

# On the Representation of Primes in $\mathbb{Q}(\sqrt{2})$ as Sums of Squares

Michele Elia  
Politecnico di Torino  
Torino, Italy  
elia@polito.it

Chris Monico  
Texas Tech University  
Lubbock, TX  
c.monico@ttu.edu

Draft of February 8, 2007

## Abstract

It is shown that the set of prime integers in  $\mathbb{Q}(\sqrt{2})$  is partitioned into two sets with respect to their representation as a sum of squares: 1) a set  $\mathcal{S}_0$  of primes that cannot be represented as a sum of squares; 2) a set  $\mathcal{S}_2$  of primes that can be represented as a sum of two squares. Moreover, we give an effective, polynomial-time Euclidean Algorithm for the ring of integers of the cyclotomic field  $\mathbb{Q}(\zeta_8)$  and use it to show how such representations in  $\mathbb{Q}(\sqrt{2})$  can be found with deterministic polynomial complexity.

**Keywords:** Euclidean field, sum of squares, cyclotomic field, Euclidean Algorithm.

## 1 - Introduction

Siegel proved that the rational field  $\mathbb{Q}$  and the quadratic field  $\mathbb{Q}(\omega)$ , with golden section unit  $\omega = \frac{1+\sqrt{5}}{2}$ , are the only real algebraic number fields with a four-square sum representation of every totally positive integer [14]. Siegel's proof of the existential four-square sum theorem does not follow the constructive vein of Lagrange's proof for integers in  $\mathbb{Q}$ , but as counterpart, it partitions the set of algebraic number fields into two well specified sets: the set consisting of only two fields  $\mathbb{Q}$  and  $\mathbb{Q}(\omega)$ , and the set consisting of all remaining fields. Restricting the attention only to prime numbers, their representation in  $\mathbb{Q}$  is well known and depends on the residue modulo 8: i) primes congruent 1, 5 modulo 8 may be represented as a sum of two squares; ii) primes congruent 3 modulo 8 may be represented as a sum of three squares; iii) primes congruent 7 modulo 8 are necessarily represented as a sum of four squares [7].

The prime representations in  $\mathbb{Q}(\omega)$  have been shown to depend on the residue modulo 20 of their field norm: i) primes having field norm congruent 1, 3, 7, 9, 13, 17 modulo 20 may be represented as a sum of two squares; ii) primes having field norm congruent 11, 19 modulo 20 are necessarily represented as a sum of three squares [5].

A significant example of what happens in fields where a square sum theorem does not hold is offered by the Euclidean field  $\mathbb{Q}(\sqrt{2})$ . In the following section the representation of every totally positive prime in  $\mathbb{Q}(\sqrt{2})$  will be described in detail.

## 2 Preliminary results

Throughout the paper, we let  $\eta$  denote a root of  $x^2 - 2$ . Then the quadratic number field  $\mathbb{Q}(\eta)$  is a totally real Euclidean field with ring of integers  $\mathbb{Z}[\eta]$  and group of units generated by  $u = 1 + \eta$ . Field elements differing by a unit factor are called associates. The elements  $\alpha = a + b\eta$  and  $\bar{\alpha} = a - b\eta$  are called conjugate. An element  $\alpha = a + b\eta$  is called totally positive if both  $a + b\sqrt{2}$  and  $a - b\sqrt{2}$  are positive (e.g., it is positive regardless of the embedding chosen). Given a  $\beta \in \mathbb{Q}(\eta)$ , then one of the four elements  $\beta$ ,  $-\beta$ ,  $(1 + \eta)\beta$ , or  $-(1 + \eta)\beta$  is totally positive. For an odd prime  $p$ , we let QR and QNR stand for quadratic residue and quadratic non-residue, respectively, in the prime field  $\mathbb{F}_p$  of  $p$  elements.

Recalling that 2 is a QR modulo  $p$  iff  $p \equiv \pm 1 \pmod{8}$ , we have the following lemma.

**Lemma 2.1** *A rational prime  $p$  is represented by the quadratic form  $x^2 - 2y^2$  if and only if  $p$  is congruent to  $\pm 1$  modulo 8. Furthermore, if  $p$  is congruent to 1 modulo 8 then  $y$  is even, and if  $p$  is congruent to  $-1$  modulo 8 then  $y$  is odd.*

*Proof:* The condition is necessary since from  $p = a^2 - 2b^2$ , it follows that  $2 = \frac{a^2}{b^2} \pmod{p}$ , hence is 2 is a QR.

