))\prod_{i=1}^{k}A_i.$$

We apply Matveev's result to get a lower bound on the expression appearing in the left hand side of (12) with $k = r + 1$. We take the field to be our $\mathbb{K}_m$, so $D = d$. We also take η_i, b_i as in (12).

We computed as leading coefficients a_0 of minimal polynomials:

m	δ	η_1	η_2	η_3, η_4, η_5
15	α	$a_0 = 2^7$	$a_0 = p^7$	$a_0 = 1$
	$\alpha + 1$	$a_0 = 2^4$		
10	α	$a_0 = 2^3$	$a_0 = p^3$	$a_0 = 1$
	$\alpha - 1$	$a_0 = 2$		

and for the A_j we found

p	$A_1 <$	$A_2 <$	$A_3 <$	$A_4 <$	$A_5 <$
41	25.02	47.80	4.371	4.247	2.976
5581	25.02	74.22	4.371	4.247	2.976
271	3.988	21.52	2.634		

Thus, by Matveev's bound we have that

$$|\log \Lambda| > -C_9(1 + \log(rB)),$$

where $C_9 > 3 \cdot 30^{r+4}(r+1)^{5.5} d^2 (1 + \log d) A_1 A_2 \ldots A_r$ satisfies

$$\begin{aligned} \text{for } p = 41: &\quad C_9 = 1.465 \cdot 10^{25}, \\ \text{for } p = 5581: &\quad C_9 = 2.275 \cdot 10^{25}, \\ \text{for } p = 271: &\quad C_9 = 1.160 \cdot 10^{18}. \end{aligned}$$

Comparing this with the fact that $B \leq d(C_7 n + C_8)$ and with inequality (12), we get

$$\frac{\log p}{d} n - \log C_3 < -\log|\Lambda| < C_9(1 + \log(rd(C_7 n + C_8))).$$

Concretely:

$$\begin{aligned} \text{for } p = 41: &\quad 0.4641n - 2.165 < 1.465 \cdot 10^{25}(1 + \log(94.80n + 108.8)) \\ &\quad \text{implying } n < N = 2.163 \cdot 10^{27}, \\ \text{for } p = 5581: &\quad 1.078n - 2.165 < 2.275 \cdot 10^{25}(1 + \log(51.45n + 108.8)) \\ &\quad \text{implying } n < N = 1.424 \cdot 10^{27}, \\ \text{for } p = 271: &\quad 1.400n - 1.441 < 1.160 \cdot 10^{18}(1 + \log(5.964n + 4.182)) \\ &\quad \text{implying } n < N = 3.970 \cdot 10^{19}. \end{aligned}$$

4 Reducing the upper bound

So, it remains to solve

$$\left\{\begin{array}{rcl} \left|1-\eta_1\eta_2^n\prod_{i=3}^{r}\eta_i^{-dm_{i-2}}\right| & < & \dfrac{C_3}{p^{n/d}}, \\ \max|m_i| & < & d(C_7n+C_8), \\ n & < & N. \end{array}\right.$$

This is a finite problem, but the upper bound N is way too large to apply brute force or the method from Section 2.1. Efficient methods for solving such problems based on lattice basis reduction using the LLL algorithm exist, see [8], and they work quite well in our case. Here are the details.

We put

$$\lambda_i^{(j)} = \left\{\begin{array}{rl} \log\left|\eta_i^{(j)}\right| & \text{for} \quad i=1,2 \\ -d\log\left|\eta_i^{(j)}\right| & \text{for} \quad i=3,\ldots,r. \end{array}\right. , \quad j=1,\ldots,r-1.$$

Let

$$\lambda^{(j)} = \lambda_1^{(j)} + n\lambda_2^{(j)} + m_1\lambda_3^{(j)} + \ldots + m_{r-2}\lambda_r^{(j)} \quad \text{for } j=1,\ldots,r-1.$$

