CHAPTER 4. S-INTEGRAL ELEMENTS OF BINARY RECURRENCE SEQUENCES.

Acknowledgements. The research for this chapter has been done partly in cooperation with A. Pethö from Debrecen. The results have been published in Pethö and de Weger [1986] and de Weger [1986^b].

4.1. Introduction.

In this chapter we present a reduction algorithm for the following problem. Let A, B, G_0, G_1 be integers, and let the recurrence sequence $\{G_n\}_{n=0}^{\infty}$ be defined by

$$G_{n+1} = A \cdot G_n - B \cdot G_{n-1} \quad \text{for} \quad n = 1, 2, \ldots .$$

Assume that $\Delta = A^2 - 4 \cdot B$ is not a square. Let w be a nonzero integer, and let $p_1, \ldots, p_s$ be distinct prime numbers. We study the diophantine equation

$$G_n = w \cdot \prod_{i=1}^{s} p_i^{m_i} \tag{4.1}$$

in nonnegative integers $n, m_1, \ldots, m_s$. We will study both the cases of positive and negative discriminant Δ (the 'hyperbolic' and 'elliptic' cases). It was shown by Mahler [1934] that (4.1) has only finitely many solutions. For the case $\Delta > 0$ Schinzel [1967] has given an effectively computable upper bound for the solutions.

Mignotte [1984^a], [1984^b] indicated how in some instances (4.1) with $s = 1$ can be solved by congruence techniques. It is however not clear that his method will work for any equation (4.1) with $s = 1$. Moreover, his method seems not to be generalizable for $s > 1$. Pethö [1985] has given a reduction algorithm, based on the Gelfond-Baker method, to treat (4.1) in the case $\Delta > 0$, $w = s = 1$.

Our reduction algorithms are based on a simple case of p-adic diophantine approximation, namely the zero-dimensional case, cf. Section 3.9. In the hyperbolic case this suffices to be able to find all solutions of (4.1). This is based on a trivial observation of the exponential growth of $|G_n|$ in this case. In the elliptic case the situation is essentially more complicated. Then information on the growth of $|G_n|$ can be obtained from the complex Gelfond-Baker theory. Therefore in this case we have to combine the p-adic arguments with the one-dimensional homogeneous or inhomogeneous real diophantine approximation method, cf. Sections 3.2 and 3.3.

We shall give explicit upper bounds for the solutions of (4.1) which are small enough to admit the practical application of the reduction algorithms, if the parameters of the equation are not too large. Pethö [1985] pointed out that essentially better upper bounds hold for all but possibly one solutions.

The generalized Ramanujan-Nagell equation

$$x^2 + k = \prod_{i=1}^{s} p_i^{z_i} , \tag{4.2}$$

where $k \in \mathbb{Z}$ is fixed, and $x, z_1, \ldots, z_s \in \mathbb{N}_0$ are the unknowns, can be reduced to a finite number of equations of type (4.1) with $\Delta > 0$. Equation (4.2) with $s = 1$ has a long history (cf. Hasse [1966], Beukers [1981] for a survey), and interesting applications in coding theory (cf. Bremner, Calderbank, Hanlon, Morton and Wolfskill [1983], MacWilliams and Sloane [1977], and Tzanakis and Wolfskill [1986], [1987]). Examples of (4.2) have been solved using the Gelfond-Baker theory by Hunt and van der Poorten (unpublished). They used real or complex, not p-adic linear forms in logarithms. As far as we know, none of the proposed methods to treat (4.2) gives rise to an algorithm which works for arbitrary values of k and the p_i's, whereas Tzanakis' elementary method (cf. Tzanakis [1983]) seems to be the only one that can be generalized to $s > 1$. Our method has both properties.

This chapter is organized as follows. In Section 4.2 we give some preliminaries on binary recurrence sequences. In Section 4.3 we study the growth of $|G_n|$, both in the hyperbolic and the elliptic case. The hyperbolic case is trivial, and in the elliptic case we give a method for solving $|G_n| < v$ for a fixed $v \in \mathbb{N}$, by proving an upper bound for n that has particularly good dependence on v, and by showing how to reduce such an upper bound. Section 4.4 gives upper bounds for the solutions of (4.1). Section 4.5 treats a special case: that of 'symmetric' recurrences.

For this special type of recurrence sequences our reduction algorithms fail, but elementary arguments will always work for solving (4.1) in these cases.

Section 4.6 gives a lemma on which the p-adic part of the reduction procedure is based, and some trivial cases are excluded. In Section 4.7 we give the algorithm for reducing upper bounds for the solutions of (4.1) in the case $\Delta > 0$, with some elaborated examples. The same is done for the case $\Delta < 0$ in Section 4.8. Section 4.9 shows how to treat the generalized Ramanujan-Nagell equation (4.2), as an application of the hyperbolic case of (4.1). As an example we determine all integers x such that $x^2 + 7$ has no prime factors larger than 20, thus extending the result of Nagell [1948] on the equation $x^2 + 7 = 2^n$ (the original Ramanujan-Nagell equation). Finally in Section 4.10 we give an application of the elliptic case of (4.1) to a certain type of mixed quadratic-exponential diophantine equation, analogous to the application of the hyperbolic case to solving (4.2). As an example, we determine the solutions X, m_1, m_2, n of

$$X^2 - 3^{m_1}\cdot 7^{m_2}\cdot X + 2\cdot\left(3^{m_1}\cdot 7^{m_2}\right)^2 = 11\cdot 2^n .$$

4.2. Binary recurrence sequences.

Let A, B, G_0, G_1 be given integers. Let the sequence $(G_n)_{n=0}^{\infty}$ be defined by

$$G_{n+1} = A\cdot G_n - B\cdot G_{n-1} \quad \text{for} \quad n = 1, 2, \dots . \tag{4.3}$$

Let α, β be the roots of $x^2 - A\cdot x + B = 0$. We assume that $\Delta = A^2 - 4\cdot B$ is not a square, and that α/β is not a root of unity (i.e. the sequence is not degenerate). Put

$$\lambda = \frac{G_1 - G_0\cdot\beta}{\alpha - \beta} , \quad \mu = \frac{G_0\cdot\alpha - G_1}{\alpha - \beta} . \tag{4.4}$$

Then λ and μ are conjugates in $K = \mathbb{Q}(\sqrt{\Delta})$. It is well known that for all $n \geq 0$

$$G_n = \lambda\cdot\alpha^n + \mu\cdot\beta^n , \tag{4.5}$$

(cf. Shorey and Tijdeman [1986], Theorem C.1). Since our aim is to solve (4.1), we see from (4.3) that we may assume without loss of generality that

$$(G_0,G_1) = (G_1,B) = (A,B) = 1 \ .$$

Namely, if $p \mid (G_1,B)$ then $p \mid (G_1,G_2)$, and if $p \mid (A,B)$ then $p \mid (G_2,G_3)$, and if $p \mid (G_{n_0},G_{n_0+1})$ then $p \mid G_n$ for all $n \geq n_0$, so the common factor p can be divided out in equation (4.1).

<u>LEMMA 4.1.</u> *Let* $n, m_1, \ldots, m_s$ *be a solution of* (4.1). *Then, with the above assumptions, we have for* $i = 1, \ldots, s$ *either* $m_i = 0$ *or* $n = 0$ *or*

$$\begin{aligned} &\mathrm{ord}_{p_i}(\alpha) = \mathrm{ord}_{p_i}(\beta) = 0 \ , \\ &\mathrm{ord}_{p_i}(\lambda) = \mathrm{ord}_{p_i}(\mu) = -\tfrac{1}{2}\cdot\mathrm{ord}_{p_i}(\Delta) \leq 0 \ . \end{aligned} \tag{4.6}$$

<u>Proof.</u> Suppose $p_i \mid B$. Then $p_i \nmid A$, hence, from (4.3) and $(B,G_1) = 1$, $p_i \nmid G_n$ for all $n \geq 0$. Thus, $m_i = 0$ or $n = 0$. Next suppose $p_i \nmid B$. Then, by $\alpha\cdot\beta = B$,

$$\mathrm{ord}_{p_i}(\alpha) + \mathrm{ord}_{p_i}(\beta) = \mathrm{ord}_{p_i}(B) = 0 \ .$$

Now, α and β are algebraic integers, so their p_i-adic orders are nonnegative. It follows that they are zero. Put $E = -\lambda\cdot\mu\cdot\Delta$. Note that $E \in \mathbb{Z}$, and for all $n \geq 0$

$$G_{n+1}^2 - A\cdot G_n\cdot G_{n+1} + B\cdot G_n^2 = E\cdot B^n \ .$$

Suppose that $p_i \mid E$, then we infer that $p_i \nmid G_n$ for all n , since $(G_0,G_1) = 1$. Hence $m_i = 0$. Next suppose $p_i \nmid E$, then

$$\mathrm{ord}_{p_i}(\lambda\cdot\sqrt{\Delta}) + \mathrm{ord}_{p_i}(\mu\cdot\sqrt{\Delta}) = \mathrm{ord}_{p_i}(E) = 0 \ .$$

Since $\lambda\cdot\sqrt{\Delta}$ and $\mu\cdot\sqrt{\Delta}$ are algebraic integers, the result follows. □

From Lemma 2.1 it follows that we may assume without loss of generality that (4.6) holds for $i = 1, \ldots, s$. Of course, we may also assume that $\mathrm{ord}_{p_i}(w) = 0$ for $i = 1, \ldots, s$. The special case $s = 0$ in equation (4.1) is trivial if $\Delta > 0$, and will be treated in the next section for all Δ .

4.3. The growth of the recurrence sequence.

First we treat the hyperbolic case $\Delta > 0$. Note that $|\alpha| \neq |\beta|$, since the sequence is not degenerate. So we may assume $|\alpha| > |\beta|$. We have the following, almost trivial, result on the exponentiality of the growth of the sequence $\{G_n\}_{n=0}^{\infty}$. Let

$$n_0 > \max \left[2, \log|\tfrac{\mu}{\lambda}|/\log|\tfrac{\alpha}{\beta}| \right],$$

$$\gamma = |\lambda| - |\mu|\cdot|\tfrac{\alpha}{\beta}|^{-n_0} .$$

Note that $\gamma > 0$.

<u>LEMMA 4.2.</u> *Let* $\Delta > 0$. *If* $n \geq n_0$ *then* $|G_n| \geq \gamma\cdot|\alpha|^n$.

<u>Proof.</u> By (4.5), $|\alpha| > |\beta|$ and $n_0 > 0$ it follows for $n \geq n_0$ that

$$|G_n|\cdot|\alpha|^{-n} = |\lambda+\mu\cdot\left(\tfrac{\alpha}{\beta}\right)^{-n}| \geq |\lambda| - |\mu|\cdot|\tfrac{\alpha}{\beta}|^{-n} \geq \gamma . \qquad \square$$

We apply this to (4.1) as follows.

