CHAPTER 2. PRELIMINARIES.

2.1. Algebraic number theory.

In this section we quote results from algebraic number theory that we use throughout the remaining chapters. We refer to Borevich and Shafarevich [1966] or other text-books on algebraic number theory for full details.

Let K be a finite algebraic extension of $\mathbb{Q}$, of degree $D = [K:\mathbb{Q}]$. There are D embeddings $\sigma : K \to \mathbb{C}$. Let $\alpha \in K$ be an element of degree d, and let $a_0 > 0$ be the leading coefficient of its minimal polynomial over $\mathbb{Z}$. We define the *(logarithmic) height* $h(\alpha)$ by

$$h(\alpha) = \frac{1}{D} \cdot \log\Big(a_0^{D/d} \cdot \prod_{\sigma} \max(1, |\sigma(\alpha)|)\Big) ,$$

where the product is taken over all embeddings σ. Note that this definition does not depend on the field K. Hence, if the conjugates of α are $\alpha = \alpha_1, \ldots, \alpha_d$, then the above definition applied for $K = \mathbb{Q}(\alpha)$ yields

$$h(\alpha) = \frac{1}{d} \cdot \log\Big(a_0 \cdot \prod_{i=1}^{d} \max(1, |\alpha_i|)\Big) .$$

In particular, if $\alpha \in \mathbb{Q}$, then with $\alpha = p/q$ for $p, q \in \mathbb{Z}$ with $(p,q) = 1$ we have $h(\alpha) = \log \max(|p|, |q|)$, and if $\alpha \in \mathbb{Z}$ then $h(\alpha) = \log|\alpha|$.

Let there be s real and $2 \cdot t$ non-real embeddings (with $D = s + 2 \cdot t$). Then Dirichlet's Unit Theorem states that there exists a system of r independent units $\epsilon_1, \ldots, \epsilon_r$, where $r = s + t - 1$, such that the group of units of K is given by

$$\{ \zeta \cdot \epsilon_1^{a_1} \cdot \ldots \cdot \epsilon_r^{a_r} \mid \zeta \text{ a root of unity}, \ a_i \in \mathbb{Z} \text{ for } i=1,\ldots,r \} .$$

There are only finitely many roots of unity in K. Any set of independent units that generate the torsion-free part of the unit group is called a system of *fundamental units*.

The number α is called an *algebraic integer* if $a_0 = 1$. Let the *norm* of an

element $\alpha \in K$ be defined by

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \Big(\prod_{i=1}^{d} \alpha_i \Big)^{D/d} .$$

For algebraic integers, $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. The units are precisely the elements of norm ± 1 . Two elements α, β of K are called *associates* if there is a unit ϵ such that $\alpha = \epsilon \cdot \beta$. Let (α) denote the ideal generated by α . Associated elements generate the same ideal, and distinct generators of an ideal are associated. There exist only finitely many non-associated algebraic integers in K with given norm. The ring of algebraic integers is denoted by $\mathcal{O}_K$. Let $\alpha_1, \ldots, \alpha_D$ be elements of $\mathcal{O}_K$ that are $\mathbb{Q}$-linearly independent. Then $\mathbb{Z}\cdot\alpha_1 \times \ldots \times \mathbb{Z}\cdot\alpha_D$ is called an *order* of K if it is a subring of the 'maximal order' $\mathcal{O}_K$.

In K any algebraic integer can be written as a product of irreducible elements. Here an *irreducible* element (*prime* element) is an element that has no integral divisors but its own associates. However, this decomposition into primes need not be unique. Ideals can also be decomposed into prime ideals, and this decomposition is unique. A *principal ideal* is an ideal generated by a single element α . Two fractional ideals are called equivalent if their quotient is principal. It is well known that there are only finitely many equivalence classes. Their number is called the *class number* h_K . For an ideal $\mathfrak{a}$ it is always true that $\mathfrak{a}^{h_K}$ is a principal ideal. The norm of the (integral) ideal $\mathfrak{a}$ is defined by $N_{K/\mathbb{Q}}(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$.