By (12), the real linear forms $\lambda^{(j)}$ satisfy

$$\left|\lambda^{(j)}\right| \le \left|1-e^{\lambda^{(j)}}\right| \le \left|1-\eta_1^{(j)}\left(\eta_2^{(j)}\right)^n\prod_{i=3}^{r}\left(\eta_i^{(j)}\right)^{-dm_{i-2}}\right| < \frac{C_3}{p^{n/d}}. \qquad (13)$$

We let K be some constant slightly larger than $N^{(r-1)/(r-2)}$, i.e. $N^{4/3}$ when $m=15$ and $r=5$, and N^2 when $m=10$ and $r=3$. We write $\theta_i^{(j)} = \left[K\lambda_i^{(j)}\right]$ for $i=1,\ldots,r$, where $[\cdot]$ denotes rounding to the nearest integer. We put

$$(\lambda')^{(j)} = \theta_1^{(j)} + n\theta_2^{(j)} + m_1\theta_3^{(j)} + \ldots + m_{r-2}\theta_r^{(j)}.$$

Then

$$\left|K\lambda^{(j)} - (\lambda')^{(j)}\right| \le \frac{1}{2} + \frac{n}{2} + \frac{r-2}{2}\max|m_i| < C_{10}n + C_{11},$$

where $C_{10} = \frac{1}{2} + \frac{r-2}{2}dC_7$ and $C_{11} = \frac{1}{2} + \frac{r-2}{2}dC_8$. Then $n \ge N$ implies

$$\left|(\lambda')^{(j)}\right| < K\left|\lambda^{(j)}\right| + C_{10}N + C_{11}. \qquad (14)$$

We now look at the matrix Γ and the vector $\underline{y}$ given as

$$\text{for } m = 15: \qquad \Gamma = \begin{pmatrix} \theta_3^{(i)} & \theta_4^{(i)} & \theta_5^{(i)} & \theta_2^{(i)} \\ \theta_3^{(j)} & \theta_4^{(j)} & \theta_5^{(j)} & \theta_2^{(j)} \\ \theta_3^{(k)} & \theta_4^{(k)} & \theta_5^{(k)} & \theta_2^{(k)} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \underline{y} = \begin{pmatrix} -\theta_1^{(i)} \\ -\theta_1^{(j)} \\ -\theta_1^{(k)} \\ 0 \end{pmatrix},$$

$$\text{where } (i,j,k) \in \{(1,2,3),(1,2,4),(1,3,4),(2,3,4)\},$$

$$\text{for } m = 10: \qquad \Gamma = \begin{pmatrix} \theta_3^{(i)} & \theta_2^{(i)} \\ 0 & 1 \end{pmatrix}, \quad \underline{y} = \begin{pmatrix} -\theta_1^{(i)} \\ 0 \end{pmatrix},$$

$$\text{where } i \in \{1,2\}.$$

Observe that for $\underline{x} = (m_1, \dots, m_{r-2}, n)^T$

$$\Gamma\underline{x} - \underline{y} = \Big((\lambda')^{(i)}, (\lambda')^{(j)}, (\lambda')^{(k)}, n \Big)^T \qquad \text{resp.} \qquad \Big((\lambda')^{(i)}, n \Big)^T.$$

The columns of Γ generate a sublattice of $\mathbb{Z}^{r-2}$. Let $d(\Gamma, \underline{y}) = \min_{\underline{x} \in \mathbb{Z}^{r-2}} \left| \Gamma\underline{x} - \underline{y} \right|$ be the distance from $\underline{y}$ to the nearest lattice point. From (14) we find

$$d(\Gamma, \underline{y}) \le \left| \Gamma\underline{x} - \underline{y} \right| < \sqrt{(r-2)\left(K \max\left|\lambda^{(j)}\right| + C_{10}N + C_{11}\right)^2 + N^2}. \quad (15)$$