Conversely, if 2 is QR, then an integer  $m$  exists such that  $m^2 - 2 = 0 \pmod{p}$ . Therefore, the quadratic form  $px^2 + 2mxy + \frac{m^2 - 2}{p}y^2$  represents  $p$  and has discriminant 2. Since the class field is 1, Mathews' reduction process yields the canonical form  $x^2 - 2y^2$  and contemporarily a representation of  $p$  [10, 2].

Furthermore,  $a$  is necessarily odd, so if  $b$  is even then  $p$  is congruent 1 modulo 8, and if  $b$  is odd  $p$  is congruent  $-1$  modulo 8.  $\square$

It follows immediately that the primes of  $\mathbb{Q}(\eta)$  fall into three classes:

- Rational primes congruent 3, 5 modulo 8 which remain inert.
- Conjugate primes  $\pi = a + b\eta$  and  $\bar{\pi} = a - b\eta$  whose product is a rational prime congruent 1, 7 modulo 8; e.g., these correspond to the rational primes that split.
- The prime  $\eta$  such that  $\eta^2 = 2$ . The rational prime 2 is the only prime equal to a square; that is, it ramifies.

## 3 Main Theorem

In this section, we describe completely which prime integers in  $\mathbb{Q}(\eta)$  can be written as sums of squares. It turns out that for primes which can be written as a sum of squares at all, two squares always suffice.

**Lemma 3.1** *Let  $p$  be a rational prime congruent 7 modulo 8, and  $\pi = a + b\eta \in \mathbb{Q}(\eta)$  a prime over  $p$ . Then  $\pi$  cannot be written as a sum of squares.*

*Proof:* Observing that the square of an integer  $(a + b\eta)^2 = a^2 + 2b^2 + 2ab\eta$  in  $\mathbb{Q}(\eta)$  has even coefficient of  $\eta$ , the conclusion follows from Lemma 2.1.  $\square$

It is clear that any prime integer  $\pi \in \mathbb{Q}(\eta)$  which can be represented as the sum of two squares is necessarily totally positive, so we restrict our attention to such primes in the following theorem. We will show in the next section how such representations can be computed in deterministic polynomial-time. The method will follow very closely the existence proof we give here.

**Theorem 3.2** *Let  $p$  be a rational prime congruent to 1, 3, or 5 modulo 8. Then any totally positive prime integer  $\pi \in \mathbb{Q}(\eta)$  over  $p$  can be written as a sum of two squares of integers in  $\mathbb{Q}(\eta)$ .*

*Proof:* Notice first that it suffices to show that the result holds for some totally positive prime  $\pi$  over  $p$ . For if  $\pi = \alpha^2 + \beta^2$  and  $\pi'$  is another totally positive integer over  $p$ , we have either  $\pi' = \pi(1 + \eta)^k$  or  $\pi' = \bar{\pi}(1 + \eta)^k$ . In the former case, since  $\pi', \pi$  are both totally positive it follows that  $(1 + \eta)^k$  is as well. Then  $0 < (1 + \sqrt{2})^k$  and  $0 < (1 - \sqrt{2})^k$  imply that  $k = 2k'$  is even and so  $\pi' = [\alpha(1 + \eta)^{k'}]^2 + [\beta(1 + \eta)^{k'}]^2$ , and  $k$  may be found easily by numerical evaluation at  $\eta = \sqrt{2}$ . The latter case  $\pi' = \bar{\pi}(1 + \eta)^k$  follows similarly.

