Chapter 7. The sum of two S-units being a square.

7.1. Introduction.

Let $p_1, \ldots, p_s$ ($s \geq 1$) be distinct primes, and let S be the set of positive rational integers which have no prime divisors different from the p_i . A rational number is called an *S-unit* if its absolute value is a quotient of elements of S . Thus the set of S-units is

$$\{ \pm p_1^{x_1} \cdot \ldots \cdot p_s^{x_s} \mid x_i \in \mathbb{Z} \text{ for } i = 1, \ldots, s \} .$$

We study the diophantine equation

$$x + y = z^2$$

in x, y S-units, and $z \in \mathbb{Q}$, where the set of primes $p_1, \ldots, p_s$ is given. We show how to find all solutions of this equation, using the theory of p-adic linear forms in logarithms, and a computational p-adic diophantine approximation method. We actually perform all the necessary computations for solving the equation completely for $\{ p_1, \ldots, p_s \} = \{ 2, 3, 5, 7 \}$.

We start with getting rid of the denominators. Let x, y, z be a solution. There is a $d \in S$ such that $|d \cdot x|$, $|d \cdot y| \in S$. Put $d = d_1 \cdot d_2^2$, where $d_1, d_2 \in S$ and d_1 squarefree. Then

$$d_1 \cdot d \cdot x + d_1 \cdot d \cdot y = (d_1 \cdot d_2 \cdot z)^2 ,$$

which has the same form as $x + y = z^2$, but now $|d_1 \cdot d \cdot x|$, $|d_1 \cdot d \cdot y| \in S \subset \mathbb{Z}$ and $d_1 \cdot d_2 \cdot z \in \mathbb{Z}$. Without loss of generality we may therefore study

$$x + y = z^2 , \tag{7.1}$$

where

$$\begin{cases} x \in S , \quad \pm y \in S , \quad z \in \mathbb{Z} , \\ x \geq y , \quad z > 0 , \\ (x,y) \text{ is squarefree} . \end{cases} \tag{7.2}$$

We shall prove the following results.

THEOREM 7.1. *Let* $p_1, \ldots, p_s$ *be given. There exists an effectively computable constant* C , *depending on* $p_1, \ldots, p_s$ *only, such that any solution* x, y, z *of equation* (7.1) *with conditions* (7.2) *satisfies* $\max(x, |y|, z) < C$.

THEOREM 7.2. *Let* $\{ p_1, \ldots, p_s \} = \{ 2, 3, 5, 7 \}$. *Equation* (7.1) *with conditions* (7.2) *has exactly the* 388 *solutions given in* Table I.

Remarks. 1. The Tables are given in Section 7.9. We stress that the aim of this chapter is not only to prove these theorems, but to show as well that for any given set of primes $\{ p_1, \ldots, p_s \}$ a result similar to Theorem 7.2 can be proved along the same lines, in a more-or-less algorithmic way.
2. Equation (7.1) with conditions (7.2) can be seen as a further generalization of the generalized Ramanujan-Nagell equation

$$x^2 + k = p_1^{n_1} \cdot \ldots \cdot p_s^{n_s} , \tag{7.3}$$

(cf. Chapter 4), namely by taking $|k| \in S$ arbitrary instead of $k \in \mathbb{Z}$ fixed. The method of this chapter to solve (7.1) is also a generalization of the method of Chapter 4 to solve (7.3).

Equation (7.1) can be transformed into a number of Pell-like equations. Put

$$x = D \cdot u^2 ,$$

where $D, u \in S$, and D is squarefree. There are only 2^s possibilities for D . Now, (7.1) is equivalent to a finite number of equations

$$z^2 - D \cdot u^2 = y \tag{7.4}$$

in $u \in S$, $\pm y \in S$, $z \in \mathbb{Z}$, with $z > 0$ and $(u,y) = 1$. We treat equation (7.4) by factorizing its both sides in the field $K = \mathbb{Q}(\sqrt{D})$. When dealing with equation (7.4) we allow z and u to be negative.

7.2. The case $D = 1$.

First we consider the special case $D = 1$. Then (7.4) is equivalent to

$$\begin{cases} z + u = y_1 \\ z - u = y_2 \end{cases} ,$$

where $y = y_1 \cdot y_2$, and $y_1 \in S$, $\pm y_2 \in S$, and $y_1 > |y_2|$. Subtraction yields

$$2 \cdot u = y_1 - y_2 , \tag{7.5}$$

where now all variables u, y_1, y_2 (apart from the sign) are in S , hence in $\mathbb{Z}$. By $(u,y_1) = (u,y_2) = 1$, equation (7.5) is of the form $a + b = c$, or $2 \cdot a + 2 \cdot b = 2 \cdot c$, where a, b, c are composed of primes $2, p_1, \ldots, p_s$ only, and $(a,b) = 1$, $a \geq b > 0$. In Chapter 6 it was shown how to solve such an equation $a + b = c$. For our $\{ p_1, \ldots, p_s \} = \{ 2, 3, 5, 7 \}$ we have the following result.

<u>LEMMA 7.3.</u> *Let* $\{ p_1, \ldots, p_s \} = \{ 2, 3, 5, 7 \}$. *Equation* (7.1) *with conditions* (7.2) *and* $D = 1$ *has exactly the* 95 *solutions given in* Table I *with* $D = 1$.

<u>Proof.</u> From Theorem 6.3 it follows that $a + b = c$ with $a, b, c \in S$, $(a,b) = 1$, $a \geq b$ has exactly 63 solutions, that are easy to compute. Each of these gives rise to three possibilities for (7.5):

$$\text{if } 2 \mid a \text{ then } (u,y_1,y_2) = (\tfrac{1}{2}a,b,c),\ (b,2c,2a),\ (c,2a,-2b),$$

$$\text{if } 2 \mid b \text{ then } (u,y_1,y_2) = (a,2b,2c),\ (\tfrac{1}{2}b,c,a),\ (c,2a,-2b),$$

$$\text{if } 2 \mid c \text{ then } (u,y_1,y_2) = (a,2b,2c),\ (b,2c,2a),\ (\tfrac{1}{2}c,a,-b).$$

Of the thus found 189 possibilities, the 95 ones given in Table I with $D = 1$ satisfy $x \geq y$ and $z > 0$, whereas the others don't. □

This completes our treatment of the case $D = 1$.

7.3. **Towards generalized recurrences.**

From now on, let $D > 1$. Put $K = \mathbb{Q}(\sqrt{D})$. Let $\sigma : K \to K$ be the automorphism of K with $\sigma(\sqrt{D}) = -\sqrt{D}$. For any number or ideal X in K we write X' for $\sigma(X)$, for convenience.

Let $\mathfrak{p}_i$ for $i = 1, \ldots, s$ be the prime ideal in K such that $\mathrm{ord}_{p_i}(\mathfrak{p}_i) > 0$. If p_i splits in $\mathcal{O}_K$, this is well defined if a choice has been made from the two possibilities for $\sqrt{D} \pmod{p_i}$. Put for a solution

z, u, y of (7.4)

$$\chi = z + u\cdot\sqrt{D}\ .$$

Then $y = \chi\cdot\chi'$, and by $(u,y) = 1$ we have

$$\min\{\ \mathrm{ord}_{p_i}(u),\ \mathrm{ord}_{p_i}(y)\ \} = 0\ . \tag{7.6}$$

Equation (7.4) leads to the conjugated ideal equations

$$\begin{cases} (\chi) = \prod_{i=1}^{s} \mathfrak{p}_i^{a_i}\cdot\mathfrak{p}_i'^{\,b_i} \\ \\ (\chi') = \prod_{i=1}^{s} \mathfrak{p}_i'^{\,a_i}\cdot\mathfrak{p}_i^{b_i} \end{cases} \tag{7.7}$$

where $a_i, b_i \in \mathbb{N}_0$, and $b_i = 0$ if $\mathfrak{p}_i = \mathfrak{p}_i'$. We need the following auxiliary lemma.

<u>LEMMA 7.4.</u> *If* $\xi \in K$ *and* $\mathrm{ord}_p(\xi) = \mathrm{ord}_p(\xi')$ *for a prime* p *, then*

$$\mathrm{ord}_p(\xi) \le \mathrm{ord}_p(\xi-\xi')\ .$$

Moreover, if $p = 2$ *and* $D \equiv 1 \pmod 8$, *then*

$$\mathrm{ord}_2(\xi) \le \mathrm{ord}_2((\xi-\xi')/2)\ ,$$

and, if $p = 2$ *and* $D \equiv 2, 3 \pmod 4$, *then*

$$\mathrm{ord}_2(\xi) \le \mathrm{ord}_2((\xi-\xi')/2\sqrt{D}) + \tfrac{1}{2}\ .$$

<u>Proof.</u> This is an easy exercise, which we leave to the reader. □

We distinguish, as usual, three cases for the factorization of the prime p_i in K : it may split, ramify or remain prime. See Borevich and Shafarevich [1966], section III.8.

(i). p_i remains prime in K . Then $p_i \nmid D$, and if $p_i = 2$ then $D \equiv 5 \pmod 8$. We have $(p_i) = \mathfrak{p}_i = \mathfrak{p}_i'$, and from $\mathrm{ord}_{p_i}(\chi) = \mathrm{ord}_{p_i}(\chi')$ and Lemma 7.4 we obtain

$$\mathrm{ord}_{p_i}(y) = 2\cdot\mathrm{ord}_{p_i}(\chi) \le 2\cdot\mathrm{ord}_{p_i}(\chi-\chi') = 2\cdot\mathrm{ord}_{p_i}(2\cdot u\cdot\sqrt{D}) .$$

It follows, using (7.6), that

if $p_i \ne 2$ then $\mathrm{ord}_{p_i}(y) = 2\cdot a_i = 0$,

if $p_i = 2$ then $\mathrm{ord}_2(y) = 2\cdot a_i = 0, 2$, and if $a_i = 1$ then $\mathrm{ord}_2(u) = 0$.

(ii). p_i ramifies in K . Then $p_i \mid D$ if $p_i \ne 2$, and $D \equiv 2, 3 \pmod 4$ if $p_i = 2$. We have $(p_i) = \mathfrak{p}_i^2$, $\mathfrak{p}_i = \mathfrak{p}_i'$, and $\mathrm{ord}_{p_i}(\chi) = \mathrm{ord}_{p_i}(\chi') = \frac{1}{2}\cdot a_i$. From Lemma 7.4 we find

$$\mathrm{ord}_{p_i}(y) = 2\cdot\mathrm{ord}_{p_i}(\chi) \le 1 + 2\cdot\mathrm{ord}_{p_i}((\chi-\chi')/2\cdot\sqrt{D}) = 1 + 2\cdot\mathrm{ord}_{p_i}(u) .$$

By (7.6) we obtain

$$\mathrm{ord}_{p_i}(y) = a_i = 0, 1 \text{ , and if } a_i = 1 \text{ then } \mathrm{ord}_{p_i}(u) = 0 .$$

(iii). p_i splits in K . Then $p_i \nmid D$, and if $p_i = 2$ then $D \equiv 1 \pmod 8$. We have $(p_i) = \mathfrak{p}_i\cdot\mathfrak{p}_i'$, $\mathfrak{p}_i \ne \mathfrak{p}_i'$. Further, $\mathrm{ord}_{p_i}(\mathfrak{p}_i) = 1$, $\mathrm{ord}_{p_i}(\mathfrak{p}_i') = 0$. Hence $\mathrm{ord}_{p_i}(\chi) = a_i$, $\mathrm{ord}_{p_i}(\chi') = b_i$. If $a_i = b_i$ then from

$$\mathrm{ord}_{p_i}(y) = 2\cdot\mathrm{ord}_{p_i}(\chi) \le 2\cdot\mathrm{ord}_{p_i}((\chi-\chi')/2) = 2\cdot\mathrm{ord}_{p_i}(u)$$

we obtain by (7.6) that

$$\mathrm{ord}_{p_i}(y) = a_i = b_i = 0 .$$

If $a_i \ne b_i$ then $\mathrm{ord}_{p_i}(y) = a_i + b_i > 0$, hence $\mathrm{ord}_{p_i}(u) = 0$, by (7.6). We infer in this case

$$\begin{aligned}\mathrm{ord}_{p_i}(y) = a_i + b_i &\ge 1 + 2\cdot\min(a_i,b_i) = 1 + 2\cdot\mathrm{ord}_{p_i}(\chi-\chi') \\ &= 1 + 2\cdot\mathrm{ord}_{p_i}(2) .\end{aligned}$$

It follows that

$$\mathrm{ord}_{p_i}(y) = \max(a_i,b_i) \ , \quad \min(a_i,b_i) = 0 \quad \text{if} \quad p_i \neq 2 \ ,$$

$$\mathrm{ord}_{p_i}(y) = \max(a_i,b_i) + 1 \ , \quad \min(a_i,b_i) = 1 \quad \text{if} \quad p_i = 2 \ .$$

Put $b_0 = \min(a_i,b_i)$ if $p_i = 2$ occurs, and $b_0 = 0$ otherwise. (Note that $\min(a_i,b_i) = 1$ may occur only if $\mathfrak{p}_i \neq \mathfrak{p}_i'$, hence only if $p_i = 2$ splits). Let us assume that the splitting primes of $p_1, \ldots, p_s$ are $p_1, \ldots, p_t$ for some $0 \le t \le s$. Put

$$I = \{ \ i \mid 1 \le i \le t \ , \quad a_i > b_i \ \} \ ,$$

$$I' = \{ \ i \mid 1 \le i \le t \ , \quad a_i < b_i \ \} \ .$$

For $i = 1, \ldots, t$, let h_i be the smallest positive integer such that $\mathfrak{p}_i^{h_i}$ is a principal ideal, say

$$\mathfrak{p}_i^{h_i} = (\pi_i) \ .$$

If h denotes the class number of K , then $h_i \mid h$. Now, $\pi_i \in K$ is determined up to multiplication by a unit. Thus we may choose π_i such that

$$|\pi_i| > |\pi_i'| \quad \text{if} \quad i \in I \ ,$$

$$|\pi_i| < |\pi_i'| \quad \text{if} \quad i \in I' \ .$$

For $i = 1, \ldots, t$, put

$$| \ a_i - b_i \ | = c_i \cdot h_i + d_i \ ,$$

with $c_i, d_i \in \mathbb{N}_0$, and $0 \le d_i \le h_i - 1$. Consider the ideal

$$\mathfrak{a} = (2)^{b_0} \cdot \prod_{i \in I} \mathfrak{p}_i^{d_i} \cdot \prod_{i \in I'} \mathfrak{p}_i'^{d_i} \cdot \prod_{i=t+1}^{s} \mathfrak{p}_i^{a_i} \ .$$

