Algorithm for Generating Primes for the Giuliani-Gong Public Key System

Maciej Grześkowiak *
Adam Mickiewicz University
Faculty of Mathematics and Computer Science
Umultowska 87, 61-614 Poznań, Poland
maciejg@amu.edu.pl

Abstract

In this paper we propose an algorithm for computing large primes p and q such that q divides $p^4+p^3+p^2+p+1$ or $p^4-p^3+p^2-p+1$. Such primes are key parameters for the Giuliani-Gong Public Key System.

Keywords: Prime generation, Public key system, Algorithm

1 Introduction

Let Φ_n be the nth cyclotomic polynomial; this is a unique monic polynomial whose roots are the primitive nth roots of unity. Algorithms for computing roots of cyclotomic polynomials modulo a prime play an important role in cryptography. They are utilized for computing key parameters (primes of special forms) in cryptosystems which work in an extension of finite field $\mathbf{F}_p$ [2], [3], [4], [7]; In that cryptosystems we need to generate primes p and q such that q divides $\Phi_n(p)$. From the security point of view it is essential to find a prime p such that $\Phi_n(p)$ has a large prime factor q having at least 160 bits to make DLP Problem in subgroup of order q of $\mathbf{F}_{p^n}^*$ intractable. On the other hand, one should find a prime p such that $n\log p \approx 2048$ to obtain security equivalent to factoring a positive integer having 2048 bits.

For instance, the XTR Public Key System [2] requires generating primes p and q such that q divides $\Phi_6(p)$. In the Gong-Harn Public Key System, it is essential to generate a prime q dividing $\Phi_3(p^{2k})$, where k is a fixed positive integer. In 2003, Giuliani and Gong [4] proposed a system analogous to both the Gong-Harn and the XTR Public Key Systems using fifth-order characteristic sequences over $\mathbf{F}_p$. In order to generate key parameters to both cryptosystems one should find large primes p and q such that q divides $\Phi_5(p)=p^4+p^3+p^2+p+1$ in the Gong-Harn case and $\Phi_{10}(p)=p^4-p^3+p^2-p+1$ in the XTR case. Giuliani and Gong suggested that the parameters p and q can be chosen using an algorithm similar to that given in [2]. We briefly recall the idea of the algorithm. The algorithm consists of two procedures. The first one randomly selects a prime $q \equiv 1 \pmod 5$ and computes r_i, the roots of $\Phi_5(x) \pmod q$, where $i=1,\ldots,4$. The second procedure finds a prime $p \equiv r_i \pmod q$ (so q divides $\Phi_5(p)$). However, a method for computing roots of $\Phi_5(x) \pmod q$ was not given there, but we can apply known algorithms to find roots of $\Phi_5(x) \pmod q$. On the one hand, we can use the deterministic method, analogous to Cardano's formulas, for finding roots of $\Phi_5(x) \pmod q$. But such an approach is connected with computing both cubic and square roots modulo q, if the roots exist. On the other hand, we can apply probabilistic algorithm, similar to that for finding a generator $\pmod q$, to find roots of $\Phi_5(x) \pmod q$. But in order to estimate the computational complexity of such an approach we need to have knowledge about prime factors of $q-1$. For this reason estimation of running time of the such procedure can be difficult.

Journal of Internet Services and Information Security, volume: 1, number: 2/3, pp. 21-31
*Partially supported by Ministry of Science and Higher Education, grant N N206 2701 33, 2007–2010

1.1 Main Result of This Paper

We propose a new method of finding primes p and q such that q divides $\Phi_5(p)$ or $\Phi_{10}(p)$. In particular, we present a new, deterministic, polynomial time algorithm for finding roots of polynomials $\Phi_5(x)$ or $\Phi_{10}(x) \pmod q$, where $q = a^2 - ab - b^2 \equiv 11 \pmod{20}$ and $a, b \in Z$. Our method of finding the roots reduces to performing only one exponentiation and two inversion modulo q. Achieving the described goals is made possible by generating the prime q, which is a value of a primitive quadratic polynomial of two variables with integer coefficients. We prove that the procedure for finding a prime of such form is random and executes in polynomial time.

The rest of this paper is organized as follows. In Section 3 we introduce the notation used throughout the paper. Section 4 presents our algorithm. In Section 5 we proving correctness of the algorithm. The running time is discussed in Section 6.

