CWI Quarterly Volume 7 (4) 1994, pp. 367 – 394

Prime Numbers in Quadratic Fields

T.J. Dekker
Department of Computer Systems, University of Amsterdam
Kruislaan 403, 1098 SJ Amsterdam, The Netherlands
e-mail: dirk@fwi.uva.nl

This paper presents an algorithm for calculating prime numbers in quadratic fields having the unique factorization property. The algorithm resembles the sieve algorithm of Eratosthenes to determine the primes in the set of natural numbers.

Quadratic fields are chosen because they can be represented naturally in a plane. Using this representation, the primes of a field can be displayed in a given bounded region of the plane. The algorithm is used to calculate the prime numbers needed for such displays.

The sieve algorithm and the production of a display are described in a Pascal program. As illustrations some examples of displays are presented.

1. Introduction

Prime numbers are a fascinating subject of research in number theory, which nowadays leads to valuable applications. Much attention has been paid, for instance, to patterns of distribution of primes. A survey of known results and open problems is given by Hardy & Wright [4].

In this paper we consider patterns of distribution of prime numbers in quadratic fields. Our aim is to describe how pictures of prime numbers can be generated. We choose quadratic fields because they can be displayed in a natural way in a plane. Moreover, we restrict ourselves to fields having the unique factorization property, because this considerably simplifies matters.

Patterns of prime numbers in quadratic fields have been considered before. In particular Van der Pol considered primes in the ring of Gauss (in an unpublished paper, 1946) and, with coauthor Speziali, in the ring obtained by adjoining a cube root of one [8].

The next three sections deal with theory of quadratic fields, prime numbers and quadratic reciprocity, needed for Section 5 in which we present our algorithm to determine prime numbers in the fields considered. Appendix 1 gives a Pascal program describing our algorithm in the form of a subprogram and generating a picture of prime numbers for one particular field, followed by several examples of pictures generated by that or a similar program.

The theory presented in the next three sections is obtained from NIVEN & ZUCKERMAN [6], BOREWICZ & SAFAREVIC [2] and IRELAND & ROSEN [5]. Some parts of it can also be found in HARDY & WRIGHT [4] and in STEWART & TALL [9]. The theory is for a great deal not new; many results can be found in the Vorlesungen über Zahlentheorie by DIRICHLET [3]. For the proofs of some theorems we refer to the literature mentioned; however, for the main theorems on primes in quadratic fields we present a proof to clarify the theory.

2. QUADRATIC FIELDS, PRIME NUMBERS AND UNIQUE FACTORIZATION

Let $\mathbb{N}$ denote the system of natural numbers (including 0), $\mathbb{Z}$ the ring of integers and $\mathbb{Q}$ the field of rational numbers. The elements of $\mathbb{Z}$ are sometimes called *rational integers*, to distinguish them from algebraic integers, mentioned below. Lower case latin letters denote rational numbers, lower case Greek letters denote elements of a quadratic field, defined below.

A *quadratic field* is obtained from $\mathbb{Q}$ by adjoining a zero of a certain irreducible quadratic polynomial over $\mathbb{Q}$. Such a zero is of the form $a + b\sqrt{d}$, where a and b are certain rational numbers and the *radicand* d is a square-free integer unequal to 1. Hence we can, without loss of generality, assume that the quadratic field is obtained by adjoining $\sqrt{d}$ to $\mathbb{Q}$. This field, denoted by $\mathbb{Q}(\sqrt{d})$, consists of the numbers $\zeta := x + y\sqrt{d}$, where x and y are rational.

An *algebraic integer* is a zero of a monic polynomial over $\mathbb{Z}$, i.e. a polynomial whose coefficients are rational integers and whose leading coefficient is equal to 1. An element of a quadratic field which is an algebraic integer, is called an *integer of the field.* The set of algebraic integers in a quadratic field forms a ring which is called *the ring of integers* of the field. It is of the form $\mathbb{Z}[\tau]$, obtained from $\mathbb{Z}$ by adjoining an appropriate algebraic integer of $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Z}$; i.e. it consists of the numbers $x + \tau y$, where x and y are rational integers. The value of τ, depending on d, has to be chosen such that all integers of $\mathbb{Q}(\sqrt{d})$ are included in $\mathbb{Z}[\tau]$. Appropriate values are mentioned in the following theorem. Note that, since d is square-free, the case $d \equiv 0 \pmod 4$ is excluded.

THEOREM 2.1 [4, 6].
Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$, where d is square-free rational integer unequal to 1. The ring of integers of a quadratic field $\mathbb{Q}(\sqrt{d})$ is of the form $\mathbb{Z}[\tau]$, where τ is given by

$$\tau = \frac{1+\sqrt{d}}{2}, \quad \textit{when } d \equiv 1 \pmod 4,$$

$$\tau = \sqrt{d}, \qquad \textit{when } d \equiv 2 \text{ or } d \equiv 3 \pmod 4.$$

PROOF. It is easy to see that in the field $\mathbb{Q}(\sqrt{d})$ the numbers $x+\tau y$ are integers of the field for any rational integers x and y. Remains to show that the field does not contain any other integers.

Each element ζ of $\mathbb{Q}(\sqrt{d})$ can be written in the form $\zeta = x + y\sqrt{d}$, where x and y are rational. If $y = 0$, then this number is rational and the number is an algebraic integer only if it is a rational integer, i.e. if x is a rational integer. If $y \neq 0$, then the number is not rational and is a zero of its minimal quadratic polynomial $(\zeta - x + y\sqrt{d})(\zeta - x - y\sqrt{d}) = \zeta^2 - 2x\zeta + x^2 - y^2 d$. Now ζ is an algebraic integer only if the coefficients of this polynomial, $2x$ and $x^2 - y^2 d$, are rational integers. We distinguish between two cases:

1) x is an integer. Then $y^2 d$ is also an integer; hence, since d is square-free, y is also an integer and ζ is of the required form $x + y\sqrt{d}$, where x and y are rational integers;
2) x is not an integer. Then $2x$ is an odd integer and $x^2 - y^2 d$ can be an integer only if $2y$ is also an odd integer and $d \equiv 1 \pmod 4$. From this it follows that ζ has the required form $x' + \tau y'$, where $x' = x - y$ and $y' = 2y$ are rational integers. □

Each irrational element of $\mathbb{Q}(\sqrt{d})$ is a zero of an irreducible quadratic polynomial over $\mathbb{Q}$, whose discriminant equals d times the square of a rational number.