From the above considerations it follows that, for given K , $p_1, \ldots, p_s$, there are only finitely many possibilities for $\mathfrak{a}$. By (7.7) it follows that

$$(\chi) = \mathfrak{a} \cdot \prod_{i \in I} (\pi_i)^{c_i} \cdot \prod_{i \in I'} (\pi_i')^{c_i}$$

(namely, $|a_i - b_i| = \max(a_i,b_i)$ if $p_i \neq 2$, since then $\min(a_i,b_i) = 0$; and

$|a_i - b_i| = \max(a_i, b_i) - 1$ if $p_i = 2$ and $b_0 = 1$). Hence $\mathfrak{a}$ is a principal ideal, say

$$\mathfrak{a} = (\alpha)$$

for an $\alpha \in \mathcal{O}_K$. Up to multiplication by a unit, there are only finitely many possibilities for α . Let ϵ be the fundamental unit of K with $\epsilon > 1$. Now, (7.7) leads to the system of equations

$$\left\{ \begin{aligned} \chi\ &= z + u\sqrt{D} = \pm\alpha \cdot \epsilon^n \cdot \prod_{i\in I} \pi_i^{c_i} \cdot \prod_{i\in I'} \pi_i'^{c_i} \\ \chi' &= z - u\sqrt{D} = \pm\alpha' \cdot \epsilon'^n \cdot \prod_{i\in I} \pi_i'^{c_i} \cdot \prod_{i\in I'} \pi_i^{c_i} \end{aligned} \right. , \tag{7.8}$$

where $n \in \mathbb{Z}$. Put for $n \in \mathbb{Z}$, $m_1, \ldots, m_t \in \mathbb{N}_0$, and for each possible α

$$G_\alpha(n, m_1, \ldots, m_t) = \frac{\alpha}{2\sqrt{D}} \cdot \epsilon^n \cdot \prod_{i\in I} \pi_i^{m_i} \cdot \prod_{i\in I'} \pi_i'^{m_i} - \frac{\alpha'}{2\sqrt{D}} \cdot \epsilon'^n \cdot \prod_{i\in I} \pi_i'^{m_i} \cdot \prod_{i\in I'} \pi_i^{m_i} ,$$

$$H_\alpha(n, m_1, \ldots, m_t) = \frac{\alpha}{2} \cdot \epsilon^n \cdot \prod_{i\in I} \pi_i^{m_i} \cdot \prod_{i\in I'} \pi_i'^{m_i} + \frac{\alpha'}{2} \cdot \epsilon'^n \cdot \prod_{i\in I} \pi_i'^{m_i} \cdot \prod_{i\in I'} \pi_i^{m_i} .$$

Then (7.8) is equivalent to

$$\left\{ \begin{aligned} \pm u &= G_\alpha(n, c_1, \ldots, c_t) \\ \pm z &= H_\alpha(n, c_1, \ldots, c_t) \end{aligned} \right. . \tag{7.9}$$

The functions G_α and H_α are generalized recurrences in the sense that if all variables but one are fixed, then they become integral binary recurrence sequences.

7.4. Towards linear forms in logarithms.

Let us write

$$u_i = \mathrm{ord}_{p_i}(u)$$

for $i = 1, \ldots, s$. Put for each α

$$I_U = \{ i \mid 1 \le i \le s ,\ \mathrm{ord}_{p_i}(G_\alpha(n, m_1, \ldots, m_t)) > 0 \text{ occurs for at least one } (n, m_1, \ldots, m_t) \in \mathbb{Z} \times \mathbb{N}_0^t \} .$$

Note that since $(u,y) = 1$ the sets I_U, I, I' are disjunct. We proceed with the first equation of system (7.9). Written out in full detail it reads

$$\frac{\alpha}{2\sqrt{D}}\cdot\epsilon^n\cdot\prod_{i\in I}\pi_i^{c_i}\cdot\prod_{i\in I'}\pi_i'^{c_i} - \frac{\alpha'}{2\sqrt{D}}\cdot\epsilon'^n\cdot\prod_{i\in I}\pi_i'^{c_i}\cdot\prod_{i\in I'}\pi_i^{c_i} = \pm\prod_{i\in I_U} p_i^{u_i} . \qquad (7.10)$$

Now, I, I', I_U depend on α, which depends on the particular solution of equation (7.4) that we presupposed. However, we know that α belongs to a finite set, which can be computed explicitly. So if we can solve (7.10) completely for each α of this set, then we can find all solutions of (7.9), hence of (7.1).

The set of the α's may be reduced, without loss of generality, as follows. If $D \equiv 1 \pmod 8$ then $b_0 = 0, 1$ may both occur, with $\alpha = \alpha_0$, $2\cdot\alpha_0$ respectively. We only have to consider $2\cdot\alpha_0$, because if $u = u_0$, $z = z_0$ is a solution of (7.9) for $\alpha = \alpha_0$, then $u = 2\cdot u_0$, $z = 2\cdot z_0$ is a solution of (7.9) for $\alpha = 2\cdot\alpha_0$. Hence it is not necessary to consider $\alpha = \alpha_0$ if also $\alpha = 2\cdot\alpha_0$ is already being considered. By the same argument, if $D \equiv 5 \pmod 8$ then with $\alpha = \alpha_0$ such that $\mathrm{ord}_2(\alpha_0) = 0$ also $\alpha = 2\cdot\alpha_0$ may occur, so that we only have to consider the latter. Note that it may now occur that $(u,y) = 2$. The condition $(u,y) = 1$ is used only to ensure that I_U and $I \cup I'$ are disjunct. This remains true in the above cases with $(u,y) = 2$. Further, if $(\alpha_0) \neq (\alpha_0')$ for some α_0, then we only have to consider one α of the pair α_0, α_0'. Namely, by $\epsilon\cdot\epsilon' = \pm 1$ we have (we denote the I, I' belonging to α_0 by I_0, I_0', then the I, I' belonging to α_0' are I_0', I_0)

$$\begin{aligned} & G_{\alpha_0'}(n,m_1,\ldots,m_t) \\ &= \frac{\alpha_0'}{2\sqrt{D}}\cdot\epsilon^n\cdot\prod_{I_0'}\pi_i^{c_i}\cdot\prod_{I_0}\pi_i'^{c_i} - \frac{\alpha_0}{2\sqrt{D}}\cdot\epsilon'^n\cdot\prod_{I_0'}\pi_i'^{c_i}\cdot\prod_{I_0}\pi_i^{c_i} \\ &= \pm\left(\frac{\alpha_0'}{2\sqrt{D}}\cdot\epsilon'^{-n}\cdot\prod_{I_0}\pi_i'^{c_i}\cdot\prod_{I_0'}\pi_i^{c_i} - \frac{\alpha_0}{2\sqrt{D}}\cdot\epsilon^{-n}\cdot\prod_{I_0}\pi_i^{c_i}\cdot\prod_{I_0'}\pi_i'^{c_i}\right) \\ &= \mp G_{\alpha_0}(-n,m_1,\ldots,m_t) , \end{aligned}$$

and analogously

$$H_{\alpha_0'}(n,m_1,\ldots,m_t) = \pm H_{\alpha_0}(-n,m_1,\ldots,m_t) .$$

From equation (7.10) we now derive p_i-adic linear forms in logarithms, in three different ways, according to $i \in I, I'$ or I_U. Put

$$\gamma_i = \tfrac{3}{2} \text{ if } p_i = 2 , \quad \gamma_i = 1 \text{ if } p_i = 3 , \quad \gamma_i = \tfrac{1}{2} \text{ if } p_i \geq 5 .$$

Then $\gamma_i > 1/(p_i-1)$, hence if $\text{ord}_{p_i}(\xi) \geq \gamma_i$ for a $\xi \in K$ then

$$\text{ord}_{p_i}(\log_{p_i}(1\pm\xi)) = \text{ord}_{p_i}(\xi) . \tag{7.11}$$

We now have the following result.

<u>LEMMA 7.5.</u> *Let* n, c_i $(i \in I \cup I')$, u_i $(i \in I_U)$ *be a solution of* (7.10).

(i). *For* $i \in I_U$ *put*

$$\lambda_i = \text{ord}_{p_i}(2\sqrt{D}/\alpha') ,$$

$$\Lambda_i = \log_{p_i}(\frac{\alpha}{\alpha'}) + n\cdot\log_{p_i}(\frac{\epsilon}{\epsilon'}) + \sum_{j\in I} c_j\cdot\log_{p_i}(\frac{\pi_j}{\pi_j'})$$

$$- \sum_{j\in I'} c_j\cdot\log_{p_i}(\frac{\pi_j}{\pi_j'}) .$$

If $u_i + \lambda_i \geq \gamma_i$ *then*

$$u_i + \lambda_i = \text{ord}_{p_i}(\Lambda_i) .$$

(ii). *For* $i \in I$ *put*

$$\kappa_i = \text{ord}_{p_i}(\frac{\alpha}{\alpha'}) ,$$

$$K_i = \log_{p_i}(\frac{\alpha'}{2\sqrt{D}}) + n\cdot\log_{p_i}(\epsilon') - \sum_{j\in I_U} u_j\cdot\log_{p_i}(p_j)$$

$$+ \sum_{j\in I} c_j\cdot\log_{p_i}(\pi_j') + \sum_{j\in I'} c_j\cdot\log_{p_i}(\pi_j) .$$

If $h_i\cdot c_i + \kappa_i \geq \gamma_i$ *then*

$$h_i\cdot c_i + \kappa_i = \text{ord}_{p_i}(K_i) .$$

(ii'). *For* $i \in I'$ *put*

$$\kappa_i' = \mathrm{ord}_{p_i}\left(\frac{\alpha'}{\alpha}\right) ,$$

$$K_i' = \log_{p_i}\left(\frac{\alpha}{2\sqrt{D}}\right) + n\cdot\log_{p_i}(\epsilon) - \sum_{j\in I_U} u_j\cdot\log_{p_i}(p_j)$$
$$+ \sum_{j\in I} c_j\cdot\log_{p_i}(\pi_j) + \sum_{j\in I'} c_j\cdot\log_{p_i}(\pi_j') .$$

If $h_i\cdot c_i + \kappa_i' \geq \gamma_i$ *then*

$$h_i\cdot c_i + \kappa_i' = \mathrm{ord}_{p_i}(K_i') .$$

Remark. Note that all the above p_i-adic logarithms are well-defined, since their arguments have p_i-adic order zero. This follows from the fact that I_U, I and I' are disjunct, and if $D \equiv 1 \pmod 8$ from the choice $\alpha = 2\cdot\alpha_0$.

Proof. For (i), divide (7.10) by its second term. For (ii), divide (7.10) by its second term, and add 1. For (ii'), divide (7.10) by its first term, and subtract 1. Then, in all three cases, take the p_i-adic order, and apply (7.11). □

The linear forms in logarithms Λ_i, K_i, K_i' , as they appear in Lemma 7.5, seem to be inhomogeneous, since the first term has coefficient 1. However, it can be made homogeneous by incorporating this first term in the other ones, as follows. Put

$$h^* = \mathrm{lcm}\ (\ 2,\ h_1,\ \ldots,\ h_s\ ) .$$

Note that, by the definition of α ,

$$\alpha^{h^*} = \pm\ \epsilon^{n_0}\cdot\prod_{i\in I}\pi_i^{n_i}\cdot\prod_{i\in I'}\pi_i'^{\,n_i}\cdot\prod_{i=t+1}^{s} p_i^{n_i}\cdot 2^{h^*\cdot b_0} , \tag{7.12}$$

where the exponents n_i for $0 \leq i \leq s$ are integral. It follows that

$$\left(\frac{\alpha}{\alpha'}\right)^{h^*} = \pm\left(\frac{\epsilon}{\epsilon'}\right)^{n_0}\cdot\prod_{i\in I}\left(\frac{\pi}{\pi'}\right)^{n_i}\cdot\prod_{i\in I'}\left(\frac{\pi'}{\pi}\right)^{n_i} .$$

Put

$$\Lambda_i^* = h^*\cdot\Lambda_i \ , \quad n^* = h^*\cdot n + n_0 \ , \quad c_j^* = h^*\cdot c_j + n_j \ .$$

Then it follows that

$$\Lambda_i^* = n^*\cdot\log_{p_i}(\frac{\epsilon}{\epsilon'}) + \sum_{j\in I} c_j^*\cdot\log_{p_i}(\frac{\pi_j}{\pi_j'}) - \sum_{j\in I'} c_j^*\cdot\log_{p_i}(\frac{\pi_j}{\pi_j'}) \ .$$

Further, note that the prime divisors of D are just the ramifying primes. So, by (7.12),

$$(\frac{\alpha}{2\sqrt{D}})^{h^*} = \pm\,\epsilon^{n_0}\cdot\prod_{i\in I}\pi_i^{n_i}\cdot\prod_{i\in I'}\pi_i'^{\,n_i}\cdot\prod_{i=t+1}^{s} p_i^{n_i-\nu_i}\cdot 2^{h^*\cdot(b_0-\nu_0)} \ ,$$

where $\nu_i = \frac{1}{2}\cdot h^*\cdot\mathrm{ord}_{p_i}(4D) \in \mathbb{Z}$ for $i = t+1, \ldots, s$, and $\nu_0 = 1$ if 2 splits, $\nu_0 = 0$ otherwise. If $p_i = 2$ splits we have assumed that $b_0 = 1$. Hence the last factor vanishes. So put

$$K_i^* = h^*\cdot K_i \ , \quad K_i'^{\,*} = h^*\cdot K_i' \ , \quad u_j^* = h^*\cdot u_j - (\,n_j - \nu_j\,) \ ,$$

$$I_U^* = I_U \cup \{\, i \mid t+1 \le i \le s \ , \ \nu_i \neq 0 \,\} \ .$$

Then it follows that

$$K_i^* = n^*\cdot\log_{p_i}(\epsilon') - \sum_{j\in I_U^*} u_j^*\cdot\log_{p_i}(p_j) + \sum_{j\in I} c_j^*\cdot\log_{p_i}(\pi_j') + $$
$$+ \sum_{j\in I'} c_j^*\cdot\log_{p_i}(\pi_j) \ ,$$

$$K_i'^{\,*} = n^*\cdot\log_{p_i}(\epsilon) - \sum_{j\in I_U^*} u_j^*\cdot\log_{p_i}(p_j) + \sum_{j\in I} c_j^*\cdot\log_{p_i}(\pi_j) + $$
$$+ \sum_{j\in I'} c_j^*\cdot\log_{p_i}(\pi_j') \ .$$

This leads to the following reformulation of Lemma 7.5.