<u>COROLLARY 4.3.</u> *Let* $\Delta > 0$. *Any solution* $n, m_1, \ldots, m_s$ *of* (4.1) *with* $n \geq n_0$ *satisfies*

$$n < \sum_{i=1}^{s} m_i\cdot\frac{\log p_i}{\log|\alpha|} - \frac{\log(\gamma/|w|)}{\log|\alpha|} .$$

<u>Proof.</u> Clear, from Lemma 4.2 and (4.1). □

Next we study the elliptic case $\Delta < 0$. Since α/β is not a root of unity, $B \geq 2$. Since (α,β) and (λ,μ) are pairs of complex conjugates, $|\alpha| = |\beta|$ and $|\lambda| = |\mu|$. Let $v \in \mathbb{R}$, $v \geq 1$ be given. We study the diophantine inequality

$$|G_n| \leq v . \qquad (4.7)$$

We apply a result of Waldschmidt (see Section 2.3) from the complex theory of linear forms in logarithms, which gives an upper bound for n that is particularly good in v . See also Kiss [1979]. Let

$$E = -\lambda\cdot\mu\cdot\Delta \ ,$$

$$U_2 = \tfrac{1}{2}\cdot\max\ (\ \pi,\ \log B\ )\ ,\quad U_3 = \tfrac{1}{2}\cdot\max\ (\ \pi,\ \log E\ )\ ,$$

$$U_2^+ = \min\ (\ U_2,\ U_3\ )\ ,\quad U_3^+ = \max\ (\ U_2,\ U_3\ )\ ,$$

$$C_1 = 3.362\times 10^{21}\cdot U_2\cdot U_3\cdot\log(2\cdot e\cdot U_2^+)\ ,\quad C_2 = \log(4\cdot e\cdot U_3^+)\ ,$$

$$C_3 = \left(\ \log(\pi/2\cdot|\mu|) + C_1\cdot C_2 + C_1\cdot\log(4\cdot C_1/\log B)\ \right)\cdot 4/\log B\ .$$

THEOREM 4.4. *Let* $v \in \mathbb{R}$, $v \ge 1$. *All solutions* $n \ge 0$ *of* (4.7) *satisfy*

$$n < C_3 + \frac{4}{\log B}\cdot\log\max\left(\ v,\ 2\cdot|G_0\cdot\mu\cdot\surd\Delta|\ \right)\ .$$

Remark. Note that C_3 does not depend on v .

The following corollary of Theorem 4.4 is immediate.

COROLLARY 4.5. *Let* $\Delta < 0$. *Any solution* $n,\ m_1,\ \ldots,\ m_s$ *of* (4.1) *satisfies*

$$n < C_3 + \frac{4}{\log B}\cdot\max\left(\ \log(2\cdot|G_0\cdot\mu\cdot\surd\Delta|),\ \log|w| + \sum_{i=1}^{s} m_i\cdot\log p_i\ \right)\ .$$

Proof (of Theorem 4.4). Note that $|\alpha| = |\beta| = \surd B \ge \surd 2$. We have from (4.7)

$$\left|\ \left(\frac{-\lambda}{\mu}\right)\cdot\left(\frac{\alpha}{\beta}\right)^n - 1\ \right| \le \frac{v}{|\mu|}\cdot B^{-n/2}\ . \qquad (4.8)$$

We may assume $n \ge 2$. Let $-\lambda/\mu = e^{2\pi i\cdot\psi}$, $\alpha/\beta = e^{2\pi i\cdot\varphi}$, with $-\frac{1}{2} < \psi \le \frac{1}{2}$ and $-\frac{1}{2} < \varphi \le \frac{1}{2}$. Let $k_0,\ k_1 \in \mathbb{Z}$ be such that $|\ j\cdot\psi + n\cdot\varphi + k_j\ | \le \frac{1}{2}$. Then $|k_j| \le 1 + \frac{1}{2}\cdot n \le n$ for $j = 0,\ 1$. Put

$$\Lambda_j = 2\pi i\cdot\left(\ j\cdot\psi + n\cdot\varphi + k_j\ \right) = j\cdot\mathrm{Log}\left(\frac{-\lambda}{\mu}\right) + n\cdot\mathrm{Log}\left(\frac{\alpha}{\beta}\right) + 2\cdot k_j\cdot\mathrm{Log}(-1)$$

for $j = 0,\ 1$. By Lemma 2.3 and (4.8) we have an upper bound for $|\Lambda_1|$:

$$|\Lambda_1| = 2\pi\cdot|\ \psi + n\cdot\varphi + k_1\ | \le \tfrac{1}{2}\pi\cdot|e^{2\pi i\cdot(\psi+n\cdot\varphi+k_1)} - 1|$$

$$= \tfrac{1}{2}\pi\cdot\left|\ \left(\frac{-\lambda}{\mu}\right)\cdot\left(\frac{\alpha}{\beta}\right)^n - 1\ \right| \le \tfrac{1}{2}\pi\cdot\frac{v}{|\mu|}\cdot B^{-n/2}\ .$$

It may happen that $\Lambda_1 = 0$. In that case, $\psi + n\cdot\varphi \in \mathbb{Z}$, hence

$-(\lambda/\mu)\cdot(\alpha/\beta)^n = 1$, and it follows that $G_n = \lambda\cdot\alpha^n + \mu\cdot\beta^n = 0$. Kiss [1979] showed that this implies $|R_n| \le 2\cdot|G_0|$, where $R_n = (\alpha^n-\beta^n)/(\alpha-\beta)$. From this, Kiss derived an upper bound for n. We shall follow his argument, but we apply another, sharper result from the Gelfond-Baker theory than Kiss did. Note that, by $|\beta| = \sqrt{B}$,

$$2\cdot|G_0| \ge |R_n| = \frac{B^{n/2}}{\sqrt{|\Delta|}}\cdot\left|\left(\frac{\alpha}{\beta}\right)^n -1\right| \ge 4\cdot\frac{B^{n/2}}{\sqrt{|\Delta|}}\cdot|\varphi\cdot n+k_0| = \frac{2}{\pi}\cdot\frac{B^{n/2}}{\sqrt{|\Delta|}}\cdot|\Lambda_0| .$$

Now $\Lambda_0 \ne 0$, since by $n \ge 2$ the contrary would imply $\varphi \in \mathbb{Q}$, which is impossible, since α/β is not a root of unity. Thus, take $j = 1$ if $\Lambda_1 \ne 0$ and $j = 0$ otherwise. Then $\Lambda_j \ne 0$, and

$$|\Lambda_j| \le \frac{\pi}{2\cdot|\mu|}\cdot\max\left(v,\ 2\cdot|G_0\cdot\mu\cdot\sqrt{|\Delta|} \right)\cdot B^{-n/2} . \tag{4.9}$$

From Lemma 2.4 we can derive a lower bound for $|\Lambda_j|$. Note that $\max(j,n,2|k_j|) \le 2\cdot n$, so that $W = \log(2\cdot n)$. We choose $V_1 = \frac{1}{2}$. The number $z = \alpha/\beta$ satisfies

$$B\cdot z^2 - (A^2-2\cdot B)\cdot z + B = 0 ,$$

hence $h(\alpha/\beta) \le \frac{1}{2}\cdot\log B$. And $z = -\lambda/\mu$ satisfies

$$E\cdot z^2 - (2\cdot E+\Delta\cdot G_0^2)\cdot z + E = 0 ,$$

hence $h(-\lambda/\mu) \le \frac{1}{2}\cdot\log E$. Thus $V_2 = U_2^+$, $V_3 = U_3^+$ satisfy the requirements for Lemma 2.4. We find

$$\begin{aligned} |\Lambda_j| &> \exp\left(-C_1\cdot(\ \log(2\cdot n) + \log(2\cdot e\cdot U_3^+)\ ) \right) \\ &= \exp\left(-C_1\cdot(\ \log n + C_2\ ) \right) . \end{aligned} \tag{4.10}$$

Combining (4.9) and (4.10) we find $n < a + b\cdot\log n$, where

$$a = \frac{2}{\log B}\cdot\left(\log \max\left(v,\ 2\cdot|G_0\cdot\mu\cdot\sqrt{\Delta}| \right) + \log\frac{\pi}{2\cdot|\mu|} + C_1\cdot C_2 \right) ,$$

$$b = 2\cdot C_1/\log B .$$

The result now follows from Lemma 2.1, since

$$b = 2\cdot C_1/\log B = 1.681\times10^{21}\cdot\frac{\max(\pi,\log B)}{\log B}\cdot\max(\pi,\log E)\cdot\log(2\cdot e\cdot U_2^+)$$

which is certainly larger than e^2. □

We now want to reduce the bound found in Theorem 4.3. We do this by studying the diophantine inequality

$$| \psi_j + n\cdot\varphi + k_j | < v_0\cdot B^{-n/2} , \tag{4.11}$$

which follows from (4.9), where $v_0 = \max \big(v,\ 2\cdot|G_0\cdot\mu\cdot\sqrt{\Delta}| \big)/4\cdot|\mu|$, and $\psi_j = j\cdot\psi$. We have to distinguish between the homogeneous case $\psi_j = 0$ and the inhomogeneous case $\psi_j \neq 0$. We apply the methods that have been described in Sections 3.2 and 3.3 respectively. Unlike in other chapters, here we give the results in the form of precisely defined algorithms.

First we study the homogeneous case $\psi_j = 0$. We have the following algorithm. Let N be an upper bound for the solutions of (4.11), for example the bound found in Theorem 4.3.

<u>ALGORITHM H.</u> (reduces given upper bound for (4.11) in the case $\psi_j = 0$).
<u>Input:</u> φ, B, $|\mu|$, v_0, N .
<u>Output:</u> new, reduced bound N^* for n .

```
 (i) (initialization) *Choose* $n_0 \geq 2/\log B$ *such that* $B^{n_0/2}/n_0 \geq 2\cdot v_0$ ;
     $N_0 := N$ ; *compute the continued fraction*

          $|\varphi| = [\ 0,\ a_1,\ a_2,\ \ldots,\ a_{\ell_0+1},\ \ldots\ ]$

     *and the denominators* $q_1, \ldots, q_{\ell_0+1}$ *of the convergents of* $|\varphi|$ *, with*
     $\ell_0$ *so large that* $q_{\ell_0} \leq N_0 < q_{\ell_0+1}$ ;  $i := 0$ ;
(ii) (compute new bound) $A_i := \max(a_1,\ldots,a_{\ell_i+1})$ ; *compute the largest*
     *integer* $N_{i+1}$ *such that*

          $B^{N_{i+1}/2}/N_{i+1} \leq v_0\cdot(A_i+2)$ ,

     *and* $\ell_{i+1}$ *such that* $q_{\ell_{i+1}} \leq N_{i+1} < q_{\ell_{i+1}+1}$ ;
(iii) (terminate loop)
     if $n_0 \leq N_{i+1} < N_i$ then $i := i + 1$ , goto (ii) ;
                                   else $N^* := \max(n_0,N_{i+1})$ , stop .
```

<u>LEMMA 4.6.</u> *Algorithm* H *terminates. Inequality* (4.11) *with* $\psi_j = 0$ *has no solutions with* $N^* < n < N$.

<u>Proof.</u> Termination is obvious, since all N_i are integers. Note that $B^{x/2}/x$ is an increasing function for $x \geq 2/\log B$. Hence, if $n \geq n_0$,

$$| \; |\varphi| - |k_j|/n \; | \le v_0 \cdot B^{-n/2}/n < 1/2n^2 .$$

It follows (cf. (3.6)) that $|k_j|/n$ is a convergent of $|\varphi|$, say $|k_j|/n = p_m/q_m$. Then $q_m \le n$, and (cf. (3.5)),

$$| \; |\varphi| - p_m/q_m \; | > 1/(a_{m+1}+2)\cdot q_m^2 .$$

Suppose $n \le N_i$ for some $i \ge 0$. Then $m \le \ell_i$. Hence,

$$B^{n/2}/n \le v_0 \cdot n^{-2} \cdot | \; |\varphi| - |k_j|/n \; |^{-1} < v_0 \cdot (a_{m+1}+2) \le v_0 \cdot (A_m+2) .$$

It follows that if $N_{i+1} \ge n_0$ then $n \le N_{i+1}$. □

Next we study the inhomogeneous case $\psi_j \ne 0$. Again, let N be an upper bound for n satisfying (4.11).