Put

$$c = \frac{N^{1/(r-2)}}{K} \left(\sqrt{\frac{d(\Gamma, \underline{y})^2 - N^2}{r-2}} - (C_{10}N + C_{11}) \right).$$

If c happens to be a positive real number, then combining (13) and (15) we get for $\lambda = \lambda^{(j)}$, such that $|\lambda| = \max\left|\lambda^{(j)}\right|$ satisfies

$$cN^{-1/(r-2)} < |\lambda| < \frac{C_3}{p^{n/d}},$$

and hence

$$n < \frac{d}{\log p} \left(\log C_3 - \log c + \frac{1}{r-2} \log N \right).$$

In particular, if c is reasonable, that is, not too tiny, then the above bound is a reduced upper bound for n. We can argue that this is reasonable, because if the lattice is generic, that is, if it satisfies

$$d(\Gamma, \underline{y}) \approx \det(\Gamma)^{1/\dim\Gamma} \approx K^{(r-2)/(r-1)},$$

then with the choice of K being somewhat larger than $N^{(r-1)/(r-2)}$, one would expect that $d(\Gamma, \underline{y})$ is somewhat larger than N, so that c just becomes positive:

$$c \approx \frac{N^{1/(r-2)}}{K} \cdot N \approx 1.$$

Clearly, a lower bound for $d(\Gamma, \underline{y})$ suffices. To compute such a bound we use Lemma 3.5 from [8], which we now state.

Lemma 1. *If $\underline{c}_1, \ldots, \underline{c}_{r-1}$ is an LLL-reduced basis for the lattice spanned by the columns of the matrix Γ, and $(s_1, \ldots, s_{r-1})$ are the coordinates of $\underline{y} \in \mathbb{Z}^{r-1}$ with respect to this basis, then*

$$d(\Gamma, \underline{y}) \geq 2^{-(r-2)/2} \|s_{r-1}\| |\underline{c}_1|,$$

where $\| \cdot \|$ denotes the distance to the nearest integer.

When a new upper N_1 on n is found, the procedure can be repeated with N_1 instead of N.

As for the practical calculations, for $p = 41$ and $p = 5581$ we use $K = 10^{39}$, and for $p = 271$ we use $K = 10^{41}$. For $p = 41$ the conjugates $(i, j, k) = (1, 3, 4)$ turned out to give the best results, and for $p = 5581$ we took the conjugates $(i, j, k) = (2, 3, 4)$ in the case $\gamma = \gamma_1$, and $(i, j, k) = (1, 3, 4)$ in the case $\gamma = \gamma_2$. For $p = 271$ we took the conjugate $i = 2$. The values of the entries of Γ and $\underline{y}$ are given in the appendix.

As a result of our computations we found:

for $p = 41$: $|\underline{c}_1| = 1.148 \ldots \cdot 10^{30}$,
for $\delta = \alpha$: $\|s_4\| = 0.2505\ldots$, $d(\Gamma, \underline{y}) \geq 1.017 \cdot 10^{29}$, $c = 0.0650\ldots$,
for $\delta = \alpha + 1$: $\|s_4\| = 0.0809\ldots$, $d(\Gamma, \underline{y}) \geq 3.286 \cdot 10^{28}$, $c = 0.0125\ldots$.
We infer $n \leq N_1 = 59$.

for $p = 5581, \gamma = \gamma_1$: $|\underline{c}_1| = 1.123 \ldots \cdot 10^{30}$,
for $\delta = \alpha$: $\|s_4\| = 0.4489\ldots$, $d(\Gamma, \underline{y}) \geq 1.784 \cdot 10^{29}$, $c = 0.1119\ldots$,
for $\delta = \alpha + 1$: $\|s_4\| = 0.3512\ldots$, $d(\Gamma, \underline{y}) \geq 1.395 \cdot 10^{29}$, $c = 0.0867\ldots$.
We infer $n \leq N_1 = 23$.

for $p = 5581, \gamma = \gamma_2$: $|\underline{c}_1| = 6.875 \ldots \cdot 10^{29}$,
for $\delta = \alpha$: $\|s_4\| = 0.3849\ldots$, $d(\Gamma, \underline{y}) \geq 9.357 \cdot 10^{28}$, $c = 0.0568\ldots$,
for $\delta = \alpha + 1$: $\|s_4\| = 0.4225\ldots$, $d(\Gamma, \underline{y}) \geq 1.027 \cdot 10^{29}$, $c = 0.0628\ldots$.
We infer $n \leq N_1 = 23$.