<u>LEMMA 7.6.</u> *Let* n, c_i *for* $i \in I \cup I'$, u_i *for* $i \in I_U$ *be a solution of* (7.10), *let* λ_i, κ_i, κ_i' *be as in Lemma* 7.5, *and let* h^*, Λ_i^*, K_i^*, $K_i'^{\,*}$, n_i^*, c_i^*, u_i^*, I_U^* *be as above.*

(i). *Let* $i \in I_U$. *If* $u_i + \lambda_i \ge \gamma_i$ *then*

$$u_i + \lambda_i + \mathrm{ord}_{p_i}(h^*) = \mathrm{ord}_{p_i}(\Lambda_i^*) \ .$$

(ii). *Let* $i \in I$. *If* $h_i \cdot c_i + \kappa_i \geq \gamma_i$ *then*

$$h_i \cdot c_i + \kappa_i + \mathrm{ord}_{p_i}(h^*) = \mathrm{ord}_{p_i}(K_i^*) .$$

(ii'). *Let* $i \in I'$. *If* $h_i \cdot c_i + \kappa_i' \geq \gamma_i$ *then*

$$h_i \cdot c_i + \kappa_i' + \mathrm{ord}_{p_i}(h^*) = \mathrm{ord}_{p_i}(K_i'^*) .$$

<u>Remark.</u> We will study the linear forms in logarithms Λ_i^*, K_i^*, $K_i'^*$ for arbitrary integral values of the variables n^*, c_i^*, u_i^* . Notice that the parameter α has disappeared completely from these linear forms. This means that we have to consider the linear forms for each D only, instead of for each α .

7.5. Upper bounds for the solutions: outline.

Let us first give a global explanation of our application of the theory of p-adic linear forms in logarithms, that gives explicit upper bounds for the variables occurring in the linear forms Λ_i^*, K_i^*, $K_i'^*$. Then we give arguments why we choose this way to apply the theory, and not other possible ways. In the next section we give full details of the derivation of the upper bounds. In the sequel, by the 'constants' $C_1, \ldots, C_{12}$ we mean numbers that depend only on the parameters of (7.10), not on the unknowns n, c_i, u_i .

Put

$$M = \max_{i \in I \cup I'} (c_i) , \quad U = \max_{i \in I_U} (u_i) , \quad B = \max (M, U, |n|) ,$$

$$M^* = \max_{i \in I \cup I'} (c_i^*) , \quad U^* = \max_{i \in I_U} (u_i^*) , \quad B^* = \max (M^*, U^*, |n^*|) ,$$

$$N = \max (|n_0|, \ldots, |n_t|, |n_{t+1} - \nu_{t+1}|, \ldots, |n_s - \nu_s|) .$$

Then it follows that

$$X^* \leq h^* \cdot X + N , \quad X \leq \frac{X^* + N}{h^*} \tag{7.13}$$

for $X = M, U, B$. We apply Lemma 2.6 to the p-adic linear forms in logarithms. For Λ_i^* we find, in view of Lemma 7.6(i),

$$U < C_1 + C_2 \cdot \log(B^*) \ , \tag{7.14}$$

and for K_i^*, $K_i'^*$ we find, in view of Lemma 7.6(ii),(ii'),

$$M < C_3 + C_4 \cdot \log(B^*) \ . \tag{7.15}$$

Here, C_1, C_2, C_3, C_4 are constants that can be written down explicitly. In order to find an upper bound for B we try to find constants C_{10}, C_{11} such that

$$B < C_{10} + C_{11} \cdot \log(B^*) \ . \tag{7.16}$$

In view of (7.13) we may insert and delete asterisks any time we like, as long as we don't specify the constants. In order to prove (7.16) it remains, in view of (7.14) and (7.15), to bound $|n|$ by a constant times $\log B$. We will introduce certain constants C_5, C_6, C_7, and distinguish three cases:

(a). $-(C_6 + C_7 \cdot M) \le n \le C_5$,
(b). $n > C_5$, (7.17)
(c). $n < -(C_6 + C_7 \cdot M)$.

In case (a) it is, by (7.15), obvious that (7.16) holds. In cases (b) and (c) one of the two terms of G_α dominates. We shall show that there exist constants C_8, C_9 such that

$$|n| < C_8 + C_9 \cdot U \ . \tag{7.18}$$

Then (7.16) follows from (7.14).

From (7.16) we derive immediately an explicit upper bound C_{12} for B, hence for all the variables involved. Since the constants $C_1, \ldots, C_4$ will be very large, also C_{12} will be very large. To find all solutions we proceed by reducing this upper bound, by applying the computational p-adic diophantine approximation technique described in Section 3.11, to the p-adic linear forms in logarithms Λ_i^*, K_i^*, $K_i'^*$. Crucial in that line of argument is that the constants $C_5, \ldots, C_9$ are very small compared to $C_1, \ldots, C_4$. This method leads to reduced bounds for the p-adic orders of the linear forms. Then we can replace (7.14) and (7.15) by much sharper inequalities, and repeat the above argument, to find a much sharper inequality for (7.16). In general we expect that it is in this way possible to reduce in one step the upper bound C_{12} for B to a reduced bound of size $\log C_{12}$.

Before going into detail we explain briefly that it is possible to treat

(7.10) partly by the theory of real (instead of p-adic) linear forms in logarithms, and subsequently by a real computational diophantine approximation technique (cf. Section 3.7), and why we prefer not to do so. First, note that K_i and K_i' have generically more terms than Λ_i, and are therefore more complicated to handle. Since K_i, K_i' occur only in case (a), this is the most difficult case. Equation (7.10) consist of three terms, each of which is purely exponential, i.e. the bases are fixed and the exponents are variable. If one of these three terms is essentially smaller than the other two (more specifically, smaller than the other terms raised to the power δ, for a fixed $\delta \in (0,1)$), then we can apply the real method. There are two ways of doing this. Write (7.10) as

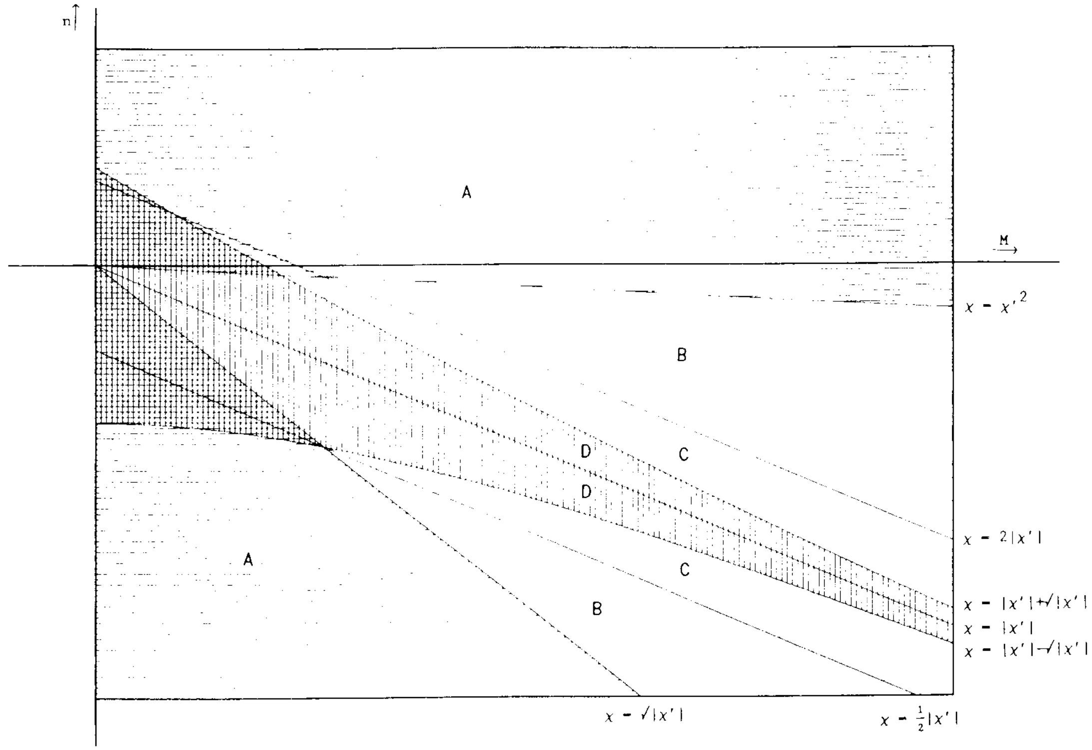
$$\chi - \chi' = 2 \cdot u \cdot \sqrt{D} .$$

First, suppose that $|\chi - \chi'| < |\chi'|^{\delta}$. Then $|n|$ cannot be very large, and we are essentially (i.e. apart from a finite domain) in case (a). Unfortunately, the region for $|n|$ that we can cover in this way becomes smaller as $M \to \infty$ (see the example below). Second, suppose that $|\chi| > |\chi'|^{1/\delta}$, or $|\chi| < |\chi'|^{\delta}$. Then we are essentially in case (b) or (c). But this area can be dealt with easier p-adically, since here we use the linear forms Λ_i, whereas the real linear forms in logarithms used in this case will generically have more terms. The areas sketched above, in which we can apply the real theory, will not cover the whole domain corresponding to case (a) (cf. the white regions in Fig. 4 below). Hence we cannot avoid working with the p-adic linear forms K_i, K_i'. But then it is more convenient to avoid the use of real linear forms.

Let us illustrate the above reasoning with an example. Let $\alpha = \alpha' = 1$, $\epsilon = 1 + \sqrt{2}$, $\pi_1 = 1 + 2 \cdot \sqrt{2}$, $s = 1$, $I = \{1\}$, $p_1 = 7$, $I' = \emptyset$, and $\delta = \frac{1}{2}$. Then we have $\chi = (1+\sqrt{2})^n \cdot (1+2 \cdot \sqrt{2})^M$. Fig. 4 below gives in the (n,M)-plane the curves $\chi = \chi'^2$, $2 \cdot |\chi'|$, $|\chi'| + \sqrt{|\chi'|}$, $|\chi'|$, $|\chi'| - \sqrt{|\chi'|}$, $\frac{1}{2} \cdot |\chi'|$, $\sqrt{|\chi'|}$, which are boundaries of the four regions A, B, C, D. We have the following possibilities.

region	case (ess.)	number of terms in linear form p-adic method	real method
A	(b),(c)	2	3
B	(b),(c)	2	–
C	(a)	3	–
D	(a)	3	2

Figure 4.



The really hard part is C. It can be reduced to $\frac{1}{c}\cdot|\chi'| < \chi < |\chi'| - |\chi'|^{\delta}$ and $|\chi'| + |\chi'|^{\delta} < \chi < c\cdot|\chi'|$ for any $c > 1$, $\delta \in (0,1)$, but will never disappear. So we cannot avoid the p-adic linear form in case (a), which then works in regions C and D together.

7.6. Upper bounds for the solutions: details.

We now proceed with filling in the details of the procedure outlined in the previous section.

We apply Yu's lemma (Lemma 2.6) as follows. We have $L = K = \mathbb{Q}(\sqrt{D})$, so $d = 2$. For the α_i we have ϵ/ϵ', π_j/π_j' , or ϵ, ϵ', p_j, π_j, π_j' . We have to compute the heights of these numbers. We have at once

$$h(p_j) = \log(p_j) \quad \text{if} \quad p_j \geq 3 \text{ ,} \quad h(2) = 1 \text{ ,}$$

$$h(\epsilon) = h(\epsilon') = \frac{1}{2}\cdot\log(\epsilon) \text{ ,}$$

$$h(\pi_j) = h(\pi_j') = \tfrac{1}{2}\cdot\log\left(\max(1,|\pi_j|)\cdot\max(1,|\pi_j'|)\right) .$$

Further, let $\beta = \epsilon$ or $\beta = \pi_j$. Then the leading coefficient of β/β' is $a_0 = |\beta\cdot\beta'|$. Hence

$$h(\tfrac{\beta}{\beta'}) = \tfrac{1}{2}\log\left(|\beta\cdot\beta'|\cdot\max(1,|\tfrac{\beta}{\beta'}|)\cdot\max(1,|\tfrac{\beta'}{\beta}|)\right)$$

$$= \log\left(\max(|\beta|,|\beta'|)\right) .$$

Hence

$$h(\tfrac{\epsilon}{\epsilon'}) = \log(\epsilon) , \quad h(\tfrac{\pi_j}{\pi_j'}) = \log\left(\max(|\pi_j|,|\pi_j'|)\right) .$$

The order of the α_i is important in two respects: it is required that the V_i for $i = 1, \ldots, n-1$ are in increasing order, and that $\mathrm{ord}_p(b_n)$ is minimal among the $\mathrm{ord}_p(b_i)$. Since the b_i are the unknowns, we should assume that $V_n \le V_1 \le \ldots \le V_{n-1}$. In the final bound however, only the product $V_1\cdot\ldots\cdot V_n$ and V_{n-1}^+ appear. So the ordering of the V_i only matters for defining V_{n-1}^+ . It follows that we can take

$$V_i = \max\left(h(\alpha_i), f_{\mathfrak{p}}\cdot(\log p)/d \right) ,$$

with the α_i in any order, if we define

$$V_{n-1}^+ = \max (1, V_1, \ldots, V_n) .$$

Further, we take

$$B = B_0 = B_n = B' = \max\left(|b_1|, \ldots, |b_n|, 2, \tfrac{4}{3}\cdot n\cdot(p^{f_{\mathfrak{p}}/d}-1) \right) .$$

Then $\log(1+\frac{3}{4n}\cdot B) \ge f_{\mathfrak{p}}\cdot(\log p)/d$. By $B \ge 2$ it follows that $1 + \frac{3}{4n}\cdot B < B$. Hence we can take

$$W = \log B .$$

There are two more conditions to be checked. The first one is that $\alpha_1^{b_1}\cdot\ldots\cdot\alpha_n^{b_n} \ne 1$. This is immediate, if we assume the obvious condition that not all b_i are zero. The second one is $[K(\alpha_1^{1/q},\ldots,\alpha_n^{1/q}):K] = q^n$, which is less obvious. For our situation it follows from the following lemma.