For a prime ideal $\mathfrak{p}$ there is always a rational prime number p such that $\mathfrak{p}$ is a divisor of (p) . We say that $\mathfrak{p}$ *lies above* p . The *ramification index* $e_{\mathfrak{p}}$ is the largest power to which $\mathfrak{p}$ divides (p) . The *residue class degree* $f_{\mathfrak{p}}$ is the integer such that

$$N_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f_{\mathfrak{p}}} .$$

We denote by $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ the exact power to which the prime ideal $\mathfrak{p}$ divides the ideal $\mathfrak{a}$. For fractional ideals $\mathfrak{a}$ this number can of course be negative. For numbers α we write $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ for $\mathrm{ord}_{\mathfrak{p}}((\alpha))$. Note that

$$\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\alpha)/e_{\mathfrak{p}}$$

can be defined for all $\alpha \in K$. We will return to this in Section 2.3, which deals with p-adic number theory.

2.2. Some auxiliary lemmas.

In this section we give a few simple auxiliary lemmas. The first one enables us to find an upper bound in closed form for some real number $x > 1$ that is bounded by a polynomial in $\log x$. See Pethö and de Weger [1986], Lemma 2.3.

LEMMA 2.1. *Let* $a \geq 0$, $h \geq 1$, $b > 0$, *and let* $x \in \mathbb{R}$, $x > 1$ *satisfy*

$$x \leq a + b \cdot (\log x)^h .$$

If $b > (e^2/h)^h$ *then*

$$x < 2^h \cdot \left(a^{1/h} + b^{1/h} \cdot \log(h^h \cdot b)\right)^h ,$$

and if $b \leq (e^2/h)^h$ *then*

$$x \leq 2^h \cdot \left(a^{1/h} + 2 \cdot e^2\right)^h .$$

Proof. We may assume that x is the largest solution of

$$x = a + b \cdot (\log x)^h .$$

By $(z_1+z_2)^{1/h} \leq z_1^{1/h} + z_2^{1/h}$ we infer

$$x^{1/h} \leq a^{1/h} + c \cdot \log(x^{1/h}) ,$$

where $c = h \cdot b^{1/h}$. Define y by $x^{1/h} = (1+y) \cdot c \cdot \log c$. From

$$\log c < \log(c \cdot \log c)$$

it follows that

$$c^h \cdot (\log c)^h < b \cdot \left(\log\left(c^h \cdot (\log c)^h\right)\right)^h ,$$

which implies $x > c^h \cdot (\log c)^h$. Hence $y > 0$. Now,

$$\begin{aligned} (1+y) \cdot c \cdot \log c = x^{1/h} &\leq a^{1/h} + c \cdot \log(1+y) + c \cdot \log c + c \cdot \operatorname{loglog} c \\ &< a^{1/h} + c \cdot y + c \cdot \log c + c \cdot \operatorname{loglog} c . \end{aligned}$$

Hence

$$y \cdot c \cdot (\log c - 1) < a^{1/h} + c \cdot \operatorname{loglog} c .$$

If $c \geq e^2$ it follows that

$$x^{1/h} = c\cdot\log c + y\cdot c\cdot\log c < c\cdot\log c + \frac{\log c}{\log c - 1}\cdot(a^{1/h}+c\cdot\log\log c)$$

$$< 2\cdot(a^{1/h}+c\cdot\log c) .$$

If $c \le e^2$, then note that $x \le a + (e^2/h)^h\cdot(\log x)^h$. So we may assume $c = e^2$ in this case. The result follows. □

The next lemmas make explicit that x and $\log(1+x)$ are near if $|x|$ is small in the real and complex case, respectively.

LEMMA 2.2. *Let* $a \in \mathbb{R}$. *If* $a < 1$ *and* $|x| < a$ *then*

$$|\log(1+x)| < \frac{-\log(1-a)}{a}\cdot|x| ,$$

and

$$|x| < \frac{a}{1-e^{-a}}\cdot|e^x-1| .$$

Proof. Note that $\log(1+x)/x$ is a strictly positive and strictly decreasing function for $|x| < 1$. Hence it is for $|x| < a$ always less than its value at $x = -a$. The same is true for the function $x/(e^x-1)$. □

