Representation of primes as the sums of two squares in the golden section quadratic field

Michele Elia†

Politecnico di Torino
Dipartimento di Elettronica
Corso Duca degli Abruzzi 24
10129 Torino
Italy

Abstract

In the quadratic number field with the golden section unit, any prime \( p \) has associated primes that are the sums of two integer squares, if and only if its field norm \( N(p) \) is not a rational prime congruent to 11 or 19 modulo 20. A proof of this property is presented, along with a method for computing the two squares with deterministic polynomial complexity, that is, using a number of arithmetical operations proportional to a power of \( \log_2 N(p) \) of bounded exponent.

**Keywords**: Golden section, real quadratic fields, polynomial complexity.

1. Introduction

Fermat stated that every rational prime \( p \) congruent to 1 modulo 4 is the sum of two squares of natural numbers. Fermat’s theorem has received many proofs [22, p. 66], although early ones did not offer a method of deterministic polynomial complexity for computing the representation \( p = s^2 + r^2 \), i.e. one using a number of sums and products proportional to some small power of the logarithm of \( p \). However, a reduction algorithm of binary quadratic forms, which can be traced back to Gauss [6], produces

---

*Presented at XXIVi`eme Journ´ees Arithm´etiques, Marseille (FR), July 4-8, 2005.
†E-mail: eliamike@tin.it

**Journal of Discrete Mathematical Sciences & Cryptography**
Vol. 9 (2006), No. 1, pp. 25–37
© Taru Publications
and s with deterministic polynomial complexity once a square root of 
\(-1\) modulo \(p\) is known [13]. The question was then settled by Schoof, 
who discovered an algorithm for evaluating the number of points on 
elliptic curves over finite fields, which also furnishes a square root of 
small numbers, in particular \(-1\), modulo \(p\) with deterministic polynomial 
complexity [18]. Fermat also stated, and Lagrange proved, that every 
natural integer is the sum of at most four squares of natural numbers [17, 
p. 7]. Some two centuries later, Siegel proved that the only real algebraic 
number fields in which exist a four-square-sum representation of the 
totally positive integers are the rational field \(\mathbb{Q}\) and the quadratic field 
\(\mathbb{Q}(\omega)\) with golden section unit \(\omega = \frac{1 + \sqrt{5}}{2}\), [20]. A direct consequence 
of Siegel’s theorem is that any prime integer \(p \in \mathbb{Q}(\omega)\) has an associated 
prime which is the sum of two squares in the same field, if its field norm 
is a rational prime not congruent to 11 or 19 modulo 20.

The paper shows that the same tools used in \(\mathbb{Q}\) can be employed 
to give a proof of the two-square-sum property for primes \(\pi\) in \(\mathbb{Q}(\omega)\), 
and provides a way of computing their representation \(\pi = a^2 + b^2\) with 
deterministic polynomial complexity.

2. Preliminaries

The real quadratic field \(\mathbb{F} = \mathbb{Q}(\omega)\) is a principal ideal domain whose 
integers are the elements of \(\mathbb{Z}(\omega)\) [5]. The conjugate of an element \(z = 
a + b\omega\) is \(\bar{z} = a + b\bar{\omega} = (a + b) - bw\), and the field norm is \(N_\mathbb{F}(z) = zz = 
a^2 + ab - b^2\). The elements of \(\mathbb{Z}(\omega)\) with norm \(\pm 1\) are called units, and 
form a group which is the direct product of a torsion group \(T_2 = \{1, -1\}\) 
of order 2, and an infinite group \(\mathcal{U}\) of rank 1, which is generated by \(\omega\). 
Two integers \(\alpha, \beta \in \mathbb{Z}(\omega)\) are said to be associated if their ratio \(\alpha/\beta\) is a 
unit. A positive integer number \(\alpha = a + b\omega \in \mathbb{Z}(\omega)\) is said to be totally 
positive if its conjugate \(a\) is also positive [15, p. 378]. Given \(\alpha\), one of the 
four associates \(\alpha, -\alpha, a\omega, \text{ and } -a\omega\) is certainly totally positive; moreover, 
let \(\mathcal{U}_2\) be the subgroup of \(\mathcal{U}\) generated by \(\omega^2\), every totally positive element 
\(\alpha \in \mathbb{Z}(\omega)\) uniquely identifies a class \(a\mathcal{U}_2 = \{au : u \in \mathcal{U}_2\}\) of totally 
positive associates.