An irrational integer of the field is a zero of an irreducible quadratic monic polynomial over $\mathbb{Z}$, whose discriminant equals d times the square of an integer. Let ζ be an integer of the field such that the discriminant of its corresponding irreducible polynomial has smallest magnitude. This discriminant value, D, is uniquely determined by the field $\mathbb{Q}(\sqrt{d})$ and is called the *discriminant of the field.* In particular, we can take $\zeta = \tau$, and we have:

THEOREM 2.2
The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$, is given by:

$$D = d, \quad \textit{when } d \equiv 1 \pmod 4;$$

$$D = 4d, \quad \textit{when } d \equiv 2 \textit{ or } d = 3 \pmod 4.$$

In $\mathbb{Q}(\sqrt{d})$, the *conjugate* of $\zeta = x + y\sqrt{d}$ is defined as $\overline{\zeta} := x - y\sqrt{d}$, and the *norm* $N(\zeta)$ of ζ, is defined as the absolute value of the product of ζ and its conjugate, i.e. $N(\zeta) := |x^2 - dy^2|$. In the ring of integers $\mathbb{Z}[\tau]$, the norm of $\zeta = x + \tau y$ is similarly as follows:

$$N(\zeta) = |x^2 + xy - \frac{d-1}{4}y^2|, \quad \textit{when } d \equiv 1 \pmod 4,$$

$$N(\zeta) = |x^2 - dy^2|, \quad \textit{when } d \equiv 2 \textit{ or } d \equiv 3 \pmod 4.$$

We here take absolute values for convenience, to ensure that the norm is always non-negative. In number theory, it is, however, more customary to define norm as the product of a number and its conjugate, without taking absolute value. The norm is then obviously non-negative for imaginary fields, where $d < 0$, but not for real fields, where $d > 0$. Norms, defined in either way, have the following important property.

Theorem 2.3 [4, 6].
In a quadratic field, the norm of a product of two elements equals the product of the norms. The norm of an integer of the field is a rational integer.

Proof. This immediately follows from the definition of *norm* and of *algebraic integer.* □

Units, irreducible integers and primes in quadratic fields

A *unit* of a quadratic field is an integer whose inverse is also an integer of the field. Hence, the units of a field are those elements of its ring of integers whose norm equals one. If $\zeta_2 = \epsilon\zeta_1$, where ϵ is a a unit, then ζ_1 and ζ_2 are called *associates* of each other.

An integer of a quadratic field is called *composite*, if it is the product of two non-unit integers of the field. An integer of a quadratic field is called *irreducible*, if it is not a unit and not composite. Thus, within the ring of integers of a field, an irreducible number is divisible only by the element itself and its associates and by the the units of the field.

Note that divisibility is always understood within the ring of integers of the field considered. Thus, for integers α and β we define: α is *divisible* by β, (or, equivalently, β is *divisor* of α, or β *divides* α), if there is an integer γ, such that $\alpha = \beta\gamma$.

An integer of a quadratic field is called a *prime* (of the field or of its ring of integers), if it is not a unit and is divisor of the product $\alpha\beta$ of any two integers α and β only if it is divisor of α or divisor of β.

Historically, irreducible numbers were called '*primes*', as some authors still do [4], [6]. In several well known rings, such as the ring $\mathbb{Z}$ of rational integers and the ring of univariate rational polynomials, the notions '*irreducible number*' and '*prime'* are equivalent.

In general, however, these notions are distinct. A prime is always an irreducible integer, as is easily seen. The converse, however, does not hold in every ring.

Theorem 2.4 [4, 6].
If ζ is an integer of a quadratic field and $N(\zeta)$ is a prime in $\mathbb{Z}$, then ζ is irreducible.

Proof. This immediately follows from Theorem 2.3. □

Theorem 2.5 [4, 6].
Every integer of a quadratic field, not zero or a unit, can be factored into a finite product of irreducible integers of the field.

PROOF. Let ζ be an integer of $\mathbb{Q}(\sqrt{d})$, not zero or a unit. We prove this theorem by induction with respect to $N(\zeta)$, assuming that the theorem holds for all integers of the field having smaller norm. The theorem is obviously true if ζ is irreducible. Otherwise, $\zeta = \beta\gamma$, where β and γ are non-unit factors, whose norms are smaller than $N(\zeta)$. Using the induction hypothesis, it follows that β and γ can be factored into a finite number of irreducible integers, and the theorem follows. □

UNIQUE FACTORIZATION

A field, or its ring of integers, is said to have the *unique factorization* property, if the factorization of any integer into irreducible factors is unique apart from the order of the factors and ambiguities between associated factors, i.e. the irreducible factors in any two factorizations of a given integer can be ordered such that corresponding factors are associates.

THEOREM 2.6 [9].

In a ring having the unique factorization property, every irreducible element is a prime. Hence, in such a ring the notions 'irreducible element' and 'prime' are equivalent.

PROOF. Let ξ be an irreducible element of the ring considered, and α and β elements such that ξ is divisor of $\alpha\beta$. The unique factorization property implies that ξ or one of its associates must occur in the factorization of $\alpha\beta$; hence, it must occur in the factorization of α or β, which completes the proof. □

Most quadratic fields, and corresponding rings of integers, do not have the unique factorization property. Some simple examples are $\mathbb{Z}[\sqrt{-5}], \mathbb{Z}[\sqrt{-6}]$ and $\mathbb{Z}[\sqrt{10}]$. In $\mathbb{Z}[\sqrt{-5}]$, for instance, we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

which are two essentially different factorizations of 6. These rings also contain irreducible numbers which are not primes; for instance, in $\mathbb{Z}[\sqrt{-5}]$ number 2 is irreducible but not prime, since it divides 6 but neither of the factors $(1+\sqrt{-5})$ and $(1-\sqrt{-5})$.

