Divulgaciones Matemáticas Vol. 14 No. 1(2006), pp. 59–72

Algorithm for Finding a Biquadratic Cyclotomic Extension Field of $\mathbb{Q}$

Algoritmo para Hallar una Extensión Ciclotómica Bicuadrática de $\mathbb{Q}$

Amílcar J. Pérez A. (`ajperez@usb.ve`)
Departamento de Matemáticas puras y Aplicadas,
Universidad Simón Bolívar, Valle de Sartenejas,
Edo. Miranda, MYS-355B, Venezuela.

Abstract

Let $p \equiv 1 \pmod 4$ be a prime number and let $\zeta = e^{2\pi i/p}$ be a primitive root of unity. Then there exists a unique biquadratic extension field $\mathbb{Q}(y)/\mathbb{Q}$ that is a subfield of $\mathbb{Q}(\zeta)$. The aim of this work is to construct an algorithm for finding such y explicitly. Finally we state a general conjecture about the y we found.
Key words and phrases: biquadratic fields, cyclotomic fields, Galois theory, algorithm.

Resumen

Sea $p \equiv 1 \pmod 4$ un primo y sea $\zeta = e^{2\pi i/p}$ una raíz primitiva de la unidad. Entonces existe una única extensión bicuadrática $\mathbb{Q}(y)/\mathbb{Q}$ que es un subcuerpo de $\mathbb{Q}(\zeta)$. El propósito de este trabajo es construir un algoritmo para hallar y explícitamente. Finalmente se enuncia una conjetura general acerca del y hallado.
Palabras y frases clave: cuerpo bicuadrático, cuerpo ciclotómico, teoría de Galois, algoritmo.

Introduction

It is known that if $p \equiv 1 \pmod 4$ then $\mathbb{Q}(\sqrt{p})$ is the unique quadratic extension field of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/p}$ (see §1 for references).

Received 2006/03/01. Accepted 2006/06/05.
MSC (2000): Primary 11Y40, 13B25; Secondary 11Y16, 13B05.

Also, there exists a unique quadratic extension field $\mathbb{Q}(y)$ of $\mathbb{Q}(\sqrt{p})$, and therefore a biquadratic extension field of $\mathbb{Q}$, contained in $\mathbb{Q}(\zeta)$. Moreover if $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = 2^k n$ with $(2, n) = 1$ then there exists a unique tower of fields:

$$\mathbb{Q} = E_0 \subset E_1 \subset \ldots \subset E_k \subset \mathbb{Q}(\zeta)$$

where $[E_j : E_{j-1}] = 2$ for all $j = 1, \ldots, k$ and $[\mathbb{Q}(\zeta) : E_k] = n$. It is known that $E_j/\mathbb{Q}$ is a simple extension i.e., for all j there is an $y_j \in \mathbb{C}$ such that $E_j = \mathbb{Q}(y_j)$. We consider this preliminaries in §1. Actually, our algorithm is for calculating such y_j's explicitly (see §2). The other major result in this work is the conjecture in §3, it states an explicit algebraic expresion for y_2 depending on p and a unique positive odd integer b such that $p = a^2 + b^2$ for some integer a.

1 Preliminary results

The aim of this section is to show some results that will allow us to construct the algorithm in §2.

1.1 Existence of a unique tower of p-th cyclotomic fields

Definition 1.1.1. Let $m \geq 1$ and $\zeta = e^{2\pi i/m}$. We say that a number field K is a m-th cyclotomic field if K is an intermediate field of $\mathbb{Q}(\zeta)/\mathbb{Q}$ i.e., $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta)$.

This is a somewhat variant of Lang's definition in [4], p. 71.

Lemma 1.1.2. *Let G be a cyclic group of order m and generator g. If d divides m then $\langle g^{m/d} \rangle \subset G$ is its unique subgroup of order d.*

Proof. See Lemma 41 in [7], p. 38. □

For basic definitions in the following theorem see [7], pp. 35,43,47.