ALGORITHM I. (reduces upper bound for (4.11) in the case $\psi_j \ne 0$).

Input: φ, ψ_j, B, v_0, N.

Output: new, reduced upper bound N^* for all but a finite number of explicitly given n.

```
  (i) (initialization) $N_0 := [N]$ ; compute the continued fraction

            $|\varphi| = [\, 0, a_1, a_2, \ldots, a_{\ell_0}, \ldots \,]$

      and the convergents $p_i/q_i$ for $i = 1, \ldots, \ell_0$, with $\ell_0$ so large
      that $q_{\ell_0} > 4\cdot N_0$ and $\|q_{\ell_0}\cdot\psi_j\| > 2\cdot N_0/q_{\ell_0}$. (If such $\ell_0$ cannot be
      found within reasonable time, take $\ell_0$ so large that $q_{\ell_0} > 4\cdot N_0$ ) ;
      $i := 0$ ;
 (ii) (compute new bound)
      if $\|q_{\ell_i}\cdot\psi_j\| > 2\cdot N_i/q_{\ell_i}$
         then $N_{i+1} := [2\cdot\log(q_{\ell_i}^2\cdot v_0/N_i)/\log B]$ ;
         else compute $K \in \mathbb{Z}$ with $|\, K - q_{\ell_i}\cdot\psi_j \,| \le \frac{1}{2}$ ; compute $n_0 \in \mathbb{Z}$,
              $0 \le n_0 < q_{\ell_i}$, with $K = n_0\cdot p_{\ell_i} \equiv 0 \pmod{q_{\ell_i}}$ ;
              if $n = n_0$ is a solution of (4.11), then print an
              appropriate message;
              $N_{i+1} := [2\cdot\log(4\cdot q_{\ell_i}\cdot v_0)/\log B]$ ;
(iii) (terminate loop)
      if $N_{i+1} < N_i$
         then $i := i + 1$ ; compute the minimal $\ell_i < \ell_{i+1}$ such that
```

```
        $q_{\ell_i} > 4\cdot N_i$ and $\|q_{\ell_i}\cdot\psi_j\| > 2\cdot N_i/q_{\ell_i}$ (if such $\ell_i$ does not
        exist, choose the minimal $\ell_i$ such that $q_{\ell_i} > 4\cdot N_i$ );
        goto (ii) ;
    else $N^* := N_i$ ; stop .
```

LEMMA 4.7. *Algorithm* I *terminates. Inequality* (4.11) *with* $\psi_j \neq 0$ *has for* $N^* < n < N$ *only the finitely many solutions found by the algorithm.*

Proof. It is clear that the algorithm terminates. Suppose that $n \le N_i$ for some $i \ge 0$. then if $\|q_{\ell_i}\cdot\psi_j\| > 2\cdot N_i/q_{\ell_i}$, we have

$$\begin{aligned}\|q_{\ell_i}\cdot\psi_j\| &= \|q_{\ell_i}\cdot(\psi_j+n\cdot\varphi+k_j) - n\cdot\varphi\cdot q_{\ell_i}\| \\ &\le q_{\ell_i}\cdot|\psi_j+n\cdot\varphi+k_j| + n/q_{\ell_i} \le q_{\ell_i}\cdot v_0\cdot B^{-n/2} + N_i/q_{\ell_i} .\end{aligned}$$

It follows that $n \le N_{i+1}$. If $\|q_{\ell_i}\cdot\psi_j\| \le 2\cdot N_i/q_{\ell_i}$, then

$$\begin{aligned}|K+n\cdot p_{\ell_i}+k_j\cdot q_{\ell_i}| &\le |K-q_{\ell_i}\cdot\psi_j| + q_{\ell_i}\cdot|\psi_j+n\cdot\varphi+k_j| + n\cdot|p_{\ell_i}-q_{\ell_i}\cdot\varphi| \\ &\le \tfrac{1}{2} + q_{\ell_i}\cdot v_0\cdot B^{-n/2} + N_i/q_{\ell_i} < \tfrac{3}{4} + q_{\ell_i}\cdot v_0\cdot B^{-n/2} .\end{aligned}$$

If $q_{\ell_i}\cdot v_0\cdot B^{-n/2} \le \frac{1}{4}$, then $K + n\cdot p_{\ell_i} + k_j\cdot q_{\ell_i} = 0$, since it is an integer. By $(p_{\ell_i}, q_{\ell_i}) = 1$ it follows that $n \equiv n_0 \pmod{q_{\ell_i}}$. Since $q_{\ell_i} > N_i$, the only possibility is $n = n_0$. If $q_{\ell_i}\cdot v_0\cdot B^{-n/2} > \frac{1}{4}$, then $n \le N_{i+1}$ follows immediately. □

We remark that in practice one almost always finds an ℓ_i such that $\|q_{\ell_i}\cdot\psi_j\| > 2\cdot N_i/q_{\ell_i}$, if N_i is large enough.

4.4. Upper bounds.

In this section we will derive explicit upper bounds for the solutions of (4.1), both in the hyperbolic and elliptic cases. Our first step is the application of the p-adic theory of linear forms in logarithms, which works the same way in both cases. We use it to find a bound for m_i in terms of $\log n$. Then we combine this with the results of Section 4.3 on the growth of the recurrence sequence, which for the solutions of (4.1) yield a bound for n in terms of the m_i (Corollaries 4.3 and 4.5).

Assume that $n_0 \geq 2$. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$. Put

$$L = \log \max \left(|e \cdot D|^{1/4},\ |\alpha \cdot \lambda \cdot \sqrt{\Delta}|,\ |\alpha \cdot \mu \cdot \sqrt{\Delta}|,\ |\beta \cdot \lambda \cdot \sqrt{\Delta}|,\ |\beta \cdot \mu \cdot \sqrt{\Delta}| \right) .$$

Let d be the squarefree part of Δ. For $i = 1, \ldots, s$ put

$\varphi_i = 2$ if $p_i \mid d$, $\varphi_i = 1$ otherwise,

$\rho_i = 2$ if $p_i = 2$, $d \equiv 5 \pmod 8$ or if $p_i > 2$, $\left(\frac{d}{p_i}\right) = -1$,

$\rho_i = 1$ otherwise,

$$C_{4,i} = 10^6 \cdot \left[\frac{2}{\rho_i \cdot \log p_i} \right]^7 \cdot \varphi_i^{-3} \cdot L^4 \cdot p_i^{4 \cdot \rho_i + 4} \cdot \left[1 + \frac{\varphi_i \cdot L \cdot p_i^{\rho_i} + 2/L}{\log n_0} \right]^3 .$$

LEMMA 4.8. *The solutions of* (4.1) *with* $n \geq n_0$ *satisfy*

$$m_i < C_{4,i} \cdot (\log n)^3 \quad \text{for } i = 1, \ldots, s .$$

Proof. Rewrite (4.1), using (4.5), as

$$\left(\frac{\alpha}{\beta}\right)^n - \left(\frac{-\mu}{\lambda}\right) = \frac{w}{\lambda} \cdot \beta^{-n} \cdot \prod_{i=1}^{s} p_i^{m_i} .$$

Then, by (4.6),

$$m_i \leq m_i - \operatorname{ord}_{p_i}(\lambda) = \operatorname{ord}_{p_i}\left(\frac{w}{\lambda} \cdot \beta^{-n} \cdot \prod_{i=1}^{s} p_i^{m_i} \right) = \operatorname{ord}_{p_i}\left(\left(\frac{\alpha}{\beta}\right)^n - \left(\frac{-\mu}{\lambda}\right) \right) .$$

Apply Lemma 2.5 (Schinzel's result) with $\xi'' = \alpha$, $\xi' = \beta$, $\chi'' = \mu \cdot \sqrt{\Delta}$, $\chi' = -\lambda \cdot \sqrt{\Delta}$. Then we find, using $\operatorname{ord}_{\mathfrak{p}_i}(\cdot) = \varphi_i \cdot \operatorname{ord}_{p_i}(\cdot)$,

$$m_i < 10^6 \cdot \left[\frac{2}{\rho_i \cdot \log p_i} \right]^7 \cdot \varphi_i^{-3} \cdot L^4 \cdot p_i^{4 \cdot \rho_i + 4} \cdot \left(\log n + \varphi_i \cdot L \cdot p_i^{\rho_i} + 2/L \right)^3 ,$$

from which the result follows, since $n \geq n_0$. □

Put

$$C_4 = \max_i (C_{4,i}) , \quad m = \max_i (m_i) , \quad P = \prod_{i=1}^{s} p_i .$$

In the case $\Delta > 0$, let $n_0 > \max\big(2, \log|\lambda/\mu|/\log|\alpha/\beta| \big)$, and put

$$C_5 = \log P \,/\, \big(\log|\alpha| + \min(0, \log(\gamma/|w|)) \big) ,$$

$$C_6 = \max\big(8\cdot C_4\cdot(\log 27\cdot C_4\cdot C_5)^3 ,\ 841\cdot C_4 \big) .$$

In the case $\Delta < 0$, put

$$C_7 = \max\left\{ C_3 + \frac{4}{\log B}\cdot\log\big(2\cdot|G_0\cdot\mu\cdot\sqrt{\Delta}|\big) ,\right.$$
$$\left. 8\cdot\left(\left(C_3 + \frac{4\cdot\log|w|}{\log B}\right)^{1/3} + \left(\frac{4\cdot C_4\cdot\log P}{\log B}\right)^{1/3}\cdot\log\left(\frac{108\cdot C_4\cdot\log P}{\log B}\right)\right)^3 \right\} ,$$

$$C_{8,i} = C_{4,i}\cdot(\log C_7)^3 \quad \text{for} \quad i = 1, \ldots, s .$$

Then we have the following result, giving explicit upper bounds for the solutions of (4.1).

THEOREM 4.9. *Let* $n, m_1, \ldots, m_s$ *be a solution of* (4.1).
(i). *If* $\Delta > 0$ *and* $n \geq n_0$ *then* $n < C_5\cdot C_6$ *and* $m < C_6$.
(ii). *If* $\Delta < 0$ *then* $n < C_7$ *and* $m_i < C_{8,i}$ *for* $i = 1, \ldots, s$.

Proof. (i). Corollary 4.3 yields $n < C_5\cdot m$. By Lemma 4.8 we now have

$$m < C_4\cdot(\log n)^3 < C_4\cdot(\log C_5\cdot m)^3 .$$

If $C_4\cdot C_5 > (e^2/3)^3$, we apply Lemma 2.1 with $a = 0$, $b = C_4\cdot C_5$, $h = 3$, and we find $m < 8\cdot C_4\cdot(\log 27\cdot C_4\cdot C_5)^3$. If $C_4 . C_5 \leq (e^2/3)^3$, then

$$n < C_5\cdot m < C_4\cdot C_5\cdot(\log n)^3 \leq (e^2/3)^3\cdot(\log n)^3 ,$$

from which we deduce $n < 12564$. Now, $m < C_4\cdot(\log n)^3 < 841\cdot C_4$.
(ii). From Lemma 4.8 and Corollary 4.5 we see that

$$n < C_3 + \frac{4}{\log B}\cdot\log\big(2\cdot|G_0\cdot\mu\cdot\sqrt{\Delta}|\big) ,$$

or

$$n < C_3 + \frac{4\cdot\log|w|}{\log B} + \frac{4\cdot C_4\cdot\log P}{\log B}\cdot(\log n)^3 .$$

The result now follows from Lemma 2.1, since $4\cdot C_4\cdot\log P/\log B > (e^2/3)^3$. □

4.5. Symmetric recurrences: an elementary method.

Before we give our reduction method for the upper bounds following from Theorem 4.9, we treat in this section separately the cases of 'symmetric' recurrences, for which the reduction methods fail. The reduction methods make use of the zero-dimensional p-adic diophantine approximation, as explained in Section 3.9, applied to the p-adic linear form

$$\log_p\left(\frac{\lambda}{\mu}\right) + n\cdot\log_p\left(\frac{\alpha}{\beta}\right)$$

for $p = p_1, \ldots, p_s$. This means that we must study the p-adic number

$$\vartheta = -\log_p\left(\frac{\lambda}{\mu}\right) / \log_p\left(\frac{\alpha}{\beta}\right) .$$

It may however happen that this number ϑ is zero, or that all digits in the p-adic expansion of ϑ are zero from a certain point on. Then obviously the reduction process of Section 3.9 breaks down, since it is based on the assumption that the p-adic expansion of ϑ contains sufficiently many non-zero digits.