Examples of quadratic rings having the unique factorization property are the ring of Gauss $\mathbb{Z}[\sqrt{-1}]$ and the ring $\mathbb{Z}[\omega]$, where $\omega = (1+\sqrt{-3})/2$. These rings are the ring of integers of the *cyclotomic* fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, respectively, generated by a fourth or sixth root of unity. For instance, the natural primes 2 and 5 are composite numbers in $\mathbb{Z}[\sqrt{-1}]$:

$$2 = (1+\sqrt{-1})(1-\sqrt{-1}),\ 5 = (2+\sqrt{-1})(2-\sqrt{-1}).$$

It is important to consider the complete ring of integers of a field. For instance, $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathbb{Z}[\omega]$ and does not have unique factorization:

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3});$$

but in $\mathbb{Z}[\omega]$, the latter two factors are equal to $\omega \cdot 2$ and $\omega^2 \cdot 2$, respectively, in accordance with the unique factorization property.

Euclidean quadratic fields

A quadratic field, or its ring of integers, is *Euclidean*, if the ring of integers satisfies a Euclidean algorithm, i.e. an algorithm to calculate the greatest common divisor of two integers by means of successive determination of quotient and remainder. Here it is important that the remainders obtained have norm smaller than the norm of the divisor. In that case, the field (the ring of integers) is called *norm-Euclidean*, i.e. Euclidean with respect to the norm defined for the field and the ring.

Theorem 2.7 [4, 6, 9].
Every Euclidean quadratic field has the unique factorization property.

There exist only a finite number of distinct Euclidean quadratic fields. We subdivide them with respect to the value of d modulo 4. The Euclidean quadratic fields are the quadratic fields $Q(\sqrt{d})$ with the following values of d:

$$d \equiv 1 \pmod 4: \quad d = -11, -7, -3, 5, 13, 17, 21, 29, 33, 37, 41, 57, 73;$$

$$d \equiv 2 \pmod 4: \quad d = -2, 2, 6;$$

$$d \equiv 3 \pmod 4: \quad d = -1, 3, 7, 11, 19.$$

Several authors have contributed to the proof of these results, namely that these and no other Euclidean fields exist. A survey of these and related results are given in Hardy & Wright [4] and Van der Linden [7].

There are also several quadratic fields which have the unique factorization property, but are not (norm-) Euclidean. In particular, this holds for the quadratic fields $\mathbb{Q}(\sqrt{d})$ for the following negative values of d (all congruent 1 modulo 4):

$$d = -163, -67, -43, -19,$$

and for no other negative values; it also holds for several positive values, the values $d < 100$ being [2, Tabelle, p. 454, where we take the fields having *class number* equal to 1] [9]:

$$d \equiv 1 \pmod 4: \quad d = 53, 61, 69, 77, 89, 93, 97;$$

$$d \equiv 2 \pmod 4: \quad d = 14, 22, 38, 46, 62, 86, 94;$$

$$d \equiv 3 \pmod 4: \quad d = 23, 31, 43, 47, 59, 67, 71, 83.$$

It is unknown if there are infinitely many values of d for which the field $\mathbb{Q}(\sqrt{d})$ has unique factorization. Behrbohm & Rédei [1, 7] showed that a quadratic field can have the unique factorization property only if the discriminant D has at most two different prime factors; if $d > 0$ then either d is prime or $d = pq$, where $p \equiv 3 \pmod 4$ and $q = 2$ or $q \equiv 3 \pmod 4$.

3. Characterization of primes of quadratic fields

We restrict ourselves to quadratic fields having the unique factorization property. In these fields, the notions '*irreducible integer*' and '*prime*' are equivalent, as stated above. In the sequel, we always use the historically original term '*prime*', rather than '*irreducible integer*'.
We denote natural numbers by n, n', n'', *natural primes*, i.e. *positive rational primes*, by p, q, and primes of quadratic fields by π, π', π'', etcetera.

To determine if an integer of a unique factorization field is a prime or not, depends only on its norm. This follows from the following theorems.

Theorem 3.1 [6].
If $\mathbb{Q}(\sqrt{d})$ has the unique factorization property, then to any prime π of $\mathbb{Q}(\sqrt{d})$ there corresponds a unique natural prime p which is divisible by π.

Proof. A prime π of $\mathbb{Q}(\sqrt{d})$ is divisor of its norm. Hence there exist natural numbers divisible by π. Let n be the least of these. Then n is a natural prime. For, otherwise, n could be factored into a product $n'n''$ of smaller natural numbers and, by the unique factorization property, either n' or n'' would be divisible by π, contradicting the assumption that n is the least natural number divisible by π. Hence, n is a natural prime p divisible by π. To prove the uniqueness of p, assume that q is another natural prime divisible by π. Then there exist rational integers x, y such that $px + qy = 1$, from which it follows that π is a divisor of 1, which is obviously false. Hence, the natural prime p such that π divides p, is unique. □

For the next theorems we need the concept of quadratic residue defined as follows.

Let a be a non-zero rational integer and p a natural prime not divisor of a. Then a is called *quadratic residue* modulo p if there is a natural number n such that $n^2 \equiv a \pmod p$; otherwise, a is called *quadratic non-residue* modulo p.

Consider the set of non-zero residues modulo p, which consists of the $p - 1$ elements $1, 2, \ldots, p-1$. For odd p this set contains $(p-1)/2$ quadratic residues and the same number of quadratic non-residues.

Theorem 3.2 [6].
If $\mathbb{Q}(\sqrt{d})$ has the unique factorization property, then

1. *Any natural prime p is either a prime π or a product $\pi'\pi''$ of two (not necessarily distinct) primes of $\mathbb{Q}(\sqrt{d})$;*
2. *The totality of primes π, π', π'', obtained by applying part 1 to all natural primes, together with their associates, constitute the set of all primes of $\mathbb{Q}(\sqrt{d})$;*

3. *An odd natural prime p not divisor of d is a product $\pi'\pi''$ of two primes if and only if d is a quadratic residue modulo p.*

PROOF.