Theorem 1.1.3 (Fundamental Theorem of Galois Theory)**.** *Let E/F be a Galois extension with Galois group $G = Gal(E/F)$. Let $H \subset G$ be a subgroup, and E^H its fixed field, and let K be an intermediate field of E/F. Then*

(1) The application $H \mapsto E^H$, is an order reversing biyection with inverse $K \mapsto Gal(E/K)$.

(2) $E^{Gal(E/K)} = K$ and $Gal(E/E^H) = H$.

(3) $[K : F] = [G : Gal(E/K)]$ *and* $[G : H] = [E^H : F]$.

(4) K/F *is a Galois extension if and only if* $Gal(E/K)$ *is a normal subgroup of* G.

Proof. See Theorem 63 in [7], pp. 49-50. □

Theorem 1.1.4. *Let* $m \geq 1$ *be an integer and let* $\zeta = e^{2\pi i/m}$. *Then,* $\mathbb{Q}(\zeta)/\mathbb{Q}$ *is a Galois extension with Galois group isomorphic to* $\mathbb{Z}_m^\times$, *whose order is* $\varphi(m)$, *where* φ *is Euler's phi function.*

Proof. See [3], pp. 193-195. □

Corollary 1.1.5. *Let* p *be a prime number, let* $\zeta = e^{2\pi i/p}$, *and let* $E = \mathbb{Q}(\zeta)$. *Then, for every divisor* d *of* $p-1$ *there exists a unique subgroup* $H \subset Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ *of order* d. *Moreover, its fixed field* E^H *is a Galois extension of* $\mathbb{Q}$.

Proof. Follows from Lemma 1.1.2 and Theorem 1.1.3 because Theorem 1.1.4 implies that $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a cyclic group. □

Corollary 1.1.6. *With the same hypothesis of the above corollary, if* $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = 2^k n$ *with* $k \geq 1,\ (2, n) = 1$ *then there exists a unique tower of fields*

$$\mathbb{Q} = E_0 \subset E_1 \subset \ldots \subset E_k \subset E = \mathbb{Q}(\zeta)$$

where $[E_j : E_{j-1}] = 2$ *for all* $j = 1, \ldots, k$ *and* $[\mathbb{Q}(\zeta) : E_k] = n$. *Hence,* $[E_j : \mathbb{Q}] = 2^j$ *for all* j.

Proof. Because of Lemma 1.1.2 and Theorem 1.1.4, there is a unique sequence of cyclic groups

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) = H_0 \supset H_1 \supset \ldots \supset H_k \supset \{0\}$$

where H_j is the unique subgroup of G with order $2^{k-j}n$. Let $E_j = E^{H_j}$ be the fixed field of H_j, then the corollary follows from the Fundamental Theorem of Galois Theory and from the following basic fact: If $[E : F]$ is finite and K is an intermediate field, then $[E : F] = [E : K][K : F]$ (see, e.g., Lemma 31 and Exercise 75 in [7], pp. 30–31). □

1.2 Cyclotomic fields are simple extensions

With the same notation of the previous subsection, we will prove that there exists $y_j \in \mathbb{C}$ such that $E_j = \mathbb{Q}(y_j)$ for all $j = 1, \ldots, k$.

Lemma 1.2.1 (Theorem of the Primitive Element). *Every Galois extension E/F is simple, i.e. there exists a y in E such that $E = F(y)$.*

Proof. See [7], p. 51. □

From this lemma, Theorem 1.1.4 and Theorem 1.1.3, the next follows.

Corollary 1.2.2. *Every E_j is a simple extension of $\mathbb{Q}$.*

Now the question is how to find an $y_j \in \mathbb{C}$ such that $E_j = \mathbb{Q}(y_j)$. Theorem 1.2.5 below addresses this question.