Define the following special 'symmetric recurrences'. For α, β as defined in Section 4.2, let

$$R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} , \quad S_n = \alpha^n + \beta^n ,$$

for $d = -1$ (d is the squarefree part of Δ) also

$$T_n^{\pm} = (1 \pm \surd(-1))\cdot\alpha^n + (1 \mp \surd(-1))\cdot\beta^n ,$$

and for $d = -3$ also (with $\omega = \rho$ or $\bar{\rho}$ for $\rho = \frac{1}{2}\cdot(1+\surd(-3))$)

$$U_n(\omega) = (1 + \omega)\cdot\alpha^n + (1 + \bar{\omega})\cdot\beta^n ,$$

$$V_n(\omega) = \omega\cdot\alpha^n + \bar{\omega}\cdot\beta^n ,$$

for all $n \in \mathbb{Z}$. Note that

$$T_n^{+}\cdot T_n^{-} = 2\cdot S_{2n} , \quad U_n(\omega)\cdot U_n(\bar{\omega})\cdot R_n = 3\cdot R_{3n} , \quad V_n(\omega)\cdot V_n(\bar{\omega})\cdot S_n = S_{3n} .$$

We have the following lemma. We assume that $\mathrm{ord}_p(\vartheta) \geq 0$.

LEMMA 4.10. *If* ϑ *has only finitely many nonzero* p-*adic digits, then there exist an* $r \in \mathbb{N}_0$ *and a* $\kappa \in \mathbb{Q}$ *such that* $G_n = \kappa\cdot R_{n-r}$ *, or* $G_n = \kappa\cdot S_{n-r}$ *, or (if* $d = -1$ *)* $G_n = \kappa\cdot T_n^{\pm}$ *, or (if* $d = -3$ *)* $G_n = \kappa\cdot U_n(\omega)$ *or* $\kappa\cdot V_n(\omega)$ *, where* $\omega = \rho$ *or* $\overline{\rho}$ *. Further,* $r = 0$ *if* $\Delta < 0$ *.*

Proof. By $\mathrm{ord}_p(\vartheta) \geq 0$ we have $\vartheta = r$ for some $r \in \mathbb{N}_0$. From the definition of ϑ we infer

$$\log_p \left(\frac{\alpha}{\beta}\right)^r \cdot \left(\frac{-\lambda}{\mu}\right) = 0 \ ,$$

hence $\eta = (\beta/\alpha)^r \cdot (\mu/\lambda)$ is a root of unity. It follows that we can write

$$G_n = \lambda\cdot\alpha^r\cdot\left(\ \alpha^{n-r} + \eta\cdot\beta^{n-r}\ \right) \ .$$

First let $B = \pm 1$. Then $\Delta > 0$ and

$$G_0 = \lambda\cdot\alpha^r\cdot\left(\ \alpha^{-r} \pm \beta^{-r}\ \right) = \pm\lambda\cdot\alpha^r\cdot\left(\ \alpha^r \pm \beta^r\ \right) \ ,$$

$$G_1 = \lambda\cdot\alpha^r\cdot\left(\ \alpha^{1-r} \pm \beta^{1-r}\ \right) = \pm\lambda\cdot\alpha^r\cdot\left(\ \alpha^{r-1} \pm \beta^{r-1}\ \right) \ .$$

Note that

$$(\ \alpha^{r-1} + \beta^{r-1},\ \alpha^r + \beta^r\ ) = (\ 2,\ \alpha + \beta\ ) = 1 \quad \text{or} \quad 2 \ ,$$

$$(\ \alpha^{r-1} - \beta^{r-1},\ \alpha^r - \beta^r\ ) = \alpha - \beta \ .$$

By $(G_0, G_1) = 1$ it follows that $\pm\lambda\cdot\alpha^r = 1,\ \frac{1}{2}$ or $1/(\alpha-\beta)$, respectively, and the assertion follows.

Next suppose $|B| \geq 2$. Then

$$G_0\cdot B\cdot(\ \eta\cdot\alpha^{r-1} + \beta^{r-1}\ ) = G_1\cdot(\ \eta\cdot\alpha^r \pm \beta^r\ ) \ .$$

Since $(B, G_1) = 1$, we have $\alpha\cdot\beta \mid \eta\cdot\alpha^r \pm \beta^r$. By $(A,B) = 1$ we have $(\alpha,\beta) = (1)$, and from $\alpha \mid \beta^r$ it then follows that $\vartheta = r = 0$. So $G_0 = \lambda\cdot(1+\eta) \in \mathbb{Z}$. The result now follows easily, since for η the only possibilities are ± 1 for all d , and moreover $\pm\sqrt{(-1)}$ if $d = -1$, and $\pm\rho$, $\pm\overline{\rho}$ if $d = -3$. □

In the cases of Lemma 4.10 we can treat (4.1) as follows. The smallest index $n = g(m\cdot p^{\ell}) > 0$ such that $m\cdot p^{\ell} \mid G_n$ grows exponentially with ℓ . Also, G_n grows exponentially with n , as follows from Lemma 4.2 and Theorem 4.4. Hence $G_{g(m\cdot p^{\ell})}$ grows doubly exponentially with ℓ . It follows that

$a = w\cdot p_1^{m_1}\cdot\ldots\cdot p_s^{m_s}$ cannot keep up with $G_{g(a)}$ as the m_i tend to infinity. It follows that if $p_1^{m_1}\cdot\ldots\cdot p_s^{m_s}$ is large enough, there exists a prime q such that $q \mid G_{g(a)}$ but $q \nmid a$. Now the sequences $\{R_n\}$, $\{S_n\}$ have special divisibility properties, such as

$$R_n \mid R_m \text{ if and only if } n \mid m ,$$

$$S_n \mid S_{kn} \text{ for odd } k ,$$

$$\mathrm{ord}_2(S_n) \le \mathrm{ord}_2(S_3) \text{ for all } n \ge 1 .$$

Making use of this kind of properties it can be proved that $q \mid G_n$ whenever $a \mid G_n$. This gives an upper bound for the solutions of (4.1), since for those solutions $a \mid G_n$ but $q \nmid G_n$. We give two examples.

Example. Let $A = 16$, $B = 1$, $G_0 = 1$, $G_1 = 8$, $w = 1$, $p_1 = 2$, $p_2 = 11$. Then $\alpha = 8 + 3\cdot\sqrt{7}$, $\beta = 8 - 3\cdot\sqrt{7}$, $\lambda = \mu = \frac{1}{2}$, so λ/μ is a root of unity. Hence $\vartheta = 0$, for both $p = 2$ and $p = 11$. Note that we have a sequence of type S_n here. We have

n	-3	-2	-1	0	1	2	3
G_n	2024	127	8	1	8	127	2024
G_n (mod 16)	8	-1	8	1	8	-1	8
G_n (mod 11)	0	6	8	1	8	6	0
G_n (mod 11^2)	88	6	8	1	8	6	88

It follows that $\mathrm{ord}_2(G_n) = 0$ or 3 , according as n is even or odd, and $\mathrm{ord}_{11}(G_n) > 0$ if and only if $n \equiv 3 \pmod 6$. Now, $G_3 \mid G_{3k}$ holds for all odd k . Note that G_3 has exactly 3 factors 2 , and 1 factor 11 . But it is larger than $2^3\cdot 11 = 88$. Hence there is a prime q , distinct from 2 and 11 , such that $q \mid G_n$ whenever $11 \mid G_n$. Thus $G_n = 2^{m_1}\cdot 11^{m_2}$ has no solutions with $m_2 \ne 0$, so that there remain only three solutions: $n = -1$, 0 and 1 . Note that it is not necessary to know the value of q explicitly. In this case it is 23 , and indeed it is easy to show directly that $23 \mid G_n$ if and only if $n \equiv 3 \pmod 6$.

Example. Let $A = 5$, $B = 13$, $G_0 = G_1 = 1$. Then $\Delta = -27$, $\alpha = 1 + 3\cdot\rho$, $\lambda = (1+\rho)/3$. We solve $G_n = \pm 2^m$. The sequence $G_n = \lambda\cdot\alpha^n + \bar{\lambda}\cdot\bar{\alpha}^n$ is related to the sequence $H_n = \bar{\lambda}\cdot\alpha^n + \lambda\cdot\bar{\alpha}^n$ and to $R_n = (\alpha^n - \bar{\alpha}^n)/(\alpha - \bar{\alpha})$ by

$G_n\cdot H_n\cdot R_n = R_{3n}/3$. Since R_n has nice divisibility properties, we have useful information on the prime divisors of G_n and H_n . We find:

n	0	1	2	3	4	5	6	7	8
G_n	1	1	-8	-53	-161	-116	1513	9073	25696
H_n	1	4	7	-17	-176	-659	-1007	3532	30751
R_n	0	1	5	12	-5	-181	-840	-1847	1685

Now, $G_n \equiv 0 \pmod{16}$ if and only if $n \equiv 8 \pmod{12}$, $H_n \equiv 0 \pmod{16}$ if and only if $n \equiv 4 \pmod{12}$, and $R_n \equiv 0 \pmod{16}$ if and only if $n \equiv 0 \pmod{12}$. Note that $G_4\cdot H_4\cdot R_4 = R_{12}/3 = -2^4\cdot 5\cdot 7\cdot 11\cdot 23$. Considering the sequences modulo 5, 7, 11 and 23 we find that $2^4\cdot 7\cdot 11\cdot 23 \mid G_n\cdot H_n$ for all $n \equiv 0 \pmod 4$, and in fact $11 \mid G_n$ whenever $16 \mid G_n$. Thus $G_n = \pm 2^m$ implies $m \le 3$. It follows from Section 3 how to solve $|G_n| \le 8$.

We note that a process as described above can always be applied when dealing with a situation as in Lemma 4.10. There is an alternative way, that we will mention in the next section. It provides immediately a very sharp upper bound for the m_i .