1. A natural prime p is either a prime, π, of $\mathbb{Q}(\sqrt{d})$, or composite, i.e. $p = \alpha\beta$, where α and β are non-unit integers of $\mathbb{Q}(\sqrt{d})$. In the latter case, $N(\alpha)N(\beta) = N(p) = p^2$. Since α and β are not units, there norms are unequal to 1, so that we must have $N(\alpha) = N(\beta) = p$. Hence, according to Theorem 2.4, α and β are primes, π', π'', of $\mathbb{Q}(\sqrt{d})$. This proves part 1.
2. This follows from Theorem 3.1 and part 1 of this theorem.
3. Let p be an odd natural prime not divisor of d and such that d is a quadratic residue modulo p. Then there exists a natural number n such that p is divisor of $n^2 - d = (n - \sqrt{d})(n + \sqrt{d})$. If p were a prime of $\mathbb{Q}(\sqrt{d})$, then one of the factors $n - \sqrt{d}$ and $n + \sqrt{d}$ would be divisible by p, which is impossible by Theorem 2.1. Therefore, by part 1 of this theorem, $p = \pi'\pi''$.

   Conversely, let p be an odd natural prime not divisor of d and equal to a product $\pi'\pi''$ of primes of $\mathbb{Q}(\sqrt{d})$. Then we can write $\pi' = x + \tau y$, and we have $N(\pi') = p$. We now distinguish between two cases.

   a) $d \equiv 2$ or $d \equiv 3 \pmod 4$.

   Then $N(\pi') = |x^2 - dy^2| = p$, so that $x^2 \equiv dy^2 (\text{mod } p)$. Now y can not be divisible by p, because this would imply that x, hence also π' would be divisible by p, which is obviously false. So, there is a rational integer w such that $wy \equiv 1 (\text{mod } p)$. Hence, $d \equiv w^2x^2 \pmod p$, i.e. d is quadratic residue modulo p, which proves this case.

   b) $d \equiv 1 \pmod 4$.

   Then $N(\pi') = |x^2 + xy - \frac{d-1}{4}y^2| = p$. Multiplying by 4 we get, since p is odd, $(2x + y)^2 \equiv dy^2 (\text{mod } p)$. Again, y can not be divisible by p; so there is a rational integer w such that $wy \equiv 1 \pmod p$. Hence, $d \equiv w^2(2x + y)^2 (\text{mod } p)$, i.e. d is quadratic residue modulo p, which proves this case and completes the proof of the theorem. □

This theorem does not cover the cases p even and p divisor of d. These cases are included in the following theorem, taken from [2].

THEOREM 3.3.
Let $\mathbb{Q}(\sqrt{d})$ have the unique factorization property and D be the discriminant of the field. Then

1. *If the natural prime p is a product $\pi'\pi''$ of primes of* $\mathbb{Q}(\sqrt{d})$, *then* $N(\pi') = N(\pi'') = p$*; otherwise, p is a prime π of* $\mathbb{Q}(\sqrt{d})$ and $N(\pi) = p^2$;

2. *Any odd natural prime p not divisor of D (or d) is a product $\pi'\pi''$ of primes of $\mathbb{Q}(\sqrt{d})$ if D (or d) is a quadratic residue modulo p; otherwise, it is itself a prime π* of $\mathbb{Q}(\sqrt{d})$;
3. *If 2 is not divisor of D, which implies D is odd, hence $d \equiv 1$ $(mod\, 4)$, then 2 is a product $\pi'\pi''$ of primes of $\mathbb{Q}(\sqrt{d})$ if $d \equiv 1$ $(mod\, 8)$; otherwise, $d \equiv 5$ $(mod\, 8)$ and 2 is a prime of $\mathbb{Q}(\sqrt{d})$*;
4. *Any (odd or even) natural prime p which is divisor of D, is equal to a product $\pi'\pi''$ of primes of $\mathbb{Q}(\sqrt{d})$; only in this case the prime factors π' and π'' are associates.*

PROOF.

1. This easily follows from the proof of Theorem 3.2 part 1.
2. This is an immediate consequence of Theorem 3.2 parts 3 and 1.
3. Let $d \equiv 1$ (mod 8). Then $1 - d = (1 + \sqrt{d})(1 - \sqrt{d})$ is divisible by 8. Hence, if 2 were a prime in $\mathbb{Q}(\sqrt{d})$, at least one of the factors $1 + \sqrt{d}$ or $1 - \sqrt{d}$ would be divisible by 4, which is impossible according to Theorem 2.1.

   Conversely, let $d \equiv 1$ (mod 4) and 2 not be prime in $\mathbb{Q}(\sqrt{d})$. Then $2 = \pi'\pi''$ and we have $N(\pi') = N(\pi'') = 2$. We can write $\pi' = x + \tau y$, so that $N(\pi') = |x^2 + xy - \frac{d-1}{4}y^2| = 2$. Now y cannot be even, because this would imply $x(x+y)$ even, so that also x would be even and π' would be divisible by 2, which is false. Multiplying by 4 we obtain $(2x+y)^2 - dy^2 = \pm 4N(\pi') = \pm 8$. Since both $2x+y$ and y are odd and the square of an odd number is congruent 1 modulo 8, it follows that $d \equiv 1$ (mod 8), which completes the proof of this part.
4. Let now p be a natural prime and divisor of D.
   We first consider the case that p is odd. Then p is a divisor of $d = (\sqrt{d})^2$. If p were a prime in $\mathbb{Q}(\sqrt{d})$, then p would be a divisor of $\sqrt{d}$, which is impossible according to Theorem 2.1. Hence, p is a product of primes $\pi'\pi''$. Since d is square-free, $w := d/p$ does not have another factor p and we have $\pi'\pi''w = (\sqrt{d})^2$, which can only be satisfied if p is equal to $(\pi')^2$, possibly up to a unit factor; i.e. π' and π'' are associates.
   We now consider the case $p = 2$. Then $d \equiv 2$ or $d \equiv 3$ (mod 4). In the former case, 2 is a divisor of d and the result follows in the same way as above. In the latter case, 2 is a divisor of $(1 + \sqrt{d})^2 = 1 + d + 2\sqrt{d} = 2\alpha$, where $\alpha = (d + 1)/2 + \sqrt{d}$. We now have $N(\alpha) = (d - 1)^2/4$, which is odd, because $d \equiv 3$ (mod 4). Hence, in the same way as above, $2 = \pi'\pi''$, where π' and π'' are associate primes. Conversely, let $p = \pi'\pi''$, where π' and π'' are associates. Then π''/π' is a unit. Writing $\pi' = a + b\sqrt{d}$, where a and b are rational integers (or, if $d \equiv 1$ (mod 4), possibly both rational integer plus 1/2), then we obtain $\pi''/\pi' = (a^2 + b^2 d - 2ab\sqrt{d})/\pm p$. This can only be an integer of $\mathbb{Q}(\sqrt{d})$ if p is a divisor of d and of a, but not of b, which proves the result and the theorem. □

4. Quadratic reciprocity

The important notion of quadratic reciprocity enables us to transform the property of quadratic residue of d (or D) modulo odd prime p to a property of odd primes p modulo D. We give some definitions and present some theorems without proof.