Remark 1.2.3. Let p be a prime and let g be a generator of $\mathbb{Z}_p^\times$, let $E = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$. It is easy to see that the application

$$\phi : \mathbb{Z}_p^\times \to Gal(E/\mathbb{Q}) \qquad g \mapsto \gamma_0$$

with $\gamma_0(\zeta) = \zeta^g$, is a group isomorphism. Based on this fact and Lemma 1.1.2 the only subgroup of $Gal(E/\mathbb{Q})$ of order d is $\phi(\langle g^{(p-1)/d}\rangle) = \langle \gamma_0^{(p-1)/d}\rangle$ where $\gamma_0^{(p-1)/d}(\zeta) = \zeta^{g^{(p-1)/d}}$. Moreover, this implies that σ is an automorphism of $\mathbb{Q}(\zeta)$ if and only if $\sigma(\zeta) = \zeta^m$ for some $1 \le m \le p-1$ (from Theorem 1.1.3 (3) we have $[E : \mathbb{Q}] = [Gal(E/\mathbb{Q}) : Gal(E/E)] = |Gal(E/\mathbb{Q})| = p-1$).

Lemma 1.2.4. *Let p be a prime and $\zeta = e^{2\pi i/p}$, and let $1 \le m \le p-1$ be an integer. If*

$$\sum_{j=1}^{m} \zeta^{k_j} = \sum_{j=1}^{m} \zeta^{\ell_j}, \text{ where } 1 \le k_j \le p-1,\ 1 \le \ell_j \le p-1,$$

then the two sets of indices $\{k_j : j = 1\ldots, m\}$ and $\{\ell_j : j = 1\ldots, m\}$ are equal.

Proof. Let $S = \{0, 1, \ldots, p-1\} \setminus \{\ell_j : j = 1, \ldots, m\}$ then

$$\sum_{j=1}^{m} \zeta^{\ell_j} + \sum_{\ell \in S} \zeta^{\ell} = 0.$$

Hence

$$\sum_{j=1}^{m} \zeta^{k_j} + \sum_{\ell \in S} \zeta^{\ell} = 0.$$

Let $h(x) = \sum_{j=1}^{m} x^{k_j} + \sum_{\ell \in S} x^{\ell} \in \mathbb{Z}[x]$, then h has degree $\deg(h) \leq p-1$ and ζ is one of its roots. Let $f(x) = 1 + x + x^2 + \ldots + x^{p-1}$ be the irreducible polynomial of ζ. Since, by definition, the irreducible polynomial has minimal degree we have $\deg(h) \geq \deg(f)$, thus $\deg(h) = \deg(f)$.

It is well known that $\{g(x) \in \mathbb{Q}[x] : g(\alpha) = 0\}$ is the principal ideal generated over $\mathbb{Q}[x]$ by the irreducible polynomial of α. From this fact and the last assertion of the above paragraph, we have $h(x) = cf(x)$ for some $c \in \mathbb{Q}$.

Now, if some $k_j \in S$ then $h(x) \neq cf(x)$ for all $c \in \mathbb{Q}$. Therefore both sets of indices are equal. □

The following theorem summarizes what we have done so far and gives us an explicit expression for y_j in terms of the group H_j. This is an important tool in the construction of algorithm in §2. We assume the notation of Corollary 1.1.6 as well as that of its proof.

Theorem 1.2.5. *Let $p = 2^k n + 1$ be a prime with $k \geq 2$, $(2, n) = 1$, and let $\zeta = e^{2\pi i/p}$. Then there exists a unique tower of p-th cyclotomic fields*

$$\mathbb{Q} = \mathbb{Q}(y_0) \subset \mathbb{Q}(y_1) \subset \cdots \subset \mathbb{Q}(y_k) \subset \mathbb{Q}(\zeta)$$

where

(1) $[\mathbb{Q}(y_j) : \mathbb{Q}(y_{j-1})] = 2$ *for all* j *and* $[\mathbb{Q}(\zeta) : \mathbb{Q}(y_k)] = n$

(2) $y_j = \sum_{\gamma \in H_j} \gamma(\zeta)$, *where* $H_j \subset Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ *is the subgroup of order* $2^{k-j} n$.