<u>LEMMA 7.7.</u> *Let* $K = \mathbb{Q}(\sqrt{D})$ *, with* ϵ *as fundamental unit, and* h *as class number. Let* $p_1, \ldots, p_s$ *be distinct prime numbers, and let* $\mathfrak{p}_i$ *be for*

$i = 1, \ldots, s$ *a prime ideal in* K *lying above* $\mathfrak{p}_i$. *Let* h_i *be a divisor of* h *such that* $\mathfrak{p}_i^{h_i}$ *is principal, and denote a generator by* π_i . *Let either*: (1) *all* p_i *split, and then*

$$\xi_0 = \frac{\epsilon}{\epsilon'} , \quad \xi_j = \frac{\pi_j}{\pi_j'} \quad \text{for} \quad i = 1, \ldots, s ,$$

or: (2)

$$\xi_0 = \epsilon \quad \text{or} \quad \epsilon' , \quad \xi_j = \pi_j \quad \text{or} \quad \pi_j' \quad \text{for} \quad j = 1, \ldots, s .$$

Let q *be an odd prime, not dividing* h . *Then*

$$[K(\xi_0^{1/q}, \ldots, \xi_s^{1/q}):K] = q^{s+1} .$$

<u>Proof.</u> Let $K_0 = K(\xi_0^{1/q})$, and $K_i = K_{i-1}(\xi_i^{1/q})$ for $i = 1, \ldots, s$. We use induction on i to prove that $[K_s:K] = q^{s+1}$. Note that $[K_0:K] = q$. Suppose that $[K_i:K] = q^{i+1}$. It remains to prove that $[K_{i+1}:K_i] = q$, hence it suffices to prove that $\xi_{i+1} \notin K_i$, since q is prime. Suppose the contrary is true. K_i is a K-vector space of dimension q^{i+1} , with as basis all the elements

$$\tau_{k_0, \ldots, k_i} = \prod_{j=0}^{i} \xi_j^{k_j/q}$$

for $k_j \in \{ 0, 1, \ldots, q-1 \}$ for $j = 0, \ldots, i$. It follows that there exist $a_{k_0, \ldots, k_i} \in K$ such that

$$\xi_{i+1}^{1/q} = \sum_{k_0, \ldots, k_i} a_{k_0, \ldots, k_i} \cdot \tau_{k_0, \ldots, k_i} . \tag{7.19}$$

The group of K-embeddings of K_i into $\mathbb{C}$ is generated by the σ_j for $j = 0, \ldots, i$ defined by

$$\sigma_j(\xi_\ell^{1/q}) = \xi_\ell^{1/q} \quad \text{for} \quad \ell = 0, \ldots, i , \quad \ell \neq j ,$$

$$\sigma_j(\xi_j^{1/q}) = \rho \cdot \xi_j^{1/q} ,$$

where ρ is a primitive q th root of unity. Hence all the embeddings are given by

$$\varphi_{\ell_0, \ldots \ell_i} = \prod_{j=0}^{i} \sigma_j^{\ell_j}$$

for $\ell_j \in \{ 0, 1, \ldots, q-1 \}$. It follows that

$$\varphi_{\ell_0,\ldots,\ell_i}(\tau_{k_0,\ldots,k_i}) = \prod_{j=0}^{i} \sigma_j^{\ell_j} \Big(\prod_{m=0}^{i} \xi_m^{k_m/q} \Big) = \prod_{j=0}^{i} \rho^{\ell_j k_j} \cdot \tau_{k_0,\ldots,k_i}$$

$$= \rho^{\sum_{j=0}^{i} \ell_j k_j} \cdot \tau_{k_0,\ldots,k_i} .$$

The minimal polynomial of $\xi_{i+1}^{1/q}$ over K is $X^q - \xi_{i+1}$. Hence the conjugates of $\xi_{i+1}^{1/q}$ are $\rho^j \cdot \xi_{i+1}^{1/q}$ for $j = 0, 1, \ldots, q-1$, all with equal multiplicity. There exist numbers $m_j \in \{ 0, 1, \ldots, q-1 \}$ such that for $j = 0, 1, \ldots, q-1$ we have

$$\sigma_j(\xi_{i+1}^{1/q}) = \rho^{m_j} \cdot \xi_{i+1}^{1/q} .$$

Hence

$$\varphi_{\ell_0,\ldots,\ell_i}(\xi_{i+1}^{1/q}) = \rho^{\sum_{j=0}^{i} \ell_j m_j} \cdot \xi_{i+1}^{1/q} .$$

Now apply $\varphi_{\ell_0,\ldots,\ell_i}$ to (7.19). Then for each tuple $(\ell_0,\ldots,\ell_i)$ we find

$$\rho^{\sum_{j=0}^{i} \ell_j m_j} \cdot \xi_{i+1}^{1/q} = \sum_{k_0,\ldots,k_i} a_{k_0,\ldots,k_i} \cdot \rho^{\sum_{j=0}^{i} \ell_j k_j} \cdot \tau_{k_0,\ldots,k_i} .$$

Here we have a system of q^{i+1} linear equations in the q^{i+1} unknowns $a_{k_0,\ldots,k_i}$. The determinant of this system is exactly the square root of the discriminant of K_i over K , hence nonzero. Consequently there is in $\mathbb{C}^{q^{i+1}}$ just one solution of the system. But we know that solution:

$$a_{k_0,\ldots,k_i} = 0 \quad \text{if} \quad (k_0,\ldots,k_i) \neq (m_0,\ldots,m_i) ,$$
$$a_{m_0,\ldots,m_i} = \xi_{i+1}^{1/q} \cdot \tau_{m_0,\ldots,m_i}^{-1} .$$

The latter equation now yields an equation over K :

$$\xi_{i+1} = a_{m_0,\ldots,m_i}^{q} \cdot \prod_{j=0}^{i} \xi_j^{m_j} .$$

In case (1) this leads to the ideal equation

$$\left(\frac{\mathfrak{p}_{i+1}}{\mathfrak{p}'_{i+1}}\right)^{h_{i+1}} = \mathfrak{a}^q \cdot \prod_{j=1}^{i} \left(\frac{\mathfrak{p}_j}{\mathfrak{p}'_j}\right)^{m_j \cdot h_j} ,$$

and in case (2) to

$$\mathfrak{p}_{i+1}^{(\prime)\, h_{i+1}} = \mathfrak{a}^q \cdot \prod_{j=1}^{i} \mathfrak{p}_j^{(\prime)\, m_j \cdot h_j} ,$$

(where $\mathfrak{p}^{(\prime)}$ stands for $\mathfrak{p}$ or $\mathfrak{p}'$) for some fractional ideal $\mathfrak{a}$ (note that $(\xi_0) = (1)$). Because of unique factorization for ideals it follows in both cases that q divides all $m_j \cdot h_j$ for $j = 1, \ldots, i$ and h_{i+1} . This contradicts the assumption $q \nmid h$. □

Remarks. 1. If $\mathrm{ord}_p(\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} - 1) > 1/(p-1)$ then

$$\mathrm{ord}_p(\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} - 1) = \mathrm{ord}_p(b_1 \cdot \log_p(\alpha_1) + \ldots + b_n \cdot \log_p(\alpha_n)) .$$

We prefer to work with the logarithmic version, since that is the one we use in the computational method of reducing the upper bounds.

2. In order to apply Yu's lemma we can take for q the smallest odd prime that does not divide $h \cdot p \cdot (p^{f_{\mathfrak{p}}} - 1)$.

We now proceed to compute the constants C_1 to C_{12} . To find C_1 and C_2 we apply Lemma 2.6 to Λ_i^* , for all $i \in I_U$. Then we find for each such i constants $C_{1,i}$, $C_{2,i}$ such that, under the conditions

$$u_i + \lambda_i \geq \gamma_i , \quad B^* \geq \max\left(2, \tfrac{4}{3} \cdot t_i \cdot (p_i^{f_{\mathfrak{p}_i}/2} - 1) \right) ,$$

(where t_i denotes the number of terms in Λ_i^*), we obtain

$$\mathrm{ord}_{\mathfrak{p}_i}(\Lambda_i^*) < C_{1,i} + C_{2,i} \cdot \log B^* .$$

By Lemma 7.6(i) and the relation $\mathrm{ord}_{\mathfrak{p}} = e_{\mathfrak{p}} \cdot \mathrm{ord}_p$ we see that, assuming the conditions

$$U \geq \max_{i \in I_U} (\gamma_i - \lambda_i) , \quad B^* \geq \max_{i \in I_U} \left(2, \tfrac{4}{3} \cdot t_i \cdot (p_i^{f_{\mathfrak{p}_i}/2} - 1) \right) \qquad (7.20)$$

it suffices to take

$$C_1 = \max_{i\in I_U} \left(-(\lambda_i+\mathrm{ord}_{p_i}(h^*)) + C_{1,i}/e_{p_i} \right) , \quad C_2 = \max_{i\in I_U} (C_{2,i}/e_{p_i}) .$$

Then (7.14) holds.

Next we apply Lemma 2.6 to K_i^* and $K_i'^*$, for all $i \in I$ and I' respectively, to obtain C_3 and C_4. By $X^{(')}$ we denote X if $i \in I$, and X' if $i \in I'$. There exist by Lemma 2.6 constants $C_{3,i}$ and $C_{4,i}$ such that under the conditions

$$h_i\cdot c_i + \kappa_i^{(')} \geq \gamma_i , \quad B^* \geq \max \left(2, \frac{4}{3}\cdot t_i\cdot (p_i^{f_{p_i}/2} -1) \right)$$

(where again t_i denotes the number of terms of $K_i^{(')*}$), it follows that

$$\mathrm{ord}_{p_i}(K_i^{(')*}) < C_{3,i} + C_{4,i}\cdot \log B^* .$$

Again, by Lemma 7.6(ii),(ii') it follows that, under the conditions

$$M \geq \max_{i\in I\cup I'} \left(\frac{\gamma_i-\kappa_i^{(')}}{h_i}\right) , \quad B^* \geq \max_{i\in I\cup I'} \left(2, \frac{4}{3}\cdot t_i\cdot (p_i^{f_{p_i}/2} -1) \right) \tag{7.21}$$

it suffices to take

$$C_3 = \max_{i\in I\cup I'} \left(\frac{\kappa_i^{(')}+\mathrm{ord}_{p_i}(h^*)}{h_i} + \frac{C_{3,i}}{h_i\cdot e_{p_i}} \right) , \quad C_4 = \max_{i\in I\cup I'} \left(\frac{C_{4,i}}{h_i\cdot e_{p_i}}\right) .$$

Then (7.15) holds.

We take C_5 to C_7 as follows:

$$C_5 = \log(2\cdot \left|\frac{\alpha'}{\alpha}\right|)/2\cdot \log \epsilon , \quad C_6 = \log(2\cdot \left|\frac{\alpha}{\alpha'}\right|)/2\cdot \log \epsilon ,$$

$$C_7 = \left(\sum_{i\in I} \log\left|\frac{\pi_i}{\pi_i'}\right| + \sum_{i\in I'} \log\left|\frac{\pi_i'}{\pi_i}\right| \right)/2\cdot \log \epsilon .$$

Note that C_5 or C_6 may be negative, but that always $-C_6 < C_5$. Further, C_7 is always strictly positive, unless $I = I' = \emptyset$. Next we show how to take C_8 and C_9. Suppose first that

$$n > \max (C_5, 0) .$$

Then, from $\epsilon\cdot \epsilon' = \pm 1$ and the choice of π_i we find by (7.8) that

$$\left|\frac{\chi}{\chi'}\right| = \left|\frac{\alpha}{\alpha'}\right| \cdot \left|\frac{\epsilon}{\epsilon'}\right|^{n} \cdot \prod_{i\in I} \left|\frac{\pi_i}{\pi'_i}\right|^{c_i} \cdot \prod_{i\in I'} \left|\frac{\pi'_i}{\pi_i}\right|^{c_i} \geq \left|\frac{\alpha}{\alpha'}\right| \cdot \epsilon^{2\cdot n} > 2 ,$$

which expresses that the first term of G_α dominates. Put

$$P = \prod_{i\in I_U} p_i .$$

Then we infer

$$p^U \geq \prod_{i\in I_U} p_i^{u_i} = |\chi-\chi'|/2\cdot\sqrt{D} > |\chi|/4\cdot\sqrt{D}$$

$$= \frac{|\alpha|}{4\sqrt{D}} \cdot \epsilon^{n} \cdot \prod_{i\in I} |\pi_i|^{c_i} \cdot \prod_{i\in I'} |\pi'_i|^{c_i} > \frac{|\alpha|}{4\sqrt{D}} \cdot \epsilon^{n} ,$$

hence

$$n < \left(\log\left(\frac{4\sqrt{D}}{|\alpha|}\right) + U\cdot\log(P) \right)/\log \epsilon .$$

Next suppose that

$$n < \min \left(-(C_6+C_7\cdot M),\ 0 \right) .$$

Then we find that the second term of G_α dominates, namely

$$\left|\frac{\chi'}{\chi}\right| = \left|\frac{\alpha'}{\alpha}\right| \cdot \left|\frac{\epsilon'}{\epsilon}\right|^{n} \cdot \prod_{i\in I} \left|\frac{\pi'_i}{\pi_i}\right|^{c_i} \cdot \prod_{i\in I'} \left|\frac{\pi_i}{\pi'_i}\right|^{c_i}$$

$$\geq \left|\frac{\alpha'}{\alpha}\right| \cdot \epsilon^{-2\cdot n} \cdot \left(\prod_{i\in I} \left|\frac{\pi'_i}{\pi_i}\right| \cdot \prod_{i\in I'} \left|\frac{\pi_i}{\pi'_i}\right| \right)^{M} = \left|\frac{\alpha'}{\alpha}\right| \cdot \epsilon^{-2\cdot(n+C_7\cdot M)}$$

$$> \left|\frac{\alpha'}{\alpha}\right| \cdot \epsilon^{2\cdot C_6} = 2 .$$

Put

$$\Gamma = \prod_{i\in I} \min\left(1,\ |\pi'_i|\right) \cdot \prod_{i\in I'} \min\left(1,\ |\pi_i|\right) .$$

Then we infer

$$p^U \geq |\chi-\chi'|/2\cdot\sqrt{D} > |\chi'|/4\cdot\sqrt{D} = \frac{|\alpha'|}{4\sqrt{D}} \cdot \epsilon^{|n|} \cdot \prod_{i\in I} |\pi'_i|^{c_i} \cdot \prod_{i\in I'} |\pi_i|^{c_i}$$

$$\geq \frac{|\alpha'|}{4\sqrt{D}} \cdot \epsilon^{|n|} \cdot \prod_{i\in I} \min(1, |\pi'_i|)^{c_i} \cdot \prod_{i\in I'} \min(1, |\pi_i|)^{c_i}$$

$$\geq \frac{|\alpha'|}{4\sqrt{D}} \cdot \epsilon^{|n|} \cdot \Gamma^M > \frac{|\alpha'|}{4\sqrt{D}} \cdot \epsilon^{|n|} \cdot \Gamma^{-(|n|-C_6)/C_7} .$$

Hence

$$|n| < \left[\log\left(\frac{4\sqrt{D}}{|\alpha'|} \cdot \Gamma^{-C_6/C_7}\right) + U \cdot \log(P) \right] / \log\left(\epsilon \cdot \Gamma^{1/C_7}\right) .$$

The remaining possibilities in cases (b) and (c) are $C_5 < n \leq 0$ and $0 \leq n < -(C_6 + C_7 \cdot M) < -C_6$. So we may take, noting that $\Gamma \leq 1$,

$$C_8 = \max \left[\log\left(\frac{4\sqrt{D}}{|\alpha|}\right)/\log \epsilon,\ \log\left(\frac{4\sqrt{D}}{|\alpha'|} \cdot \Gamma^{-C_6/C_7}\right)/\log\left(\epsilon \cdot \Gamma^{1/C_7}\right),\ -C_5,\ -C_6 \right] ,$$

$$C_9 = (\log P)/\log\left(\epsilon \cdot \Gamma^{1/C_7}\right) .$$

Then (7.18) holds in the cases (b) and (c) . Now take

$$C_{10} = \max \left(C_1,\ C_3,\ |C_5|,\ |C_6| + C_3 \cdot C_7,\ C_8 + C_1 \cdot C_9 \right) ,$$

$$C_{11} = \max \left(C_2,\ C_4,\ C_4 \cdot C_7,\ C_2 \cdot C_9 \right) .$$

Then it follows that (7.16) is true, if conditions (7.20) and (7.21) hold. Hence, by Lemma 2.1, we infer the following result.