1.2 Notation

Throughout this paper, $K = Q(\omega) = \{x + y\omega : x, y \in Q\}$ denotes the quadratic number field with the ring of integers $\mathcal{O}_K = \{a + b\omega : a, b \in Z\}$. The field K is obtained from Q by adjoining $\omega = (-1+\sqrt{5})/2$ the root of irreducible over the rationals polynomial $g(x) = x^2 + x - 1$. We will denote by $\overline{\omega} = (-1-\sqrt{5})/2$ the second root of $g(x)$ and $\varepsilon = (1+\sqrt{5})/2$ denotes the fundamental unit of K. The symbol $N(\alpha) = (x + y\omega)(x + y\overline{\omega})$ will denote the norm of any element $\alpha = x + y\omega \in K$ with respect to Q. Here and throughout, $\rho(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha))$ denotes the geometric representation of the number $\alpha \in K$, where $\sigma_1(\alpha) = x + y\omega$, $\sigma_2(\alpha) = x + y\overline{\omega}$ are different embedding of K into R. That is $\rho(\alpha) = (x + y\omega, x + y\overline{\omega})$ is the point of the space R^2. By the norm $N(\rho(\alpha))$ of any point $\rho(\alpha)$, we shall understand $N(\rho(\alpha)) = \sigma_1(\alpha)\sigma_2(\alpha)$, so that $N(\rho(\alpha))$ coincides with $N(\alpha)$, $\alpha \in K$. We write $\alpha \gg 0$ to indicate that $\alpha \in K$ is a totally positive number. We will denote by $\mathcal{X}$ the fundamental domain for the field K, and by $\mathcal{L}(\mathcal{O}_K)$ the 2-dimensional lattice in R^2 which consists of all images $\rho(\alpha)$, where $\alpha \in \mathcal{O}_K$. The interested reader is referred to [9], p. 315 for an illustration of $\mathcal{X}$ for arbitrary quadratic number field. The reader is cautioned that our notation is in conflict with that of [9].

2 The Algorithm

We define the sets

$$R(x) \quad = \quad \{\alpha \in \mathcal{O}_K : \quad x \le |N(\alpha)| \le 2x, \quad \rho(\alpha) \in \mathcal{X}\}$$

and

$$S(x) \quad = \quad \{\beta \in \mathcal{O}_K : \quad \beta = \varepsilon^i \alpha, \quad \alpha \in R(x), \quad i = 1, \ldots, 60\}.$$

Let us fix $n = 5$ or $n = 10$. We describe an algorithm which generate primes p and q such that q divides $\Phi_n(p)$. The algorithm consist of the three following procedures.

Procedure FINDPRIMEQ(k, l, x). Let us fix $k, l \in N$, $(k, l) = 1$, $k^2 - kl - l^2 \equiv 11 \pmod{20}$, where $k + l\omega \gg 0$ and let $x > 1$. This procedure finds $a + b\omega \in S(x)$, where $a \equiv k \pmod{20}$, $b \equiv l \pmod{20}$ and $a + b\omega \gg 0$, such that $N(a + b\omega) = q$ is a prime. We assume that $x \le q \le 2x$.

1. Choose $a + b\omega$ at random in $S(x)$ such that $a \equiv k \pmod{20}$, $b \equiv l \pmod{20}$ and $a + b\omega \gg 0$.
2. Compute $q = a^2 - ab - b^2$. If q is a prime, then terminate the procedure. Otherwise go to step 1.

3. Return a, b and q.

Procedure FINDROOTMODULOQ(a,b,q). Let $n = 5$ or $n = 10$. Given a prime q and a,b such that $q = a^2 - ab - b^2 \equiv 11 \pmod{20}$, this procedure computes r a root of $\Phi_n(x)$ modulo q.

1. Compute x_0, y_0 such that $-(a+b)x_0 - ay_0 = 1$
2. Compute $s = -(ax_0 + by_0) \pmod{q}$.
3. Compute $t = (s^2-4)^{(q+1)/4} \pmod{q}$
4. Compute $w = (s-t)2^{-1} \pmod{q}$
5. If $n = 5$, then $r = w$. If $n = 10$, then $r \equiv -w \pmod{q}$.
6. Return r.

Procedure FINDPRIMEP(r,q). Given a prime q and $r < q$, this procedure finds a prime $p \equiv r \pmod{q}$.

1. Choose randomly $m \in N$.
2. Compute $p = qm + r$. If p is a prime, then terminate the procedure. Otherwise go to step 1.
3. Return p.

Algorithm 1 Generating primes p and q, such that $q|\Phi_n(p)$

Input: $k + l \in N : (k,l) = 1, k^2 - kl - l^2 \equiv 11 \pmod{20}, k + l\omega \gg 0; n = 5$ or $n = 10; x > 1$.
Output: Primes p and q such that $q|\Phi_n(p)$.

1: FINDPRIMEQ(k,l,x);
2: FINDROOTMODULOQ(a,b,q,n);
3: FINDPRIMEP(r,q);
4: **Return** p, q;

3 Correctness of the Algorithm

Theorem 3.1. *Let us fix $n = 5$ or $n = 10$. Then Algorithm 1 generates primes p and q such that q divides $\Phi_n(p)$.*

Proof. We begin by proving three auxiliary lemmas.

Lemma 3.1. *Let $\alpha = a + b\omega \in \mathcal{O}_K$, where $|N(\alpha)|$ is a prime. If there exists $\beta \in \mathcal{O}_K$, $\beta = -r + (r-1)\omega$, for some $r \in Z$ such that $N(\alpha)$ divides $N(\beta)$, then $r \equiv -(ax_0 + by_0) \pmod{|N(\alpha)|}$, where $(a+b)x_0 + ay_0 = -1$ or $r \equiv (b-a)x_1 + (a-2b)y_1 \pmod{|N(\alpha)|}$, where $(2b-a)x_1 + (2a-3b)y_1 = 1$.*