LEMMA 2.3. *Let* $0 < a \le \pi$. *If* $|x| < a$ *then*

$$|x| < \frac{a}{2\cdot\sin(a/2)}\cdot|e^{i\cdot x}-1| .$$

If $a < 2$, $|e^{i\cdot x}-1| < a$ *and* $|x| < \pi$ *then*

$$|x| < \frac{2\cdot\arcsin(a/2)}{a}\cdot|e^{i\cdot x}-1| .$$

Proof. Note that $|e^{i\cdot x}-1| = 2\cdot|\sin(\frac{1}{2}\cdot x)|$. and that $2\cdot\sin(\frac{1}{2}\cdot x)/x$ is a positive and even function, that decreases on $0 \le x < a$. Hence it takes its minimal value at $x = a$. The first inequality now follows. The second one can be proved in a similar way. □

2.3. p-adic numbers and functions.

In this section we mention the facts about p-adic numbers and functions that we use. For details we refer to Bachman [1964] and Koblitz [1977], [1980].

We assume that the reader is familiar with the field of p-adic numbers $\mathbb{Q}_p$ and the p-adic valuation ord_p. Note that the ordinary ord_p as defined in $\mathbb{Q}_p$ coincides with the definition given in Section 2.1. We denote by Ω_p the completion of the algebraic closure of $\mathbb{Q}_p$, i.e. the field to which all p-adic theory is applied.

Every nonzero number $\alpha \in \mathbb{Q}_p$ has a p-adic expansion

$$\alpha = \sum_{i=k}^{\infty} u_i \cdot p^i ,$$

where $k = \mathrm{ord}_p(\alpha)$ and the p-adic digits u_i are in $\{ 0, 1, \ldots, p-1 \}$, with $u_k \neq 0$. The number 0 can be represented in this way by taking $k = 0$ and all digits equal to 0, and $\mathrm{ord}_p(0) = \infty$ by definition. If $\mathrm{ord}_p(\alpha) \geq 0$ then α is called a p-adic integer. The set of p-adic integers is denoted by $\mathbb{Z}_p$. A p-adic *unit* is an $\alpha \in \mathbb{Q}_p$ with $\mathrm{ord}_p(\alpha) = 0$. For any p-adic integer α and any $\mu \in \mathbb{N}_0$ there exists a unique rational integer $\alpha^{(\mu)} = \sum_{i=0}^{\mu-1} u_i \cdot p^i$ satisfying

$$\mathrm{ord}_p(\alpha - \alpha^{(\mu)}) \geq \mu , \quad 0 \leq \alpha^{(\mu)} \leq p^\mu - 1 .$$

For $\mathrm{ord}_p(\alpha) \geq k$ we also write $\alpha \equiv 0 \pmod{p^k}$. The p-adic norm is defined by

$$|\alpha|_p = p^{-\mathrm{ord}_p(\alpha)} .$$

In Section 2.1 we have seen how to define ord_p and ord_p on algebraic extensions of $\mathbb{Q}$. For any $\alpha \in \Omega_p$ with $\mathrm{ord}_p(\alpha) > 1/(p-1)$ we can define the p-adic logarithm $\log_p(1+\alpha)$ by the Taylor series

$$\log_p(1+\alpha) = \alpha - \alpha^2/2 + \alpha^3/3 - \ldots .$$

This logarithmic function has the well known properties, such as $\log_p(\xi_1 \cdot \xi_2) = \log_p(\xi_1) + \log_p(\xi_2)$ for all ξ_1, ξ_2 for which it is defined. Further, $\log_p(\xi) = 0$ if and only if ξ is a root of unity. In $\mathbb{Q}_p$ the only roots of unity are the (p-1) th roots of unity (if p is odd). Using these properties, this logarithmic function can be extended to all $\xi \in \Omega_p$ with $\mathrm{ord}_p(\xi) = 0$, as follows. Let $k \in \mathbb{N}$ such that $\mathrm{ord}_p(\xi^k - 1) > 1/(p-1)$. Then

$$\log_p(\xi) = \frac{1}{k}\cdot\log_p\left(1+(\xi^k-1)\right) .$$

An equivalent definition is $\log_p(\xi) = \log_p(\xi/\zeta)$, where ζ is a root of unity such that $\mathrm{ord}_p(\xi-\zeta) > 0$. In this way the p-adic logarithm is a well defined function. Note that $\log_p(\xi)$ lies in the subfield of Ω_p generated by ξ . Finally we note that if $\mathrm{ord}_p(\xi) > 1/(p-1)$ then