4.6. A basic lemma, and some trivial cases.

We introduce some notation, and then give an almost trivial lemma that is at the heart of our reduction methods for both the hyperbolic and the elliptic cases. Let for $i = 1, \ldots, s$

$$e_i = -\mathrm{ord}_{p_i}(\lambda) \ , \quad f_i = \mathrm{ord}_{p_i}\left(\log_{p_i}\left(\frac{\alpha}{\beta}\right)\right) \ , \quad g_i = f_i - e_i \ ,$$

$$\vartheta_i = -\log_{p_i}\left(\frac{-\lambda}{\mu}\right)/\log_{p_i}\left(\frac{\alpha}{\beta}\right) \ .$$

By Lemma 4.1 the p_i-adic logarithms of α/β and $-\lambda/\mu$ exist. Note that $\log_{p_i}(\alpha/\beta) \neq 0$, since the sequence $\{G_n\}$ is not degenerate. Note that for conjugated ξ, ξ' also $\log_p\xi$ and $\log_p\xi'$ are conjugates, hence $\log(\xi/\xi') \in \sqrt{\Delta}\cdot\mathbb{Q}_p$. Hence both numerator and denominator of ϑ_i are in $\sqrt{\Delta}\cdot\mathbb{Q}_{p_i}$, so $\vartheta_i \in \mathbb{Q}_{p_i}$. Hence, if $\vartheta_i \neq 0$, we can write

$$\vartheta_i = \sum_{\ell=k_i}^{\infty} u_{i,\ell}\cdot p_i^{\ell} \ ,$$

where $k_i = \mathrm{ord}_{p_i}(\vartheta_i)$ and $u_{i,\ell} \in \{ 0, 1, \ldots, p_i-1 \}$ for all ℓ. The following lemma localizes the elements of $\{G_n\}$ with many factors p_i, in terms of the p_i-adic expansion of ϑ_i.

LEMMA 4.11. *Let* $n \in \mathbb{N}_0$. *If* $\mathrm{ord}_{p_i}(G_n) + e_i > 1/(p_i-1)$ *then*

$$\mathrm{ord}_{p_i}(G_n) = g_i + \mathrm{ord}_{p_i}(n-\vartheta_i) .$$

Proof. By Lemma 4.1 we have

$$\mathrm{ord}_{p_i}(G_n) + e_i = \mathrm{ord}_{p_i}\left(\left(\frac{\alpha}{\beta}\right)^n - \left(\frac{-\mu}{\lambda}\right)\right) = \mathrm{ord}_{p_i}\left(\left(\frac{-\lambda}{\mu}\right)\cdot\left(\frac{\alpha}{\beta}\right)^n - 1\right) .$$

With $\xi = (-\lambda/\mu)\cdot(\alpha/\beta)^n - 1$ we have $\mathrm{ord}_{p_i}(\xi) > 1/(p_i-1)$. Hence $\mathrm{ord}_{p_i}(\xi) = \mathrm{ord}_{p_i}(\log_{p_i}(1+\xi))$, and it follows that

$$\mathrm{ord}_{p_i}(G_n) + e_i = \mathrm{ord}_{p_i}\left(n\cdot\log_{p_i}\left(\frac{\alpha}{\beta}\right) + \log_{p_i}\left(\frac{-\lambda}{\mu}\right) \right)$$

$$= \mathrm{ord}_{p_i}(n-\vartheta_i) + f_i . \qquad \square$$

We have to exclude some trivial cases first. The case where all p_i-adic digits of ϑ_i from a certain point on are all zero has been dealt with in the previous section. But this case can also be dealt with as follows. Note that $\vartheta_i = r$ holds for all $i = 1, \ldots, s$ with the same r, which is the r from Lemma 4.10. Thus, by Lemma 4.11,

$$m_i \le \max\left(g_i + \mathrm{ord}_{p_i}(n-r),\ 1 - e_i \right) \le g_i + 1 + \mathrm{ord}_{p_i}(n-r) . \qquad (4.12)$$

Then we have, if $\Delta > 0$, by Corollary 4.3,

$$n\cdot\log|\alpha| < \sum_{i=1}^{s} (g_i+1)\cdot\log p_i - \log(\gamma/|w|) + \log|n-r| ,$$

from which a good upper bound for n can be derived. And if $\Delta < 0$, the proof of Lemma 4.10 yields $\vartheta_i = 0$, whence, by (4.12),

$$|G_n| = |w|\cdot\prod_{i=1}^{s} p_i^{m_i} \le v_0\cdot n$$

for some constant v_0. Only minor changes in the results and algorithms of

Section 4.3 suffice to deal with this inequality instead of (4.7).

Another trivial case is that of $\operatorname{ord}_{p_i}(\vartheta_i) < 0$. Then the solutions of (4.1) satisfy $m_i \leq 1/(p_i-1) - e_i$, so, by Lemma 4.11,

$$m_i = f_i - e_i + \operatorname{ord}_{p_i}(n-\vartheta_i) \ .$$

Since $n \in \mathbb{Z}$ and $\operatorname{ord}_{p_i}(\vartheta_i) < 0$ we have $\operatorname{ord}_{p_i}(n-\vartheta_i) = \operatorname{ord}_{p_i}(\vartheta_i)$. Hence

$$m_i \leq \max \left\{ f_i + \operatorname{ord}_{p_i}(\vartheta_i),\ 1/(p_i-1) \right\} - e_i \ .$$

Thus we may assume without loss of generality that $\operatorname{ord}_{p_i}(\vartheta_i) \geq 0$ for all $i = 1, \ldots, s$, and that infinitely many p_i-adic digits $u_{i,\ell}$ of ϑ_i are nonzero.

4.7. The reduction algorithm in the hyperbolic case.

First we give the reduction algorithm for the case $\Delta > 0$. It is based on Lemma 4.11 and Corollary 4.3 only. Let N be an upper bound for n for the solutions $n, m_1, \ldots, m_s$ of (4.1). For example, $N = C_5 \cdot C_6$ as in Theorem 4.9.

<u>ALGORITHM P.</u> (reduces given upper bounds for (4.1) if $\Delta > 0$).

<u>Input:</u> $\alpha, \beta, \lambda, \mu, w, p_1, \ldots, p_s, N$.

<u>Output:</u> new, reduced upper bounds M_i for m_i for $i = 1, \ldots, s$, and N^* for n .

(i) (initialization) *Choose an* $n_0 \geq 0$ *such that* $n_0 > \log|\mu/\lambda|/\log|\alpha/\beta|$;

$$\gamma := |\lambda| - |\mu| \cdot |\alpha/\beta|^{-n_0} \ ;$$

$$\left.\begin{aligned} g_i &:= \operatorname{ord}_{p_i}(\lambda) + \operatorname{ord}_{p_i}(\log_{p_i}(\alpha/\beta)) \\ h_i &:= \operatorname{ord}_{p_i}(\lambda) + \begin{cases} 3/2 & \text{if } p_i = 2 \\ 1 & \text{if } p_i = 3 \\ 1/2 & \text{if } p_i \geq 5 \end{cases} \end{aligned}\right\} \text{ for } i = 1, \ldots, s \ ;$$

$$g := \gamma \ / \ |w| \cdot \prod_{i=1}^{s} p_i^{g_i} \ ; \quad N_0 := N \ ;$$

```
(ii) (computation of the $\vartheta_i$'s) Compute for $i = 1, \dots, s$ the first $r_i$
     $p_i$-adic digits $u_{i,\ell}$ of

         $\vartheta_i = -\log_{p_i}\left(\frac{-\lambda}{\mu}\right)/\log_{p_i}\left(\frac{\alpha}{\beta}\right) = \sum_{\ell=0}^{\infty} u_{i,\ell}\cdot p_i^{\ell}$ ,

     where $r_i$ is so large that $p_i^{r_i} \geq N_0$ and $u_{i,r_i} \neq 0$ ;
(iii) (further initialization, start outer loop) $s_{i,0} := r_i + 1$ for
     $i = 1, \dots, s$ ; $j := 1$ ;
(iv) (start inner loop) $i := 1$ ; $K_j :=$ .false. ;
(v) (computation of the new bounds for $m_i$ , terminate inner loop)
     $s_{i,j} := \min\{\, s \in \mathbb{N}_0 \mid p_i^s \geq N_{j-1}$ and $u_{i,s} \neq 0 \,\}$ ;
     if $s_{i,j} < s_{i,j-1}$
         then $K_j :=$ .true. ;
     if $i < s$
         then $i := i + 1$ ; goto (v) ;
(vi) computation of the new bound for $n$ , terminate outer loop)
     $N_j := \min\left( N_{j-1}, \left(\sum_{i=1}^{s} s_{i,j}\cdot\log p_i - \log g\right)/\log|\alpha| \right)$ ;
     if $N_j \geq n_0$ and $K_j$
         then $j := j + 1$ ; goto (iv) ;
         else $N^* := \max(N_j, n_0)$ ;
              $M_i := \max(h_i, g_i + s_{i,j})$ for $i = 1, \dots, s$ ; stop.
```

THEOREM 4.12. *With all the above assumptions, Algorithm* P *terminates. Equation* (4.1) *with* $\Delta > 0$ *has no solutions with* $N^* \leq n < N$, $m_i > M_i$ *for* $i = 1, \dots, s$.

Proof. Since the p_i-adic expansion of ϑ_i is assumed to be infinite, there exist r_i with the required properties. It is clear that $s_{i,1} \leq r_i < s_{i,0}$, and that $N_j \leq N_{j-1}$. So $s_{i,j} \leq s_{i,j-1}$ holds for all $j \geq 1$. Since $s_{i,j} \geq 0$, there is a j such that $N_j \leq n_0$ or $s_{i,j} = s_{i,j-1}$ for all $i = 1, \dots, s$. In the latter case, K_j remains .false. ; in both cases the algorithm terminates.

We prove by induction on j that $m_i \leq g_i + s_{i,j}$ for $i = 1, \dots, s$, and $n < N_j$ hold for all j . For $j = 0$, it is clear that $n < N_0$. Suppose $n < N_{j-1}$ for some $j \geq 1$. Suppose there exists an i such that $m_i > g_i + s_{i,j}$. From Lemma 4.11 we have

$$\mathrm{ord}_{p_i}(n-\vartheta_i) = m_i - g_i \ge s_{i,j} + 1 ,$$

hence, by $u_{i,s_{i,j}} \neq 0$,

$$n \ge \sum_{\ell=0}^{s_{i,j}} u_{i,\ell}\cdot p^{\ell} \ge p^{s_{i,j}} \ge N_{j-1} ,$$

which contradicts our assumption. Thus, $m_i \le g_i + s_{i,j}$ for $i = 1, \dots, s$. Then from Corollary 4.3 it follows that

$$n < \left[\sum_{i=1}^{s} (g_i+s_{i,j})\cdot \log p_i - \log(\gamma/|w|) \right]/\log|\alpha| ,$$

hence $n < N_j$. □

<u>Remark 1.</u> In general, one expects that $p_i^{s_{i,j}}$ will not be much larger than N_j , i.e. not too many consecutive p_i-adic digits of ϑ_i will be zero. Then N_j is about as large as $\log N_{j-1}$. In practice, the algorithm will often terminate in three or four steps, near to the largest solution. The computation time is polynomial in s , the bottleneck of the algorithm is the computation of the p_i-adic logarithms.

<u>Remark 2.</u> Pethö [1985] gives for $s = 1$ a different reduction algorithm. For a prime p_i he computes the function $g(u)$, defined for $u \in \mathbb{N}$ as the smallest index $n \ge 0$ such that $G_n \neq 0$ and $p_i^u \mid G_n$. Note that if the p_i-adic limit $\lim_{u\to\infty} g(u)$ exists, then by Lemma 4.11 it is equal to ϑ_i .