Proof. Suppose that there is $\beta = -r + (r-1)\omega$, $r \in Z$ such that $N(\alpha)$ divides $N(\beta)$, so $\alpha|N(\beta)$ and $\overline{\alpha}|N(\beta)$. Since $|N(\alpha)|$ is a prime, hence α is a prime element of $\mathcal{O}_K$ and we have two cases.
Case I: $\alpha|\beta$. We shall prove that $r \equiv -(ax_0 + by_0) \pmod{|N(\alpha)|}$, where $(a-b)x_0 + ay_0 = -1$. If $\alpha|\beta$, then there exists $\gamma \in \mathcal{O}_K$, $\gamma = x + y\omega$, $x, y \in \mathbf{Z}$ such that $\alpha\gamma = \beta$. Hence

$$ax + by + (bx + (a-b)y)\omega = -r + (r-1)\omega$$

and we have

$$\begin{cases} ax+by=-r \\ bx+(a-b)y=r-1. \end{cases} \tag{1}$$

Substituting the first equation to the second one we get

$$(a+b)x+ay=-1. \tag{2}$$

Since $|N(\alpha)|$ is a prime, so $(a,b)=1$ and conseguently $(a+b,a)=1$. Hence there exists an integer solution x_0,y_0 of (2). It can be found by applying the extended Euclid's algorithm. Consequently, by (1) $r\equiv -(ax_0+by_0) \pmod{|N(\alpha)|}$.
Case II: $\alpha|\overline{\beta}$. We shall prove that $r\equiv (b-a)x_1+(a-2b)y_1 \pmod{|N(\alpha)|}$, where $(2b-a)x_1+(2a-3b)y_1=1$ in this case. If $\alpha|\overline{\beta}$, then there exists $\gamma\in\mathscr{O}_K$, $\gamma=x+y\omega$, $x,y\in\mathbf{Z}$ such that $\alpha\gamma=\overline{\beta}$. We have $\omega+\overline{\omega}=-1$, and so

$$(a-b)x+(2b-a)y-(bx+(a-b)y)\overline{\omega}=-r+(r-1)\overline{\omega}.$$

Hence

$$\begin{cases} (a-b)x+(2b-a)y=-r \\ bx+(a-b)y=1-r. \end{cases} \tag{3}$$

Substituting the first equation to the second one we get

$$(2b-a)x+(2a-3b)y=1. \tag{4}$$

Since $(a,b)=1$ then $(2b-a,2a-3b)=1$. Hence there exists an integer solution x_1,y_1 of (4). It can be found by applying the extended Euclid's algorithm. Consequently, by (3) $r\equiv((b-a)x_1+(a-2b)y_1) \pmod{|N(\alpha)|}$. This finishes the proof. □

Lemma 3.2. *Let $\alpha=a+b\omega\in\mathscr{O}_K$, where $|N(\alpha)|\equiv 1 \pmod 5$ and assume that $|N(\alpha)|$ is a prime. Then the congruence*

$$g(r)=r^2+r-1\equiv 0 \pmod{|N(\alpha)|} \tag{5}$$

is solvable and solutions r_1, r_2 satisfy $r_1\equiv -(ax_0+by_0) \pmod{|N(\alpha)|}$, where $(a+b)x_0+ay_0=-1$ and $r_2\equiv (b-a)x_1+(a-2b)y_1 \pmod{|N(\alpha)|}$, where $(2b-a)x_1+(2a-3b)y_1=1$.

Proof. Let $\alpha=a+b\omega\in\mathscr{O}_K$, $N(\alpha)=|a^2-ab-b^2|\equiv 1 \pmod 5$, and let $|N(\alpha)|$ be a prime. First, note that the solutions of (5) exists. Indeed $|N(\alpha)|\equiv 1 \pmod 5$, and so 5 is a quadratic residue modulo $|N(\alpha)|$. Hence ω, $\overline{\omega}$ modulo $|N(\alpha)|$ exist, so the solutions of (5) exists. Finally, we shall compute the values r_i, $i=1,2$ modulo $|N(\alpha)|$. We have

$$\begin{aligned} 0 &\equiv r_i^2+r_i-1 \pmod{|N(\alpha)|} \\ &\equiv (-r_i+(r_i-1)\omega)(-r_i+(r_i-1)\overline{\omega}) \pmod{|N(\alpha)|} \\ &\equiv N(\beta) \pmod{|N(\alpha)|}, \end{aligned}$$

where $\beta=(-r_i+(r_i-1)\omega) \pmod{|N(\alpha)|}$. Hence $N(\alpha)|N(\beta)$. Since β can be considered as an element of $\mathscr{O}_K$, then Lemma 3.1 shows that the assertion of the Lemma follows. This finishes the proof. □

Lemma 3.3. *Let ξ_5 be a primitive 5th root of unity and let $g(x) = x^2 + x - 1 \in Z[x]$. Then $g(x)$ is the minimal polynomial of $\eta_i = \xi_5^i + \xi_5^{-i}$, $i = 1, 2$.*

Proof. We have

$$(x - \eta_1)(x - \eta_2) = x^2 - (\eta_1 + \eta_2)x + \eta_1\eta_2.$$

We shall compute the coefficients of $g(x)$. We have

$$\Phi_5(\xi_5) = \xi_5^4 + \xi_5^3 + \xi_5^2 + \xi_5 + 1 = 0,$$

dividing by ξ_5^2 we obtain

$$\xi_5^2 + \xi_5 + 1 + \xi_5^{-1} + \xi_5^{-2} = 0.$$

Thus

$$\eta_1 + \eta_2 = -1.$$

A short computation yields

$$\eta_1\eta_2 = (\xi_5 + \xi_5^{-1})(\xi_5^2 + \xi_5^{-2}) = \xi_5^3 + \xi_5^{-1} + \xi_5 + \xi_5^{-3} = \xi_5^{-2} + \xi_5^{-1} + \xi_5 + \xi_5^2 = -1.$$