$$\mathrm{ord}_p(\xi) = \mathrm{ord}_p(\log_p(1+\xi)) .$$

2.4. Lower bounds for linear forms in logarithms.

In this section we quote in detail the results from the Gelfond-Baker theory that we use. They yield lower bounds for linear forms in logarithms of algebraic numbers. We do not always give the theorems in their full generality, since in this thesis only linear forms with rational unknowns occur, whereas most Gelfond-Baker theorems are formulated for linear forms with algebraic unknowns. We selected results that give completely explicit constants. The first result in this field for a linear form in logarithms with at least three terms is due to Baker [1966], and in the p-adic case to Coates [1969], [1970]. For a survey of this theory, see Baker [1977] and van der Poorten [1977]. We will use more recent, sharper results, due to Waldschmidt [1980] and Yu [1987^a]. Further improvements of the constants have been reached, but too recently to be taken into account in this thesis.

First we deal with real/complex linear forms in logarithms. We quote the result of Waldschmidt [1980].

LEMMA 2.4 (Waldschmidt). *Let* K *be a number field with* $[K:\mathbb{Q}] = D$. *Let* $\alpha_1, \ldots, \alpha_n \in K$, *and* $b_1, \ldots, b_n \in \mathbb{Z}$ $(n \geq 2)$. *Let* $V_1, \ldots, V_n$ *be positive real numbers satisfying* $1/D \leq V_1 \leq \ldots \leq V_n$ *and*

$$V_j \geq \max\left\{ h(\alpha_j), |\log \alpha_j|/D \right\} \quad \text{for } j = 1, \ldots, n .$$

where $\log \alpha_j$ *for* $j = 1, \ldots, n$ *is an arbitrary but fixed determination of the logarithm of* α_j . *Let* $V_j^+ = \max(V_j, 1)$ *for* $j = n, n-1$, *and put*

$$\Lambda = \sum_{j=1}^{n} b_j\cdot\log \alpha_j .$$

Put $B = \max_{1\le i\le n} |b_i|$. *If* $\Lambda \neq 0$ *then*

$$|\Lambda| > \exp\left(-2^{e(n)}\cdot n^{2\cdot n}\cdot D^{n+2}\cdot V_1\cdot\ldots\cdot V_n\cdot \log(e\cdot D\cdot V_{n-1}^{+})\cdot \right.$$

$$\left. \cdot\left(\log B + \log(e\cdot D\cdot V_n^{+}) \right) \right) ,$$

where $e(n) = \min\left(8\cdot n + 51,\ 10\cdot n + 33,\ 9\cdot n + 39 \right)$. *If, moreover, it is known that* $[\mathbb{Q}(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_n}):\mathbb{Q}] = 2^n$, *then we can take* $e(n) = 9\cdot n + 26$ *and replace the factor* $n^{2\cdot n}$ *in the above bound for* $|\Lambda|$ *by* n^{n+4} .

Waldschmidt's main theorem does not give the constant $e(n)$ as detailed as we do, but he does so in his proof, cf. p. 283. We remark that improvements of the above bounds have recently been found by Blass, Glass, Meronk and Steiner [1987^c], [1987^d], Loxton, Mignotte, van der Poorten and Waldschmidt [1987], and Philippon and Waldschmidt [1987]. For the case $n = 2$, a sharp bound has been given by Mignotte and Waldschmidt [1978].

In the p-adic case we quote two results: one due to Schinzel [1967] (Theorem 1) for the case of a linear form in logarithms with two terms, and another for the general case, due to Yu [1987^a] (Theorem 1, see also Yu [1987^b]). We note that Yu's bounds improve much upon the results of van der Poorten [1977]. Moreover, van der Poorten's proofs seem to contain some errors. We give Schinzel's result for quadratic fields only.