Let  $\mathbb{K} = \mathbb{Q}(\eta)$  and  $\mathbb{F} = \mathbb{K}(i) = \mathbb{Q}(\zeta_8)$  where  $\zeta_8 = \frac{\eta}{2}(1 + i)$  is a primitive eighth root of unity. Then  $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\eta]$ ,  $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\zeta_8]$  are the respective rings of integers of these fields. By [11, Prop. 10.3], we have in  $\mathbb{Z}[\zeta_8]$  that

$$\langle p \rangle = \begin{cases} \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 \text{ with } N(\mathfrak{p}_j) = p, & \text{if } p \equiv 1 \pmod{8} \\ \mathfrak{p}_1 \mathfrak{p}_2 \text{ with } N(\mathfrak{p}_j) = p^2, & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Since  $\mathbb{Z}[\zeta_8]$  is a PID, it follows from the above that

- if  $p \equiv 1 \pmod{8}$  there exists  $\gamma \in \mathbb{Z}[\zeta_8]$  with  $N_{\mathbb{F}/\mathbb{Q}}(\gamma) = p$ ,
- if  $p \equiv 3, 5 \pmod{8}$  there exists  $\gamma \in \mathbb{Z}[\zeta_8]$  with  $N_{\mathbb{F}/\mathbb{Q}}(\gamma) = p^2$ .

In either case, if  $\gamma = a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3$  with  $a, b, c, d \in \mathbb{Z}$  we have

$$N_{\mathbb{F}/\mathbb{Q}}(\gamma) = N_{\mathbb{K}/\mathbb{Q}}(N_{\mathbb{F}/\mathbb{K}}(\gamma)) = N_{\mathbb{K}/\mathbb{Q}} \left( \left[ a + \frac{\eta}{2}(b - d) \right]^2 + \left[ c + \frac{\eta}{2}(b + d) \right]^2 \right).$$

Then  $\pi = \left[ a + \frac{\eta}{2}(b - d) \right]^2 + \left[ c + \frac{\eta}{2}(b + d) \right]^2$  is easily seen to be an integer in  $\mathbb{K}$  with norm  $N_{\mathbb{F}/\mathbb{Q}}(\gamma)$ , so  $\pi$  is a prime over  $p$ . Furthermore, being a sum of two squares it is necessarily totally positive, so in fact  $N_{\mathbb{F}/\mathbb{Q}}(\gamma) = \pi\bar{\pi} > 0$ .

If  $b \equiv d \pmod{2}$ , then with  $\alpha = a + \frac{\eta}{2}(b - d)$ , and  $\beta = c + \frac{\eta}{2}(b + d)$ , we have  $\alpha, \beta \in \mathbb{Z}[\eta]$  and  $\pi = \alpha^2 + \beta^2$  so we're done.

Suppose now that  $b \not\equiv d \pmod{2}$  and  $\pi = x + \eta y$  with  $x, y \in \mathbb{Z}$ . If  $p \equiv 1 \pmod{8}$ , we have  $N_{\mathbb{K}/\mathbb{Q}}(\pi) = p \equiv 1 \pmod{8}$  and if  $p \equiv 3, 5 \pmod{8}$  we have  $N_{\mathbb{K}/\mathbb{Q}}(\pi) = p^2 \equiv 1 \pmod{8}$ . So in any case,  $\pi\bar{\pi} = x^2 - 2y^2 \equiv 1 \pmod{8}$  and it follows that  $y$  must be even. So  $y = a(b - d) + c(b + d) \equiv 0 \pmod{2}$ . But since  $b \not\equiv d \pmod{2}$  it follows that

$b - d \equiv b + d \equiv 1 \pmod{2}$ , hence  $a \equiv c \pmod{2}$ . Then with  $\alpha = b + \frac{\eta}{2}(c + a)$ , and  $\beta = d + \frac{\eta}{2}(c - a)$  we have  $\alpha, \beta \in \mathbb{Z}[\eta]$  and

$$\alpha^2 + \beta^2 = \left[ b + \frac{\eta}{2}(c + a) \right]^2 + \left[ d + \frac{\eta}{2}(c - a) \right]^2 = \left[ a + \frac{\eta}{2}(b - d) \right]^2 + \left[ c + \frac{\eta}{2}(b + d) \right]^2 = \pi,$$

as desired.  $\square$

**Corollary 3.3** *A totally positive integer in  $\mathbb{Q}(\eta)$  is a sum of two squares if and only if each of its prime factors of field norm congruent to  $-1$  modulo  $8$  occurs with even exponent.*

*Proof:* The sufficiency follows precisely as in the classical case over  $\mathbb{Z}$ , by using the algebraic identity