The quadratic residues modulo a given odd prime p are characterised by the *Legendre symbol* defined as follows.

Definition. Let a be any rational integer and p an odd natural prime not divisor of a. Then the *Legendre symbol* $(\frac{a}{p})$ has the value $+1$ if a is quadratic residue, and the value -1 if a is not quadratic residue modulo p.

The Legendre symbol satisfies the following theorems.

Theorem 4.1. [2, 4, 5, 6].
Let p be an odd natural prime and let a and b denote rational integers not divisible by p. Then

i) $\left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

ii) $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = \left(\dfrac{ab}{p}\right)$,

iii) $a \equiv b \pmod{p}$ *implies* $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$,

iv) $\left(\dfrac{-1}{p}\right) = (-1)^{(p-1)/2}$,

v) $\left(\dfrac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Note, that the parts ii, iii, iv are immediate consequences of part i. Part iv is equivalent with: -1 is quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$. Part v is equivalent with: 2 is quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 8$.

4.2 Theorem of quadratic reciprocity [2, 4, 5, 6].
Let p and q be distinct odd natural primes. If at least one of them is congruent 1 modulo 4, then p is quadratic residue modulo q if and only if q is quadratic residue modulo p; in formula:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right);$$

if, however, p and q both are congruent 3 modulo 4, then p is quadratic residue modulo q if and only if q is not quadratic residue modulo p; in formula:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Thus, the two cases together can equivalently be formulated as follows: if p and q are distinct odd natural primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2.(q-1)/2}.$$

Definition. Let a be any rational integer and b an odd natural number, such that a and b have no common prime factor. Let $b = p_1 p_2 \dots p_m$, where the factors $p_1, \dots p_m$, are (not necessarily distinct) natural primes. Then the *Jacobi symbol* $\left(\frac{a}{b}\right)$ is defined by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right).$$

This definition includes the case $b = 1$ for which case the Jacobi symbol has the value 1. If all factors $(\frac{a}{p_1}), \dots, (\frac{a}{p_m})$ have the value $+1$, then a is quadratic residue modulo b, according to the Chinese remainder theorem. Thus, $(\frac{a}{b}) = 1$ is necessary, but not sufficient, to ensure that a is quadratic residue modulo b.

The Jacobi symbol satisfies the following theorems.

Theorem 4.3 [2] [5] [6].
Let a, b, c denote rational integers. If c is odd and a and b do not have a prime factor in common with c, then

i) $\left(\frac{a}{c}\right)\left(\frac{b}{c}\right) = \left(\frac{ab}{c}\right)$,

ii) $a \equiv b \pmod{c}$ *implies* $\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right)$,

iii) $\left(\frac{-1}{c}\right) = (-1)^{(c-1)/2}$,

iv) $\left(\frac{2}{c}\right) = (-1)^{(c^2-1)/8}$.

4.4. Theorem of quadratic reciprocity for Jacobi symbol [2, 5, 6].
Let a and b be any odd natural numbers having no common prime factor. Then

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)/2.(b-1)/2}.$$

Examples

To illustrate the theory, we give some examples, from [4], for which the discriminant is positive or negative and is congruent 1 modulo 4 or not. The results stated for these examples follow from Theorem 3.3 using Theorem 4.1, and in examples 2 and 4 also Theorem 4.2.

1. $d = -1, D = -4$.
This is field $\mathbb{Q}(\surd -1)$ and its ring of integers $\mathbb{Z}[\surd -1]$, which is the well known *ring of Gauss.* For odd natural prime p, the number $d = -1$ (or $p-1$) is quadratic residue modulo p if and only if $p \equiv 1 \pmod 4$. Moreover, D has the prime divisor 2. So, the primes in this ring are:

the numbers whose norm is a natural prime congruent 1 modulo 4;
the natural primes congruent 3 modulo 4 and associates;
the numbers whose norm equals 2; i.e. $1 + \surd -1$ and associates.

2. $d = D = -3$.
This is field $\mathbb{Q}(\surd -3)$ and its ring of integers $\mathbb{Z}[\frac{1}{2}(1 + \surd -3)]$.
For odd natural prime $p \neq 3$, the number $d = -3$ (or $p-3$) is quadratic residue modulo p if and only if $p \equiv 1 \pmod 3$. Moreover, 2 is a prime of the field, because $d \equiv 5 \pmod 8$, and D has the prime divisor 3. So, the primes in this ring are:

the numbers whose norm is a natural prime congruent 1 modulo 3;
the natural primes congruent 2 modulo 3 and associates; this includes 2, as it should;
the numbers whose norm equals 3; i.e. the number $\surd -3$ and associates.

3. $d = 2, D = 8$.
This is field $\mathbb{Q}(\surd 2)$ and its ring of integers $\mathbb{Z}[\surd 2]$.
For odd natural prime p, number $d = 2$ is quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 8$. Moreover, D has the prime divisor 2. So, the primes in this ring are:

the numbers whose norm is a natural prime congruent $\pm$ 1 modulo 8;
the natural primes congruent ± 3 modulo 8 and associates;
the numbers whose norm equals 2; i.e. the number $\surd 2$ and associates.

4. $d = D = 5$.
This is field $\mathbb{Q}\surd 5)$ and its ring of integers $\mathbb{Z}[\frac{1}{2}(1 + \surd 5)]$.
For odd natural prime p other than 5, number $d = 5$ is quadratic residue modulo p if and only if $p \equiv 1$ or $4 \pmod 5$. Moreover, 2 is a prime of the field, because $d \equiv 5 \pmod 8$, and D has the prime divisor 5. So, the primes in this ring are:

the numbers whose norm is a natural prime congruent ± 1 modulo 5;

the natural primes congruent ±2 modulo 5 and associates; this includes 2, as it should;

the numbers whose norm equals 5; i.e. the number $\sqrt{5}$ and associates.