LEMMA 7.8. *In the above notation,*

$$B^* < C^*_{12} , \quad B < C_{12}$$

hold unconditionally, where

$$C^*_{12} = \max \left[2 \cdot \left(N + h^* \cdot C_{10} + h^* \cdot C_{11} \cdot \log(h^* \cdot C_{11})\right),\ \max_{i \in I_U} \left(h^* \cdot (\gamma_i - \lambda_i) + N\right),\right.$$

$$\left. \max_{i \in I \cup I'} \left(h^* \cdot \frac{\gamma_i - \kappa_i^{(')}}{h_i} + N\right),\ 2,\ \max_{i \in I \cup I' \cup I_U} \left(\frac{4}{3} \cdot t_i \cdot (p_i^{f_{p_i}/2} - 1)\right) \right] ,$$

$$C_{12} = \frac{1}{h^*} \cdot (C^*_{12} + N) .$$

Proof. Clear. □

Remarks. 1. Theorem 7.1 is an immediate corollary of Lemma 7.8.
2. In practice, almost always the first term in the max-definition of C_{12}^{*} dominates. Moreover, the term N will in practice disappear in the rounding off. Similarly, in the definitions of C_{10} and C_{11}, the dominating factors are in practice C_1 to C_4.

7.7. The reduction technique.

We now want to reduce the upper bound C_{12} for B (or C_{12}^{*} for B^{*}, which is equivalent), to a much smaller upper bound. We do so using the p-adic computational diophantine approximation technique described in Section 3.11.

We perform this procedure for $\Lambda = \Lambda_i^{*}, K_i^{*}, K_i'^{*}$, for the relevant i. We work in the p-adic approximation lattices Γ_μ themselves, and not in the sublattices described in Section 3.13. The computational bottlenecks are the computation of the p-adic logarithms to the desired precision, and the application of the L^3-Algorithm. We refer to Chapter 3 for details. Once we have found reduced bounds for $ord_p(\Lambda)$ for the above mentioned Λ, we combine these bounds with Lemma 7.6 and with estimates (7.13), (7.17) and (7.18) to find reduced bounds for B and B^{*}.

When reduced upper bounds for B, B^{*} are found in this way, we may try the above procedure again, with C_{12}, C_{12}^{*} replaced by their reduced analogons. We may repeat the argument as long as improvement is still being made. But at a certain stage, usually near to the actual largest solution, the procedure will not yield any further improvement. Then we have to find all solutions by some other method. One technique that may be useful is the algorithm of Fincke and Pohst, described in Section 3.6. Another way is to search directly for solutions of the original diophantine equation below the reduced bounds. In our present equation this may well be done by employing congruence arguments for finding all solutions of the second equation of system (7.9) below the obtained bounds.

7.8. The standard example.

In this section we shall work out the procedure outlined above for our standard example $\{ p_1, \ldots, p_s \} = \{ 2, 3, 5, 7 \}$, thus proving Theorem

7.2. In Tables II and III we give the necessary data on the fields $K = \mathbb{Q}(\sqrt{D})$ for the 15 values of D, and on the factorization of 2, 3, 5, 7 in K.

Explanation of Tables II and III. For $p_i = 2, 3, 5, 7$ we give in Table II a generator of the ideal $\mathfrak{p}_i$ with $\mathrm{ord}_{p_i}(\mathfrak{p}_i) > 0$ if $\mathfrak{p}_i$ is a principal ideal, and we give "$\mathfrak{p}_i$" if it is not principal. In all the latter cases, $h_i = 2$, so $\mathfrak{p}_i^2 = (\pi_i)$ is principal. An asterisk (*) denotes a splitting prime. Note that for each D at most one of the primes 2, 3, 5, 7 splits, so $t \le 1$. In the final column of Table II we give for the splitting prime p_i a generator π_i of the ideal $\mathfrak{p}_i^{h_i}$. In Table III, when $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are not principal, but $\mathfrak{p}_i \cdot \mathfrak{p}_j$ is, we give a generator of it.

From Tables II and III it is easy to find all possibilities for I, I' and α. We may assume $I' = \emptyset$. In Table IV we give all possible I, I_U, α (we give primes p_i instead of indices i). An asterisk (*) appears when $(\alpha) \ne (\alpha')$. The set I_U is found by checking $G_\alpha \pmod{p_i}$ for all p_i.

There are 54 cases with $I = \emptyset$ (the "symmetric" cases), and 54 cases with $I \ne \emptyset$ (the "asymmetric" cases). We start with the symmetric cases. This incorporates all cases with $D = 3, 5, 35, 42, 210$, when none of the primes 2, 3, 5, 7 splits in $\mathbb{Q}(\sqrt{D})$. Now, $t = 0$, hence equation (7.10) becomes

$$G_\alpha(n) = \frac{\alpha}{2\sqrt{D}} \cdot \epsilon^n - \frac{\alpha'}{2\sqrt{D}} \cdot \epsilon'^n = \pm \prod_{i \in I_U} p_i^{u_i} . \qquad (7.22)$$

With $A = \epsilon + \epsilon' \in \mathbb{Z}$, $B = N\epsilon = \epsilon \cdot \epsilon' = \pm 1$, we have for all $n \in \mathbb{Z}$

$$G_\alpha(n+2) = A \cdot G_\alpha(n+1) - B \cdot G_\alpha(n) .$$

Since $(\alpha) = (\alpha')$, there is an $n_0 \in \mathbb{Z}$ such that $\alpha' = \pm\epsilon^{n_0} \cdot \alpha$. Hence

$$|G_\alpha(n_0 - n)| = |G_\alpha(n)|$$

for all $n \in \mathbb{Z}$, which explains why we call these cases "symmetric". In this situation we can apply elementary congruence arguments, as explained in Section 4.5. We have the following result.

<u>LEMMA 7.9.</u> *Let* $\{ p_1, \ldots, p_4 \} = \{ 2, 3, 5, 7 \}$. *Equation* (7.1) *with conditions* (7.2) *and* $I = \emptyset$ *has exactly* 91 *solutions, that appear in* Table I *marked with an asterisk* (*).

Sketch of proof. In Table V we give the necessary data for these 54 cases. We explain this table, and leave many details to the reader to check. For each $p = 2, 3, 5, 7$ we give $\ell_1, n_1, a_1, h_2, \dots, h_7$. If for a p only ℓ_1 is given, then $p^{\ell_1+1} \nmid G_\alpha(n)$ for all $n \in \mathbb{Z}$, and $p^{\ell_1} \mid G_\alpha(n)$ for at least one $n \in \mathbb{Z}$. If n_1, a_1 are given, then

$$p^{\ell_1+1} \mid G_\alpha(n) \Leftrightarrow n \equiv n_1 \pmod{a_1} .$$

Define $n_2 = a_1$ if $n_1 = 0$, and $n_2 = n_1$ if $n_1 \neq 0$. Then n_2 is the smallest positive index such that $p^{\ell_1+1} \mid G_\alpha(n_2)$. Now it is true that

$$G_\alpha(n_2) \mid G_\alpha(n) \quad \text{whenever} \quad n \equiv n_1 \pmod{a_1} ,$$

This is related to symmetry properties of the recurrence sequence $\{G_\alpha(n)\}_{n=-\infty}^{\infty}$. For $q = 2, 3, 5, 7$ we have defined

$$h_q = \operatorname{ord}_q(G_\alpha(n_2)) .$$

Hence $2^{h_2}\cdot 3^{h_3}\cdot 5^{h_5}\cdot 7^{h_7} \mid G_\alpha(n)$ whenever $p^{\ell_1+1} \mid G_\alpha(n)$. We have taken ℓ_1 so large that always

$$G_\alpha(n_2) > 2^{h_2}\cdot 3^{h_3}\cdot 5^{h_5}\cdot 7^{h_7} . \tag{7.23}$$

Consequently, there exists some prime $r \geq 11$ that divides $G_\alpha(n_2)$, hence r divides all $G_\alpha(n)$ with $p^{\ell_1+1} \mid G_\alpha(n)$. It follows that for a solution of equation (7.22) we must have

$$\operatorname{ord}_p(G_\alpha(n)) \leq \ell_1 .$$

In this way we find with ease all solutions of (7.22). □

Let us illustrate this with the example $D = 3$, $\alpha = \sqrt{3}$. Then

$$G_\alpha(n) = \tfrac{1}{2}\cdot(2+\sqrt{3})^n + \tfrac{1}{2}\cdot(2-\sqrt{3})^n ,$$

and $G_\alpha(-n) = G_\alpha(n)$. We have for $G_\alpha(n)$:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$G_\alpha(n)$	1	2	7	26	97	362	....					$G_\alpha(14) = 50843527$				
mod 4	1	2	-1	2	1	2	-1	2	1	2	-1	2	1	2	-1	2
mod 3	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
mod 5	1	2	2	1	2	2	1	2	2	1	2	2	1	2	2	1
mod 49	1	2	7	-23	-1	19	-21	-5	1	9	-14	-16	-1	12	0	-12

We see that $2^2, 3, 5 \nmid G_\alpha(n)$ for all $n \in \mathbb{Z}$, and $2 \mid G_\alpha(n)$ if and only if n odd. So $p = 7$ is the only interesting case. We have $7 \mid G_\alpha(n)$ if and only if $n \equiv 2 \pmod 4$, $7^2 \mid G_\alpha(n)$ if and only if $n \equiv 14 \pmod{28}$, (and in general

$$7^k \mid G_\alpha(n) \Leftrightarrow n \equiv 2\cdot 7^{k-1} \pmod{4\cdot 7^{k-1}}$$

for $k \geq 1$, and a similar relation holds for any symmetric recurrence and any prime p for which arbitrary high powers of p occur in $G_\alpha(n)$). Now, $\ell_1 = 0$ does not lead to (7.23), since then $n_2 = 2$, and $G_\alpha(2) = 7$, so that no suitable r exists. But with $\ell_1 = 1$ we have $n_2 = 14$, and $h_2 = h_3 = h_5 = 0$, $h_7 = 2$, and (7.23) holds, since $G_\alpha(14) > 7^2$. Hence there exists a prime $r \geq 11$ such that $r \mid G_\alpha(14)$, and thus $r \mid G_\alpha(n)$ whenever $7^2 \mid G_\alpha(n)$. It follows that for solutions of (7.22) we have $G_\alpha(n) \leq 2^1\cdot 3^0\cdot 5^0\cdot 7^1 = 14$, so that all solutions can be read from the above table. Note that it is not necessary that r is known explicitly, only that $G_\alpha(n_2)$ is large enough. In our example, $r = 337$ or $r = 3079$ satisfy.

Finally we treat the remaining 54 cases, where $I \neq \emptyset$. Then we need the non-elementary reduction technique described in Sections 7.5 to 7.7.

In all our instances, the set I contains only one element, since there is only one splitting prime. We denote by π the π_i belonging to this prime, and we write m for c_i. Equation (7.10) now reads

$$\frac{\alpha}{2\sqrt{D}}\cdot\epsilon^n\cdot\pi^m - \frac{\alpha'}{2\sqrt{D}}\cdot\epsilon'^n\cdot\pi'^m = \pm\prod_{j\in I_U} p_j^{u_j} .$$

We computed the constants C_1 to C_{12}, C_{12}^*, according to Section 7.6, for each of the 54 cases. We omit the details of these computations, and simply give the data in Table VI. In this table we give for each D the $p_i \in I_U$ together with the ν_i and λ_i (it turns out that the λ_i do not depend on the α , only on the p_i). The values "n_ϵ, n_π, n_2, n_3, n_5, n_7" are the integers such that

$$\alpha^2 = \pm\, \epsilon^{n_\epsilon}\cdot\pi^{n_\pi}\cdot 2^{n_2}\cdot\ldots\cdot 7^{n_7} .$$

It follows that in all cases we have $C_{12}^* < 3.23\times10^{30}$.

The next step is to define the lattices, and find lower bounds for the shortest nonzero vectors in the lattices. We start with treating the Λ_i^* , of which there are 3 for each of the 10 D's . We have computed the 30 values of

$$\vartheta = -\frac{\log_{p_i}\left(\frac{\pi}{\pi'}\right)}{\log_{p_i}\left(\frac{\epsilon}{\epsilon'}\right)} \quad\text{or}\quad -\frac{\log_{p_i}\left(\frac{\epsilon}{\epsilon'}\right)}{\log_{p_i}\left(\frac{\pi}{\pi'}\right)} ,$$

such that it is a p_i-adic integer, to the desired precision of μ digits. We took μ as follows:

p_i	μ	p_i^μ
2	209	8.22×10^{62}
3	133	2.87×10^{63}
5	95	2.52×10^{66}
7	76	1.69×10^{64}

in order to have p_i^μ somewhat larger than the maximal C_{12}^{*2} , being 1.05×10^{61} . We computed the 30 values of the $\vartheta^{(\mu)}$'s , but do not give them here. The lattices Γ_μ are generated by the column vectors of the matrices

$$\begin{pmatrix} 1 & 0 \\ \vartheta^{(\mu)} & p^\mu \end{pmatrix} .$$

We performed the p-adic continued fraction algorithm of Section 3.10 for each of these 30 lattices. In the table below we give for each D the maximal C_{12}^* (there is one for each α), and the minimal bound for $\ell(\Gamma_\mu)$ (there is one for each $i \in I_U$) that we found. We omit further details. In all cases, $\ell(\Gamma_\mu) > \sqrt{2}\cdot C_{12}^*$. Hence Lemma 3.14 with $n = 2$, $c_1 = 0$, $c_2 = 1$ yields

$$\mathrm{ord}_{p_i}(\Lambda_i^*) < \mu + \mu_0 , \quad i \in I_U ,$$

where

$$\mu_0 = \min\left[\ \mathrm{ord}_{p_i}(\log_{p_i}(\tfrac{\epsilon}{\epsilon'})),\ \mathrm{ord}_{p_i}(\log_{p_i}(\tfrac{\pi}{\pi'}))\ \right] ,$$

D	p	μ_0	$c_{12}^* \le$	$\ell(\Gamma_\mu) >$	$U \le$
2	2, 3, 5	1.5, 1.0, 1.0	3.19×10^{28}	8.26×10^{30}	210
6	2, 3, 7	1.5, 1.5, 1.0	2.72×10^{26}	2.05×10^{31}	210
7	2, 5, 7	2.0, 1.0, 0.5	1.07×10^{30}	2.43×10^{31}	210
10	2, 5, 7	1.5, 0.5, 1.0	3.22×10^{29}	2.22×10^{31}	210
14	2, 3, 7	1.5, 1.0, 0.5	4.80×10^{26}	1.48×10^{31}	210
15	2, 3, 5	3.5, 1.5, 0.5	2.15×10^{28}	1.55×10^{31}	212
21	2, 3, 7	3.0, 0.5, 0.5	1.90×10^{26}	7.78×10^{30}	211
30	2, 3, 5	2.5, 0.5, 0.5	4.15×10^{28}	1.37×10^{31}	211
70	2, 5, 7	2.5, 0.5, 0.5	3.23×10^{30}	2.51×10^{31}	211
105	3, 5, 7	1.5, 0.5, 0.5	4.54×10^{29}	3.96×10^{31}	134

as given above. By $\lambda_i + \text{ord}_{p_i}(h^*) \ge 0$ we obtain from Lemma 7.6(i) upper bounds for u_i , $i \in I_U$, hence the upper bounds for U , as given in the table above.