The set of primes in \(\mathbb{Q}(\omega)\) consists of: (i) a prime \(\pi_5 = 2 + \omega\) of 
field norm 5, and its associates; (ii) all rational primes \(q \equiv \pm 2 \pmod{5}\), and 
their associates; and (iii) all pairs of prime factors \(\pi_q = a + b\omega\) and \(\pi_q = \)
$a + b - b\omega$ of every rational prime $q \equiv \pm 1 \mod 5$, and their respective associates [5, p. 25], in particular $\pi q$ may be chosen totally positive and such that $q = \pi q \overline{\pi q} = a^2 + ab - b^2$. This explicit representation is obtained from the process that reduces the quadratic form

$$pX^2 + s_5 XY + \frac{s_5^2 - 5}{4p} Y^2$$

of discriminant 5 to the canonical form $X^2 + XY - Y^2$, where $s_5$ is the odd root of $x^2 = 5 \mod p$.

This reduction algorithm, outlined by Gauss and cleverly reported in Buell [3], was described in a masterly fashion in Mathews’ book [13], and thus it will be referred to as Mathews’ reduction. It can be applied to any quadratic form of a non-perfect square discriminant. The square root $s_5$ may be computed with deterministic polynomial complexity by distinguishing whether $p$ is congruent 3 or 1 modulo 4. In the first case, $s_5$ is one of the two square roots $\pm \sqrt{\frac{5}{p} + \frac{1}{4}} \mod p$, and the computation clearly has deterministic polynomial complexity. In the second case Schoof’s algorithm [18, 21] is applied to compute both $\sqrt{-1}$ and $\sqrt{-5}$ modulo $p$, thus $s_5$ is one of the two values $\pm \sqrt{-1} \sqrt{-5} \mod p$. Schoof’s algorithm evaluates a square root modulo $p$ in a number of arithmetical operations of order $O(\log^3 p)$ with $t \leq 10$, that is with deterministic polynomial complexity [18]. A description of Schoof’s algorithm can be found in the original paper [18] or in Washington’s book [21], and is based on properties of elliptic curves that are briefly summarized.

Let $L$ be an algebraic number field of degree $m$ over $\mathbb{Q}$, which has an imaginary quadratic subfield $\mathbb{Q}(\sqrt{-d})$, $d > 0$. Let $P = (x, y) \in L^2$ be a point of an elliptic curve $E(L)$ over $L$, whose coordinates satisfy the cubic $y^2 = x^3 + ax + b$, with $a, b \in L$. Let $q = p^m$ be a power of a prime $p$. If $E(L)$ is taken modulo $p$, an elliptic curve $E(\mathbb{F}_q)$ over a Galois field $\mathbb{F}_q$ is obtained. The number of points on $E(\mathbb{F}_q)$, including the point at infinity, is $N_q = q - t_q + 1$, where $t_q$ satisfies the Hasse bound $|t_q| \leq 2\sqrt{q}$. For elliptic curves having a complex multiplier in $\mathbb{Q}(\sqrt{-d})$, a theorem of Deuring’s [4, 18] states that if $p = \pi \overline{\pi}$ splits in $\mathbb{Q}(\sqrt{-d})$, and $E(\mathbb{F}_q)$ is obtained considering $E(L)$ modulo $p$, then with $q = p^m$ we have $t_q = \pi^m + \overline{\pi}^m$, and

$$q = \frac{t_q^2}{4} + dw^2 \quad t_q, w \in \mathbb{Z}, \quad t_q \equiv 0 \mod 2.$$ (1)
Thus a square root of $-d \mod p$ is obtained as $\sqrt{-d} = \frac{t_q}{2w} \mod p$. In particular, if $p = 1 \mod 4$, the representation $p = r^2 + s^2$ is computed considering the elliptic curve $E(\mathbb{Q})$ of equation $y^2 = x^3 - x$, which has complex multiplier $i$, Schoof's algorithm gives $r = \frac{t_p}{2}$, and by equation (1) $s = \sqrt{p - r^2}$, furthermore $\sqrt{-1} = \frac{r}{s} \mod p$.

If $p$ is congruent $1 \mod 4$ and $\pm 1 \mod 5$, $\sqrt{-5} \mod p$ is computed from $p^2 = f^2 + 5x^2$ which is obtained from the elliptic curve $E(\mathbb{Q}(\sqrt{5}))$ of equation $y^2 = x^3 - 3\frac{j}{1728}x - 2\frac{j}{1728}$, with complex multiplier $1 + \sqrt{-5}$. The $j$-invariant is a root of a second degree Hilbert polynomial for $\mathbb{Q}(\sqrt{-5})$ $H_{20}(z) = z^2 - 1264000z - 681472000$, since $\mathbb{Q}(\sqrt{-5})$ has class number 2. School's algorithm gives the number of points on the elliptic curve $E(\mathbb{F}_p)$, and we get $p^2 = \frac{t^2}{4} + 5z^2$, $\sqrt{-5} = \frac{t_p}{2z} \mod p$.