$\underline{\text{for } p = 271}$: $|\underline{c}_1| = 2.826\ldots \cdot 10^{20}$,
for $\delta = \alpha$: $\|s_2\| = 0.2302\ldots$, $d(\Gamma, \underline{y}) \geq 4.602 \cdot 10^{19}$, $c = 0.0014\ldots$,
for $\delta = \alpha - 1$: $\|s_2\| = 0.2565\ldots$, $d(\Gamma, \underline{y}) \geq 5.127 \cdot 10^{19}$, $c = 0.0050\ldots$.
We infer $n \leq N_1 = 37$.

All reduced upper bounds are well below the lower bound $n \geq 239$ we had already found in Section 2.1. Hence, the given equations have no positive integer solutions (n, x).

We used the built-in LLL implementation of Mathematica 7.0. The total computation time was about 0.5 second on a standard laptop.

Acknowledgement. We like to thank both N. Bruin and S. Akhtari for sketching other approaches to proving Theorem 1. Both these approaches seem more involved than ours. On the other hand, we cannot exclude that less preliminary considerations on their part would lead to a shorter proof than ours. Also, we thank M. Bennett for some helpful remarks.

The information on value sets given in Section 2.2 was kindly provided to us by D. Wan and N. Alexander.

Work on this paper started during a visit of the first author to the Max-Planck-Institute of Mathematics in the spring of 2009.

References

[1] Z. Akhlaghi, M. Khatami and B. Khosravi, Characterization of $PGL(2, p^k)$, by prime graphs, where $k > 1$, is odd, in preparation.

[2] Y. Bugeaud and M. Mignotte, L'équation de Nagell-Ljunggren $\frac{x^n-1}{x-1} = y^q$, *Enseign. Math.* (2) **48** (2002), 147–168.

[3] G. Drauschke and M. Tasche, Prime factorizations for values of cyclotomic polynomials in $\mathbb{Z}[i]$, *Arch. Math. (Basel)* **49** (1987), 292–300.

[4] M.H. Le, A note on the Diophantine equation $(x^m - 1)/(x - 1) = y^n + 1$, *Math. Proc. Cambridge Philos. Soc.* **116** (1994), 385–389.

[5] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. (Russian) *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), no. 6, 125–180; translation in *Izv. Math.* **64** (2000), no. 6, 1217–1269.

[6] PARI/GP, version `2.3.4`, Bordeaux, 2006, `http://pari.math.u-bordeaux.fr/`.

[7] T.N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, Cambridge, 1986.

[8] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract **65**, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
e-mail: `fluca@matmor.unam.mx`

Pieter Moree
Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.
e-mail: `moree@mpim-bonn.mpg.de`

Benne de Weger
Department of Mathematics and Computer Science,
Eindhoven University of Technology,
PO Box 513, 5600 MB Eindhoven, The Netherlands,
e-mail: `b.m.m.d.weger@tue.nl`