Note that $\eta_j = e^{2j\pi i/5} + e^{-2j\pi i/5} \in R$, so $g(x)$ is the minimal polynomial of η_i. □

Proof of Theorem 3.1. Let us assume that numbers $k, l \in N$, $(k,l) = 1$, $k^2 - kl - l^2 \equiv 11 \pmod{20}$ and $n \in \{5, 10\}$ are the input to the algorithm. The algorithm executes the procedure FINDPRIMEQ in the first step. Let us assume that a, b, and q are the output of this procedure. Then q is a prime such that $q = a^2 - ab - b^2$, $a \equiv k \pmod{20}$, $b \equiv l \pmod{20}$, $a + b\omega \gg 0$. We shall show that the procedure FINDROOTMODULOQ, with the input a, b, q and n, computes r such that $\Phi_n(r) \equiv 0 \pmod{q}$. Firstly, suppose that $n = 5$. It is an elementary check that $q \equiv 1 \pmod{5}$. Lemma 3.2 shows that the solutions of $g(x) = x^2 + x - 1 \equiv 0 \pmod{q}$ exists and one of them is given by $s \equiv -(ax_0 + by_0) \pmod{q}$, where $(a-b)x_0 + ay_0 = -1$. By Lemma 3.3, $s \equiv \xi_5 + \xi_5^{-1} \pmod{q}$ or $s \equiv \xi_5^2 + \xi_5^{-2} \pmod{q}$. Hence ξ_5, ξ_5^2 are the roots of $g(x) = x^2 - sx + 1 \pmod{q}$ and one of them is equal to $(s + \sqrt{(s^2-4)})/2 \pmod{q}$. Note that $s^2 - 4$ is quadratic residue modulo q. Indeed, $q \equiv 1 \pmod{5}$, so ξ_5 modulo q exist, and hence $\xi_5 \in \mathbf{F}_q$. Suppose that $s^2 - 4$ is quadratic nonresidue modulo q, then $g(x)$ is irreducible modulo q, and so $\xi_5 \in \mathbf{F}_{q^2} \backslash \mathbf{F}_q$. This contradicts the fact that $\xi_5 \in \mathbf{F}_q$. Consequently $(s + \sqrt{(s^2-4)})/2 \pmod{q}$ can be computed. Now, since $q \equiv 3 \pmod{4}$, then computing a square root of $s^2 - 4$ modulo q reduce to performing exponentiation modulo q. Let t the square root of $s^2 - 4 \pmod{q}$, so $t \equiv (s^2-4)^{(q+1)/4} \pmod{q}$. Hence ξ_5 or ξ_5^2 is equal to $(s-t)/2 \pmod{q}$, and putting $r \equiv (s-t)/2 \pmod{q}$ we obtain $\Phi_5(r) \equiv 0 \pmod{q}$. Finally, suppose that $n = 10$. We have $\Phi_5(x) = \Phi_{10}(-x)$, so $\Phi_{10}(-r) \equiv 0 \pmod{q}$. We have shown that the procedure FINDROOTMODULOQ finds roots of $\Phi_n(x)$ modulo q. Now, let us assume that the procedure FINDPRIMEP returns a prime $p \equiv r \pmod{q}$. Hence $\Phi_n(p) \equiv \Phi_n(r) \pmod{q}$ and so $q | \Phi_n(p)$. This finishes the proof. □

4 Run-time analysis of the Algorithm

4.1 The Procedure FINDPRIMEQ

Let m be a positive integer. We will denote by $\mathscr{PT}$ number of bit operations necessary to carry out the deterministic primality test [5]. For simplicity, assume that $\mathscr{PT}$ takes no less than $O(\log^3 m)$ bit operations.

Theorem 4.1. *Let us fix $k,l \in N$, $(k,l)=1$, $k^2-kl-l^2 \equiv 11 \pmod{20}$, $k+l\omega \gg 0$. Then there exist constants $c>0$ and x_0 such that for every integer $x \geq x_0$ and an arbitrary real $\lambda \geq 1$, the procedure* FINDPRIMEQ *finds $c+d\omega \in S(x)$, $c+d\omega \gg 0$, where $c \equiv k \pmod{20}$, $d \equiv l \pmod{20}$, such that $q=N(c+d\omega)$ is a prime, with probability greater than or equal to $1-e^{-\lambda}$ after repeating $[c\lambda(\log x)]$ steps of the procedure. Every step of the procedure takes no more than $\mathscr{P}\mathscr{T}$ bit operations.*

Proof. We begin by proving three auxiliary lemmas. Let us define the number

$$r_{a,b}(n) = \sharp\{\alpha \in \mathscr{O}_K : |N(\alpha)| = n, \quad \rho(\alpha) \in \mathscr{L}(\mathscr{O}_K) \cap \mathscr{X}\}.$$