Lastly, in this section we collect the main properties of a totally complex field $\mathbb{K} = \mathbb{Q}(\rho)$ useful in our proofs, where $\rho$ is a root of the irreducible polynomial $m(X) = X^4 + 3X^2 + 1$ with discriminant $\Delta = 24^2$. $\mathbb{K}$ is a Euclidean field [11], thus factorization is unique. The only ramified rational prime is $5 = \pi_5^2 = (2\rho^2 + 3)^2$, with inertia index 1, while 2 splits as $2 = \pi_2\sigma(\pi_2) = (1 - 2\rho - \rho^3)(1 + 2\rho + \rho^3)$. In $\mathbb{K}$, $\rho$ is a generator of the unit group of rank 1, and the torsion group is $T_4 = \{1, -1, i, -i\}$. An integral basis of $\mathbb{K}$ is $B = \{1, \rho, \rho^2, \rho^3\}$, thus every $a$ in the maximal order $\mathcal{O}_K$ is represented as

$$a = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 \quad \text{with} \quad a_0, a_1, a_2, a_3 \in \mathbb{Z}.$$  

The Galois group $\mathfrak{G}(\mathbb{K}) = \{e, \sigma, \eta, \sigma\eta\}$ of $m(X)$ is isomorphic to the Klein group, and $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$ with subfields $\mathbb{Q}(\omega), \mathbb{Q}(i)$, and $\mathbb{Q}(\xi)$, where $\xi = \sqrt{-5}$. We will assume that the action of the automorphisms of the Galois group $\mathfrak{G}(\mathbb{K})$ restricted to the subfields $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$ is specified as $\sigma(i) = -i$, and $\eta(\omega) = 1 - \omega$, respectively. Since it is immediate to check that $\rho = i\omega$, we have $i = -2\rho - \rho^3$, and $\omega = -1 + \rho^2$, hence the action of $\mathfrak{G}(\mathbb{K})$ on the roots of $m(X)$ is as follows

$$e(\rho) = \rho, \quad \sigma(\rho) = -\rho, \quad \eta(\rho) = -3\rho - \rho^3, \quad \sigma(\eta(\rho)) = 3\rho + \rho^3.$$  

The following factorization of $m(x)$ in the subfields of $\mathbb{K}$ is immediately
verifying:

\[ m(x) = (x^2 + 2 - \omega)(x^2 + 1 + \omega) = (x^2 + x\xi - 1)(x^2 - x\xi - 1) \]
\[ = (x^2 + xi + 1)(x^2 - ix + 1). \]  

Field trace and norm of any \( a \in \mathbb{K} \) are invariant under the Galois group, thus they are rational expressions of \( a, s \). Explicitly the trace \( \text{Tr}(a) = a + \sigma(a) + \eta(a) + \eta(\sigma(a)) \) is \( \text{Tr}(a) = 4a_0 - 6a_2 \), and the norm \( \text{Nr}(a) = a\sigma(a)\eta(a)\eta(\sigma(a)) \) is

\[ \text{Nr}(a) = a_0^4 + a_1^4 + a_2^4 + a_3^4 - 6(a_0^3a_2 + a_0^2a_1 + a_1^2a_2 + a_3^2a_1) \]
\[ + 3(a_0^2a_1^2 + a_1^2a_2^2 + a_2^2a_3^2) + 18a_0^2a_3^2 + 11(a_0^2a_2^2 + a_1^2a_3^2) \]
\[ - 4(a_0a_1^2a_2^2 + a_1a_2^2a_3^2) - 14(a_2a_3^2a_0 + a_0a_2^2a_1) + 12a_0a_1a_2a_3. \]

3. **Representation of primes in \( \mathbb{Z}(\omega) \)**

In \( \mathbb{Q}(\omega) \), a representation \( r = a^2 + b^2 \), \( a, b \in \mathbb{Z}(\omega) \) of every totally positive integer \( r \) is obtained from the representations of its prime factors using the identity \((a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2\). Hence, limited to primes \( \pi \in \mathbb{Q}(\omega) \), it will be shown that a two-square-sum representation is computed with deterministic polynomial complexity. To this aim, it is convenient to consider the rational primes separately by their remainders \( 1, 3, 7, 9, 11, 13, 17, 19 \) modulo 20, plus the primes 2 and 5.