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

For the necessity, suppose  $p \equiv -1 \pmod{8}$  and  $\pi \in \mathbb{Z}[\eta]$  is a prime over  $p$ . Then there is a ring homomorphism  $\psi : \mathbb{Z}[\eta] \rightarrow \mathbb{Z}/p\mathbb{Z}$  with  $\ker \psi = \langle \pi \rangle$ . By way of contradiction, suppose  $\pi^{2k+1}\delta = \alpha^2 + \beta^2$  with  $\delta, \alpha, \beta \notin \langle \pi \rangle$ . Then

$$0 \equiv \psi(\pi^{2k+1}\delta) = \psi(\alpha)^2 + \psi(\beta)^2 \pmod{p}.$$

Since  $\psi(\alpha), \psi(\beta)$  are both nonzero, it would follow that  $-1$  is a quadratic residue modulo  $p$ , contradicting that  $p \equiv -1 \pmod{8}$ .  $\square$

## 4 Computing the representation

As before, we take  $\mathbb{K} = \mathbb{Q}(\eta)$  and  $\mathbb{F} = \mathbb{K}(i) = \mathbb{Q}(\zeta_8)$  where  $\zeta_8 = \frac{\eta}{2}(1 + i)$  is a primitive eighth root of unity. Then  $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\eta]$ ,  $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\zeta_8]$  are the respective rings of integers. The method that we propose here follows very closely the method by which we proved existence in Theorem 3.2.

In particular, for  $p \equiv 1, 3, 5 \pmod{8}$ , it suffices to produce a prime integer  $\gamma \in \mathbb{F}$  over  $p$ . It is well-known that  $\mathbb{F}$  is a norm-Euclidean field and, in particular, a principal ideal domain. If  $p \equiv 1 \pmod{8}$ , we may use Schoof's algorithm [12] to, in deterministic polynomial time, find  $s, \iota \in \mathbb{Z}/p\mathbb{Z}$  so that  $s^2 \equiv 2 \pmod{p}$  and  $\iota^2 \equiv -1 \pmod{p}$ ; of course, in practice, one should use a faster method for computing square roots modulo  $p$ , but Schoof's method is deterministic polynomial-time with respect to  $p$ . Then the four distinct solutions to  $x^4 + 1 \equiv 0 \pmod{p}$  are given by  $x = (\pm s/2)(1 \pm \iota)$  and it is well known (e.g., [3]) that the ideal  $\langle p \rangle \subseteq \mathcal{O}_{\mathbb{F}}$  splits completely as

$$\langle p \rangle = \langle p, \zeta_8 - x_1 \rangle \langle p, \zeta_8 - x_2 \rangle \langle p, \zeta_8 - x_3 \rangle \langle p, \zeta_8 - x_4 \rangle, \quad (4.1)$$

where  $x_1, \dots, x_4$  are these four distinct roots of  $x^4 + 1$  modulo  $p$ . Since the ideals on the right hand side of 4.1 each have norm  $p$  and are principal, it suffices to find a generator  $\gamma$  for one of them. In practice, the straightforward method of applying LLL to the HNF matrix seems always to produce a generator, but we have not attempted to prove that this is the case.

Instead, our approach is to give an effectively computable division algorithm for  $\mathbb{Z}[\zeta_8]$ . An effective Euclidean Algorithm for computing gcd's in  $\mathbb{Z}[\zeta_8]$  then follows as an immediate consequence, and we may use it to solve the principal ideal problem in this setting.

The remaining two cases are equally straightforward. If  $p \equiv 3 \pmod{8}$ , one may use Schoof to, in polynomial-time, find  $t \in \mathbb{Z}/p\mathbb{Z}$  so that  $t^2 \equiv -2 \pmod{p}$ . Then  $x^4 + 1$  factors over  $\mathbb{Z}/p\mathbb{Z}$  as  $x^4 + 1 \equiv (x^2 + tx - 1)(x^2 - tx - 1)$ . Since  $x^4 + 1$  has no roots in  $\mathbb{Z}/p\mathbb{Z}$ , it follows that this is an irreducible factorization so that

$$\langle p \rangle = \langle p, \zeta_8^2 + t\zeta_8 - 1 \rangle \langle p, \zeta_8^2 - t\zeta_8 - 1 \rangle, \quad (4.2)$$

and both ideals on the RHS are prime, each with norm  $p^2$ .