Lemma 4.1. *We have*

$$\sum_{n \leq x} r_{a,b}(n) \leq \frac{2x\log\omega}{\sqrt{5}} + O(\sqrt{x}).$$

Proof. Let $v(T)$ denote the volume of the set T which consists of all points $\rho(\alpha)$ of $\mathscr{X}$ for which $|N(\rho(\alpha))| \leq 1$, and let Δ be the volume of fundamental parallelepiped of $\mathscr{L}(\mathscr{O}_K)$. First, we shall prove that

$$\frac{v(T)}{\Delta} = \frac{2\log\omega}{\sqrt{5}}. \tag{6}$$

Consider the Dedekind zeta functions $\zeta_K(s)$, defined for $s=\sigma+it$, $\sigma>1$ by absolutely convergent series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s},$$

where $\mathfrak{a}$ runs through all integral ideals of K, and $N\mathfrak{a}$ denotes the norm of the ideal $\mathfrak{a}$. Since in $\mathscr{O}_K$ all ideals are principal we obtain

$$\zeta_K(s) = \sum_{\substack{(\alpha) \\ \alpha \neq 0}} \frac{1}{|N(\alpha)|^s}, \tag{7}$$

where the summation is taken over all principal ideals of K. Since two principal ideals (α_1) and (α_2) are equal if and only if the numbers α_1 and α_2 are associate, the by (see [9, Theorem 1, p. 313]), we can write (7) in the form

$$\zeta_K(s) = \sum_{\rho(\alpha) \in \mathscr{L}(\mathscr{O}_K) \cap \mathscr{X}} \frac{1}{|N(\rho(\alpha))|^s},$$

where the summation is taken over all points $\rho(\alpha)$ in the lattice $\mathscr{L}(\mathscr{O}_K)$ which are contained in $\mathscr{X}$. Moreover by (see [9, Theorem 3, p. 321]) we have

$$\lim_{s \to 1^+ 0} (s-1) \sum_{\rho(\alpha) \in \mathscr{L}(\mathscr{O}_K) \cap \mathscr{X}} \frac{1}{|N(\rho(\alpha))|^s} = \frac{v(T)}{\Delta}. \tag{8}$$

On the other hand, by (see [9, Theorem 2, p. 313]) we have

$$\lim_{s \to 1^+ 0} (s-1)\zeta_K(s) = \frac{2\log w}{\sqrt{5}},$$

and consequently by the above and (8) the equation (6) holds. Let ηT denotes the set of points ηt, for $\eta \in R$ and $t \in T$, and let $\lambda(\eta) = \lambda(\eta, T, \mathscr{L}(\mathscr{O}_K))$ be the number o point of $\mathscr{L}(\mathscr{O}_K) \cap \mathscr{X}$ in ηT. We shall compute $\lambda(\sqrt{x})$, $x \geq 1$. This follows immediately from (see [6, Theorem 2, p.128]). We have

$$\lambda(\sqrt{x}) = \frac{v(T)}{\Delta} x + O(\sqrt{x}).$$

It is obvious that if $\rho(\alpha) \in \sqrt{x}T$ then $|N(\rho(\alpha))| \leq x$. Hence by the above and (6) we obtain

$$\sum_{n \leq x} r_{a,b}(n) \leq \frac{2x \log \omega}{\sqrt{5}} + O(\sqrt{x}). \tag{9}$$

This finishes the proof. □

Lemma 4.2. *Let us fix $k,l \in N$, $(k,l)=1$, $k^2-kl-l^2 \equiv 11 \pmod{20}$ such that $k+l\omega \in \mathscr{O}_K$, $k+l\omega \gg 0$. Denote by $\pi_{a,b}(x)$ number of primes $q \leq x$ which can be represented in the form $q=a^2-ab-b^2$ with integers $a \equiv k \pmod{20}$, $b \equiv l \pmod{20}$ and $a+b\omega \gg 0$. Then*

$$\pi_{a,b}(x) = \frac{1}{8}\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Proof. Let $\mathfrak{f} = 20\mathscr{O}_K$ be the ideal of $\mathscr{O}_K$, and let

$$A_{\mathfrak{f}} \quad = \quad \{\alpha \in K^* : \alpha = mn^{-1}, m \equiv n \pmod{\mathfrak{f}},\ (mn\mathscr{O}_K, \mathfrak{f}) = 1,\ m,n \in \mathscr{O}_K\},$$

where K^* denote the multiplicative group of K. Let us denote by

$$H_{\mathfrak{f}}^*(K) = G_{\mathfrak{f}}(K)/P_{\mathfrak{f}}^+(K)$$

the group of narrow ray classes mod $\mathfrak{f}$, where $G_{\mathfrak{f}}(K)$ is the group of all fractional ideals of K which are quotients of two ideals prime to $\mathfrak{f}$, and $P_{\mathfrak{f}}^+(K)$ be the subgroup of $G_{\mathfrak{f}}(K)$ consisting of principal fractional ideals generated by elements of $A_{\mathfrak{f}}$ having totally positive generators. Let us fix k and l, $(k,l)=1$, $k^2-kl-l^2 \equiv 11 \pmod{20}$, $k+l\omega \gg 0$. Let $\mathfrak{a} = (k+l\omega)\mathscr{O}_K$ be the ideal in $\mathscr{O}_K$. Since $N(\mathfrak{a}) = k^2-kl-l^2 \equiv 11 \pmod{20}$, so $(\mathfrak{a},\mathfrak{f})=1$. Assume that X is a class in $H_{\mathfrak{f}}^*(K)$ such that $\mathfrak{a} \in X$. Firstly, we shall show that for any prime ideal $\mathfrak{p} \in X$, $N\mathfrak{p}$ the norm of the ideal $\mathfrak{p}$ is equal to a^2-ab-b^2, for some $a \equiv k \pmod{20}$ and $b \equiv l \pmod{20}$ and $a+b\omega \gg 0$. To prove this, consider a prime ideal $\mathfrak{p} \in X$. Then