(3) Moreover, if g *is a generator of* $\mathbb{Z}_p^{\times}$ *and* $a = g^{(p-1)/d}$ *is an element of order* $d = |H_j|$ *(actually* $a = a_j$ *and* $d = d_j$*), then*

$$y_j = \sum_{\ell=1}^{d} \zeta^{a^{\ell}}.$$

Proof. From Remark 1.2.3 we have $H_j = \{\gamma_\ell : \gamma_\ell(\zeta) = \zeta^{a^{\ell}}, \ell = 1, \ldots, d\}$, thus

$$\sum_{\gamma \in H_j} \gamma(\zeta) = \sum_{\ell=1}^{d} \zeta^{a^{\ell}}. \tag{1.1}$$

Then, because of Corollaries 1.1.6 and 1.2.2 we only need to prove that $E_j = \mathbb{Q}(y_j)$. By definition we have $E_j = E^{H_j}$. As well, it is clear that $y_j \in E^{H_j}$, therefore $\mathbb{Q}(y_j) \subset E_j$. On the other hand, we know that $Gal(\mathbb{Q}(y_j)/\mathbb{Q})$ is a cyclic subgroup (by Theorem 1.1.4), hence and from Theorem 1.1.3, (4) $\mathbb{Q}(y_j)/\mathbb{Q}$ is a Galois extension. Then, from Theorem 1.1.3, (2) we have $\mathbb{Q}(y_j) = E^{Gal(E/\mathbb{Q}(y_j))}$. Thus $\mathbb{Q}(y_j) = E_j$ if and only if $Gal(E/\mathbb{Q}(y_j)) = H_j$.

It is clear that $H_j \subset Gal(E/\mathbb{Q}(y_j))$. Let $\sigma \in Gal(E/\mathbb{Q}(y_j))$, then $\sigma(y_j) = y_j$, and this implies

$$\sum_{\gamma \in H_j} \sigma\gamma(\zeta) = \sum_{\gamma \in H_j} \gamma(\zeta)$$

From this equality, equation (1.1) and Remark 1.2.3 we have two sums of $|H_j|$ powers of ζ, then from Lemma 1.2.4 follows that the two sets of exponents of these powers are equal i.e., $\sigma H_j = H_j$, thus $\sigma \in H_j$. This completes the proof of $Gal(E/\mathbb{Q}(y_j)) = H_j$. $\square$

1.3 A known case: $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta)$

In this subsection $p \geq 3$ is prime and $\zeta = e^{2\pi i/p}$ a primitive root of unity.

Lemma 1.3.1. *The subgroup of $\mathbb{Z}_p^\times$ of order $\dfrac{p-1}{2}$ is:*

$$R = \left\{ a \in \mathbb{Z}_p^\times : \left(\frac{a}{p}\right) = 1 \right\}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. (R is the subgroup of quadratic residues *mod p).*

Proof. By Lemma 1.1.2 we know that there is an unique subgroup of each order d that divides $p-1$. For a proof of the rest of the lemma see, e.g., Corollaries 1 and 2 in [3], p. 51. $\square$

Proposition 1.3.2. *Let $\mathcal{G} = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a$ (a Gauss sum), then*

(1) $\mathcal{G} = 1 + 2\sum_{a \in R} \zeta^a$ with R as in the previous lemma.

(2) If $p \equiv 1 \pmod 4$ then $\mathcal{G} = \sqrt{p}$.

Proof. (1): $\mathcal{G} = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a + \left(1 + \sum_{a=1}^{p-1} \zeta^a\right) = 1 + 2\sum_{a\in R} \zeta^a$.