Next, we treat the K_i^* , one for each D , having 5 terms, namely

$$K_i^* = n^*\cdot\log_{p_i}(\epsilon') + m^*\cdot\log_{p_i}(\pi') - \sum_{\substack{1\le j\le 4\\ j\ne i}} u_j^*\cdot\log_{p_i}(p_j) ,$$

where $i \in I$, so p_i is the splitting prime. We have the following data. From this table our choice for $\sqrt{D} \pmod{p_i}$ becomes clear.

D	p_i	$\sqrt{D} \pmod{p_i}$	$\text{ord}_{p_i}(\log_{p_i}(\cdot))$ ϵ'	π'	2	3	5	7
2	7	3	1	2	1	1	1	-
6	5	4	1	1	1	1	-	2
7	3	1	1	1	1	-	1	1
10	3	2	1	1	1	-	1	1
14	5	2	1	1	1	1	-	2
15	7	6	1	1	1	1	1	-
21	5	4	1	1	1	1	-	2
30	7	4	1	1	1	1	1	-
70	3	2	1	1	1	-	1	1
105	2	1 (mod 4)	2	4	-	2	2	3

It follows that $\text{ord}_{p_i}(\log_{p_i}(\epsilon'))$ is always the least one of the five ord_{p_i}'s in the above table. So we define:

$$\vartheta_1 = -\frac{\log_{p_i}(\pi')}{\log_{p_i}(\epsilon')}, \quad \vartheta_{2,3,4} = -\frac{\log_{p_i}(p_j)}{\log_{p_i}(\epsilon')}, \quad (j \in \{1,2,3,4\},\ j\neq i),$$

and we computed these numbers up to μ digits, with μ as follows.

p_i	μ	p_i^{μ}
2	539	1.80×10^{162}
3	343	4.49×10^{163}
5	245	1.77×10^{171}
7	196	4.36×10^{165}

so that p_i^{μ} is somewhat larger than the maximal C_{12}^{*5}. We computed the 40 values of the $\vartheta_{1,2,3,4}^{(\mu)}$, but do not give them here. The lattices Γ_{μ} are generated by the columns of the following matrices:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \vartheta_1^{(\mu)} & \vartheta_2^{(\mu)} & \vartheta_3^{(\mu)} & \vartheta_4^{(\mu)} & p^{\mu} \end{pmatrix}.$$

We computed the reduced bases of the 10 lattices by the L^3-algorithm. Again, we omit the computational details. We found data as follows.

D	p in I	μ	μ_0	$C_{12}^{*} \le$	$\ell(\Gamma_{\mu}) >$	M $\le$
2	7	196	1	3.19×10^{28}	2.25×10^{32}	196
6	5	245	1	2.72×10^{26}	2.16×10^{33}	245
7	3	343	1	1.07×10^{30}	1.14×10^{32}	343
10	3	343	1	3.22×10^{29}	1.07×10^{32}	343
14	5	245	1	4.80×10^{26}	4.92×10^{33}	245
15	7	196	1	2.15×10^{28}	2.78×10^{32}	196
21	5	245	1	1.90×10^{26}	4.37×10^{33}	245
30	7	196	1	4.15×10^{28}	2.69×10^{32}	196
70	3	343	1	3.23×10^{30}	1.03×10^{32}	343
105	2	539	2	4.54×10^{29}	6.68×10^{31}	540

In all instances, $\ell(\Gamma_\mu) > \sqrt{5}\cdot C_{12}^*$, so that by Lemmas 3.14 and 7.6(ii) and $\kappa_i + \mathrm{ord}_{p_i}(h^*) \geq 0$ and $h_i \geq 1$ we have $M \leq \mathrm{ord}_{p_i}(K_i^*) < \mu + \mu_0$, hence an upper bound for M as given in the table above.

Finally, we compute the new, reduced bounds for $|n|$, and thus for B . This we do by

$$|n| < \max\left(C_5,\ C_6 + C_7\cdot M,\ C_8 + C_9\cdot U \right) .$$

Hence we find data as in the following table.

Here we used $B^* \leq h^*\cdot B + N$ and $h^* = 2$. So in one step we have reduced the bound $B^* < 3.23\times10^{31}$ to $B^* \leq 1627$. The total computation time was 1715 sec, on average 0.7 sec for each 2-dimensional lattice, and 170 sec for each 5-dimensional lattice.

D	$C_5 <$	$C_6 <$	$C_7 <$	$C_8 <$	$C_9 <$	$M \leq$	$U \leq$	$\|n\| \leq$	$B \leq$	$N \leq$	$B^* \leq$
2	0.394	0.394	0.420	1.967	3.859	196	210	812	812	3	1627
6	0.152	0.652	0.190	1.345	1.631	245	210	343	343	3	689
7	0.126	0.626	0.357	2.702	2.757	343	210	581	581	2	1164
10	0.601	0.191	0.181	1.396	2.337	343	210	492	492	3	987
14	0.102	0.602	0.325	1.861	1.508	245	210	318	318	3	639
15	0.540	0.668	0.257	1.394	1.649	196	212	350	350	2	702
21	0.222	0.722	0.142	1.564	2.386	245	211	505	505	1	1011
30	0.414	0.613	0.399	1.239	1.102	196	211	233	233	3	469
70	0.362	0.556	0.390	2.729	1.505	343	211	320	343	3	689
105	0.390	0.579	0.379	3.232	2.545	540	134	344	540	1	1081

We made a further reduction step, now using the reduced bound for B^* as given above in stead of C_{12}^* . We give the data for the Λ_i^* in the table below. For μ we took $\mu_1\cdot\mu_2$, with μ_1 as above, and μ_2 as below:

p	2	3	5	7
μ_2	11	7	5	4

We found $\ell(\Gamma_\mu)$ and bounds for U as given above. For the K_i^* we found, with $\mu = \mu_1\cdot\mu_2$ with μ_2 as above, and μ_1 as in the first table below, the results given in the second table below.

D	$B^* \leq$	$\sqrt{2}\cdot B^* <$	μ_1	$\mu \leq$	$\ell(\Gamma_\mu) \geq$	$\mu_0 \leq$	$U \leq$
2	1627	2301	2	22	1.82×10^3	1.5	23
6	689	975	3	33	3.99×10^4	1.5	34
7	1164	1647	3	33	4.50×10^4	2	34
10	987	1396	3	33	5.91×10^4	1.5	34
14	639	904	3	33	2.58×10^4	1.5	34
15	702	993	3	33	7.36×10^4	3.5	36
21	1011	1430	3	33	2.00×10^4	3	35
30	469	664	2	22	9.98×10^2	2.5	24
70	689	975	3	33	5.76×10^4	2.5	35
105	1081	1529	3	21	3.89×10^4	1.5	22

D	$B^* \leq$	$\sqrt{5}\cdot B^* <$	μ_1	$\mu \leq$	$\ell(\Gamma_\mu) \geq$	$\mu_0 \leq$	$M \leq$	$\lvert n\rvert \leq$	$B \leq$	$B^* \leq$
2	1627	3639	7	28	1.24×10^4	1	28	90	90	183
6	689	1541	6	30	4.04×10^3	1	30	145	145	293
7	1164	2603	7	49	1.07×10^4	1	49	96	96	194
10	987	2207	7	49	1.16×10^4	1	49	80	80	163
14	639	1429	6	30	3.07×10^3	1	30	53	53	109
15	702	1570	6	24	2.70×10^3	1	24	60	60	122
21	1011	2261	6	30	3.88×10^3	1	30	85	85	171
30	469	1049	6	24	2.50×10^3	1	24	27	27	57
70	689	1541	6	42	1.90×10^3	1	42	55	55	113
105	1081	2418	7	77	1.00×10^4	2	78	59	78	157

The computation time was 15 sec. We made a third step, with for Λ_i^*, K_i^* :

D	$B^* \leq$	$\sqrt{2}\cdot B^* <$	μ_1	$\mu \leq$	$\ell(\Gamma_\mu) \geq$	$\mu_0 \leq$	$U \leq$
2	183	258.9	2	22	1821	1.5	23
6	299	414.4	2	22	875	1.5	23
7	194	274.4	2	22	1285	2	23
10	163	230.6	2	22	634	1.5	23
14	109	154.2	2	22	268	1.5	23
15	122	172.6	2	22	873	3.5	25
21	171	241.9	2	22	818	3	25
30	57	80.7	2	22	998	2.5	24
70	113	159.9	2	22	585	2.5	24
105	157	222.1	2	14	281	1.5	15

D	$B^* \leq$	$\sqrt{5}\cdot B^* <$	μ_1	$\mu \leq$	$\ell(\Gamma_\mu) \geq$	$\mu_0 \leq$	$M \leq$
2	183	409.3	5	20	440	1	20
6	293	655.2	5	25	665	1	25
7	194	433.8	6	42	602	1	42
10	163	364.5	5	35	473	1	35
14	109	243.8	5	25	626	1	25
15	122	272.9	6	24	2700	1	24
21	171	382.4	5	25	645	1	25
30	57	127.5	4	16	129	1	16
70	113	252.7	5	35	366	1	35
105	157	351.1	5	55	354	2	56

and finally for $|n|$, and in more detail for $\text{ord}_{p_i}(u)$ for $i \in I_U$

D	$M \leq$	$u_2 \leq$	$u_3 \leq$	$u_5 \leq$	$u_7 \leq$	$\|n\| \leq$
2	20	23	14	10	0	90
6	25	23	15	0	8	38
7	42	23	0	10	8	66
10	35	23	0	10	8	55
14	25	23	14	0	8	36
15	24	25	15	10	0	42
21	25	24	14	0	8	61
30	16	24	14	10	0	27
70	35	24	0	10	8	65
105	56	0	14	10	8	41

Now we will not find any further improvement if we proceed in the same way. But the upper bounds are now small enough to admit enumeration of the remaining possibilities, making use of mod p arithmetic for $p = 2, 3, 5, 7$. We did so, and found the remaining solutions, presented in Table I. We used only 3 sec computer time for this last step.

This completes the proof of Theorem 7.2. □

7.9. Tables.

Table I. (Theorem 7.2.)

Nr	X	Y	Z	D	Nr	X	Y	Z	D
1	4375	-4374	1	7	51	7	2	3	7
2	2401	-2400	1	1	52	6	3	3	6
3	225	-224	1	1	53	5	4	3	5
4	126	-125	1	14	54	70	-54	4	70
5	81	-80	1	1	55	30	-14	4	30
6	64	-63	1	1	56	25	-9	4	1
7	50	-49	1	2	57	21	-5	4	21
8	49	-48	1	1	58	18	-2	4	2
9	36	-35	1	1	59	15	1	4	15
10	28	-27	1	7	60	14	2	4	14
11	25	-24	1	1	61	10	6	4	10
12	21	-20	1	21	62	9	7	4	1
13	16	-15	1	1	63	5145	-5120	5	105
14	15	-14	1	15	64	270	-245	5	30
15	10	-9	1	10	65	160	-135	5	10
16	9	-8	1	1	66	105	-80	5	105
17	8	-7	1	2	67	81	-56	5	1
18	7	-6	1	7	68	70	-45	5	70
19	6	-5	1	6	69	60	-35	5	15
20	5	-4	1	5	70	49	-24	5	1
21	4	-3	1	1	71	45	-20	5	5
22	3	-2	1	3	72	40	-15	5	10
23	2	-1	1	2	73	35	-10	5	35
24	490	-486	2	10	74	32	-7	5	2
25	54	-50	2	6	75	30	-5	5	30
26	49	-45	2	1	76	28	-3	5	7
27	25	-21	2	1	77	27	-2	5	3
28	18	-14	2	2	78	24	1	5	6
29	14	-10	2	14	79	21	4	5	21
30	10	-6	2	10	80	20	5	5	5
31	9	-5	2	1	81	18	7	5	2
32	7	-3	2	7	82	16	9	5	1
33	6	-2	2	6	83	15	10	5	15
34	5	-1	2	5	84	50	-14	6	2
35	3	1	2	3	85	42	-6	6	42
36	2	2	2	2	86	35	1	6	35
37	384	-375	3	6	87	30	6	6	30
38	105	-96	3	105	88	21	15	6	21
39	84	-75	3	21	89	1750	-1701	7	70
40	49	-40	3	1	90	945	-896	7	105
41	30	-21	3	30	91	625	-576	7	1
42	25	-16	3	1	92	224	-175	7	14
43	24	-15	3	6	93	189	-140	7	21
44	21	-12	3	21	94	175	-126	7	7
45	16	-7	3	1	95	112	-63	7	7
46	15	-6	3	15	96	105	-56	7	105
47	14	-5	3	14	97	84	-35	7	21
48	12	-3	3	3	98	81	-32	7	1
49	10	-1	3	10	99	70	-21	7	70
50	8	1	3	2	100	64	-15	7	1

Table I. (cont.)