The rational prime 2 is inert in \( \mathbb{Z}(\omega) \), thus its representation \( 2 = 1^2 + 1^2 \) is trivial.

The rational prime 5 ramifies in \( \mathbb{Z}(\omega) \), thus it is a perfect square \( \Pi_5^2 = (2\omega - 1)^2 \) of a non positive prime. The associated prime \( \pi_5 = \omega \Pi_5 = 2 + \omega \) is positive, and admits of the representation \( \pi_5 = 1 + \omega^2 \).

Primes congruent to 3, 7, 13, 17 modulo 20 are inert and remain primes in \( \mathbb{Z}(\omega) \), and thus their representation as the sum of squares is almost direct. Primes congruent to 1, 9, 11, 19 modulo 20, on the contrary, split into pairs of conjugate primes \( \pi_0 \) and \( \pi_0 \), and their representation may require the solution of a Diophantine equation of degree 4 provided by the norm in \( \mathbb{K} \). These representations are disposed of in the following Theorems, working in the quartic field \( \mathbb{K} \), where any rational prime splits into at least two factors:

(i) the decomposition containing \( \omega \) holds for every prime \( p \equiv 1, 9, 11, 19 \mod 20 \), in which case \( \sqrt{p} \in \mathbb{Z}_p \).
(ii) the decomposition containing $\xi$ holds for every prime $p \equiv 3,7 \mod 20$, in which case $\sqrt{-5} \in \mathbb{Z}_p$; and

(iii) the decomposition containing $i$ holds for every prime $p \equiv 13,17 \mod 20$, in which case $\sqrt{-1} \in \mathbb{Z}_p$.

**Theorem 1.** Let $p$ be a rational prime congruent to $11,19 \mod 20$, then $p$ splits in $\mathbb{Q}(\omega)$ with factors

$$\pi_0 = x_0 + y_0 \omega \quad \text{and} \quad \bar{\pi}_0 = x_0 + y_0 - y_0 \omega.$$ 

Furthermore, $\pi_0$ cannot be represented as a sum of two squares in $\mathbb{Q}(\omega)$, hence it is inert in $\mathbb{Q}(\rho)$.

**Proof.** Since every $p = \pm 1 \mod 5$ splits in $\mathbb{Q}(\omega)$, let $\pi_0$ denote a totally positive prime factor. If $\pi_0$ can be written as the sum of two squares, then $\pi_0$ splits in $\mathbb{Q}(\rho)$, that is $\pi_0 = \wp \sigma(p)$ and $p = \wp \sigma(p) \eta(p) \eta(\sigma(p))$, thus $p$ can be written as the sum of two rational squares, a condition that is contradicted by $p = 3 \mod 4$. □

The following Theorems establish that the remaining primes are representable as sums of two squares, and how such representations can be computed.

**Theorem 2.** Every rational prime $p \equiv 3,7,13,17 \mod 20$ is inert in $\mathbb{Q}(\omega)$, and is represented with deterministic polynomial complexity as the sum of two squares in $\mathbb{Z}(\omega)$. Precisely:

(a) if $p \equiv 13,17 \mod 20$, then $p$ is the sum of two squares of natural numbers;
(b) if $p \equiv 3,7 \mod 20$, then $p$ is the sum of two conjugate squares

$$p = (a + b\omega)^2 + (a + b\bar{\omega})^2.$$ 

**Proof.** Every rational prime $p \equiv 3,7,13,17 \mod 20$ is inert in $\mathbb{Q}(\omega)$. If $p \equiv 13,17 \mod 20$, then $p \equiv 1 \mod 4$, thus $p$ is the sum of two squares of natural numbers by Fermat’s theorem.

If $p \equiv 3,7 \mod 20$, then $p \equiv 3 \mod 4$, thus $p$ is the sum of two squares of conjugate numbers

$$p = (x_1 + y_1 \omega)^2 + (x_1 + y_1 \bar{\omega})^2 = 2x_1^2 + 2x_1^2y_1 + 3y_1^2$$

and $2x_1^2 + 2x_1y_1 + 3y_1^2$ is the non-principal genus of discriminant $-5$ and represents every prime congruent $3,7 \mod 20$ [4]. □
Lemma 1. Every rational prime $p \equiv 1, 9 \text{ mod } 20$ fully splits in $\mathbb{Q}(\rho)$, and is the field norm $\text{Nr}(p)$ of a prime $p = a_0 + a_1 \rho + a_2 \rho^2 + a_3 \rho^3 \in \mathbb{Q}(\rho)$. The product $\pi_1 = p \eta(p) = u + vi$ is unique except for a sign change and complex conjugation. Moreover, the components $u$ and $v$ of $\pi_1$ satisfy the congruences

$$v \equiv 0 \text{ mod } 5 \text{ if } p \equiv 1 \text{ mod } 5, \quad u \equiv 0 \text{ mod } 5 \text{ if } p \equiv -1 \text{ mod } 5.$$  