$$\mathfrak{p}P_{\mathfrak{f}}^+(K) = \mathfrak{a}P_{\mathfrak{f}}^+(K) \Longleftrightarrow \mathfrak{p}\mathfrak{a}^{-1} \quad \in \quad P_{\mathfrak{f}}^+(K) \Longleftrightarrow \mathfrak{p}\mathfrak{a}^{-1} = (\alpha),$$

where $\alpha \in A_{\mathfrak{f}}$, and $\alpha \gg 0$. Set

$$\alpha(k+l\omega) = \beta \tag{10}$$

Then $\beta \gg 0$ and $N(\beta) = N\mathfrak{p}$. Hence $\beta \in \mathscr{O}_K$. On the other hand, since $\alpha \in A_{\mathfrak{f}}$, then $\alpha = mn^{-1}$ where $m \equiv n \pmod{\mathfrak{f}}$, $m,n \in \mathscr{O}_K$ and there exist $u,v \in \mathbf{Z}$ such that $m = 20(u+v\omega)+n$. So $\alpha = (20(u+v\omega)+n)n^{-1}$ and consequently by (10)

$$\beta \quad = \quad \frac{20(u+v\omega)(k+l\omega)}{n} + (k+l\omega),$$

where $n|(u+v\omega)(k+l\omega)$. Thus there exist $s,t \in Z$ such that

$$\beta \quad = \quad 20(s+t\omega) + (k+l\omega)$$

and hence

$$N\mathfrak{p} = (20s+k)^2 - (20s+k)(20t+l) - (20t+l)^2.$$

Secondly, we compute the number prime ideals in X of degree one with norms not exceeding $x \in R$. To do this, we denote by $\pi_X(x)$ the number of prime ideals in X with norms not exceeding n, and by $\pi(x)$

the number of primes $p \leq x$. Then by the rules of decompositions of primes in $Q(\omega)$ (see [9, Theorem 1, p. 236]) we have

$$\pi_X(x) = \sum_{\substack{\mathfrak{p}\in X \\ N\mathfrak{p}\leq x}} 1 = \sum_{\substack{\mathfrak{p}\in X \\ N\mathfrak{p}=p \\ p\leq x}} 1 + \sum_{\substack{\mathfrak{p}\in X \\ N\mathfrak{p}=p^2 \\ p\leq\sqrt{x}}} 1 = \sum_{\substack{\mathfrak{p}\in X \\ N\mathfrak{p}=p \\ p\leq x}} 1 + O(\pi(\sqrt{x})). \tag{11}$$

On the other hand, by the Prime Ideal Theorem for Ideal Classes (see [8, Corollary 11, p. 358]) with a certain constant $B > 0$, $B = B(\mathfrak{f})$ we have

$$\pi_X(x) = \frac{\operatorname{li} x}{h^*_{\mathfrak{f}}(K)} + O(\exp(-B(\sqrt{\log x}))),$$

where $h^*_{\mathfrak{f}}(K)$ denotes the number of elements in $H^*_{\mathfrak{f}}(K)$, and $\operatorname{li} x = \int_2^x \frac{dt}{\log t}$ for $x > 2$. Since

$$\operatorname{li} x = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

then by (11) and by the Prime Number Theorem (see [1, Theorem 2, p. 67]),

$$\sum_{\substack{\mathfrak{p}\in X \\ N\mathfrak{p}=p \\ p\leq x}} 1 = \frac{1}{h^*_{\mathfrak{f}}(K)} \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Finally, we shall prove that $h^*_{\mathfrak{f}}(K) = 8$. Let $h(K)$ denotes the number of elements the class group of K, $\Phi(\mathfrak{f})$ be the number of invertible elements of the factor-ring $\mathcal{O}_K/\mathfrak{f}$, and $\psi(I)$ denotes the number of residue classes $\bmod \mathfrak{f}$ which can be represented by units of K. We have the equality (see [8, Theorem 3.35, p. 109]),

$$h^*_{\mathfrak{f}}(K) = 2^{r_1-t} h(K) \frac{\Phi(\mathfrak{f})}{\psi(\mathfrak{f})},$$

where r_1 denotes the number of different embedding of K into the field of real numbers, and 2^t is the number of possible signatures of units congruent to unity $\bmod \mathfrak{f}$. It is a well-known fact that $h(K) = 1$ (see [9, Table 1, p. 422]), and is obvious that $r_1 = 2$. Moreover, we have

$$\Phi(\mathfrak{f}) = N\mathfrak{f} \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \frac{1}{N\mathfrak{p}}\right) = 20^2 \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{5}\right) = 240.$$