5. Algorithm to determine prime numbers in quadratic fields

Now we are ready to present our algorithm to determine primes in quadratic fields having the unique factorization property. Our purpose is to generate pictures of primes in certain bounded regions of the fields. Here *bounded region* is understood according to a representation of the field in the plane, such that the rational numbers are placed on the x-axis and the rational multiples of $\sqrt{d}$ on the y-axis.

Whether an integer of a quadratic field considered is prime or not, depends only on its norm. This follows from Theorems (3.2) and (3.3). We propose, therefore, an algorithm to calculate a set of norms of prime numbers of a given quadratic field, from which the corresponding set of prime numbers of the field is easily obtained.

We give, besides the radicand d or the discriminant D of quadratic field $\mathbb{Q}(\sqrt{d})$, also a certain maximum value M. The task of our algorithm is then to determine the norms of all primes of the field which are not larger than M.

First an appropriate set S of natural numbers is formed, to be used as starting set for a sieve algorithm. S must contain the norms of all prime numbers of the field and may contain also the norms of composite numbers. Subsequently, a sieve algorithm, defined below, is applied to S in order to remove the norms of all composite numbers of the field. Analogous to the sieve of Eratosthenes to determine natural primes, the sieve algorithm applied to S should thus yield all norms of prime numbers of the field considered up to the maximum value M.

How do we determine an appropriate starting set S?

A simple method, suitable for complex fields, where $d < 0$, is the following. Calculate the norm of all integers of the field in a certain bounded region which is large enough to yield all norms up to the given maximum value M. This method requires fewer operations than the subsequent sieve process, and is therefore acceptable for complex fields. For real fields, where $d > 0$, the method does not work, because we do not know how large region of numbers of the field we need, such that all norms up to M are obtained. This is related to the fact that real fields contain infinitely many units and, hence, also infinitely many numbers whose norm has a certain value.

Another method to define an appropriate starting set S uses Theorem 3.3 and the theorems of the previous section on quadratic reciprocity.

Primes characterized by norms modulo the discriminant

By means of the Jacobi symbol, the properties used in Theorem 3.3 are expressed in terms of a function which is periodic modulo the discriminant D of the field considered.

DEFINITION [2].
Consider a quadratic field $\mathbb{Q}(\sqrt{d})$, where the *radicand* d is a square-free rational integer, and let D be the discriminant of the field. The *quadratic character* of this field is the function $\chi(x) = \chi_d(x)$, defined as follows for any rational integer x:

If x and D have a common prime factor, then $\chi_d(x) = 0$, otherwise, for the cases indicated, where $h = d/2$ for d even:

i) $d \equiv 1 \pmod 4$: $\qquad \chi_d(x) = \left(\frac{x}{|d|}\right)$;

ii) $d \equiv 3 \pmod 4$: $\qquad \chi_d(x) = (-1)^{(x-1)/2}\left(\frac{x}{|d|}\right)$;

iii) $d \equiv 2 \pmod 4$: $\qquad \chi_d(x) = (-1)^{(x^2-1)/8+(x-1)/2.(h-1)/2}\left(\frac{x}{|h|}\right)$.

Note that x is odd in cases (ii) and (iii) so that the exponents of -1 are natural numbers. These cases are equivalent with:

ii) $d \equiv 3 \pmod 4$:
$\chi_d(x) = \left(\frac{x}{|d|}\right)$, $x \equiv 1 \pmod 4$, and $= -\left(\frac{x}{|d|}\right)$, $x \equiv 3 \pmod 4$;

iiia) $d \equiv 6 \pmod 8$:
$\chi_d(x) = \left(\frac{x}{|h|}\right)$, $x \equiv 1$ or $3 \pmod 8$, and $= -\left(\frac{x}{|h|}\right)$ otherwise;

iiib) $d \equiv 2 \pmod 8$:
$\chi_d(x) = \left(\frac{x}{|h|}\right)$, $x \equiv \pm 1 \pmod 8$, and $= -\left(\frac{x}{|h|}\right)$, $x \equiv \pm 3 \pmod 8$.

We use case (iiib) only for $d = 2$, which is the only value of $d \equiv 2 \pmod 8$ for which the field $\mathbb{Q}(\sqrt{d})$ has the unique factorization property. This follows from the theorem by BEHRBOHM & RÉDEI [1] mentioned at the end of Section 2.

THEOREM 5.1 [2].
The quadratic character $\chi(x) = \chi_d(x)$ of a field $\mathbb{Q}(\sqrt{d})$ is a multiplicative and periodic function of x modulo $|D|$; i.e.

$$\chi(xy) = \chi(x)\chi(y) \text{ and if } x \equiv y \ (mod\,|D|) \text{ then } \chi(x) = \chi(y).$$

Moreover, for the following specific values the quadratic character satisfies:

i) *if x is an odd natural prime p not divisor of D (or d), then*

$$\chi_d(x) = \left(\frac{d}{p}\right);$$

ii) *if $x = 2$ is not divisor of D, hence, $d \equiv 1$ (mod 4), then*

$$\chi_d(x) = 1 \; if \; d \equiv 1 \pmod 8, \; \chi_d(x) = -1 \; if \; d \equiv 5 \pmod 8;$$

iii) *if x is the square of a natural prime not divisor of D then $\chi_d(x) = 1$.*

Using the theorems of Section 4, we can reformulate Theorem 3.3 as follows.

Theorem 5.2.
Let $\mathbb{Q}(\sqrt{d})$ be a field having the unique factorization property, and D be its discriminant. Then the primes of this field are those numbers whose norm, n, has one of the following values:

i) *n is a prime divisor of D; in this case n is product of two associated primes of the field;*
ii) *n is a prime not divisor of D such that $\chi_d(n) = 1$; in this case n is product of two non-associated primes of the field;*
iii) *n is the square of a prime p not divisor of D such that $\chi_d(p) = -1$; in this case p itself is a prime of the field.*

This theorem enables us to determine an appropriate starting set S in a simple way, using the quadratic character of the field considered. This is expressed in Theorem 5.3 below, using the following definition.