Finally, if  $p \equiv 5 \pmod{8}$  we find  $\iota \in \mathbb{Z}/p\mathbb{Z}$  for which  $\iota^2 \equiv -1 \pmod{p}$ . Then the factorization of  $x^4 + 1$  over  $\mathbb{Z}/p\mathbb{Z}$  is  $x^4 + 1 \equiv (x^2 + \iota)(x^2 - \iota)$ , and in this case  $\langle p \rangle$  factors as

$$\langle p \rangle = \langle p, \zeta_8^2 + \iota \rangle \langle p, \zeta_8^2 - \iota \rangle. \quad (4.3)$$

So, if we can compute gcd's in  $\mathbb{Z}[\zeta_8]$ , we can solve the principal ideal problem and find principal generators for the ideals on the RHS of Equations 4.1, 4.2, and 4.3. Then it is clear how to use the remainder of the proof in Theorem 3.2 to solve the original problem.

#### 4.1 A division algorithm for $\mathbb{Z}[\zeta_8]$

To establish an effective division algorithm we first require a lemma.

**Lemma 4.1** *Let  $\zeta_8$  be a primitive eighth root of unity and  $\mathbb{F} = \mathbb{Q}(\zeta_8)$  as above. There exists a constant  $0 < C < 1$  so that for all  $\delta = a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3 \in \mathbb{F}$  with  $-1/2 \leq a, b, c, d \leq 1/2$ ,  $\delta$  satisfies  $|N_{\mathbb{F}/\mathbb{Q}}(\delta)| \leq C$ .*

*Proof:* For  $w, x, y, z \in [-1/2, 1/2] \subset \mathbb{R}$ , set  $u = w^2 + x^2 + y^2 + z^2$ ,  $v = wx - wz + xy + yz$ , and

$$F(w, x, y, z) = (w^2 + x^2 + y^2 + z^2)^2 - 2(wx - wz + xy + yz)^2 = u^2 - 2v^2.$$

For all  $w, x, y, z$  in the given region, we have that  $0 \leq u \leq 1$  and  $-1/2 \leq v \leq 1/2$ . From these bounds, we find immediately that  $-1/2 \leq u^2 - 2v^2 \leq 1$ . But the only possibility for  $u^2 - 2v^2 = 1$  to occur is if  $u = 1, v = 0$ . Then  $u = 1$  implies  $w, x, y, z \in \{\pm\frac{1}{2}\}$ . Checking each of these 16 cases, we find that  $v = 0$  does not occur and so  $u^2 - 2v^2 < 1$  for all  $w, x, y, z \in [-1/2, 1/2]$ . It follows now that  $|F(w, x, y, z)| < 1$  over the region in question. But since this region is compact and  $F$  is continuous,  $F$  must achieve a maximum and a minimum and we conclude that there exists  $0 < C < 1$  with  $|F(w, x, y, z)| \leq C$  for all  $w, x, y, z \in [-1/2, 1/2]$ . The result follows since for  $a, b, c, d \in \mathbb{Q} \cap [-1/2, 1/2]$  we have

$$|N_{\mathbb{F}/\mathbb{Q}}(a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3)| = |F(a, b, c, d)| \leq C.$$

□

Optimization of  $F$  over the hypercube  $[-1/2, 1/2]^4$  by usual calculus techniques yields an explicit value for  $C$ . We avoid those calculations here, but mention that the computer software MAPLE suggests that the result is  $C = 9/16$ .

An immediate consequence of Lemma 4.1 is the following effective division algorithm for  $\mathbb{Z}[\zeta_8]$ . Let  $\alpha = a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3$  and  $\beta = b_0 + b_1\zeta_8 + b_2\zeta_8^2 + b_3\zeta_8^3$  be elements of  $\mathbb{Z}[\zeta_8]$  with  $\beta \neq 0$  and  $n = N_{\mathbb{F}/\mathbb{Q}}(\beta)$ . If the conjugates of  $\beta$  in  $\mathbb{F}$  over  $\mathbb{Q}$  are  $\beta_1, \beta_2, \beta_3, \beta_4$  with  $\beta = \beta_1$ , we set