Proof. Since $p = \pm 1 \text{ mod } 5$, then $p = p_1 \eta(p_1)$ for some $p_1 \in \mathbb{Q}(\omega)$, furthermore, since $p = 1 \text{ mod } 4$, then $p = p_2 \sigma(p_2)$ for some $p_2 \in \mathbb{Q}(i)$. All factors are in the PID $\mathbb{Q}(\rho)$, therefore, if $p_2$ is prime, then either $p_1 = u_2 p_2$, or $p_1 = u_2 \sigma(p_2)$. In any case, the real product $p_1 \eta(p_1)$ is either $u_2 \eta(u_2) \rho^2$ or $u_2 \eta(u_2) \sigma(p_2^2)$, which force $p_2$ to be real, a contradiction. Given that $\mathbb{Q}(\rho)$ is a PID, the factorization of a rational prime is unique except for a unit factor $u = \rho^k \omega^{k_2}$, with $k_1 \in \{0, 1, 2, 3\}$, and $k_2 \in \mathbb{Z}$. Let $\eta$ and $\tilde{\eta}$ be associated primes, since $\eta(u) = \rho^k \omega^{k_2}$, then

$$\tilde{\eta}(p) = \rho^k \omega^{k_2} \rho \eta(p) = (-1)^{k_1 + k_2} \rho \eta(p) = (-1)^{k_1 + k_2} (u + vi).$$

It follows that $\pi_1$ is uniquely specified except for a sign change and complex conjugation, thus among the four complex numbers $u + vi$, $-(u + vi)$, $u - vi$, and $-(u - vi)$, one has positive real and imaginary parts. The congruence property satisfied by $u$ and $v$ is proved by writing $p \in \mathbb{Q}(\rho)$ as $p = (a_0 + a_2)^2 + 3i(a_1 + a_3) + \pi_5[-a_2 + i(a_1 - 2a_3) - i\pi_3 a_3]$, where $\pi_5 = 2 + \omega$ satisfies $\pi_5 \pi_5 = 5$ and $\pi_5 + \pi_5 = 5$, from which it follows that $p = \eta(p) = (a_0 + a_2)^2 + 3i(a_1 + a_3) \text{ mod } \pi_5$, and in turn

$$\pi_1 = \eta(p) = (a_0 + a_2)^2 + (a_1 + a_3)^2 + i(a_0 + a_2)(a_1 + a_3) \text{ mod } \pi_5$$

$$p = [(a_0 + a_2)^2 + (a_1 + a_3)^2]^2 + [(a_0 + a_2)(a_1 + a_3)]^2 \text{ mod } \pi_5.$$  

Hence, if $p \equiv -1 \text{ mod } 5$, necessarily $(a_0 + a_2)^2 = -(a_1 + a_3)^2 \text{ mod } \pi_5$, which implies $u \equiv 0 \text{ mod } 5$. While, if $p \equiv 1 \text{ mod } 5$ necessarily $(a_0 + a_2) \times (a_1 + a_3) \equiv 0 \text{ mod } \pi_5$, which implies $v \equiv 0 \text{ mod } 5$. (It is remarked that whenever $a$ is a rational integer then $a \equiv 0 \text{ mod } 5 \iff a \equiv 0 \text{ mod } 5$.) \ 

Theorem 3. Let $p$ be a prime in $\mathbb{Q}(\rho)$. With the same hypotheses as Lemma 1, we have

1. $\pi_0 = p \sigma(p) = x_0 + y_0 \omega \in \mathbb{Q}(\omega)$ with $x_0 > y_0 > 0$ is unique except for a factor $\omega^{2n}$; furthermore, we have $\pi_0 = p \sigma(p) = (a_0 + a_2 \rho^2)^2 - (a_1 \rho + a_3 \rho^3)^2 = (a_0 - a_2 \omega^2)^2 + \omega^2(a_1 - a_3 \omega^2)^2$.  