LEMMA 2.5 (Schinzel). *Let* p *be prime. Let* Δ *be a squarefree integer, and let* D *be the discriminant of* $K = \mathbb{Q}(\sqrt{\Delta})$. *Let* $\xi = \xi''/\xi'$ *and* $\chi = \chi''/\chi'$ *be elements of* K , *where* ξ', ξ'', χ', χ'' *are algebraic integers. Put*

$$L = \log \max\left(|e\cdot D|^{1/4},\ \|\xi'\cdot\chi'\|,\ \|\xi'\cdot\chi''\|,\ \|\xi''\cdot\chi'\|,\ \|\xi''\cdot\chi''\| \right) ,$$

where $\|\gamma\|$ *denotes the maximal absolute value of the conjugates of* $\gamma \in K$. *Let* $\mathfrak{p}$ *be a prime ideal of* K *with norm* $N\mathfrak{p} = p^{\rho}$. *Put* $\psi = 2/\rho\cdot\log p$, $\varphi = \mathrm{ord}_{\mathfrak{p}}(p)$. *If* ξ *or* χ *is a* $\mathfrak{p}$*-adic unit and* $\xi^n \neq \chi^m$, *then*

$$\mathrm{ord}_{\mathfrak{p}}(\xi^n-\chi^m) < 10^6\cdot\psi^7\cdot\varphi^{-2}\cdot L^4\cdot p^{4\cdot\rho+4}\cdot\left(\log\max(|m|,|n|)+\varphi\cdot L\cdot p^{\rho}+2/L\right)^3 .$$

LEMMA 2.6 (Yu). *Let* $\alpha_1, \ldots, \alpha_n$ ($n \ge 2$) *be nonzero algebraic numbers. Put* $L = \mathbb{Q}(\alpha_1,\ldots,\alpha_n)$, $d = [L:\mathbb{Q}]$. *Let* $b_1, \ldots, b_n$ *be rational integers. Let* $\mathfrak{p}$ *be a prime ideal of* L , *lying above the rational prime* p . *Let* $e_{\mathfrak{p}}$ *be the ramification index, and* $f_{\mathfrak{p}}$ *the residue class degree of* $\mathfrak{p}$. *Write* $L_{\mathfrak{p}}$ *for the completion of* L *with respect to* $\mathrm{ord}_{\mathfrak{p}}$. *(Note that for all*

$\beta \in L_{\mathfrak{p}}$ *we have* $\mathrm{ord}_{\mathfrak{p}}(\beta) = e_{\mathfrak{p}} \cdot \mathrm{ord}_{p}(\beta)$ *.) Let* q *be a rational prime such that*

$$q \nmid p \cdot (p^{f_{\mathfrak{p}}} - 1) \ .$$

Let

$$V_j \geq \max \left(h(\alpha_j),\ f_{\mathfrak{p}} \cdot (\log p)/d \right) \quad \text{for} \quad j = 1, \ldots, n \ ,$$

$$\text{such that} \quad V_1 \leq \ldots \leq V_{n-1} \ , \quad V_{n-1}^{+} = \max(1, V_{n-1}) \ ,$$

$$B_0 \geq \min_{1 \leq j \leq n,\, b_j \neq 0} |b_j| \ , \quad B_n \geq |b_n| \ , \quad B' \geq \max_{1 \leq j \leq n-1} |b_j| \ ,$$

$$B \geq \max \left(|b_1|, \ldots, |b_n|, 2 \right) \ ,$$

$$W \geq \max \left(\log(1 + \frac{3}{4 \cdot n} \cdot B,\ \log B_0,\ f_{\mathfrak{p}} \cdot (\log p)/d \right) \ .$$

Suppose that $\mathrm{ord}_{\mathfrak{p}}(\alpha_j) = 0$ *for* $j = 1, \ldots, n$ *, that*

$$[L(\alpha_1^{1/q}, \ldots, \alpha_n^{1/q}) : L] = q^n \ , \tag{2.1}$$

that $\mathrm{ord}_{\mathfrak{p}}(b_n) \leq \mathrm{ord}_{\mathfrak{p}}(b_j)$ *for* $j = 1, \ldots, n$ *, and* $\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} \neq 1$ *. Then*

$$\mathrm{ord}_{\mathfrak{p}}\left(\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} - 1\right) < C_1(p,n) \cdot a_1^n \cdot n^{n+5/2} \cdot q^{2 \cdot n} \cdot (q-1) \cdot \log^2(n \cdot q) \cdot$$