(2): From (1) and Lemma 1.3.1 we have $\mathcal{G} = \sum_{a=0}^{p-1} \zeta^{a^2}$. For a proof of $\sum_{a=0}^{p-1} \zeta^{a^2} = \sqrt{p}$ if $p \equiv 1 \pmod 4$ see, e.g., [2], pp. 13-16. □

Corollary 1.3.3. *Suppose $p \equiv 1 \ (mod\ 4)$ and let $y = \sum_{a\in R} \zeta^a$. Then:*

(1) $\mathbb{Q}(y)$ is the quadratic p-th cyclotomic field, i.e. it is the quadratic intermediate field of $\mathbb{Q}(\zeta)/\mathbb{Q}$.

(2) $\mathbb{Q}(y) = \mathbb{Q}(\sqrt{p})$.

Remark 1.3.4. Let $K/\mathbb{Q}$ be an extension field such that $K = \mathbb{Q}(a + b\alpha)$ with $a, b \in \mathbb{Q}$ and $\alpha \in \mathbb{C}$. Then it is easy to see that $K = \mathbb{Q}(\alpha)$.

Proof. We know that there is only one quadratic subfield of $\mathbb{Q}(\zeta)$ (see Corollary 1.1.6 aforementioned). From Proposition 1.3.2 it follows that $\sqrt{p} = 1 + 2y \in \mathbb{Q}(\zeta)$, thus $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta)$. By Remark 1.3.4 $\mathbb{Q}(1 + 2y) = \mathbb{Q}(y)$, hence $\mathbb{Q}(y) = \mathbb{Q}(\sqrt{p})$. □

2 Algorithm and Results

In this section we will use the same notation as in the previous section. Let us make two more remarks:

Remark 2.0.5. Recall that $[\mathbb{Q}(y_j) : \mathbb{Q}] = 2^j$, i.e. $\mathbb{Q}(y_j)$ is a vector space over $\mathbb{Q}$ of dimension 2^j.

Definition 2.0.6 (Vectors of Variables)**.** Let $p = 2^k n + 1$ be a prime, with $(2, n) = 1$. Let $V_0 = (1)$ be a vector in $\mathbb{C}$ and, for $0 < j \leq k$, $V_{j+1} = (V_j, y_{j+1}V_j) \in \mathbb{C}^{2^j}$, where $y_{j+1}V_j$ is the standard scalar product of the scalar $y_{j+1} \in \mathbb{C}$ and the vector V_j.

Example 2.0.7. $V_1 = (1, y_1)$,
$V_2 = (1, y_1, y_2, y_1y_2)$,
$V_3 = (1, y_1, y_2, y_1y_2, y_3, y_1y_3, y_2y_3, y_1y_2y_3)$.

Lemma 2.0.8. *Let $m = 2^j$ and $V_j = (v_{1j}, \ldots, v_{mj})$ as before. Then $\mathbb{Q}(y_j) = \mathbb{Q}^m \cdot V_j = \{\mathbf{c} \cdot V_j = \sum_{\ell=1}^{m} c_\ell v_{\ell j},\ with\ \mathbf{c} \in \mathbb{Q}^m\}$.*

Proof. If $j = 1$ then $\mathbb{Q}(y_1) = \{a + by_1 = (a, b) \cdot V_1$ with $a, b \in \mathbb{Q}\}$. The lemma follows by induction on j because of $\mathbb{Q}(y_{j+1}) = \mathbb{Q}(y_j)(y_{j+1})) = \{A + By_{j+1} : A, B \in \mathbb{Q}(y_j)\}$. Therefore, by the inductive hypothesis $A = \mathbf{c_1} \cdot V_j$ and $B = \mathbf{c_2} \cdot V_j$ with $\mathbf{c_i} \in \mathbb{Q}^{2^j}$, thus $A + By_j = (\mathbf{c_1}, \mathbf{c_2}) \cdot (V_j, y_{j+1}V_j) = \mathbf{c} \cdot V_{j+1}$ with $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2}) \in \mathbb{Q}^{2m}$. But $2m = 2^{j+1}$. $\square$

Corollary 2.0.9. *If $j \geq 1$, then y_j is a root of some equation:*

$$y_j^2 + \mathbf{c} \cdot V_j = 0$$

where $\mathbf{c} \in \mathbb{Q}^m$ with $m = 2^j$.