<u>Remark 3.</u> If $B = \pm 1$ (hence $\Delta > 0$), we can extend the sequence $\{G_n\}_{n=0}^{\infty}$ to negative indices by the recursion formula

$$G_{n-1} = A\cdot B\cdot G_n - B\cdot G_{n+1} \quad \text{for} \quad n = 0, -1, -2, \dots$$

(cf. (4.3)). Then (4.5) is true for $n < 0$ also. We can solve equation (4.1) with $n \in \mathbb{Z}$ not necessarily nonnegative, by applying Algorithm P twice: once for $\{G_n\}_{n=0}^{\infty}$, and once for the sequence $\{G'_n\}_{n=0}^{\infty}$, defined by $G'_n = G_{-n}$. Note that $G'_n = B^n\cdot\left(\mu\cdot\alpha^n+\lambda\cdot\beta^n\right)$, and

$$\vartheta'_i = -\frac{\log_{p_i}(-\mu/\lambda)}{\log_{p_i}(\alpha/\beta)} = +\frac{\log_{p_i}(-\lambda/\mu)}{\log_{p_i}(\alpha/\beta)} = -\vartheta_i \quad \text{for} \quad i = 1, \dots, s .$$

Now, instead of applying Algorithm P twice, we can modify it, so that it works for all $n \in \mathbb{Z}$, as follows. Lemmas 4.8 and 4.11 remain correct if we replace n by $|n|$. In Theorem 4.9 the lower bound for n_0 must be replaced by

$$n_0 > \max \left(2,\ |\log|\mu/\lambda||/\log|\alpha/\beta|,\ |\log|\lambda/\mu||/\log|\alpha/\beta| \right) ,$$

and γ has to be replaced by

$$\gamma = \min \left(|\lambda| - |\mu|\cdot|\alpha/\beta|^{-n_0},\ |\mu| - |\lambda|\cdot|\alpha/\beta|^{-n_0} \right) .$$

Similar modifications should be made in step (i) of Algorithm P. Further, in step (ii), r_i should be chosen so large that

$$\underline{\text{if}}\ \ p_i \neq 2\ \ \underline{\text{then}}\ \ p_i^{r_i} \geq N_0\ \text{ and }\ u_{i,r_i} \neq 0\ ,\ \ u_{i,r_i} \neq p-1\ ;$$
$$\underline{\text{else}}\ \ p_i^{r_i-1} \geq N_0\ \text{ and }\ u_{i,r_i} \neq u_{i,r_i-1}\ ;$$

and similar modifications have to be made in step (v) for $s_{i,j}$. With these changes, Theorem 4.12 remains true with n replaced by $|n|$.

We conclude this section with an example.

Example. Let $A = 6$, $B = 1$, $G_0 = 1$, $G_1 = 4$, $w = 1$, $p_1 = 2$, $p_2 = 11$. Then $\alpha = 3 + 2\cdot\surd 2$, $\beta = 3 - 2\cdot\surd 2$, $\lambda = (\ 1 + 2\cdot\surd 2\ )/4\cdot\surd 2$, $\mu = (\ -1 + 2\cdot\surd 2\ )/4\cdot\surd 2$, and $\Delta = 32$. With $n_0 = e^{60} = 1.142\times10^{26}$ we find $C_4 < 2.49\times10^{20}$. With the modifications of Remark 3 above we have $\gamma > 0.323$, $C_5 < 1.76$, $C_6 < 2.62\times10^{26}$, $C_5\cdot C_6 < 4.62\times10^{26}$. Hence all solutions of $G_n = 2^{m_1}\cdot 11^{m_2}$ satisfy $|n| < 4.62\times10^{26}$, $\max(m_1,m_2) < 2.62\times10^{26}$. We perform the reduction Algorithm P step by step. (We write the p-adic number $\sum_{\ell=0}^{\infty} u_\ell\cdot p^\ell$ as $0.u_0u_1u_2\ldots.$, and if $p > 10$ we denote the digits larger than 9 by the symbols A, B, C, ...).

(i) $n_0 = 2$, $\gamma > 0.303$, $g_1 = 0$, $g_1 = 1$, $g > 0.0275$,
$h_1 = -1$, $h_2 = \frac{1}{2}$, $N_0 = 4.62\times10^{26}$.

(ii) $\vartheta_1 = 0.10111\ 10111\ 01000\ 11100\ 10100\ 01001\ 10001\ 10010$
$00001\ 11101\ 01000\ 10000\ 01001\ 10011\ 10101\ 01101$
$11100\ 01011\ 00001\ 11010\ 00011\ 01001\ 01010\ 00101$
$10001\ 01011\ 00000\ 11001\ 01011\ 11101\ 10100\ 01011$
$001\ldots.$,

ϑ_2 = 0.A9359 05530 7330A 1A223 96230 3A006 A3366 83368 8270.... ,

so $r_1 = 90$ (since $u_{1,89} = 1$, $u_{1,90} = 0$, $2^{89} > N_0$),

$r_2 = 29$ (since $u_{2,29}) = 6$, $11^{29} > N_0$).

(iii) $s_{1,0} = 91$, $s_{2,0} = 30$;

(v)-(vi) $s_{1,1} = 90$, $s_{2,1} = 29$, $K_1 =$ .true., $N_1 < 76.9$;

(v)-(vi) $s_{1,2} = 10$, $s_{2,2} = 2$, $K_2 =$ .true., $N_2 < 8.7$;

(v)-(vi) $s_{1,3} = 6$, $s_{2,3} = 1$, $K_3 =$ .true., $N_3 < 5.8$;

(v)-(vi) $s_{1,4} = 6$, $s_{2,4} = 1$, $K_4 =$ .false., $N_4 < 5.8$.

Hence $|n| \le 5$, $m_1 \le 6$, $m_2 \le 2$. We have

n	−5	−4	−3	−2	−1	0	1	2	3	4	5
G_n	2174	373	64	11	2	1	4	23	134	781	4552

So there are 5 solutions: with $n = -3, -2, -1, 0, 1$.

4.8. The reduction algorithm in the elliptic case.

We now present an algorithm to reduce upper bounds for the solutions of (4.1) in the case $\Delta < 0$. The idea is to apply alternatingly Algorithms P and one of H and I. Let N be an upper bound for n , for example $n = C_7$ as in Theorem 4.9.

ALGORITM C. (reduces upper bounds for (4.1) in the case $\Delta < 0$).

Input: $\alpha, \beta, \lambda, \mu, w, p_1, \dots, p_s, N$.

Output: new, reduced upper bounds N^* for n , and M_i for m_i for $i = 1, \dots, s$.

(i) (initialization) $N_0 := [N]$; $j := 1$;

$$\left.\begin{array}{l} g_i := \mathrm{ord}_{p_i}(\lambda) + \mathrm{ord}_{p_i}(\log_{p_i}(\alpha/\beta)) \\ \\ h_i := \mathrm{ord}_{p_i}(\lambda) + \begin{cases} 3/2 & \text{if } p_i = 2 \\ 1 & \text{if } p_i = 3 \\ 1/2 & \text{if } p_i \ge 5 \end{cases} \end{array}\right\} \text{ for } i = 1, \dots, s ;$$

(ii) (computation of the ϑ_i's, φ, ψ) *Compute for* $i = 1, \dots, s$ *the first* r_i p_i*-adic digits* $u_{i,\ell}$ *of*

$$\vartheta_i = -\log_{p_i}\left(\frac{-\lambda}{\mu}\right)/\log_{p_i}\left(\frac{\alpha}{\beta}\right) = \sum_{\ell=0}^{\infty} u_{i,\ell}\cdot p_i^{\ell} ,$$

where r_i *is so large that* $p_i^{r_i} \ge N_0$ *and* $u_{i,r_i} \ne 0$ *; compute* $\psi = \mathrm{Log}(-\lambda/\mu)/2\pi i$ *, and the continued fraction*

$$|\varphi| = \left|\frac{1}{2\pi i}\cdot\mathrm{Log}(\alpha/\beta)\right| = [\ 0,\ a_1,\ \ldots,\ a_{\ell_0},\ \ldots\ ]$$

with the convergents p_i/q_i *for* $i = 1, \ldots, \ell_0$ *, where* ℓ_0 *is so large that* $q_{\ell_0-1} \le N_0 < q_{\ell_0}$ if $\psi = 0$ *;* $q_{\ell_0} > 4\cdot N_0$ *and* $\|q_{\ell_0}\| > 2\cdot N_0/q_{\ell_0}$ *if* $\psi \ne 0$ *and such* ℓ_0 *can be found in a reasonable amount of time,* $q_{\ell_0} > 4\cdot N_0$ *otherwise;*

```
(iii) (one step of Algorithm P)  For  $i = 1, \ldots, s$  put
      $M_{i,j} := \max\left( h_i,\ g_i + \min\{\ s \in \mathbb{N}_0 \mid p_i^s \ge N_{j-1} \text{ and } u_{i,s} \ne 0\ \}\right)$ ;
 (iv) (one step of Algorithm H or I)
      if  $\psi = 0$
        then $A := \max(a_1,\ldots,a_{\ell_j-1})$ ;  $v := |w|\cdot\prod_{i=1}^{s} p_i^{M_{i,j}}$ ;
             choose  $n_0 \ge 2/\log B$  such that  $B^{n_0/2}/n_0 \ge v/2\cdot|\mu|$ ;
             compute the largest integer  $N_j$  such that
                 $B^{N_j/2}/N_j \le (A+2)\cdot v/4\cdot|\mu|$ ;
             $N_j := \max(n_0,N_j)$ ;
             if  $N_j < N_{j-1}$  then  compute  $\ell_j$  with  $q_{\ell_j-1} \le N_j < q_{\ell_j}$ ;
                                          $j := j + 1$ ; goto (iii) ;
        else if  $\|q_{\ell_{j-1}}\cdot\psi\| > 2\cdot N_{j-1}/q_{\ell_{j-1}}$
                 then $N_j := [2\cdot\log\left(q_{\ell_{j-1}}^2\cdot v/4\cdot|\mu|\cdot N_{j-1}\right)/\log B]$ ;
                 else compute  $K \in \mathbb{Z}$  with  $|K-q_{\ell_{j-1}}\cdot\psi| \le \frac{1}{2}$ ;
                      compute  $n_0 \in \mathbb{Z}$ ,  $0 \le n_0 < q_{\ell_{j-1}}$ , with
                      $K + n_0\cdot p_{\ell_{j-1}} \equiv 0 \pmod{q_{\ell_{j-1}}}$ ;
                      if  $n = n_0$  is a solution of (4.1)
                          then print an appropriate message;
                      $N_j := [2\cdot\log\left(q_{\ell_{j-1}}\cdot v/|\mu|\right)/\log B]$ ;
             if  $N_j < N_{j-1}$
                 then compute the minimal  $\ell_j < \ell_{j-1}$  such that
```

$q_{\ell_j} > 4\cdot N_j$ *and* $\|q_{\ell_j}\cdot\psi\| > 2\cdot N_j/q_{\ell_j}$ *(if such* ℓ_j
does not exist, choose the minimal ℓ_j *such that*
$q_{\ell_j} > 4\cdot N_j$ *)* ; $j := j + 1$; goto (iii) ;

(v) (termination) $N^* := N_{j-1}$; $M_i := M_{i,j}$ for $i = 1, \dots, s$; stop.

The following theorem now follows at once from the proofs of Lemmas 4.6, 4.7 and Theorem 4.12.

THEOREM 4.13. *Algorithm C terminates. Equation (4.1) with* $\Delta < 0$ *has no solutions with* $N^* < n < N$ *and* $m_i > M_i$ *for* $i = 1, \dots, s$ *, apart from those spotted by the algoritm.*

We conclude this section with an example.