$$(p^{f_{\mathfrak{p}}} - 1) \cdot \left(2 + \frac{1}{p-1}\right)^n \cdot (f_{\mathfrak{p}} \cdot (\log p)/d)^{-(n+2)} \cdot V_1 \cdot \ldots \cdot V_n \cdot$$

$$\cdot \left(\frac{W}{6 \cdot n} + \log(4 \cdot d)\right) \cdot \left(\log(4 \cdot d \cdot V_{n-1}^{+}) + f_{\mathfrak{p}} \cdot (\log p)/8 \cdot n\right) \ ,$$

where

$$a_1 = 56 \cdot e/15 \quad \textit{if} \quad n \leq 7 \ , \quad a_1 = 8 \cdot e/3 \quad \textit{if} \quad n \geq 8 \ ,$$

and $C_1(p,n)$ *is given by the following table, with for* $p \geq 5$

$$C_1(p,n) = C_1'(p,n) \cdot \left(2 + \frac{1}{p-1}\right)^2 \ .$$

n	2	3	4	5	6	7	≥ 8
$C_1(2,n)$	768523	476217	373024	318871	284931	261379	2770008
$C_1(3,n)$	167881	104028	81486	69657	62243	57098	116055
$C_1'(p,n)$	87055	53944	42255	36121	32276	24584	311077

Remark. Yu [1987[a]] announces that the 'independence condition' (2.1) can be removed. This may be at the cost of somewhat larger constants.

2.5. Numerical methods.

In solving diophantine equations using computational methods from diophantine approximation theory, as we will do in Chapters 4 to 8, it is necessary to have logarithms (real, complex or p-adic) of algebraic numbers available to a large enough precision (maybe several hundreds of digits). We will not go deeply into the problems of computing such approximations, but make only a few remarks on it in this section.

To start with, the precision with which most computers (mainframes as well as personal computers) work, is insufficient for our purposes. Usually at most double precision (52 bits, equivalent to 15 decimal digits), or at best quadruple precision (112 bits, equivalent to 33 decimal digits) is standard available. This is not sufficient for our purposes, not only because we may require larger precision, but also because we want to have the rounding off errors under control, to be sure that no solution of a diophantine equation is missed by unexpected consequences of rounding off errors.

Packages for computations with arbitrary precision are available and very useful, e.g. the MP package of R.P. Brent (cf. Brent [1978]). It is not difficult to write one's own package for simple manipulations on multi-precision numbers, such as addition, multiplication and division (cf. Knuth [1981] for efficient algorithms). No such packages are available for manipulations on p-adic numbers, but the programs are similar to those for real numbers.

Computing roots of polynomials with integral coefficients can be done by Newton's method, both in the real and the p-adic case. One should make sure that the result obtained is correct to the desired precision, preferably not (only) by substituting the found approximation of the root into the polynomial and checking that the result is 0 within the desired precision, but (also) by theoretical error estimates for the Newton method.

Computing logarithms can be done by the Newton method too. However, we did it by using the Taylor series

$$\log(1+x) = x - x^2/2 + x^3/3 - \ldots ,$$

or by the more rapidly converging series

$$\log\frac{1+x}{1-x} = 2\cdot\left(x + x^3/3 + x^5/5 + \ldots \right) .$$

For $|x|$ very small this method works fast, whereas for larger $|x|$ the following idea works well. Compute approximations to the desired precision of log 1.1, log 1.0001, log 1.00000001 , say, and store them. Now compute $x_1 \in [1,1.1)$ and $k_1 \in \mathbb{N}_0$ such that

$$x = x_1\cdot 1.1^{k_1} ,$$

which is a matter of a few divisions of a multi-precision number with a rational number with small numerator and denominator (11 and 10) only, that can be done fast. Next, compute $x_2 \in [1,1.0001)$ and $k_2 \in \mathbb{N}_0$ such that

$$x_1 = x_2\cdot 1.0001^{k_2} ,$$

and $x_3 \in [1,1.00000001)$ and $k_3 \in \mathbb{N}_0$ such that

$$x_2 = x_3\cdot 1.00000001^{k_3} .$$

Then compute $\log x_3$ by the Taylor series, which converges very fast, and compute $\log x$ by

$$\log x = \log x_3 + k_3\cdot\log 1.00000001 + k_2\cdot\log 1.0001 + k_1\cdot\log 1.1 .$$

When computing all this, one should take care of having the rounding off errors at each addition/multiplication under control. This can e.g. be done by doing all computations twice, rounding off in different directions at each step, such that finally a small interval is found in which the exact number lies (with mathematical certainty).