$$\gamma = \alpha\beta_2\beta_3\beta_4,$$

and write  $\gamma = g_0 + g_1\zeta_8 + g_2\zeta_8^2 + g_3\zeta_8^3$ . For  $0 \leq j \leq 3$ , let  $q_j$  denote the nearest integer to  $\frac{g_j}{n}$  and  $r_j = g_j - nq_j$ . It follows that with  $\rho = \frac{r_0}{n} + \frac{r_1}{n}\zeta_8 + \frac{r_2}{n}\zeta_8^2 + \frac{r_3}{n}\zeta_8^3$ , we have

$$\frac{\alpha}{\beta} = \frac{\gamma}{n} = (q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3) + \rho.$$

By construction,  $|\frac{r_j}{n}| \leq 1/2$ , and so an application of Lemma 4.1 yields  $|N_{\mathbb{F}/\mathbb{Q}}(\rho)| \leq C < 1$ . Then  $|N_{\mathbb{F}/\mathbb{Q}}(\rho\beta)| \leq C|N_{\mathbb{F}/\mathbb{Q}}(\beta)| < |N_{\mathbb{F}/\mathbb{Q}}(\beta)|$  and  $\rho\beta \in \mathbb{Z}[\zeta_8]$  since  $\rho\beta = \alpha - \beta(q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3)$ . Thus we have

$$\alpha = (q_0 + q_1\zeta_8 + q_2\zeta_8^2 + q_3\zeta_8^3)\beta + \rho\beta, \quad \rho\beta \in \mathbb{Z}[\zeta_8], \quad \text{and} \quad |N_{\mathbb{F}/\mathbb{Q}}(\rho\beta)| < |N_{\mathbb{F}/\mathbb{Q}}(\beta)|,$$

providing the computationally effective division algorithm we sought. It is interesting to note that the norm of the remainder is actually bounded by the absolute constant  $C < 1$  times the norm of the divisor; this is a situation which certainly does not occur over  $\mathbb{Z}$  or polynomial rings (although it does occur, for example, in the Gaussian integers with  $C = 1/2$ ).

## 4.2 Computing the representations as sums of squares

With this division algorithm in hand, we immediately have a working Euclidean Algorithm in  $\mathbb{Z}[\zeta_8]$  and may find a principal generator for any one of the ideals in Equations 4.1, 4.2, or 4.3, thus producing an element of norm  $p$ . Furthermore, since  $0 < C < 1$  in Lemma 4.1, it follows that the absolute value of the norms of the remainders decrease exponentially so that the resulting Euclidean Algorithm requires a number of steps which is polynomially bounded by the size (log) of the norm of the inputs. Since the size of the norms are polynomially bounded by the input size, we conclude that this Euclidean Algorithm is polynomial-time in the input size. Thus, we have shown the following theorem.

**Theorem 4.2** *If division is performed as described in Section 4.1, the resulting Euclidean Algorithm in  $\mathbb{Z}[\zeta_8]$  is polynomial-time.*

The entire process can be compactly summarized as follows.

**Algorithm 4.3** *(Compute the representation)*

*Input:* A rational prime  $p \equiv 1, 3, \text{ or } 5 \pmod{8}$ .

*Output:* Integers  $\alpha, \beta \in \mathbb{Z}[\eta]$  so that  $\pi = \alpha^2 + \beta^2$  is a (totally positive) prime over  $p$ .

1. Find a two element representation of an irreducible factor of  $\langle p \rangle$  using Equation 4.1, 4.2 or 4.3, according to whether  $p \equiv 1, 3, \text{ or } 5 \pmod{8}$  respectively.

2. If the two element representation obtained above is  $\langle p, g(\zeta_8) \rangle$ , use the Euclidean Algorithm (with Division Algorithm as described in this paper) to find  $a + b\zeta_8 + c\zeta_8^2 + d\zeta_8^3 = \gcd(p, g(\zeta_8))$ .
3. If  $b \equiv d \pmod{2}$ , set  $\alpha = a + \frac{\eta}{2}(b - d)$  and  $\beta = c + \frac{\eta}{2}(b + d)$ . Otherwise, set  $\alpha = b + \frac{\eta}{2}(c + a)$  and  $\beta = d + \frac{\eta}{2}(c - a)$ .