Proof. Since $\sigma(p\sigma(p)) = p\sigma(p)$ and $\eta(p\eta(p)) = p\eta(p)$, then $p\sigma(p) \in \mathbb{Q}(\omega)$ and $p\eta(p) \in \mathbb{Q}(i)$. Thus we have $\pi_0 = p\sigma(p) = x_0 + wy_0$, $\pi_i = u + iv = p\eta(p)$, and the two representations

$$p = u^2 + v^2 = x_0^2 + x_0y_0 - y_0^2. \quad (4)$$

The representation $\pi_0 = [(a_0 - a_2) - a_2\omega]^2 + [-a_3 + (a_1 - 2a_3)\omega]^2$, is obtained by writing $i\omega$ for $\rho$ in

$$p = a_0 + a_1i\omega - a_2(1 + \omega) - a_3i(1 + 2\omega)$$

$$= [(a_0 - a_2) - a_2\omega] + i[-a_3 + (a_1 - 2a_3)\omega].$$

Since $p$ is unique except for a unit, its associated primes are $i^{n_1}p^{n_2}p$, then $\pi_0$ is unique except for a unit factor $\omega^{n_2}$, and $\pi_i$ is unique except for a unit factor $(-1)^{n_3}$. □

As previously observed, both $\pi_i = u + iv$ and $\pi_0 = x_0 + y_0\omega$ are computed with deterministic polynomial complexity. Finally, it is remarked that finding a representation of $\pi_0 \in \mathbb{Q}(\omega)$ as the sum of two squares is equivalent to factorizing $p$ in $\mathbb{Q}(\rho)$.

4. Computational remarks

The representations of primes $\pi \in \mathbb{Q}(\omega)$ as the sums of two squares, established by Theorems 2 and 3, are computed with deterministic polynomial complexity using procedures that will be described separately for the different cases.

4.1 Primes $p \equiv 13, 17 \mod 20$

The representation $p = a^2 + b^2$ does not need any further comment, since $p = 1 \mod 4$ is the sum of two integer squares by Fermat's theorem, and its computation was shown in Section 2.

4.2 Primes $p \equiv 3, 7 \mod 20$

The representation $p = (x_1 + y_1\omega)^2 + (x_1 + y_1\bar{\omega})^2 = 2x_1^2 + 2x_1y_1 + 3y_1^2$ is the representation of $p$ by the non-principal genus of discriminant $-20$ [4]. Since $p \equiv 3 \mod 4$, $\sqrt{-5} \mod p$ is computed as $s_5 = (-5)^{\frac{p+1}{4}} \mod p$, thus Mathews’ reduction is applied to the quadratic form

$$Q(x, y) = px^2 + 2s_5xy + \frac{s_5^2 + 5}{p}y^2$$

when the non-principal genus $2x^2 + 2xy + 3y^2$ is obtained, then $x_1$ and $y_1$ are also obtained [3].
4.3 Primes $p \equiv 1, 9 \mod 20$

The representation $\pi_0 = [(a_0 - a_2) - a_2^2] + [-a_3 + (a_3 - 2a_3)\omega]^2$ of a totally positive prime $\pi_0 = x_0 + \omega y_0$ of norm $p$ is computed solving a norm equation, namely a quartic Diophantine equation $N(p) = p$ in four variables, with $p = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3$, an element in the order of $\mathbb{Q}(\rho)$. This quartic is solved by applying the method of infinite descent to a sequence of quadratic Diophantine equations in two variables. The descent ends when a quadratic form representing $1$ is obtained, which is then solved using Mathews’ reduction. The most cumbersome part of this procedure is to show that all operations are done with deterministic polynomial complexity.

To begin, both representations $\pi_i = u + iv$, and $\pi_0 = x + \omega y$ of factors of $p$ are computed with deterministic polynomial complexity, and respecting certain compatibility conditions.

As regards $\pi_i$ of the eight choices $(\pm u \pm iv)$, and $(\pm v \pm iu)$, only one, denoted $u_0 + iv_0$, satisfies the conditions of Theorem 3, $v_0 \equiv 0 \mod 5$ if $p \equiv 1 \mod 5$, or $u_0 \equiv 0 \mod 5$ if $p \equiv -1 \mod 5$, and contemporarily has $u_0 > 0, v_0 > 0$.