Example. Let $A = 1$, $B = 2$, $G_0 = 2$, $G_1 = 3$, then $\Delta = -7$, $\alpha = (1 + \sqrt{-7})/2$ and $\lambda = (2 + \sqrt{-7})/\sqrt{-7}$. Let $w = \pm 1$, $p_1 = 3$, $p_2 = 7$. We have with $n_0 = 2$ the following results: $C_4 < 6.40\times 10^{16}$, $C_3 < 9.14\times 10^{29}$, $C_7 < 7.42\times 10^{30}$, $\max(C_{8,1}, C_{8,2}) < 2.30\times 10^{22}$. Further, $g_1 = 1$, $g_2 = 0$, $h_1 = 1$, $h_2 = 0$. By Theorem 4.9 we may choose $N_0 = 7.42\times 10^{30}$. We have

$$\begin{aligned} \varphi &= (\pi - \arctan(\sqrt{7}/3)) / 2\pi \\ &= [\, 0,\ 2,\ 1,\ 1,\ 2,\ 16,\ 6,\ 1,\ 2,\ 2,\ 13, \\ &\qquad 1,\ 1,\ 3,\ 1,\ 1,\ 2,\ 1,\ 2,\ 1,\ 1, \\ &\qquad 1,\ 1,\ 1,\ 9,\ 2,\ 1,\ 2,\ 1,\ 7,\ 1, \\ &\qquad 6, 269,\ 4,\ 3,\ 1,\ 1,\ 50,\ 2,\ 1,\ 6, \\ &\qquad 1,\ 1,\ 2,\ 1,\ 1,\ 7,\ 1,\ 61,\ 1,\ 12, \\ &\qquad 3,\ 7,\ 4,\ 7,\ 3, 121,\ 1,\ 21,\ 2,\ 1,\ 7,\ \dots\,] , \end{aligned}$$

$$\begin{aligned} \psi &= (\pi - \arctan(4\cdot\sqrt{7}/3)) / 2\pi \\ &= 0.29396\ 28336\ 99645\ 40267\ 89566\ 60520\ 01908\ 06203\dots , \end{aligned}$$

$$\begin{aligned} \vartheta_1 = 0.&20010\ 12210\ 00011\ 02102\ 00211\ 00222\ 02220\ 12021 \\ &10020\ 20202\ 21102\ 00121\ 01000\ 01002\ 11100\ 20122 \\ &11111\ 22202\ 21021\ 02212\ 2200\dots , \end{aligned}$$

$$\begin{aligned} \vartheta_2 = 0.&32542\ 12042\ 43561\ 34020\ 61561\ 13452\ 10116\ 33152 \\ &25336\ 45044\ 11254\ 55033\dots . \end{aligned}$$

Now we choose $\ell_0 = 61$, since

$$q_{61} = 142\ 51183\ 31142\ 44361\ 19375\ 51238\ 81743 > 4\cdot N_0 ,$$

and $\|q_{61}\cdot\psi\| = 0.24487\ldots > 2\cdot N_0/q_{61} = 0.104\ldots$. We have $M_{1,1} = 67$, $M_{2,1} = 37$, and we find $N_1 = 637$. Next we choose $\ell_1 = 9$, since $q_9 = 10102 > 4\times 637$ and $\|q_9\cdot\psi\| = 0.38745\ldots > 2\times 637/10102$. We have $M_{1,2} = 7$, $M_{2,2} = 4$, and we find $N_2 = 74$. Next we choose $\ell_2 = 6$, since $q_6 = 1291 > 4\times 74$, and $\|q_6\cdot\psi\| = 0.49398 > 2\times 74/1291$. We have $M_{1,3} = 6$, $M_{2,3} = 3$, and we find $N_3 = 60$. In the next step we find no improvement. Hence $n \le 60$, $m_1 \le 6$, $m_2 \le 3$. It is a matter of straightforward computation to check that there are only the following 6 solutions of $G_n = \pm 3^{m_1}\cdot 7^{m_2}$: $G_1 = 3$, $G_2 = -1$, $G_3 = -7$, $G_5 = 3^2$, $G_7 = 1$, $G_{17} = 3^2\cdot 7^2$.

4.9. The generalized Ramanujan-Nagell equation.

The most interesting application of the reduction algorithms of the preceding section seems to be the solution of the generalized Ramanujan-Nagell equation (4.2). Let k be a nonzero integer, and let $p_1, \ldots, p_s$ be distinct prime numbers. Then we ask for all nonnegative integers $x, z_1, \ldots, z_s$ with

$$x^2 + k = \prod_{i=1}^{s} p_i^{z_i} .$$

First we note that $z_i = 0$ whenever $-k$ is a quadratic nonresidue (mod p_i) . Thus we assume that this is not the case for all i . Let $p_i \mid k$ for $i = 1, \ldots, t$ and $p_i \nmid k$ for $i = t+1, \ldots, s$. Let $\mathrm{ord}_{p_i}(k)$ be odd for $i = 1, \ldots, r$ and even for $i = r+1, \ldots, t$. Dividing by large enough powers of p_i for $i = 1, \ldots, t$, (4.2) reduces to a finite number of equations

$$D_0\cdot x_1^2 + k_1 = \prod_{i=r+1}^{s} p_i^{z_i'} \tag{4.13}$$

with $p_i \nmid k_1$ for $i = 1, \ldots, s$, and D_0 composed of $p_1, \ldots, p_r$ only, and squarefree. We distinguish between the 2^{s-r} combinations of z_i' odd or even for $i = r+1, \ldots, s$. Suppose that z_i' is odd for $i = r+1, \ldots, u$ and even for $i = u+1, \ldots, s$. Put

$$y = \prod_{i=r+1}^{u} p_i^{(z'_i-1)/2} \cdot \prod_{i=u+1}^{s} p_i^{z'_i/2} \quad . \tag{4.14}$$

Then, from (4.13),

$$D_0 \cdot x_1^2 - \Big(\prod_{i=r+1}^{u} p_i \Big) \cdot y^2 = -k_1 \quad . \tag{4.15}$$

Put $D = D_0 \cdot \prod_{i=r+1}^{u} p_i$. Then (4.14) and (4.15) lead to

$$\begin{cases} v^2 - D \cdot w^2 = k_2 \\ v = \prod_{i=r+1}^{s} p_i^{m_i} \end{cases} , \tag{4.16}$$

with $v = y \cdot \prod_{i=r+1}^{u} p_i$, $w = x_1$, $k_2 = k_1 \cdot \prod_{i=r+1}^{u} p_i$, and also to

$$\begin{cases} v^2 - D \cdot w^2 = k_2 \\ w = \prod_{i=r+1}^{s} p_i^{m_i} \end{cases} , \tag{4.17}$$

with $v = D_0 \cdot x_1$, $w = y$, $k_2 = -k_1 \cdot D_0$. We proceed with either (4.16) or (4.17), whichever is the most convenient (e.g. the one with the smaller $|k_2|$).

If $D = 1$, then (4.16) and (4.17) are trivial. So assume $D > 1$. Let ϵ be the smallest unit in $\mathbb{Z} + \sqrt{D} \cdot \mathbb{Z}$ with $\epsilon > 1$ and $N(\epsilon) = \pm 1$. It is well known that the solutions v, w of $v^2 - D \cdot w^2 = k_2$ fall apart into a finite number of classes of associated solutions. Let there be T such classes, and choose for $\tau = 1, \ldots, T$ in the τ th class the solution $v_{\tau,0}$, $w_{\tau,0}$ such that $\gamma_t = v_{\tau,0} + w_{\tau,0} \cdot \sqrt{D} > 1$ is minimal. Then all solutions of $v^2 - D \cdot w^2 = k_2$ are given by $v = \pm v_{\tau,n}$, $w = \pm w_{\tau,n}$, with

$$\begin{cases} v_{\tau,n} = \big(\gamma_\tau \cdot \epsilon^n + \gamma'_\tau \cdot \epsilon^{-n} \big)/2 \\ w_{\tau,n} = \big(\gamma_\tau \cdot \epsilon^n - \gamma'_\tau \cdot \epsilon^{-n} \big)/2 \cdot \sqrt{D} \end{cases} \tag{4.18}$$

for $n \in \mathbb{Z}$, where $\gamma'_t = v_{\tau,0} - w_{\tau,0} \cdot \sqrt{D}$. That is, $\{v_{\tau,n}\}_{n=-\infty}^{\infty}$ and $\{w_{\tau,n}\}_{n=-\infty}^{\infty}$ are linear binary recurrence sequences. Now, (4.16) and (4.17) reduce to T equations of type (4.1). If $k_2 = 1$, then $T = 1$, $\gamma_1 = \epsilon$, $\gamma'_1 = \epsilon^{-1}$. If $k_2 \mid 2 \cdot D$, $k_2 \neq 1$, then it is easy to prove that $\gamma_\tau^2 = |k_2| \cdot \epsilon$, $\gamma'^2_t = |k_2| \cdot \epsilon^{-1}$, so that

$$v_{\tau,n} = \sqrt{|k_2|}\cdot\left[\, (\gamma_\tau/\sqrt{|k_2|})^{2n+1} + (\gamma'_\tau/\sqrt{|k_2|})^{2n+1} \right]/2 ,$$

$$w_{\tau,n} = \sqrt{|k_2|}\cdot\left[\, (\gamma_\tau/\sqrt{|k_2|})^{2n+1} - (\gamma'_\tau/\sqrt{|k_2|})^{2n+1} \right]/2\cdot\sqrt{D} .$$

In both cases, (4.16) and (4.17) can be solved by elementary means (see Section 4.5, of related interest are Størmer [1897], Mahler [1935], Lehmer [1964], Rumsey and Posner [1964] and Mignotte [1985]). If $k_2 \nmid 2\cdot D$, then we apply the reduction algorithm to one of the equations $v_{\tau,n} = \prod_{i=r+1}^{s} p_i^{m_i}$, $w_{\tau,n} = \prod_{i=r+1}^{s} p_i^{m_i}$. Note that n is allowed to be negative, since $B = \pm 1$, so we can use the modified algorithm of Remark 3, Section 4.7.

Thus we have a procedure for solving (4.2) completely. It is well known how the unit ϵ and the minimal solutions $v_{\tau,0}$, $w_{\tau,0}$ for $\tau = 1, \ldots, T$ can be computed by the continued fraction algorithm for $\sqrt{D}$. We conclude this section with an example. It extends the result of Nagell [1948] (also proved by many others) on the original Ramanujan-Nagell equation $x^2 + 7 = 2^z$.

THEOREM 4.14. *The only nonnegative integers* x *such that* $x^2 + 7$ *has no prime divisors larger than* 20 *are the* 16 *in the following table.*

x	$x^2 + 7$	x	$x^2 + 7$	x	$x^2 + 7$
0	7	7	$56 = 2^3\cdot 7$	31	$968 = 2^3\cdot 11^2$
1	$8 = 2^3$	9	$88 = 2^3\cdot 11$	35	$1232 = 2^4\cdot 7\cdot 11$
2	11	11	$128 = 2^7$	53	$2816 = 2^8\cdot 11$
3	$16 = 2^4$	13	$176 = 2^4\cdot 11$	75	$5632 = 2^9\cdot 11$
5	$32 = 2^5$	21	$448 = 2^6\cdot 7$	181	$32768 = 2^{15}$
				273	$74536 = 2^3\cdot 7\cdot 11^3$

Proof. Since -7 is a quadratic nonresidue modulo 3, 5, 13, 17 and 19 , we have only the primes 2, 7 and 11 left, Only one factor 7 can occur in $x^2 + 7$, thus we have to solve the two equations

$$x^2 + 7 = 2^{z_1}\cdot 11^{z_2} , \qquad (4.19)$$

$$x^2 + 7 = 7\cdot 2^{z_1}\cdot 11^{z_2} . \qquad (4.20)$$

Equation (4.20) can be solved in an elementary way. We distinguish four cases, each leading to an equation of the type

$$y^2 - D\cdot z^2 = c$$

with $c \mid 2\cdot D$, and either y or z composed of factors 2 and 11 only. We have:

(i) z_1 even, z_2 even, $y = 2^{z_1/2}\cdot 11^{z_2/2}$, $z = x/7$, $c = 1$, $D = 7$;

(ii) z_1 odd, z_2 even, $y = 2^{(z_1+1)/2}\cdot 11^{z_2/2}$, $z = x/7$, $c = 2$, $D = 14$;

(iii) z_1 even, z_2 odd, $y = x$, $z = 2^{z_1/2}\cdot 11^{(z_2-1)/2}$, $c = -7$, $D = 77$;

(iv) z_1 odd, z_2 odd, $y = x$, $z = 2^{(z_1-1)/2}\cdot 11^{(z_2-1)/2}$, $c = -7$, $D = 154$.