**Example 4.4** Let  $p = 1033$  and we will compute an element of  $\mathbb{Z}[\zeta_8]$  of norm  $p$ . Since  $p \equiv 1 \pmod{8}$ , we compute square roots of 2 and  $-1$  modulo  $p$  and find that  $404^2 \equiv 2 \pmod{p}$  and  $355^2 \equiv -1 \pmod{p}$ . Therefore,  $x_1 = 635 \equiv (404/2)(1+355) \pmod{p}$  is a root of  $x^4 + 1$  modulo  $p$ , so it suffices to find a principal generator of the ideal  $\langle 1033, \zeta_8 - 635 \rangle \subseteq \mathbb{Z}[\zeta_8]$ . Applying the division algorithm as described above, we find successively

$$\begin{aligned}
1033 &= (\zeta_8 - 635)(-2) + (-237 + 2\zeta_8), \\
\zeta_8 - 635 &= (-237 + 2\zeta_8)(3) + (76 - 5\zeta_8), \\
-237 + 2\zeta_8 &= (76 - 5\zeta_8)(-3) + (-9 - 13\zeta_8), \\
76 - 5\zeta_8 &= (-9 - 13\zeta_8)(-1 + 2\zeta_8 - 3\zeta_8^2 + 5\zeta_8^3) + (2 - \zeta_8^2 + 6\zeta_8^3).
\end{aligned}$$

The norms of the remainders obtained above are  $(17)(1033)(179657)$ ,  $(1033)(32297)$ ,  $(2)(17)(1033)$ , and  $1033$  respectively. From the element  $\gamma = 2 - \zeta_8^2 + 6\zeta_8^3$  of norm  $1033$ , we obtain a solution to the original problem,

$$(2 - 3\eta)^2 + (-1 + 3\eta)^2 = \pi = 41 - 18\eta,$$

where  $\pi$  is a totally positive factor of  $1033$  in  $\mathbb{Z}[\eta]$ .

**Example 4.5** Let  $p = 1051$ . Since  $p \equiv 3 \pmod{8}$ , to use Equation 4.2 we find that  $t = 650$  is a square root of  $-2$  modulo  $p$  and so  $x^4 + 1 \equiv (x^2 + 650x - 1)(x^2 - 650x - 1) \pmod{p}$ . Using the Euclidean Algorithm, we find a principal generator for the ideal  $\mathfrak{p}_1 = \langle 1051, \zeta_8^2 + 650\zeta_8 - 1 \rangle = \langle 21\zeta_8^3 + 21\zeta_8 - 13 \rangle$ . In this case, we have  $a = -13$ ,  $b = 21$ ,  $c = 0$ ,  $d = 21$ , so we take  $\alpha = -13$  and  $\beta = 21\eta$ . Then  $\alpha^2 + \beta^2 = 1051$ . In principle, we could have obtained a representation of some associate of the prime  $1051$ , but in that case we could find the differing unit factor by numerical evaluation at  $\eta = \sqrt{2}$ , and still obtain a representation of  $1051$  itself as the sum of two squares.

**Example 4.6** Let  $p = 1061$ . Since  $p \equiv 5 \pmod{8}$ , we appeal to Equation 4.3 with  $\iota = 103$ . Then  $\langle 1061, \zeta_8^2 + 103 \rangle = \langle -10\zeta_8^2 + 31 \rangle$ , so that  $a = 31$ ,  $b = 0$ ,  $c = -10$ ,  $d = 0$ . Then  $\alpha = 31$ ,  $\beta = -10$  and we have  $1061 = 31^2 + (-10)^2$ . It is no coincidence that in this case we obtain a representation as the sum of rational squares, and we will prove below that this is always the case when  $p \equiv 5 \pmod{8}$ .

**Proposition 4.7** If  $p \equiv 5 \pmod{8}$ , then the output of Algorithm 4.3 will be two rational integers  $\alpha, \beta \in \mathbb{Z}$  with  $\alpha^2 + \beta^2 = p$ .