As regards $\pi_0$, of the eight choices $\pm(x + wy), \pm(y + \omega(x + y)), \pm(y + ox)$, and $\pm(x + \omega(x + y))$, only one, denoted $x_0 + wy_0$, is totally positive and contemporarily satisfies the conditions $x_0 > 0, y_0 > 0$. Since any totally positive associate $\pi'_0 = x_k + \omega y_k \in \pi_0 U_2$ may be used in our procedure, this freedom will be exploited to facilitate the solution of the norm equation by satisfying certain conditions obtained as follows. Since $p\sigma(p) = \pi_0$ and $p\eta(p) = \pi_i$, the chain $p\eta(p)\sigma(p) = (u_0 + iv_0)\sigma(p) = (x_0 + wy_0)\eta(p)$ of equalities yields a linear system for the unknowns $a_0, a_1, a_2$, and $a_3$:

$$\begin{align*}
v_0a_0 + (y_0 - x_0)a_1 - v_0a_2 + (-2y_0 + 3x_0 + u_0)a_3 &= 0 \\
y_0a_0 + v_0a_1 + (-u_0 - x_0 + y_0)a_2 - 2v_0a_3 &= 0.
\end{align*}$$

Solving for $a_1$ and $a_3$ we have:

$$\begin{align*}
a_1 &= \frac{-2x_0 + y_0 + 2u}{v_0}a_0 + \frac{5x_0 - 3y_0 - u}{v_0}a_2 \\
a_3 &= \frac{-x_0 + u}{v_0}a_0 + \frac{2x_0 - y_0 - u}{v_0}a_2.
\end{align*}$$

Furthermore, from $p\eta(p) = u_0 + iv_0$ we get a quadratic equation $a_0a_1 + a_1a_2 + a_2a_3 - 4a_0a_3 = v_0$ in four variables, which is reduced to a quadratic
Diophantine equation in two variables using (5):

$$(2x_0 + y_0 - 2u_0)a_0^2 + 2(-3x_0 + y_0 + 3u_0)a_2a_0 + (7x_0 - 4y_0 - 2u_0)a_2^2 = v_0^2. \quad (6)$$

Let the quadratic form on the left side of (6) be written as $Q(0)(x, y) = Ax^2 + 2Bxy + Cy^2$ with

$$A = -2u_0 + 2x_0 + y_0, \quad B = -3x_0 + 3u_0 + y_0, \quad C = -4y_0 - 2u_0 + 7x_0,$$

and discriminant $\Delta(0) = 4B^2 - 4AC = -20v_0^2$. Furthermore, rewriting $Q(0)(x, y) = v_0^2$ as

$$(Ax + By)^2 + 5v_0^2 y^2 = Av_0^2,$$

we have $Ax + By = tv_0$, and $A = i^2 + 5y^2 > 0$. Analogously, exchanging the roles of $A$ and $C$ we have $Bx + Cy = sv_0$ and $C = s^2 + 5x^2 > 0$. Thus $(x_0, y_0)$ must be chosen so that $A$ and $C$ are both positive integers, and contemporarily both are also quadratic residues modulo 5. As previously observed, $(x_0, y_0)$ uniquely identify a set $\Pi(\omega) = \{(x_k, y_k) : x = x_0F_{2k-1} + y_0F_{2k}, y = x_0F_{2k} + y_0F_{2k+1}, k \in \mathbb{Z}\}$ where $F_n$ denotes a Fibonacci number. Then $(x_0, y_0) \in \Pi(\omega)$ may be chosen to make 1 the greatest common divisor $G_d = \gcd\{A, 2B, C\}$. Since of $A$ and $C$ at least one is odd, because $x_0$ and $y_0$ cannot both be even, we also have $G_d = \gcd\{A, B, C\}$, thus, we have

$$G_d = \gcd\{2x_0 + y_0 - 2u_0, -3x_0 + y_0 + 3u_0, 7x_0 - 4y_0 - 2u_0\} = \gcd\{2x_0 + y_0 - 2u_0, -5y_0 + 5x_0\}$$

$$= \gcd\{5y_0, -x_0 + u_0 + 2y_0, -5y_0 + 5x_0\} = \gcd\{5y_0, -x_0 + u_0 + 2y_0, 5x_0\}.$$

If $L_1 = -x_0 + u_0 + 2y_0 = 0 \mod 5$, then some $k$ exists such that $L_1' = (-x_0 + u_0 + 2y_0) \neq 0 \mod 5$, as shown in Table 4.3, in conclusion $G_d = 1$.

In general, equation $Q(0)(x, y) = v_0^2$ cannot be solved with deterministic polynomial complexity in a straightforward way, but an infinite descent may be devised which gives at each step a Diophantine equation $Q(i)(x, y) = v_i^2$, with discriminant $\Delta(i) = -20v_i^2$, and $v_i$ a divisor of $v_0$ strictly less than $v_{i-1}$.