We will prove that $\psi(\mathfrak{f}) = 120$. Let $\varepsilon = (1+\sqrt{5})/2$ be the fundamental unit of K. Then every units of K can be uniquely written of the form $\pm\varepsilon^n$, $n \in \mathbf{Z}$. It is an elementary check that $\varepsilon^{10} \equiv -1 \pmod 5$ and $\varepsilon^6 \equiv 1 \pmod 4$, hence $\varepsilon^{120} \equiv 1 \pmod{20}$, so the order of ε divides 120 modulo 20. It is an elementary check using computer algebra system, that the order of ε modulo 20 is equal to 60. Hence

$$\varepsilon^{60} \equiv 1 \pmod{20}. \tag{12}$$

Assume that $\varepsilon^u \equiv -\varepsilon^w \pmod{20}$ for some integers u, w. Then $\varepsilon^v \equiv -1 \pmod{20}$ for some $0 < v \leq 60$, but this does not hold. Consequently elements $\pm\varepsilon^k$, $k = 1, \ldots, 60$ represent different residue classes $\bmod \mathfrak{f}$, and hence $\psi(\mathfrak{f}) = 120$. Let $\sigma_1 = a + b\omega$, $\sigma_2 = a + b\overline{\omega}$ be different embeddings of K into R. We have $\sigma_1(\omega^{60l}) = \omega^{60l} = \varepsilon^{-60l} > 0$, $\sigma_2(\omega^{60l}) = \overline{\omega}^{60l} = (-\varepsilon)^{60l} > 0$ for $l \in Z$, and hence $t = 0$. Consequently $h^*_{\mathfrak{f}}(K) = 8$. This finishes the proof. □

We define the sets

$$\begin{aligned} P(x) &= \{p-prime : \exists \quad a+b\omega \in \mathscr{O}_K, \quad N(a+b\omega)=p, \quad x \le N(a+b\omega) \le 2x, \\ &\quad a \equiv k \,(\mathrm{mod}\ 20), \quad b \equiv l \,(\mathrm{mod}\ 20), \quad a+b\omega \gg 0\} \end{aligned}$$

and

$$\begin{aligned} T(x) &= \{c+d\omega \in S(x) : N(c+d\omega)=p-prime, \quad c \equiv k \,(\mathrm{mod}\ 20), \\ &\quad d \equiv l \,(\mathrm{mod}\ 20), \quad c+d\omega \gg 0\} \end{aligned}$$

Lemma 4.3. *Let us fix $k, l \in N$, $(k,l)=1$, $k^2-kl-l^2 \equiv 11 \pmod{20}$ such that $k+l\omega \in \mathscr{O}_K$, $k+l\omega \gg 0$. There is an injective function $\Psi : P(x) \to T(x)$.*

Proof. Let $p \in P(x)$, where $p=N(\gamma)$ and $\gamma = a+b\omega$. By (see [9, Lemma 1,p. 313]) $\rho(\gamma)$ has a unique representation in the form $\rho(\gamma)=\rho(\alpha)\rho(\delta)$, where $\rho(\alpha)$ is a point of the fundamental domain $\mathscr{X}$ and δ is a unit of K. Hence $\gamma=\alpha\delta \in \mathscr{O}_K$ and $N(\gamma)=|N(\alpha)|$, so $\alpha \in R(x)$. We shall show that there exists $v \in N$, $1 \le v \le 60$ such that $\alpha\varepsilon^v = c+d\omega \gg 0$ and $c \equiv k \pmod{20}$, $d \equiv l \pmod{20}$. Every units of K can be uniquely written of the form $\pm\varepsilon^t$, where $\varepsilon=(1+\sqrt{5})/2$, $t \in \mathbf{Z}$. Hence $\gamma = \pm\varepsilon^t\alpha$, but $\gamma > 0$, so $\gamma = \varepsilon^t\alpha$. Moreover $\overline{\gamma} > 0$, so

$$\gamma = \begin{cases} \alpha\varepsilon^{2k}, & k \in Z \qquad \text{for} \quad \overline{\alpha} > 0, \\ \alpha\varepsilon^{2k+1}, & k \in Z \qquad \text{for} \quad \overline{\alpha} < 0. \end{cases}$$

Writing $2k = 60i_1+u$ and $2k+1 = 60i_2+v$, where $i_1, i_2 \in Z$, $u, v \in N$, $1 \le u, v \le 60$, we see that there exists and $j \in Z$ such that

$$\gamma\varepsilon^{60j} = \begin{cases} \alpha\varepsilon^u, & u \equiv 0 \,(\mathrm{mod}\ 2), \qquad \text{for} \quad \overline{\alpha} > 0, \\ \alpha\varepsilon^v, & v \equiv 1 \,(\mathrm{mod}\ 2), \qquad \text{for} \quad \overline{\alpha} < 0, \end{cases}$$

where $\alpha\varepsilon^u$ and $\alpha\varepsilon^v$ are totally positive. By (12) $\varepsilon^{60} \equiv 1 \pmod{20}$, hence writing $\alpha\varepsilon^u = c_1+d_1\omega$ and $\alpha\varepsilon^v = c_2+d_2\omega$ we obtain

$$\gamma = a+b\omega \equiv c_i+d_i\omega \,(\mathrm{mod}\ 20),$$

and consequently $a \equiv c_i \pmod{20}$ and $b \equiv d_i \pmod{20}$ and the conclusion holds. Now, it is easy to observe that, if $\Psi(p)=\Psi(q)$, where $p, q \in P(x)$, then $p=q$. This completes the proof. □