Definition of sieve algorithm
Let S be a finite set of natural numbers larger than 1. The *sieve algorithm* applied to S yields a set consisting of those elements of S which are not product of two other elements of S. This is achieved by removing all elements which are products of elements of S, as follows.

Starting from set $T := S$, the algorithm proceeds in successive steps, where in each step certain elements are removed from T.

In each step, let t be the smallest element of T which has not yet been treated in previous steps. Then we remove those elements of T which are product of t and some element of S. In fact, the products are removed starting from t^2, since the smaller products have already been removed in previous steps.

The algorithm is completed when the next element of T to be treated is larger than $\sqrt{M}$, and set T is then delivered as the result of the algorithm.

For details of this algorithm, see procedure ‘sieve’ in the Pascal program given below.

Theorem 5.3
Let $\mathbb{Q}(\sqrt{d})$ be a field having the unique factorization property, and D be its discriminant.

Let $S = S(d, M)$ be the set of natural numbers n satisfying $2 \leq n \leq M$ and, moreover, either n is divisor of D, or otherwise n satisfies $\chi_d(n) = 1$.

Then the sieve algorithm, defined above, applied to $S(d,M)$ yields a set which contains the norms not larger than M of all prime numbers of $\mathbb{Q}(\sqrt{d})$ and no norms of composite numbers of the field.

PROOF. This follows from Theorems 5.1 and 5.2. □

REMARKS

1. Set S and the set obtained after completing the sieve process contains also numbers which are not norm of any number of the field considered; e.g. for $d=-1$, set S contains number 21, which is not the sum of two squares. These numbers are harmless for the sieve process, and also for determining if a given element of the field is prime or not.
2. For $d \equiv 1 \pmod 4$, we prefer, for efficiency reason, to remove from S all even norms of composite elements of the field. This means that S contains the prime divisors of d, and the numbers satisfying $\chi_d(n)=1$ and either $n=2$ or 4, or n is odd. Thus, the odd numbers are periodic modulo $2|D|$.
3. The number of operations required for this algorithm is of the order $\rho M \Sigma_{p \le \sqrt{M}}(1/p)$, where ρ is the density of (odd) numbers of quadratic character $\chi_d(n)=+1$ within a period $|D|$ (or $2|D|$). This is asymptotically equal to $\rho M \log\log M$ and is a fraction ρ of the number of operations required for the sieve of Eratosthenes to calculate natural primes. The density ρ is equal to $\phi(|D|)/2|D|$, where ϕ denotes Euler's function, i.e. the number of natural numbers smaller than and relative prime to $|D|$.

PROGRAM AND PICTURES

In Appendices 1–2, we present a Pascal program generating a picture of prime numbers, and some examples of pictures generated by this or a similar program.

Our algorithm is described in detail in subprogram 'sieve' of the Pascal program. Note that the 'set' type in Pascal is very convenient to describe the sieve process. The program was executed on a Macintosh Plus computer using Macintosh Pascal system with QuickDraw library. The constant 'maxnorm' denotes the maximum value M mentioned above.

The program generates a picture of prime numbers in a certain region for one specific quadratic field. In the pictures, rational integers are placed on the x-axis and numbers of the form $\sqrt{d}$ times rational integers on the y-axis.

The pictures displayed have a *size* 47 which is the largest magnitude of the x- and y-coordinates of the numbers $\zeta = x + \tau y$ in the displays. The primes are drawn in the form of squares of 2 by 2 pixels if $d \equiv 2$ or $3 \pmod 4$, or plus-shapes of 5 pixels if $d \equiv 1 \pmod 4$.

EXAMPLES

To illustrate Theorem 5.3, we give some examples of quadratic fields in the following table, listing radicand d, discriminant D, generator τ of the ring of integers, and starting set S, consisting of the natural numbers listed not larger than M. In this table, n takes the values of the natural numbers up to an appropriate maximum.

These examples are displayed in the pictures on the next pages in Appendix 2. Note that the pictures for real fields show a higher density of primes near the hyperbolas $x^2 - dy^2 = \pm 1$.

d	D	τ	S
-1	-4	$\sqrt{-1}$	$\{2, 4n+5\}$
-2	-8	$\sqrt{-2}$	$\{2, 8n+3, 8n+9\}$
-3	-3	$(1+\sqrt{-3})/2$	$\{3, 4, 6n+7\}$
-7	-7	$(1+\sqrt{-7})/2$	$\{2, 7, 14n+r, r = 9, 11, 15\}$
-11	-11	$(1+\sqrt{-11})/2$	$\{4, 11, 22n+r, r = 3, 5, 9, 15, 23\}$
-19	-19	$(1+\sqrt{-19})/2$	$\{4, 19, 38n+r, r = 5, 7, 9, 11, 17, 23, 25, 35, 39\}$
2	8	$\sqrt{2}$	$\{2, 8n+7, 8n+9\}$
3	12	$\sqrt{3}$	$\{2, 3, 12n+11, 12n+13\}$
5	5	$(1+\sqrt{5})/2$	$\{4, 5, 10n+9, 10n+11\}$
6	24	$\sqrt{6}$	$\{2, 3, 24n+r, r = 5, 19, 23, 25\}$
7	28	$\sqrt{7}$	$\{2, 7, 28n+r, r = 3, 9, 19, 25, 27, 29\}$
13	13	$(1+\sqrt{13})/2$	$\{4, 13, 26n+r, r = 3, 9, 17, 23, 25, 27\}$
17	17	$(1+\sqrt{17})/2$	$\{2, 17, 34n+r, r = 9, 13, 15, 19, 21, 25, 33, 35\}$
21	21	$(1+\sqrt{21})/2$	$\{3, 4, 7, 42n+r, r = 5, 17, 25, 37, 41, 43\}$

Acknowledgements

The author is grateful to H.W. Lenstra jr. for his valuable suggestions, and to P. Stevenhagen and H.J.J. te Riele for reading the manuscript and giving valuable comments.