Nr	X	Y	Z	D	Nr	X	Y	Z	D
101	63	-14	7	7	151	72	49	11	2
102	56	-7	7	14	152	294	-150	12	6
103	54	-5	7	6	153	150	-6	12	6
104	50	-1	7	2	154	147	-3	12	3
105	48	1	7	3	155	729	-560	13	1
106	45	4	7	5	156	512	-343	13	2
107	42	7	7	42	157	294	-125	13	6
108	40	9	7	10	158	250	-81	13	10
109	35	14	7	35	159	225	-56	13	1
110	28	21	7	7	160	196	-27	13	1
111	25	24	7	1	161	189	-20	13	21
112	750	-686	8	30	162	175	-6	13	7
113	189	-125	8	21	163	168	1	13	42
114	162	-98	8	2	164	162	7	13	2
115	70	-6	8	70	165	160	9	13	10
116	63	1	8	7	166	144	25	13	1
117	54	10	8	6	167	120	49	13	30
118	50	14	8	2	168	105	64	13	105
119	49	15	8	1	169	250	-54	14	10
120	375	-294	9	15	170	210	-14	14	210
121	256	-175	9	1	171	189	7	14	21
122	105	-24	9	105	172	175	21	14	7
123	96	-15	9	6	173	126	70	14	14
124	84	-3	9	21	174	960	-735	15	15
125	80	1	9	5	175	245	-20	15	5
126	75	6	9	3	176	240	-15	15	15
127	60	21	9	15	177	224	1	15	14
128	56	25	9	14	178	210	15	15	210
129	49	32	9	1	179	120	105	15	30
130	343	-243	10	7	180	270	-14	16	30
131	135	-35	10	15	181	250	6	16	10
132	105	-5	10	105	182	175	81	16	7
133	98	2	10	2	183	6561	-6272	17	1
134	90	10	10	10	184	1024	-735	17	1
135	70	30	10	70	185	625	-336	17	1
136	625	-504	11	1	186	343	-54	17	7
137	441	-320	11	1	187	324	-35	17	1
138	256	-135	11	1	188	294	-5	17	6
139	196	-75	11	1	189	288	1	17	2
140	175	-54	11	7	190	280	9	17	70
141	135	-14	11	15	191	240	49	17	15
142	128	-7	11	2	192	225	64	17	1
143	126	-5	11	14	193	189	100	17	21
144	125	-4	11	5	194	294	30	18	6
145	120	1	11	30	195	1225	-864	19	1
146	112	9	11	7	196	486	-125	19	6
147	105	16	11	105	197	441	-80	19	1
148	100	21	11	1	198	375	-14	19	15
149	96	25	11	6	199	360	1	19	10
150	81	40	11	1	200	343	18	19	7

Table I. (cont.)

Nr	X	Y	Z	D
201	336	25	19	21
202	280	81	19	70
203	256	105	19	1
204	490	-90	20	10
205	405	-5	20	5
206	525	-84	21	21
207	448	-7	21	7
208	420	21	21	105
209	336	105	21	21
210	729	-245	22	1
211	490	-6	22	10
212	486	-2	22	6
213	1215	-686	23	15
214	1029	-500	23	21
215	729	-200	23	1
216	625	-96	23	1
217	525	4	23	21
218	504	25	23	14
219	480	49	23	30
220	448	81	23	7
221	625	-49	24	1
222	945	-320	25	105
223	640	-15	25	10
224	630	-5	25	70
225	576	49	25	1
226	490	135	25	10
227	686	-10	26	14
228	675	1	26	3
229	1029	-300	27	21
230	750	-21	27	30
231	735	-6	27	15
232	1134	-350	28	14
233	1225	-384	29	1
234	840	1	29	210
235	729	112	29	1
236	625	216	29	1
237	441	400	29	1
238	6561	-5600	31	1
239	2401	-1440	31	1
240	1024	-63	31	1
241	960	1	31	15
242	945	16	31	105
243	625	336	31	1
244	1029	-5	32	21
245	2625	-1536	33	105
246	1029	60	33	21
247	1792	-567	35	7
248	1260	-35	35	35
249	1215	10	35	15
250	1120	105	35	70

Nr	X	Y	Z	D
251	945	280	35	105
252	1372	-3	37	7
253	1344	25	37	21
254	1225	144	37	1
255	729	640	37	1
256	1458	-14	38	2
257	1536	-15	39	6
258	1500	21	39	15
259	896	625	39	14
260	2401	-720	41	1
261	1701	-20	41	21
262	1680	1	41	105
263	1600	81	41	1
264	1750	14	42	70
265	1800	49	43	2
266	1120	729	43	70
267	1250	686	44	2
268	1920	105	45	30
269	16384	-14175	47	1
270	2401	-192	47	1
271	2205	4	47	5
272	2160	49	47	15
273	2625	-224	49	105
274	2400	1	49	6
275	1701	700	49	21
276	2430	70	50	30
277	2625	-24	51	105
278	2401	200	51	1
279	15309	-12500	53	21
280	2800	9	53	7
281	2025	784	53	1
282	3430	-405	55	70
283	3024	1	55	21
284	3150	-14	56	14
285	3200	49	57	2
286	4050	-686	58	2
287	3456	25	59	6
288	2401	1080	59	1
289	35721	-32000	61	1
290	4096	-375	61	1
291	3969	-125	62	1
292	2625	1344	63	105
293	3969	256	65	1
294	4480	9	67	70
295	4374	250	68	6
296	5145	-384	69	105
297	15625	-10584	71	1
298	5040	1	71	35
299	4096	945	71	1
300	4704	625	73	6

Table I. (cont.)

Nr	X	Y	Z	D
301	5145	480	75	105
302	3375	2401	76	15
303	6804	-875	77	21
304	6561	-320	79	1
305	6250	-9	79	10
306	3840	2401	79	15
307	8505	-1280	85	105
308	7840	81	89	10
309	65625	-57344	91	105
310	8505	-224	91	105
311	10240	-1215	95	10
312	9408	1	97	3
313	9800	1	99	2
314	10206	-5	101	14
315	9375	1029	102	15
316	10584	25	103	6
317	11250	-14	106	2
318	12544	225	113	1
319	10368	2401	113	2
320	13230	-5	115	30
321	15625	-1701	118	1
322	14336	-175	119	14
323	14175	-14	119	7
324	14406	-6	120	6
325	18225	-3584	121	1
326	16128	1	127	7
327	15625	504	127	1
328	15625	1536	131	1
329	17500	189	133	7
330	18144	625	137	14
331	18750	294	138	30
332	117649	-97200	143	1
333	21504	105	147	21
334	24010	15	155	10
335	23625	1024	157	105
336	25920	1	161	5
337	26250	-6	162	42
338	16807	13122	173	7
339	30618	7	175	42
340	32768	-7	181	2
341	33614	-125	183	14
342	43740	-1715	205	15
343	43750	-486	208	70
344	46305	-80	215	105
345	50625	-896	223	1
346	49000	729	223	10
347	129654	-78125	227	6
348	55566	-3125	229	14
349	60025	-1944	241	1
350	59535	1	244	15

Nr	X	Y	Z	D
351	59049	1960	247	1
352	63000	1	251	70
353	64000	9	253	10
354	48384	15625	253	21
355	59049	7000	257	1
356	69120	49	263	30
357	85750	-486	292	70
358	83349	2500	293	21
359	140625	-43904	311	1
360	109375	-1134	329	7
361	82944	30625	337	1
362	128625	256	359	105
363	137781	-140	371	21
364	76545	71680	385	105
365	196830	-33614	404	30
366	117649	48000	407	1
367	168070	30	410	70
368	179200	6561	431	7
369	137200	59049	443	7
370	201684	-1875	447	21
371	201600	1	449	14
372	214375	-6	463	7
373	252105	-24576	477	105
374	243000	49	493	30
375	245760	-735	495	15
376	262144	5145	517	1
377	390625	-112896	527	1
378	688905	-5	830	105
379	1058841	-20480	1019	1
380	1440000	2401	1201	1
381	1640625	336	1281	105
382	4214784	25	2053	21
383	4782969	4375	2188	1
384	5764801	-9600	2399	1
385	19140625	-17496	4373	1
386	23049600	1	4801	6
387	76545000	1	8749	42
388	199290375	-686	14117	15

Table II.

D	h	ϵ	$N\epsilon$	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	π_i
2	1	$1+\sqrt{2}$	-1	$\sqrt{2}$	3	5	$1+2\sqrt{2}^*$	$1+2\sqrt{2}$
3	1	$2+\sqrt{3}$	1	$1+\sqrt{3}$	$\sqrt{3}$	5	7	–
5	1	$\frac{1}{2}(1+\sqrt{5})$	-1	2	3	$\sqrt{5}$	7	–
6	1	$5+2\sqrt{6}$	1	$2+\sqrt{6}$	$3+\sqrt{6}$	$1+\sqrt{6}^*$	7	$1+\sqrt{6}$
7	1	$8+3\sqrt{7}$	1	$3+\sqrt{7}$	$2+\sqrt{7}^*$	5	$\sqrt{7}$	$2+\sqrt{7}$
10	2	$3+\sqrt{10}$	-1	$\mathfrak{p}_1$	$\mathfrak{p}_2^*$	$\mathfrak{p}_3$	7	$1+\sqrt{10}$
14	1	$15+4\sqrt{14}$	1	$4+\sqrt{14}$	3	$3+\sqrt{14}^*$	$7+2\sqrt{14}$	$3+\sqrt{14}$
15	2	$4+\sqrt{15}$	1	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4^*$	$8+\sqrt{15}$
21	1	$\frac{1}{2}(5+\sqrt{21})$	1	2	$\frac{1}{2}(3+\sqrt{21})$	$\frac{1}{2}(1+\sqrt{21})^*$	$\frac{1}{2}(7+\sqrt{21})$	$\frac{1}{2}(1+\sqrt{21})$
30	2	$11+2\sqrt{30}$	1	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$5+\sqrt{30}$	$\mathfrak{p}_4^*$	$13+2\sqrt{30}$
35	2	$6+\sqrt{35}$	1	$\mathfrak{p}_1$	3	$\mathfrak{p}_3$	$\mathfrak{p}_4$	–
42	2	$13+2\sqrt{42}$	1	$\mathfrak{p}_1$	$\mathfrak{p}_2$	5	$7+\sqrt{42}$	–
70	2	$251+30\sqrt{70}$	1	$\mathfrak{p}_1$	$\mathfrak{p}_2^*$	$25+3\sqrt{70}$	$\mathfrak{p}_4$	$17+2\sqrt{70}$
105	2	$41+4\sqrt{105}$	1	$\mathfrak{p}_1^*$	$\mathfrak{p}_2$	$10+\sqrt{105}$	$\mathfrak{p}_4$	$\frac{1}{2}(11+\sqrt{105})$
210	4	$29+2\sqrt{210}$	1	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	–

Table III.

D	$\mathfrak{p}_1\cdot\mathfrak{p}_2$	$\mathfrak{p}_1\cdot\mathfrak{p}_3$	$\mathfrak{p}_1\cdot\mathfrak{p}_4$	$\mathfrak{p}_2\cdot\mathfrak{p}_3$	$\mathfrak{p}_2\cdot\mathfrak{p}_4$	$\mathfrak{p}_3\cdot\mathfrak{p}_4$
10	$-2+\sqrt{10}$	$\sqrt{10}$	–	$5-\sqrt{10}$	–	–
15	$3+\sqrt{15}$	$5+\sqrt{15}$	$1+\sqrt{15}$	$\sqrt{15}$	$6-\sqrt{15}$	$-5+2\sqrt{15}$
30	$6+\sqrt{30}$	–	$-4+\sqrt{30}$	–	$3+\sqrt{30}$	–
35	–	$5+\sqrt{35}$	$7+\sqrt{35}$	–	–	$\sqrt{35}$
42	$6+\sqrt{42}$	–	–	–	–	–
70	$-8+\sqrt{70}$	–	$42+5\sqrt{70}$	–	$7+\sqrt{70}$	–
105	$\frac{1}{2}(-9+\sqrt{105})$	–	$\frac{1}{2}(7+\sqrt{105})$	–	$21+2\sqrt{105}$	–
210	–	–	$14+\sqrt{210}$	$15+\sqrt{210}$	–	–

Table IV.

D	α	I	I_U
2	1	–	2357
	1	7	235
	$\sqrt{2}$	–	3 7
	$\sqrt{2}$	7	35
3	1	–	2357
	$\sqrt{3}$	–	2 7
	$1+\sqrt{3}$	–	3
	$3+\sqrt{3}$	–	5
5	2	–	2357
	$2\sqrt{5}$	–	23 7
6	1	–	2357
	1	5	23 7
	$\sqrt{6}$	–	57
	$\sqrt{6}$	5	7
	$2+\sqrt{6}$	–	3
	$2+\sqrt{6}$	5	3
	$3+\sqrt{6}$	–	–
	$3+\sqrt{6}$	5	2
7	1	–	2357
	1	3	2 57
	$\sqrt{7}$	–	2
	$\sqrt{7}$	3	2 5
	$3+\sqrt{7}$	–	7
	$3+\sqrt{7}$	3	57
	$7+3\sqrt{7}$	–	35
	$7+3\sqrt{7}$	3	5
10	1	–	2357
	1	3	2 57
	$\sqrt{10}$	–	3 7
	$\sqrt{10}$	3	7
	$-2+\sqrt{10}$*	3	57
	$5-\sqrt{10}$*	3	2 7
14	1	–	2357
	1	5	23 7
	$\sqrt{14}$	–	35
	$\sqrt{14}$	5	3
14	$4+\sqrt{14}$	–	7
	$4+\sqrt{14}$	5	7
	$7+2\sqrt{14}$	–	2
	$7+2\sqrt{14}$	5	2
15	1	–	2357
	1	7	235
	$\sqrt{15}$	–	2
	$\sqrt{15}$	7	2
	$3+\sqrt{15}$	–	57
	$3+\sqrt{15}$	7	5
	$5+\sqrt{15}$	–	3
	$5+\sqrt{15}$	7	3
	$1+\sqrt{15}$*	7	35
	$15+\sqrt{15}$*	7	–
	$6-\sqrt{15}$*	7	2 5
	$-5+2\sqrt{15}$*	7	23
21	2	–	2357
	2	5	23 7
	$2\sqrt{21}$	–	2 5
	$2\sqrt{21}$	5	2
	$3+\sqrt{21}$	–	2 7
	$3+\sqrt{21}$	5	2 7
	$7+\sqrt{21}$	–	23
	$7+\sqrt{21}$	5	23
30	1	–	2357
	1	7	235
	$\sqrt{30}$	–	–
	$\sqrt{30}$	7	–
	$5+\sqrt{30}$	–	3 7
	$5+\sqrt{30}$	7	3
	$6+\sqrt{30}$	–	5
	$6+\sqrt{30}$	7	5
	$3+\sqrt{30}$*	7	5
	$10+\sqrt{30}$*	7	3
	$-4+\sqrt{30}$*	7	35
	$15-2\sqrt{30}$*	7	2
35	1	–	2357
	$\sqrt{35}$	–	23
	$5+\sqrt{35}$	–	7
	$7+\sqrt{35}$	–	5
42	1	–	2357
	$\sqrt{42}$	–	–
	$6+\sqrt{42}$	–	57
	$7+\sqrt{42}$	–	3
70	1	–	2357
	1	3	2 57
	$\sqrt{70}$	–	–
	$\sqrt{70}$	3	–
	$25+3\sqrt{70}$	–	3 7
	$25+3\sqrt{70}$	3	7
	$42+5\sqrt{70}$	–	5
	$42+5\sqrt{70}$	3	5
	$7+\sqrt{70}$*	3	5
	$10+\sqrt{70}$*	3	7
	$-8+\sqrt{70}$*	3	57
	$35-4\sqrt{70}$*	3	2
105	2	–	2357
	2	2	357
	$2\sqrt{105}$	–	2
	$2\sqrt{105}$	2	–
	$20+2\sqrt{105}$	–	23 7
	$20+2\sqrt{105}$	2	3 7
	$42+4\sqrt{105}$	–	2 5
	$42+4\sqrt{105}$	2	5
	$7+\sqrt{105}$*	2	35
	$15+\sqrt{105}$*	2	7
	$-9+\sqrt{105}$*	2	57
	$35-3\sqrt{105}$*	2	3
210	1	–	2357
	$\sqrt{210}$	–	–
	$14+\sqrt{210}$	–	35
	$15+\sqrt{210}$	–	7

Table V.