Appendix

The lattices

The entries of the matrices Γ defining the lattices are as follows:

for $m = 15, \delta = \alpha$:

$$\begin{aligned}
\theta_1^{(1)} &= -535\,701\,078\,188\,445\,393\,051\,889\,499\,285\,315\,834\,220\\
\theta_1^{(2)} &= -10\,521\,455\,713\,307\,993\,677\,385\,282\,203\,941\,784\,101\\
\theta_1^{(3)} &= 355\,033\,171\,043\,874\,873\,964\,550\,682\,314\,268\,786\,484\\
\theta_1^{(4)} &= 191\,189\,362\,857\,878\,512\,764\,724\,099\,174\,988\,831\,837
\end{aligned}$$

for $m = 15, \delta = \alpha + 1$:

$$\begin{aligned}
\theta_1^{(1)} &= -5\,333\,047\,497\,874\,799\,261\,155\,020\,173\,693\,482\,953\,059\\
\theta_1^{(2)} &= -4\,250\,022\,567\,236\,740\,912\,821\,155\,978\,113\,906\,762\,299\\
\theta_1^{(3)} &= -1\,540\,575\,842\,877\,807\,282\,174\,111\,433\,652\,517\,111\,903\\
\theta_1^{(4)} &= 11\,123\,645\,907\,989\,347\,456\,150\,287\,585\,459\,906\,827\,261
\end{aligned}$$

for $p = 41$:

$$\begin{aligned}
\theta_2^{(1)} &= -1\,197\,628\,306\,264\,185\,932\,489\,953\,704\,644\,364\,201\,811\\
\theta_2^{(3)} &= -9\,700\,547\,565\,070\,802\,018\,377\,652\,854\,737\,318\,414\,526\\
\theta_2^{(4)} &= 8\,243\,424\,043\,479\,329\,682\,142\,908\,094\,257\,321\,227\,079
\end{aligned}$$

for $p = 5581, \gamma = \gamma_1$:

$$\begin{aligned}
\theta_2^{(2)} &= 5\,263\,605\,697\,123\,944\,704\,135\,127\,379\,599\,885\,704\,579\\
\theta_2^{(3)} &= -2\,963\,152\,790\,434\,752\,959\,027\,304\,664\,082\,271\,081\,924\\
\theta_2^{(4)} &= -3\,947\,334\,581\,756\,113\,011\,114\,453\,716\,363\,543\,662\,171
\end{aligned}$$

for $p = 5581, \gamma = \gamma_2$:

$$\begin{aligned}
\theta_2^{(1)} &= -5\,054\,887\,673\,357\,776\,148\,549\,731\,828\,016\,451\,580\,048\\
\theta_2^{(3)} &= -428\,141\,974\,047\,405\,559\,024\,836\,857\,709\,161\,235\,654\\
\theta_2^{(4)} &= 1\,813\,722\,745\,018\,650\,232\,158\,593\,055\,388\,028\,132\,405
\end{aligned}$$

for $m = 15$:

$$\begin{aligned}
\theta_3^{(1)} &= -12\,304\,678\,543\,120\,429\,319\,016\,409\,568\,929\,653\,779\,543\\
\theta_3^{(2)} &= -5\,175\,490\,583\,287\,403\,600\,999\,179\,581\,345\,876\,700\,402\\
\theta_3^{(3)} &= 1\,315\,339\,656\,720\,872\,223\,605\,488\,041\,323\,010\,300\,861\\
\theta_3^{(4)} &= 16\,164\,829\,469\,686\,960\,696\,410\,101\,108\,952\,520\,179\,084\\
\theta_4^{(1)} &= -6\,491\,857\,667\,627\,931\,313\,552\,738\,347\,206\,761\,471\,914\\
\theta_4^{(2)} &= 2\,839\,823\,311\,449\,225\,025\,315\,462\,816\,154\,576\,105\,761\\
\theta_4^{(3)} &= 14\,146\,641\,173\,722\,516\,215\,599\,502\,471\,468\,729\,095\,500\\
\theta_4^{(4)} &= -10\,494\,606\,817\,543\,809\,927\,362\,226\,940\,416\,543\,729\,347\\
\theta_5^{(1)} &= -161\,428\,308\,887\,546\,310\,612\,673\,805\,712\,708\,268\,679\\
\theta_5^{(2)} &= 11\,901\,276\,304\,984\,011\,058\,128\,117\,013\,664\,970\,112\,594\\
\theta_5^{(3)} &= -2\,614\,169\,460\,911\,830\,182\,254\,627\,350\,998\,769\,663\,233\\
\theta_5^{(4)} &= -9\,125\,678\,535\,184\,634\,565\,260\,815\,856\,953\,492\,180\,682
\end{aligned}$$