References

1. H. Behrbohm & L. Rédei (1936). Der Euklidische Algorithmus in quadratischen Köpern, *J. für reine und angewandte Mathematik* **174**, 192–205.
2. S. I. Borewicz & I. R. Safarevic (1966). *Zahlentheorie* (aus dem Russischen übersetzt von H. Koch); Birkhäuser Verlag, Basel.
3. P. G. Lejeune Dirichlet (1893).*Vorlesungen über Zahlentheorie*, herausgegeben von R. Dedekind, 4. Auflage, Vieweg, Braunschweig; reprint: Chelsea, New York (1968).
4. G. H. Hardy & E. M. Wright (1985). *An introduction to the theory of numbers*; (5-th ed., reprinted with corrections), Clarendon Press, Oxford.
5. K. Ireland & M. Rosen (1982). *A classical introduction to modern number theory*; Springer Verlag, New York.
6. I. Niven & H. S. Zuckerman (1960). *An introduction to the theory of numbers*; Wiley, New York.
7. F. J. van der Linden (1984). *Euclidean rings with two infinite primes* (thesis, University of Amsterdam); CWI, Amsterdam.
8. B. van der Pol & P. Speziali (1951). The primes in $k(\rho)$, *Indagationes Mathematicae* XIII p. 9–15.
9. I. Stewart & D. Tall (1979, 1987). *Algebraic number theory*; Chapman & Hall.

Appendix 1. The Pascal program text

```
program QuadraticPrimesPicture (output);

{ This program computes, by means of a sieve algorithm, (the norm of)  }
{ primes of a quadratic field having the unique factorization property,}
{ and draws a picture of them, in a region bounded by given constants. }
{ Example:  field Q(sqrt(3)), discriminant D = 12, square size 47.     }

const
   maxnorm = 6627; { norms are in the subrange 0..maxnorm.             }
type
   intset = set of 0..maxnorm;
var
   qstart, primenorms :  intset;

procedure sieve (max :  integer;
   start :  intset;
   function next (v :  integer) :  integer;
   var prinorms :  intset);

{ This procedure calculates a set containing the norms <= max of       }
{ primes of a quadratic field having the unique factorization property.}
{ The method used is a sieve algorithm applied to the set containing   }
{ the elements of start and the numbers in [2..max] obtained by        }
{ repeatedly applying next, starting from 1.  This should generate the }
{ odd numbers of quadratic character +1, whereas start should contain  }
{ the prime divisors of discriminant D, and number 2 if D mod 8 = 1 or }
{ number 4 if D mod 8 = 5.  The result is delivered in prinorms.       }
var
   i, ii, m, mult :  integer;

begin  { Form superset of prime norms.                                 }
   prinorms := start;
   i := next(1);
   repeat
      prinorms := prinorms + [i];
      i := next(i)
   until i > max;
{ Now prinorms is ready as starting set for the sieve process.         }
   i := next(1); { Start sieve process.                                }
   ii := sqr(i);
```

```
{ Program QuadraticPrimesPicture, continued.                             }
   repeat
      if i in prinorms then { delete multiples of i:                     }
      begin
         m := i; mult := ii;
         repeat
            prinorms := prinorms - [mult];
            m := next(m);
            mult := i * m
         until mult > max
      end;
      i := next(i); ii := sqr(i)
   until ii > max; { sieve process completed.                            }
end; { sieve                                                             }

function qnext (k : integer) : integer;
{ Returns next odd number of character value +1 for the                  }
{ field considered.                                                      }
begin
   qnext := k + (6 - k mod 6) * 2; { i.e.  next 12n+11 or 12n+13.        }
end; { qnext                                                             }

function qnorm (a, b : integer) : integer;
{ Returns the norm of a + b * sqrt(3).                                   }
begin
   qnorm := abs(sqr(a) - 3 * sqr(b))
end; { qnorm                                                             }

procedure drawprime (a, b : integer);
{ Draws a block of size dx by dy on a position determined by a and b.    }
const
   x0 = 250; y0 = 150; { origin for pixel coordinates                    }
   hx = 3;   { number of pixels in x-direction                           }
   hy = 3;   { number of pixels in y-direction                           }
   dx = 2;   { block length in x-direction                               }
   dy = 2;   { block length in y-direction                               }
var
   k, x, y : integer;
begin
   x := a * hx + x0;
   y := b * hy + y0;
   for k := 1 to dx do
   begin
      MoveTo(x + k, y + 1);
      LineTo(x + k, y + dy)
   end;
end; {drawprime                                                          }
```

```
{ Program QuadraticPrimesPicture, continued.                         }
procedure drawpicture (var prims :  intset);
{ Draws picture of primes in region bounded by given constants       }
const
   amax = 47;   { maxima for a and b                                 }
   bmax = 47;
   amin = -amax; { minima for a and b                                }
   bmin = -bmax;
var
   a, b :  integer;
begin
   for b := bmin to bmax do
   for a := amin to amax do
      if qnorm(a, b) in prims then
         drawprime(a, b);
end; { primespicture                                                 }

begin  { Calculates and draws picture of primes of the ring Z[sqrt(3)].}
   qstart := [2, 3]; { set of prime divisors of discriminant D = 12    }
   sieve(maxnorm, qstart, qnext, primenorms); { calculate prime norms  }
   showdrawing; { shows drawing window                               }
   drawpicture(primenorms); { draws picture of primes                }
   savedrawing('zd12'); { saves drawing in file                      }
end.
```

Appendix 2. Pictures of primes in quadratic fields

$\mathbb{Z}[\sqrt{-1}]$

$\mathbb{Z}[\sqrt{-2}]$

$\mathbb{Z}[(1+\sqrt{-3})/2]$

$\mathbb{Z}[(1+\sqrt{-7})/2]$

$\mathbb{Z}[(1+\sqrt{-11})/2]$

$\mathbb{Z}[(1+\sqrt{-19})/2]$

$\mathbb{Z}[\sqrt{2}]$

$\mathbb{Z}[\sqrt{3}]$

$\mathbb{Z}[\sqrt{6}]$

$\mathbb{Z}[\sqrt{7}]$

$\mathbb{Z}[(1+\sqrt{5})/2]$

$\mathbb{Z}[(1+\sqrt{13})/2]$

$\mathbb{Z}[(1+\sqrt{17})/2]$

$\mathbb{Z}[(1+\sqrt{21})/2]$

$\mathbb{Z}[(1+\surd -3)/2],\ N(\pi)\ \leq 1657$

$\mathbb{Z}[(1+\surd 5)/2],\ N(\pi)\ \leq 661$