In the first example of Section 4.5 we have worked out case (i). We leave the other cases to the reader.

Equation (4.19) can be solved by the reduction algorithm. Again we have four cases, each leading to an equation of the type

$$y^2 - D\cdot z^2 = c$$

with either y or z composed of factors 2 and 11 only. We have

(i) z_1 even, z_2 even, $y = x$, $z = 2^{z_1/2}\cdot 11^{z_2/2}$, $c = -7$, $D = 1$;

(ii) z_1 odd, z_2 even, $y = x$, $z = 2^{(z_1-1)/2}\cdot 11^{z_2/2}$, $c = -7$, $D = 2$;

(iii) z_1 even, z_2 odd, $y = x$, $z = 2^{z_1/2}\cdot 11^{(z_2-1)/2}$, $c = -7$, $D = 11$;

(iv) z_1 odd, z_2 odd, $y = x$, $z = 2^{(z_1-1)/2}\cdot 11^{(z_2-1)/2}$, $c = -7$, $D = 22$.

Case (i) is trivial. The other three cases each lead to one equation of type (4.1). In the example in Section 4.7 we have worked out case (ii). With the following data the reader should be able to perform Algorithm P by hand for the cases (iii) and (iv), thus completing the proof. In these cases $N < 10^{30}$ is a correct upper bound.

Case (iii): $\alpha = 10 + 3\cdot\sqrt{11}$, $\lambda = (2 + \sqrt{11})/2\cdot\sqrt{11}$,

ϑ_1 = 0.10011 01000 00110 10100 00110 10110 01001 11110
11011 10010 00001 10110 10111 10100 00110 01101
01010 10010 11101 11001 10000 10010 01010 11011
00010 00111 01110 00101 01101 01111 10101 11110
10.... ,

ϑ_2 = 0.23075 76425 39004 26090 A92A1 03757 07314 58414
7A238.... .

Case (iv): $\alpha = 197 + 42\cdot\sqrt{22}$, $\lambda = (9 + 2\cdot\sqrt{22})/2\cdot\sqrt{22}$,

$$\begin{aligned}\vartheta_1 = 0.&11101\ 01101\ 01110\ 01010\ 10111\ 10001\ 00100\ 00011\\ &10000\ 00110\ 10101\ 01100\ 01101\ 01111\ 01101\ 10101\\ &01011\ 10100\ 01100\ 11101\ 10011\ 00011\ 00010\ 11110\\ &10101\ 01100\ 10011\ 11111\ 01001\ 01110\ 00000\ 01110\\ &011\ldots\ ,\end{aligned}$$

$$\begin{aligned}\vartheta_2 = 0.&6A001\ 68184\ 22921\ 902A0\ 724A4\ 16769\ 45650\ 16482\\ &5A6AA\ldots\ .\end{aligned}$$ □

Remarks. 1. The computation time for the above proof was less than 2 sec.
2. Let $\Phi(X,Y) = a \cdot X^2 + b \cdot X \cdot Y + c \cdot Y^2$ be a quadratic form with integral coefficients, and $\Delta = b^2 - 4 \cdot a \cdot c$ positive or negative. Let k be a nonzero integer, and $p_1, \ldots, p_s$ distinct prime numbers. Then we note that

$$4 \cdot a \cdot \Phi(X,Y) = (2 \cdot a \cdot X + b \cdot Y)^2 - \Delta \cdot Y^2 ,$$

so that the diophantine equations

$$\Phi(X,k) = \prod_{i=1}^{s} p_i^{z_i} , \quad \Phi(X, \prod_{i=1}^{s} p_i^{z_i}) = k$$

in integers $X \neq 0$ and $z_1, \ldots, z_s \in \mathbb{N}_0$, can be solved by our method.

4.10. A mixed quadratic-exponential equation.

In this section we give an application of Algorithm C to the following diophantine equation. Let

$$\Phi(X,Y) = a \cdot X^2 + b \cdot X \cdot Y + c \cdot Y^2$$

be a quadratic form with integral coefficients, such that $D = b^2 - 4 \cdot a \cdot c$ is negative. Let q, v, w be nonzero integers, and $p_1, \ldots, p_s$ distinct prime numbers. Consider the equation

$$\Phi(X, w \cdot \prod_{i=1}^{s} p_i^{m_i}) = v \cdot q^n \tag{4.21}$$

in integers X , and $n, m_1, \ldots, m_s \in \mathbb{N}_0$.

Let β, $\bar{\beta}$ be the roots of $\Phi(x,1) = 0$. Let h be the class number of $\mathbb{Q}(\sqrt{D})$. There exists a $\pi \in \mathbb{Q}(\sqrt{D})$ such that we have the principal ideal equation $(\pi) \cdot (\bar{\pi}) = (q^h)$ .Put $n = n_1 + h \cdot n_2$, with $0 \le n_1 < h$. Then

$\Phi(X,Y) = v\cdot q^{n}$ is equivalent to finitely many ideal equations

$$(a\cdot X-a\cdot\beta\cdot Y)\cdot(a\cdot X-a\cdot\bar{\beta}\cdot Y) = (\sigma)\cdot(\bar{\sigma})\cdot(\pi)^{n_2}\cdot(\bar{\pi})^{n_2} ,$$

with $(\sigma)\bullet(\bar{\sigma}) = (a\cdot v\cdot q^{n_1})$. Hence we have the equations in algebraic numbers

$$\begin{cases} a\cdot X - a\cdot\beta\cdot Y = \gamma\cdot\pi^{n_2} \\ a\cdot X - a\cdot\bar{\beta}\cdot Y = \bar{\gamma}\cdot\bar{\pi}^{n_2} \end{cases} , \quad \begin{cases} a\cdot X - a\cdot\beta\cdot Y = \gamma\cdot\bar{\pi}^{n_2} \\ a\cdot X - a\cdot\bar{\beta}\cdot Y = \bar{\gamma}\cdot\pi^{n_2} \end{cases} ,$$

where γ is composed of σ , units, and common divisors of $a\cdot X - a\cdot\beta\cdot Y$ and $a\cdot X - a\cdot\bar{\beta}\cdot Y$. Note that there are only finitely many choices for γ possible. Thus, (4.21) is equivalent to a finite number of equations

$$a\cdot(\bar{\beta}-\beta)\cdot w\cdot \prod_{i=1}^{s} p_i^{m_i} = \gamma\cdot\pi^{n_2} - \bar{\gamma}\cdot\bar{\pi}^{n_2} ,$$

or, if we put $\lambda = \gamma/a\cdot(\bar{\beta}-\beta)$ and $G_{n_2} = \lambda\cdot\pi^{n_2} + \bar{\lambda}\cdot\bar{\pi}^{n_2}$,

$$G_{n_2} = w\cdot \prod_{i=1}^{s} p_i^{m_i} . \tag{4.22}$$

Here, $\{G_{n_2}\}_{n_2=\infty}^{\infty}$ is a recurrence sequence with negative discriminant. So (4.22) is of type (4.1), and can thus be solved by the reduction algorithm of Section 4.8.

Before giving an example we remark that (4.21) with $D > 0$ is not solvable with the methods of this chapter. This is due to the fact that in $\mathbb{Q}(\sqrt{D})$ with $D > 0$ there are infinitely many units, hence infinitely many possibilities for γ . Another generalization of equation (4.21) is to replace q^n by $\prod_{i=1}^{t} q_i^{n_i}$. This problem is also not solvable by the method of this chapter, since it does not lead to a binary recurrence sequence if $t \geq 2$. These problems can however be dealt with using multi-dimensional approximation techniques, that are presented in other chapters of this thesis. See Chapter 7.

We finally present an example.

THEOREM 4.15. *The equation*

$$X^2 - 3^{m_1}\cdot 7^{m_2}\cdot X + 2\cdot\left(3^{m_1}\cdot 7^{m_2}\right)^2 = 11\cdot 2^n$$

in $X \in \mathbb{Z}$, n, m_1, $m_2 \in \mathbb{N}_0$ *has only the following* 24 *solutions:*

n	m_1	m_2	X	n	m_1	m_2	X
1	1	0	-1, 4	5	2	0	-10, 19
1	0	0	-4, 5	6	0	0	-26, 27
2	0	0	-6, 7	7	0	0	-37, 38
3	0	1	2, 5	7	3	0	2, 25
3	1	0	-7, 10	11	1	1	-137, 158
4	0	1	-6, 13	17	2	2	-829, 1270

Proof. Put $\beta = (1 + \sqrt{-7})/2$. Then

$$X^2 - X\cdot Y + 2\cdot Y^2 = (X-\beta\cdot Y)\cdot(X-\bar{\beta}\cdot Y) .$$

Note that $\mathbb{Q}(\sqrt{-7})$ has class number 1 , and that

$$2 = \frac{1+\sqrt{-7}}{2}\cdot\frac{1-\sqrt{-7}}{2} , \quad 11 = (2+\sqrt{-7})\cdot(2-\sqrt{-7}) .$$

Suppose $\gamma \mid X - \beta\cdot Y$ and $\gamma \mid X - \bar{\beta}\cdot Y$. Then $\gamma \mid (\bar{\beta}-\beta)\cdot Y = -\sqrt{-7}\cdot 3^{m_1}\cdot 7^{m_2}$. On the other hand, $\gamma \mid 11\cdot 2^n$. It follows that $\gamma = \pm 1$, hence $X - \beta\cdot Y$ and $X - \bar{\beta}\cdot Y$ are coprime. Thus we have two possibilities:

$$X - \beta\cdot Y = \pm\,(2 \pm \sqrt{-7})\cdot\left(\frac{1 \pm \sqrt{-7}}{2}\right)^n ,$$

$$X - \beta\cdot Y = \pm\,(2 \mp \sqrt{-7})\cdot\left(\frac{1 \pm \sqrt{-7}}{2}\right)^n ,$$

in each equation the 2nd and 3rd ± being independent. Hence we have to solve

$$G_n^{(j)} = \lambda^{(j)}\cdot\beta^n + \bar{\lambda}^{(j)}\cdot\bar{\beta}^n = 3^{m_1}\cdot 7^{m_2} \quad \text{for } j = 1, 2 ,$$

with $G_{n+1}^{(j)} = G_n^{(j)} - 2\cdot G_{n-1}^{(j)}$ for $j = 1, 2$, and $\lambda^{(1)} = \bar{\lambda}^{(2)} = (2+\sqrt{-7})/\sqrt{-7}$, so that $G_0^{(1)} = G_0^{(2)} = 1$, $G_1^{(1)} = 3$, $G_1^{(2)} = -1$. Note that $\vartheta_i^{(1)} = -\vartheta_i^{(2)}$ for $i = 1, 2$, and $\psi^{(1)} = -\psi^{(2)}$. For $j = 1$ we have solved (4.22) in the example of Section 4.8. It is left to the reader to solve (4.22) for $j = 2$. This can be done with the numerical data given for the case $j = 1$. □

Remark. The computation time for the above proof was less than 3 sec.