Proof. We have that $a + by_j + y_j^2 = 0$ for some $a, b \in \mathbb{Q}(y_{j-1})$. By the previous lemma $a + by_j \in \mathbb{Q}^m \cdot V_j$. $\square$

2.1 Main algorithm

We use Mathematica for running our algorithms. For details about the commands used see [9].

For running the main algorithm we need another algorithm for calculating a generator of $\mathbb{Z}_p^\times$. See Table 1 for its description. Table 3 has the generators for the first forty prime numbers $p \equiv 1 \pmod 4$.

The algorithm for calculating the y_j is described in Table 2, and Table 4 has the results for y_2 and y_3 and for the first forty prime numbers $p \equiv 1 \pmod 4$.

Table 1: Generator

Mathematica code
$p =$ *input prime number value*;
$d =$Complement[Divisors[$p-1$], $\{1, p-1\}$];
$l =$DivisorSigma[$0, p-1$] $- 2$;
For[$a = 2, a < p$,
$b =$Table[PowerMod[$a, d[[j]], p$], $\{j, l\}$];
$c = 0$;
Do[If[$b[[j]] == 1, c == 0, c = c + 1$], $\{j, l\}$];
IF[$c == 1, g = a$;Print[g];Break[ ]]; $a++$]

Table 2: Main Algorithm

Mathematica Code
$p =$ (*Input a Prime*);
$g =$ (*Input a Generator*);
$q = p-1$; $F =$FactorInteger$[q]$; $k =$F[[1]][[2]]; $n = q/2^k$;
$P =$Sum$[\zeta^{(i-1)}, \{i, p\}]$
(*Variables*)
$V[0] = \{1\}$; Do$[V[i] =$Union$[V[i-1], V[i-1] * ye_i], \{i, k\}]$;
(*Intermediate Field $0 < ne \leq k$*)
$ne =$ (*Number "j" *) ; $o[ne] = 2^{k-ne} n$; $nv = 2^{ne}$;
(*Galois Group*)
$H[ne] =$Table[PowerMod$[g, j * q/o[ne], p], \{j, o[ne]-1\}]$;
$y_{ne} =$Sum$[\zeta^{H[ne][[j]]}, \{j, o[ne]\}]$; $V[ne]$;
Do$[v[i] =$PolynomialRemainder[Expand$[V[ne][[i]]], P, \zeta], \{i, nv\}]$;
$v[nv+1] =$PolynomialRemainder[Expand$[ye[ne]^2], P, \zeta]$; $v[ne+2] = P$;
$vvf =$Table[Coefficient$[v[i], \zeta, j-1], \{i, nv+2\}, \{j, p\}]$;
$vvc =$Transpose$[vvf]$; $coef = NullSpace[vvc]$;
(*Radicals expression for y_{ne}*)
$Ve[0] = \{1\}$; Do$[Ve[i] =$Union$[Ve[i-1], Ve[i-1] * y_i], \{i, k\}]$;
$Ec[ne] =$Sum$[coef[[1]][[i]] * Ve[ne][[i]], \{i, nv\}] + coef[[1]][[nv+1]] * y_{ne}^2$
$y_{ne-1} =$(*Input Previous Result*); Solve$[Ec[ne] == 0, y_{ne}]$

2.2 Meaning of Results on Table 4

The results for y_2 are of the following form, with the β's given by Table 4.

$$y_2 = \frac{1}{4}\left(-1 + \sqrt{p} + \sqrt{(-1)^r 2p + 2\beta\sqrt{p}}\right) \text{ where } r = \frac{p-1}{4}.$$

All the results for y_3, with $p \equiv 1 \pmod 8$ have a much more complicated form: The c, c', c'' are given in Table 4 and $r' = \frac{p-1}{8}$.