D	A	B	a	b	n_0	p = 2							p = 3							p = 5							p = 7						
						ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7
2	2	-1	1	0	0	2	0	8	3	1	0	0	1	0	12	2	2	1	1	1	0	15	0	0	2	0	1	0	42	1	0	1	2
2	2	-1	0	1	0	0							1	6	12	0	2	0	0	0							1	21	42	0	0	0	2
3	4	1	1	0	0	3	0	8	4	0	0	1	1	0	9	0	2	1	0	1	0	15	0	1	2	0	1	0	28	3	0	0	2
3	4	1	0	1	0	1							0							0							1	14	28	0	0	0	2
3	4	1	1	1	-1	0							1	4	9	0	2	0	0	0							0						
3	4	1	3	1	-1	0							0							1	7	15	0	0	2	0	0						
5	1	-1	2	0	0	4	0	24	5	2	0	1	2	0	36	4	3	0	0	1	0	25	0	0	2	0	1	0	56	0	1	0	2
5	1	-1	0	2	0	2							2	18	36	1	3	0	0	0							1	28	56	0	0	0	2
6	10	1	1	0	0	3	0	8	4	0	1	2	0	0	3	1	2	0	0	1	0	10	2	0	2	0	2	0	28	3	0	1	3
6	10	1	0	1	0	0							0							1	5	10	0	0	2	0	2	14	28	0	0	0	3
6	10	1	2	1	-1	0							2	4	9	0	3	0	0	0							0						
6	10	1	3	1	-1	0							0							0							0						
7	16	1	1	0	0	4	0	4	5	1	0	0	1	0	3	0	2	1	0	0	0	3	0	2	1	0	0	0	7	0	1	0	1
7	16	1	0	1	0	3							0							0							0						
7	16	1	3	1	-1	0							0							0							0	3	7	0	0	0	1
7	16	1	7	3	-1	0							2	4	9	0	3	1	0	1	7	15	0	2	2	0	0						
10	6	-1	1	0	0	1	0	4	2	1	0	0	1	0	6	1	2	0	0	0	0	5	0	0	1	0	0	0	8	3	1	0	1
10	6	-1	0	1	0	0							1	3	6	0	2	0	0	0							0	4	8	0	0	0	1
14	30	1	1	0	0	3	0	4	4	1	1	0	1	0	6	3	2	1	0	1	0	10	3	1	2	0	0	0	7	2	0	0	1
14	30	1	0	1	0	0							1	3	6	0	2	1	0	1	5	10	0	1	2	0	0						
14	30	1	4	1	-1	0							0							0							0	3	7	0	0	0	1
14	30	1	7	2	-1	1							0							0							0						
15	8	1	1	0	0	3	0	4	4	0	0	0	2	0	9	0	3	0	1	0	0	5	0	0	1	0	1	0	21	0	2	0	2
15	8	1	0	1	0	2							0							0							0						
15	8	1	3	1	-1	0							0							0	2	5	0	0	1	0	1	10	21	0	0	0	2
15	8	1	5	1	-1	0							2	4	9	0	3	0	0	0							0						
21	5	1	2	0	0	3	0	6	4	1	1	0	1	0	9	3	2	0	0	1	0	10	0	0	2	0	0	0	7	0	0	0	1
21	5	1	0	2	0	1							0							1	5	10	0	0	2	0	0						
21	5	1	3	1	-1	2							0							0							0	3	7	0	0	0	1
21	5	1	7	1	-1	1							1	4	9	1	2	0	0	0							0						
30	22	1	1	0	0	1	0	2	2	0	0	0	0	0	3	1	1	0	1	0	0	5	1	0	1	0	0	0	3	1	1	0	1
30	22	1	0	1	0	0							0							0							0						
30	22	1	5	1	-1	0							1	4	9	0	2	0	1	0							1	10	21	0	1	0	2
30	22	1	6	1	-1	0							0							0	2	5	0	0	1	0	0						
35	12	1	1	0	0	2	0	4	3	1	0	0	1	0	6	2	2	0	0	0	0	5	0	0	1	0	0	0	7	0	0	0	1
35	12	1	0	1	0	1							1	3	6	1	2	0	0	0							0						
35	12	1	5	1	-1	0							0							0							0	3	7	0	0	0	1
35	12	1	7	1	-1	0							0							0	2	5	0	0	1	0	0						

Table V. (cont.)

						p = 2							p = 3							p = 5							p = 7						
D	A	B	a	b	n_0	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7	ℓ_1	n_1	a_1	h_2	h_3	h_5	h_7
42	26	1	1	0	0	1	0	2	2	0	0	0	3	0	9	1	4	2	0	2	0	15	1	3	3	0	0	0	7	1	0	0	1
42	26	1	0	1	0	0							0							0							0						
42	26	1	6	1	-1	0							0							2	7	15	0	0	3	0	0	3	7	0	0	0	1
42	26	1	7	1	-1	0							3	4	9	0	4	0	0	0							0						
70	502	1	1	0	0	1	0	2	2	1	1	0	1	0	3	1	2	1	0	1	0	5	1	1	2	0	0	0	7	1	1	1	1
70	502	1	0	1	0	0							0							0							0						
70	502	1	25	3	-1	0							1	1	3	0	2	0	0	0							0	3	7	0	1	0	1
70	502	1	42	5	-1	0							0							1	2	5	0	0	2	0	0						
105	82	1	2	0	0	3	0	2	4	0	0	0	0	0	3	3	4	0	0	0	0	5	3	0	1	0	0	0	7	3	0	0	1
105	82	1	0	2	0	1							0							0							0						
105	82	1	20	2	-1	1							4	4	9	1	5	0	0	0							0	3	7	1	0	0	1
105	82	1	42	4	-1	2							0							0	2	5	2	0	1	0	0						
210	58	1	1	0	0	1	0	2	2	0	0	0	0	0	3	1	1	0	0	0	0	5	1	0	1	0	0	0	7	1	0	0	1
210	58	1	0	1	0	0							0							0							0						
210	58	1	14	1	-1	0							0	1	3	0	1	0	0	0	2	5	0	0	1	0	0						
210	58	1	15	1	-1	0							0							0							0	3	7	0	0	0	1

($\alpha = a + b\sqrt{D}$)

Table VI.

D	p_i			ν_i			λ_i			$(i \in I_U^*)$
2	2	3	5	3	0	0	1.5	0	0	
6	2	3	7	3	1	0	1.5	0.5	0	
7	2	5	7	2	0	1	1	0	0.5	
10	2	5	7	3	1	0	1.5	0.5	0	
14	2	3	7	3	0	1	1.5	0	0.5	
15	2	3	5	2	1	1	1	0.5	0.5	
21	2	3	7	2	1	1	0	0.5	0.5	
30	2	3	5	3	1	1	1.5	0.5	0.5	
70	2	5	7	3	1	1	1.5	0.5	0.5	
105	3	5	7	1	1	1	0.5	0.5	0.5	

D	α	n_ϵ	n_π	n_2	n_3	n_5	n_7	I_U	I_U^*	N	κ	C_{12}^*
2	1	0	0	0	0	0	0	2 3 5	2 3 5	3	0	3.190×10^{28}
	$\sqrt{2}$	0	0	1	0	0	0	3 5	2 3 5	2	0	3.190×10^{28}
6	1	0	0	0	0	0	0	2 3 7	2 3 7	3	0	2.712×10^{26}
	$\sqrt{6}$	0	0	1	1	0	0	7	2 7	2	0	4.604×10^{22}
	$2+\sqrt{6}$	1	0	1	0	0	0	3	2 3	2	0	2.090×10^{22}
	$3+\sqrt{6}$	1	0	0	1	0	0	2	2 3	3	0	2.090×10^{22}
7	1	0	0	0	0	0	0	2 5 7	2 5 7	2	0	1.065×10^{30}
	$\sqrt{7}$	0	0	0	0	0	1	2 5	2 5	2	0	2.146×10^{28}
	$3+\sqrt{7}$	1	0	1	0	0	0	5 7	2 5 7	1	0	1.065×10^{30}
	$7+3\sqrt{7}$	1	0	1	0	0	1	5	2 5	1	0	2.146×10^{25}
10	1	0	0	0	0	0	0	2 5 7	2 5 7	3	0	3.214×10^{29}
	$\sqrt{10}$	0	0	1	0	1	0	7	2 7	2	0	8.414×10^{24}
	$-2+\sqrt{10}$	-1	1	1	0	0	0	5 7	2 5 7	2	1	3.214×10^{29}
	$5-\sqrt{10}$	-1	1	0	0	1	0	2 7	2 7	3	1	8.414×10^{24}
14	1	0	0	0	0	0	0	2 3 7	2 3 7	3	0	4.791×10^{26}
	$\sqrt{14}$	0	0	1	0	0	1	3	2 3	2	0	4.347×10^{22}
	$4+\sqrt{14}$	1	0	1	0	0	0	7	2 7	2	0	8.143×10^{22}
	$7+2\sqrt{14}$	1	0	0	0	0	1	2	2	3	0	8.371×10^{18}

Table VI. (cont.)

D	α	n_ϵ	n_π	n_2	n_3	n_5	n_7	I_U	I_U^*	N	κ	C_{12}^*
15	1	0	0	0	0	0	0	2 3 5	2 3 5	2	0	2.144×10^{28}
	$\sqrt{15}$	0	0	0	1	1	0	2	2	2	0	9.427×10^{19}
	$3+\sqrt{15}$	1	0	1	1	0	0	5	2 5	1	0	1.694×10^{24}
	$5+\sqrt{15}$	1	0	1	0	1	0	3	2 3	1	0	1.035×10^{24}
	$1+\sqrt{15}$	0	1	1	0	0	0	3 5	2 3 5	1	1	2.144×10^{28}
	$15+\sqrt{15}$	0	1	1	1	1	0		2	1	1	9.427×10^{19}
	$6-\sqrt{15}$	-1	1	0	1	0	0	2 5	2 5	2	1	1.694×10^{24}
	$-5+2\sqrt{15}$	-1	1	0	0	1	0	2 3	2 3	2	1	1.035×10^{24}
21	2	0	0	2	0	0	0	2 3 7	2 3 7	1	0	1.898×10^{26}
	$2\sqrt{21}$	0	0	2	1	0	1	2	2	0	0	2.640×10^{18}
	$3+\sqrt{21}$	1	0	2	1	0	0	2 7	2 7	1	0	3.220×10^{22}
	$7+\sqrt{21}$	1	0	2	0	0	1	2 3	2 3	1	0	1.435×10^{22}
30	1	0	0	0	0	0	0	2 3 5	2 3 5	3	0	4.141×10^{28}
	$\sqrt{30}$	0	0	1	1	1	0		2	2	0	2.022×10^{20}
	$5+\sqrt{30}$	1	0	0	0	1	0	3	2 3	3	0	2.217×10^{24}
	$6+\sqrt{30}$	1	0	1	1	0	0	5	2 5	2	0	3.276×10^{24}
	$3+\sqrt{30}$	0	1	0	1	0	0	5	2 5	3	1	3.276×10^{24}
	$10+\sqrt{30}$	0	1	1	0	1	0	3	2 3	2	1	2.217×10^{24}
	$-4+\sqrt{30}$	-1	1	1	0	0	0	3 5	2 3 5	2	1	4.141×10^{28}
	$15-2\sqrt{30}$	-1	1	0	1	1	0	2	2	3	1	2.022×10^{20}
70	1	0	0	0	0	0	0	2 5 7	2 5 7	3	0	3.229×10^{30}
	$\sqrt{70}$	0	0	1	0	1	1		2	2	0	2.115×10^{21}
	$25+3\sqrt{70}$	1	0	0	0	1	0	7	2 7	3	0	8.482×10^{25}
	$42+5\sqrt{70}$	1	0	1	0	0	1	5	2 5	2	0	7.003×10^{25}
	$7+\sqrt{70}$	0	1	0	0	0	1	5	2 5	3	1	7.003×10^{25}
	$10+\sqrt{70}$	0	1	1	0	1	0	7	2 7	2	1	8.482×10^{25}
	$-8+\sqrt{70}$	-1	1	1	0	0	0	5 7	2 5 7	2	1	3.229×10^{30}
	$35-4\sqrt{70}$	-1	1	0	0	1	1	2	2	3	1	2.115×10^{21}
105	2	0	0	2	0	0	0	3 5 7	3 5 7	1	0	4.533×10^{29}
	$2\sqrt{105}$	0	0	2	1	1	1			0	0	4.295×10^{16}
	$20+2\sqrt{105}$	1	0	2	0	1	0	3 7	3 7	1	0	1.690×10^{25}
	$42+4\sqrt{105}$	1	0	2	1	0	1	5	5	1	0	8.655×10^{20}
	$7+\sqrt{105}$	0	1	2	0	0	1	3 5	3 5	1	1	1.396×10^{25}
	$15+\sqrt{105}$	0	1	2	1	1	0	7	7	1	1	1.049×10^{21}
	$-9+\sqrt{105}$	-1	1	2	1	0	0	5 7	5 7	1	1	2.485×10^{25}
	$35-3\sqrt{105}$	-1	1	2	0	1	1	3	3	1	1	5.880×10^{20}