for $m = 10, \delta = \alpha$:

$$\theta_1^{(2)} = 20\,573\,051\,403\,432\,594\,483\,552\,713\,981\,506\,015\,700\,526$$

for $m = 10, \delta = \alpha - 1$:

$$\theta_1^{(2)} = -164\,737\,397\,928\,296\,691\,084\,558\,149\,213\,695\,646\,090\,715$$

for $p = 271$:

$$\theta_2^{(2)} = -235\,291\,255\,321\,496\,775\,213\,784\,479\,523\,882\,283\,953\,939$$

for $m = 10$:

$$\theta_3^{(2)} = -473\,639\,142\,381\,457\,478\,770\,121\,733\,659\,580\,922\,571\,619$$

Note that the lattice is the same for both δ's.

The reduced bases

The reduced bases consist of $\underline{c}_1, \ldots, \underline{c}_{r-2}$, as follows:

for $p = 41$:

$$\begin{aligned}
(\underline{c}_1)_1 &= -843\,368\,108\,647\,665\,336\,486\,188\,942\,253\\
(\underline{c}_1)_2 &= 559\,320\,925\,743\,467\,198\,006\,242\,173\,197\\
(\underline{c}_1)_3 &= -216\,383\,108\,330\,870\,212\,927\,002\,535\,916\\
(\underline{c}_1)_4 &= 496\,997\,227\,075\,433\,258\,177\,840\,213\,736\\
(\underline{c}_2)_1 &= 769\,480\,157\,105\,025\,085\,610\,593\,698\,120\\
(\underline{c}_2)_2 &= -662\,868\,868\,597\,435\,011\,284\,138\,490\,262\\
(\underline{c}_2)_3 &= -441\,058\,071\,515\,342\,369\,896\,390\,140\,053\\
(\underline{c}_2)_4 &= 553\,662\,092\,722\,375\,932\,830\,016\,396\,748\\
(\underline{c}_3)_1 &= 1\,155\,341\,406\,784\,529\,993\,021\,845\,712\,621\\
(\underline{c}_3)_2 &= 840\,501\,797\,894\,665\,608\,764\,467\,297\,238\\
(\underline{c}_3)_3 &= 309\,221\,863\,441\,485\,463\,114\,052\,803\,652\\
(\underline{c}_3)_4 &= 88\,295\,819\,881\,082\,922\,448\,465\,078\,569\\
(\underline{c}_4)_1 &= 168\,850\,638\,387\,891\,366\,230\,077\,577\,847\\
(\underline{c}_4)_2 &= 181\,452\,778\,443\,755\,987\,291\,974\,440\,710\\
(\underline{c}_4)_3 &= -1\,260\,179\,394\,564\,692\,820\,585\,182\,354\,202\\
(\underline{c}_4)_4 &= -248\,925\,942\,970\,751\,183\,092\,370\,837\,739
\end{aligned}$$

for $p = 5581, \gamma = \gamma_1$:

$$\begin{aligned}
(\underline{c}_1)_1 &= -872\,546\,237\,539\,535\,752\,706\,428\,843\,319\\
(\underline{c}_1)_2 &= -223\,156\,093\,910\,873\,919\,802\,195\,050\,685\\
(\underline{c}_1)_3 &= -665\,677\,021\,232\,961\,022\,546\,590\,079\,279\\
(\underline{c}_1)_4 &= -94\,687\,160\,788\,259\,520\,945\,395\,183\,066\\
(\underline{c}_2)_1 &= -229\,473\,248\,927\,567\,102\,740\,277\,014\,756\\
(\underline{c}_2)_2 &= 617\,468\,741\,928\,841\,755\,274\,798\,916\,669\\
(\underline{c}_2)_3 &= -543\,563\,619\,528\,735\,973\,870\,401\,294\,450\\
(\underline{c}_2)_4 &= -537\,677\,026\,147\,002\,857\,567\,211\,509\,644\\
(\underline{c}_3)_1 &= 8\,031\,004\,037\,197\,869\,937\,202\,716\,189\\
(\underline{c}_3)_2 &= 938\,093\,837\,932\,029\,873\,000\,709\,129\,402\\
(\underline{c}_3)_3 &= 195\,844\,084\,019\,775\,552\,360\,982\,500\,961\\
(\underline{c}_3)_4 &= 885\,190\,138\,056\,570\,983\,101\,607\,196\,266\\
(\underline{c}_4)_1 &= -950\,859\,499\,566\,648\,889\,250\,675\,739\,630\\
(\underline{c}_4)_2 &= 241\,382\,209\,533\,837\,385\,381\,803\,382\,951\\
(\underline{c}_4)_3 &= 1\,301\,768\,138\,134\,948\,436\,200\,391\,686\,948\\
(\underline{c}_4)_4 &= -486\,686\,546\,347\,026\,084\,492\,973\,627\,149
\end{aligned}$$

for $p = 5581, \gamma = \gamma_2$:

$$\begin{aligned}
(\underline{c}_1)_1 &= -33\,193\,247\,358\,059\,218\,472\,153\,374\,410\\
(\underline{c}_1)_2 &= -87\,912\,309\,797\,970\,325\,116\,462\,454\,668\\
(\underline{c}_1)_3 &= -385\,045\,401\,453\,711\,728\,562\,495\,875\,789\\
(\underline{c}_1)_4 &= 561\,756\,923\,681\,125\,138\,115\,555\,382\,317\\
(\underline{c}_2)_1 &= 837\,832\,987\,097\,082\,927\,861\,574\,573\,535\\
(\underline{c}_2)_2 &= -334\,493\,013\,704\,131\,410\,344\,879\,715\,557\\
(\underline{c}_2)_3 &= -300\,519\,808\,958\,157\,408\,324\,600\,505\,185\\
(\underline{c}_2)_4 &= 150\,629\,549\,282\,709\,200\,215\,988\,361\,882\\
(\underline{c}_3)_1 &= -291\,643\,217\,145\,890\,486\,004\,982\,245\,792\\
(\underline{c}_3)_2 &= -919\,165\,296\,754\,992\,652\,058\,056\,637\,120\\
(\underline{c}_3)_3 &= -632\,210\,387\,744\,580\,417\,281\,335\,093\,914\\
(\underline{c}_3)_4 &= -324\,284\,573\,321\,981\,804\,426\,907\,933\,819\\
(\underline{c}_4)_1 &= 114\,589\,075\,187\,135\,712\,515\,900\,349\,220\\
(\underline{c}_4)_2 &= -1\,775\,169\,784\,941\,313\,515\,682\,421\,428\,402\\
(\underline{c}_4)_3 &= 1\,954\,496\,644\,806\,618\,832\,618\,848\,766\,208\\
(\underline{c}_4)_4 &= 1\,333\,361\,249\,271\,924\,783\,631\,535\,912\,835
\end{aligned}$$

for $p = 271$:

$$\begin{aligned}
(\underline{c}_1)_1 &= -108\,609\,470\,650\,628\,019\,733\\
(\underline{c}_1)_2 &= 260\,932\,521\,991\,777\,346\,329\\
(\underline{c}_2)_1 &= 1\,538\,463\,890\,677\,024\,617\,653\\
(\underline{c}_2)_2 &= 664\,802\,792\,622\,780\,399\,454
\end{aligned}$$