Let $\rho_1 = \sqrt{p}$ and $\rho_2 = \sqrt{(-1)^r 2p + 2\beta\sqrt{p}}$, then

$$y_3 = \frac{1}{8}\left(4y_2 \pm \sqrt{(-1)^{r'} 4p + 4c\rho_1 + 2c'\rho_2 + 2c''\rho_1\rho_2}\right).$$

Table 3: Primes $p = 2^k n + 1$ with $(n, 2) = 1$ & Generator g of $\mathbb{Z}_q$

p	k	n	g	p	k	n	g
5	2	1	2	257	8	1	3
13	2	3	2	281	3	35	3
17	4	1	3	313	3	39	10
29	2	7	2	337	4	21	10
37	2	9	2	401	4	25	3
41	3	5	6	409	3	51	21
53	2	13	2	433	4	27	5
61	2	15	2	449	6	7	3
73	3	9	5	457	3	57	13
89	3	11	3	521	3	65	3
97	5	3	5	577	6	9	5
101	2	25	2	593	4	37	3
109	2	27	6	601	3	75	7
113	4	7	3	641	7	5	3
137	3	17	3	673	5	21	5
149	2	37	2	769	8	3	11
157	2	39	5	881	4	55	3
193	6	3	5	929	5	29	3
233	3	29	3	977	4	61	3
241	4	15	7	1153	7	9	5

Table 4: Results for y_2 and y_3

p	β	c	c'	c''	p	β	c	c'	c''
5	-1				257	-1	15	15	1
13	3				281	-5	-9	9	-1
17	-1	3	-3	-1	313	-13	5	5	-1
29	-5				337	-9	7	7	1
37	-1				401	-1	3	-3	-1
41	-5	-3	-3	-1	409	3	11	11	1
53	7				433	-17	19	-19	-1
61	-5				449	7	-21	21	-1
73	3	1	-1	1	457	-21	13	13	-1
89	-5	9	-9	1	521	11	-3	-3	-1
97	-9	-5	5	-1	577	-1	-17	-17	1
101	-1				593	23	-9	-9	1
109	3				601	-5	-23	23	1
113	7	-9	-9	1	641	-25	-21	21	-1
137	11	3	3	1	673	23	-10	10	-1
149	7				769	-25	11	-11	-1
157	11				881	-25	-9	-9	1
193	7	11	-11	-1	929	23	27	-27	-1
233	-13	-15	15	1	977	31	3	-3	-1
241	15	-13	13	-1	1153	-33	-1	-1	1

Lemma 2.2.1. *Let $p \equiv 1$ (mod 4) be a prime. Then there is a unique pair of positive integers a, b with b odd (and hence a even) such that $p = a^2 + b^2$.*

Proof. For existence of integers a, b sucht that $p = a^2 + b^2$ see, e.g., [8], p. 156, or [1], pp. 17-22. It is clear that only one of them is odd.

Uniqueness: Let $R = \mathbb{Z}[i]$ the ring of gaussian integers. We will use the following three known facts: (a) R is a unique factorization domain, (b) if the for norm of $\alpha \in R$ is a rational prime, then α is irreducible in R, and (c) the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. Hence if $\alpha = a+ib$, $\beta = c+id$ and $p = a^2+b^2 = c^2+d^2$, then $p = \alpha\bar{\alpha} = \beta\bar{\beta}$ with the bar indicating complex conjugation. Therefore α and β are associates, i.e., there exists a unit $u \in R$ such that $\beta = u\alpha$. □

With the notations as in Table 4 and previous Lemma, we can rewrite the constants in this table as follows.