Computation of $\arctan x$ is done by the Taylor series

$$\arctan x = x - x^3/3 + x^5/5 - \ldots .$$

The number $\pi = 3.14159\ldots$ can be computed rapidly by this series for the arctan function, by the identity

$$\pi = 16\cdot\arctan 1/5 - 4\cdot\arctan 1/239 .$$

Doing p-adic arithmetic has the advantage above real arithmetic that rounding off errors do not tend to become larger, as long as one is not dividing by a number with large p-adic order. If $\mathrm{ord}_p(x) > 0$ then $\log_p(1+x)$ can be computed by the Taylor series

$$\log_p(1+x) = x - x^2/2 + x^3/3 + \ldots ,$$

and also it may be useful to compute

$$\log_p \frac{1+x}{1-x} = 2\cdot\left(x + x^3/3 + x^5/5 + \ldots \right) .$$

If $x \not\equiv 0 \pmod p$ and $x \not\equiv 1 \pmod p$ then $\log_p x$ can be computed, since there exists a $k \in \mathbb{N}$ such that $x^k \equiv 1 \pmod p$, and then

$$\log_p x = \frac{1}{k}\cdot\log_p\left(1+(x^k-1)\right)$$

and the above given Taylor series can be used to compute $\log_p x$. Note that in computing the above mentioned Taylor series there will be factors p in the denominators of the terms. Hence, to find the first μ p-adic digits of $\log_p(1+x)$, it is not enough to compute only the first $\mu/\mathrm{ord}_p(x)$ terms of the Taylor series, but the first k terms must be taken into account, where k is the smallest integer satisfying

$$k\cdot\mathrm{ord}_p(x) - \log k/\log p \geq \mu .$$

For rapid convergence of Taylor series it is desirable to apply them only for numbers x with large p-adic order. For example,

$$\log_3 4 = 3 - 3^2/2 + 3^3/3 - \ldots$$

converges not as fast as

$$\log_3 4 = \frac{1}{3}\cdot\log_3 64 = \frac{1}{3}\cdot\left(7\cdot 3^2 - 7^2\cdot 3^4/2 + 7^3\cdot 3^6/3 - \ldots \right) ,$$

or as

$$\log_3 4 = \log_3 \frac{1+3/5}{1-3/5} = 2\cdot\left(3/5 + 3^3/3\cdot 5^3 + 3^5/5\cdot 5^5 + \ldots \right) ,$$

or as

$$\log_3 4 = \frac{1}{3}\cdot\log_3 \frac{1+7\cdot 3^2/65}{1-7\cdot 3^2/65} = \frac{2}{3}\cdot\left(7\cdot 3^2/65 + 7^3\cdot 3^6/3\cdot 65^3 + 7^5\cdot 3^{10}/5\cdot 65^5 + \ldots \right) .$$

The above considerations are sufficient for doing exact computations with the L^3-algorithm, as we present it in Section 3.5. We also use the simple continued fraction algorithm in some instances. This we do as follows. Suppose we want to compute the continued fraction expansion of a real number ϑ, that we have approximated by rational numbers ϑ_1, ϑ_2 such that

$$\vartheta_1 < \vartheta < \vartheta_2 < \vartheta_1 + \epsilon$$

for some small ϵ. We can compute the continued fraction expansions of ϑ_1 and ϑ_2 exactly. As far as they coincide, they coincide also with the continued fraction expansion of ϑ. If the continued fraction expansion of ϑ is needed so far that the k th convergent with denominator $q_k > X_0$ be known exactly, for a given (large) constant X_0, then ϵ should be at least as small as X_0^{-2}.

Almost all computer calculations done for the research of this thesis were performed on an IBM 3083 computer at the Centraal Rekeninstituut of the University of Leiden, using the Fortran-77 language. Also some computations were done at a VAX 11/750 computer at the Rekencentrum of the University of Twente.