The idea behind the descent is to perform a linear transformation

$$\begin{cases} X = v_0X + \beta Y \\ y = \theta Y \end{cases}$$
on variables $x$ and $y$, with the aim of obtaining an equation $A_0v_0^2X^2 + 2B_0v_0^2XY + v_0^2Y^2 = v_0^2$ all of whose coefficients are multiples of $v_0^2$ and which has the solution $X = 0, Y = 1$. This is always possible, with $\beta$ and $\theta$ satisfying $\mathcal{Q}(x, y) = v_0^2$, and linearly expressed in terms of two variables $\kappa$ and $\mu$ satisfying $A_1\mu^2 + 2B_1\kappa\mu + C_1\kappa^2 = \frac{d_0^2}{d_1^2}$, where

$$d_0 = \gcd\{A, B\}, \quad d_1 = \gcd\{A, B, v_0\}, \quad \text{and} \quad B_1 = A_1C_1 - \frac{5}{2}d_0^2.\$$

This quadratic equation can be solved by Mathews’ reduction when $d_0 = d_1$, otherwise it is a quadratic equation of the same sort as $\mathcal{Q}(x, y) = v_0^2$, but with a smaller known term: this is sufficient to show the existence of an infinite descent. As we have proved it is not restrictive to assume that $\gcd\{A, 2B, C\} = 1$ and $5 \nmid A$, furthermore, clearly $d_0 \mid v_0^2$ since $-5v_0^2 = B^2 - AC$, but $d_0 \nmid v_0$ if $d_1 < d_0$. Moreover, if $d_1 = d_0$ then $d_0^2 \mid A$

because we have

$$\frac{-5v_0^2}{d_0^2} = B^2 - AC = \frac{B_0 v_0^2}{d_0} = \frac{62 x}{d_0^2} - \frac{A}{d_0^2}.\$$

Specifically, parameters $\beta, \theta$, and $A_0, B_0, C_0 = 1$ are computed to satisfy the conditions

$$\begin{cases}
A_0v_0^2 = A_0v_0^2 \\
v_0(\beta A + \theta B) = B_0v_0^2 \\
A\beta^2 + 2B\beta\theta + C\theta^2 = v_0^2.
\end{cases} \quad (7)$$

We immediately have $A_0 = A$. Setting $B_0 = \mu d_1$, the second equation is

$$\frac{\beta_0 A}{d_0} + \frac{\theta_0 B}{d_0} = \mu v_0.\quad (8)$$

Let $\beta_0$ and $\theta_0$ be two integers satisfying the condition $\beta_0 A d_0 + \theta_0 B d_0 = 1$, computed with the generalized Euclidean algorithm, thus a general
solution of (8) is
\[
\begin{cases}
\beta = \mu v_0 \frac{d_1}{d_0} \beta_0 + \kappa \frac{B}{d_0} \\
\theta = \mu v_0 \frac{d_1}{d_0} \theta_0 - \kappa \frac{B}{d_0}.
\end{cases}
\]
The third equation in (7) turns out to be a quadratic form in $\mu$ and $\kappa$
\[
d_0^2 \left( A \mu^2 + 2B \mu \kappa + C \kappa^2 \right) \mu^2 - 10 \frac{v_0}{d_1} \theta_0 \mu \kappa + 5 \frac{A}{d_1^2} \kappa^2 = v_0^2.
\]
Defining $d_a = \frac{d_0}{d_1}$, we obtain $A_1 \mu^2 - 2B_1 \mu \kappa + C_1 \kappa^2 = d_t^2$, where the discriminant of the quadratic form is $-20d_t^2$. This last equation completes the description of a step of the infinite descent. At the end of the descent, say after $\ell$ steps, we obtain a quadratic equation of the form $A_\ell \mu^{2\ell} - 2B_\ell \mu \kappa + C_\ell \kappa^{2\ell} = 1$, with discriminant $-20$, which is solved by Mathews’ reduction. Thus, proceeding backwards, $a_0$ and $a_2$ are computed, and finally $a_1$ and $a_3$ are obtained from equation (5).

5. Conclusions

The representation of primes as sums of two squares in $\mathbb{Z}(\omega)$ allows us to formulate a theorem concerning the representation of any integer in $\mathbb{Z}(\omega)$:

**Theorem 4.** In the field $\mathbb{Q}(\omega)$, any totally positive integer
\[
n = \prod \zeta_j^{2\beta_j} \prod \pi_i^{\alpha_i}
\]
where $\zeta_j$ and $\pi_i$ are primes, whose norms respectively are and are not primes congruent 11 and 19 mod 20, is a sum of two integer squares.

The computation of the two-square representation of any element in $\mathbb{Z}(\omega)$ is equivalent to factoring, as in $\mathbb{Z}$, therefore at the present time only the two-square representations of primes can be computed with deterministic polynomial complexity.

References


Revised: October, 2005