Remark 2.2.2. Let $p \leq 1153$, $p \equiv 1$ (mod 4) be a prime. Then we have:

(1) $\beta = (-1)^{\ell} b$ where $\ell = \dfrac{b+1}{2}$ and b as in Lemma 2.2.1.

(2) For such primes with $p \equiv 1$ (mod 8) we have: $c = (-1)^{r'+s} c_p$, $c' = (-1)^{r'+t} c_p$ and $c'' = (-1)^{r'-(s+t)}$, with c_p, s, t obtained from Table 4.

3 Conjecture statement

Now we can state the following:

Conjecture 3.0.3. *Let $p = a^2 + b^2 \equiv 1$ (mod 4) be a prime where b is odd, and let K be the biquadratic p-th cyclotomic field. Then $K = \mathbb{Q}(y_+) = \mathbb{Q}(y_-)$ where*

$$y_{\pm} = \frac{1}{4}\left(-1 + \sqrt{p} \pm \sqrt{(-1)^r 2p + (-1)^{\ell} 2b\sqrt{p}}\right)$$

with $r = (p-1)/4$ and $\ell = (b+1)/2$.

We can verify this conjecture in the following case:

Example 3.0.4. For $p = 5$ we have

$$y_{\pm} = \frac{1}{4}\left(-1 + \sqrt{5} \pm i\sqrt{10 + 2\sqrt{5}}\right)$$

and it is easy to see by direct calculation that $y_{\pm}$ are roots of $x^4 + x^3 + x^2 + x + 1 = 0$ i.e., $y_{\pm}$ are conjugates of $\zeta = e^{2\pi i/5}$. Then $\mathbb{Q}(\zeta) = \mathbb{Q}(y_{\pm})$ because of the next

Proposition 3.0.5. *Let p be a prime and $\zeta = e^{2\pi i/p}$, then $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^d)$ for all $d = 1, \dots, p-1$.*

Proof. It is clear that $\mathbb{Q}(\zeta^d) \subset \mathbb{Q}(\zeta)$. Since $d < p$ we have $(d, p) = 1$; this implies that there are integers k, ℓ such that $1 = kd + \ell p$. Hence $\zeta = (\zeta^d)^k$, then $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta^d)$ follows. □

Remark 3.0.6. Conjecture 3.0.3 implies that our algorithm can be used for finding integers a, b such that $p = a^2 + b^2$. In a forthcoming paper [6] we consider another approach to study all the quadratic field extensions E/F such that $\mathbb{Q} \subset F \subset E \subset \mathbb{Q}(\zeta)$. This is a natural extension of the present paper, in a more general setting.

Acknowledgment

The results of this paper were obtained during my graduate studies at Universidad Simón Bolívar and are also contained in [5]. I would like to express deep gratitude to my supervisor Dmitry Logachëv whose guidance was crucial for the successful completion of this project.

References

[1] Aigner, M., Ziegler, G. M., *Proofs from The Book* (second edition), Springer-Verlag, 2000.

[2] Davenport, H., *Multiplicative Number theory* (second edition), Springer-Verlag, 1967.

[3] Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1972.

[4] Lang, S., *Algebraic Number Theory*, Addison-Wesley, 1970.

[5] Pérez, A. A. J., *Cálculo Explícito de Extensiones Policuadráticas Ciclotómicas de* $\mathbb{Q}$, Tesis de Maestría, Universidad Simón Bolívar, 2001.

[6] Pérez, A. A. J., *Equations of Polyquadratic Cyclotomics Extensions of* $\mathbb{Q}$, in preparation.

[7] Rotman, J., *Galois Theory*, Springer-Verlag, 1990.

[8] Silverman, J. H., *A Friendly Introduction to Number Theory*, Prentice Hall, 1997.

[9] Wolfram, S., *Mathematica* (2nd edition), Addison-Wesley,1993.