*Proof:* If  $p \equiv 5 \pmod{8}$ , then each prime ideal on the RHS of Equation 4.3 has the form  $\langle p, \zeta_8^2 + m \rangle$  for some  $m \in \mathbb{Z}$ . In particular, each generator of this ideal is in the subfield  $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_8)$ . Suppose now that  $\sigma, \tau \in \mathbb{Q}(\zeta_8)$  happen to lie in the subfield  $\mathbb{Q}(i) = \mathbb{Q}(\zeta_8^2)$  and the division algorithm is applied to  $\sigma$  divided by  $\tau$ . Then all conjugates of  $\tau$  are in  $\mathbb{Q}(i)$ , so in the notation of Section 4.1,  $\sigma\tau_2\tau_3\tau_4 \in \mathbb{Q}(i)$ . It follows that the coefficients of  $\zeta_8$  and  $\zeta_8^3$  in both the quotient and remainder are all zero, so that the resulting quotient and remainders are again in  $\mathbb{Q}(i)$ .

So repeated application of the division algorithm to find the gcd of  $p$  and  $\zeta_8^2 + m$  will give a greatest common divisor of the form  $a + c\zeta_8^2$  with  $a, c \in \mathbb{Z}$ , and the output of Algorithm 4.3 at Step 3 will thus be  $\alpha = a, \beta = c \in \mathbb{Z}$ .  $\square$

## 5 Conclusions

In this paper we have described the representation of integers in  $\mathbb{Q}(\sqrt{2})$  as a sum of squares. If  $p \equiv 7 \pmod{8}$ , then no primes over  $p$  can be written as a sum of squares. If  $p \not\equiv 7 \pmod{8}$ , then every totally positive prime over  $p$  can be written as the sum of two squares. From this, we concluded that a totally positive integer in  $\mathbb{Q}(\sqrt{2})$  is a sum of two squares if and only if each of its prime factors of field norm congruent to  $-1$  modulo 8 occurs with even exponent.

Additionally, we gave a division algorithm for integers in  $\mathbb{Q}(\zeta_8)$  resulting in a polynomial-time Euclidean Algorithm for computing a greatest common divisor of integers in  $\mathbb{Q}(\zeta_8)$ . We showed how this can be used to find the representation of primes in  $\mathbb{Q}(\sqrt{2})$  as the sums of two squares in deterministic polynomial-time.

## References

- [1] G.E. Andrews, *Number Theory*, New York: Dover, 1994.
- [2] D.A. Buell, *Binary Quadratic Forms*, New York: Springer-Verlag, 1989.
- [3] H. Cohen, *A Course in Computational Algebraic Number Theory*, New York: Springer-Verlag, 1996.
- [4] M. Elia, Representation of Primes as the Sums of Two Squares in the Golden Section Quadratic Field, *J. Discrete Math. Sci. Cryptography*, Vol.9, No.1, 2006, p.25-37.
- [5] M. Elia, On the Representation of Primes as Sums of Squares in the Golden Section Field, to appear *Proceedings Twelve International Conference on Fibonacci Numbers and Their Applications*, San Francisco, July 18-21, 2006.
- [6] K.F. Gauss, *Disquisitiones Arithmeticae*, New York: Springer, 1986.
- [7] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford: Oxford University Press, 1971.
- [8] E. Landau, *Elementary Number Theory*, Chelsea, NY, 1966.

- [9] F. Lemmermeyer, *Reciprocity Laws*, New York: Springer-Verlag, 2000.
- [10] G.B. Mathews, *Theory of Numbers*, New York: Chelsea, 1930.
- [11] J. Neukirch, *Algebraic Number Theory*, Berlin: Springer-Verlag, 1999.
- [12] R. Schoof, Elliptic Curves Over Finite Fields and the Computation of the Square Roots mod  $p$ , *Mathematics of Computation*, vol. 44, number 170, April 1985, pp.483-494.
- [13] J.P. Serre, *Cours d'Arithmétique*, Paris: P.U.F., 1970.
- [14] C.L. Siegel, The trace of totally positive and real algebraic integers, *Annals of Math.*, 46, 1945, p.302-312.
- [15] L.C. Washington, *Introduction to Cyclotomic fields*, New York: Springer, 1997.
- [16] H. Weyl, *Algebraic Theory of Numbers*, Princeton, NJ: Princeton Univ. Press, 1980.