Lemma 4.4. *Let us fix $k, l \in N$, $(k,l)=1$, $k^2-kl-l^2 \equiv 11 \pmod{20}$ such that $k+l\omega \in \mathscr{O}_K$, $k+l\omega \gg 0$. Then for every $\varepsilon > 0$ there exists x_0 such that for every $x \ge x_0$ the number of elements of $T(x)$ is no less than $(1-\varepsilon)x(\log x)^{-1}$.*

Proof. Lemmas 4.2 and 4.3 shows that for every $\varepsilon > 0$ the number of elements of $T(x)$ is greater than

$$\pi_{a,b}(2x) - \pi_{a,b}(x) \ge \frac{(1-\varepsilon)x}{\log x}, \tag{13}$$

for sufficiently large x. This completes the proof. □

Proof of Theorem 4.1. Let us denote by $A_{c,d}$ the event that randomly chosen $c+d\omega \in S(x)$, $c \equiv k \pmod{20}$, $d \equiv l \pmod{20}$, $c+d\omega \gg 0$, is such that $N(c+d\omega)$ is a prime. Firstly, we shall compute the probability that in v trials $A_{c,d}$ will occur. By Lemma 4.1 there exist $c_1 > 0$ such that for every $\varepsilon > 0$ the number of element of $S(x)$ is at most

$$\sum_{n \le 2x} r_{a,b}(n) \le (c_1+\varepsilon)x,$$

for sufficiently large x. Hence, by Lemma 4.4 there exists $c_2 > 0$ such that for sufficiently large x the probability that in v trials $A_{c,d}$ does not occur is

$$\begin{aligned}\left(1-\frac{c_2}{\log x}\right)^v &= \exp\left(v\log\left(1-\frac{c_2}{\log x}\right)\right) \leq \\ &\leq \exp\left(\frac{-c_2 v}{\log x}\right) \leq e^{-\lambda},\end{aligned}$$

for an arbitrary real $\lambda \geq 1$ and $v = c_3\lambda\log x$, where $c_3 = c_2^{-1}$. Consequently the probability that in v trials $A_{c,d}$ does occur is greater than or equal to $1-e^{-\lambda}$. So after repeating $[c_3\lambda\log x)]$ steps, the procedure finds $c+d\omega \in S(x)$, $c+d\omega \gg 0$, such that $N(c+d\omega)$ is a prime with probability greater than or equal to $1-e^{-\lambda}$. Finally, we shall estimate the number of bit operations required to carry out the steps of the procedure. It takes a fixed numbers of time to generate a random bit, and $O(\log x)$ bit operations to generate random integers $c \equiv k \pmod{20}$ and $d \equiv l \pmod{20}$, $c+d\omega \gg 0$. Computation $q = c^2 - cd - d^2$ can be done with $O(\log^2 x)$ bit operations. The most time-consuming step of the algorithm is the deterministic primality test for number q which takes no more than $\mathscr{P}\mathscr{T}$ operations. This finishes the proof. □

4.2 The Procedure FINDROOTMODULOQ

Theorem 4.2. *Let $n = 5$ or $n = 10$, and let $\Phi_n(x)$ denote the n-th cyclotomic polynomial. Given a prime q and a, b such that $q = a^2 - ab - b^2 \equiv 11 \pmod{20}$, then the procedure* FINDROOTMODULOQ *finds a root of $\Phi_n(x) \pmod{q}$ using $O(\log^3 q)$ bit operations.*

Proof. The proof follows immediately from the construction of the procedure FINDROOTMODULOQ. The complexity of the procedure is completely determined by the running time of the extended Euclidean algorithm and modular exponentiation algorithm. This finishes the proof. □

References

[1] Karatsuba A. *Basic Analytic Number Theory*. Springer-Verlag, 1993.

[2] Lenstra A. and Verhuel E. The XTR Public Key System. In *Proc. of 20th Annual International Cryptology Conference Crypto 2000, Advances in Cryptology (CRYPTO 2000), Santa Barbara, California, USA, LNCS*, volume 1880, pages 1–19. Springer-Verlag, August 2000.

[3] Gong G. and Harn L. Public-key cryptosystems based on cubic finite field extension. *IEEE Transactions on Information Theory*, 45(7):2601–2605, November 1999.

[4] Giuliani K. and Gong G. Analogues to the Gong-Harn and XTR cryptosystems. Technical Report 34, CORR, The University of Waterloo, 2003.

[5] Agrawal M., Kayal K., and Saxena N. Primes is in P. *Annals of Mathematics*, 160(2):781–793, September 2004.

[6] Lang S. *Algebraic Number Theory*. Springer-Verlag, 1994.

[7] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, and D. Woodruff. Practical cryptography in high dimensional tori. In *Proc. of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology - (EUROCRYPT'05), Aarhus, Denmark, LNCS*, volume 3494, pages 234–250. Springer-Verlag, May 2005.

[8] Narkiewicz W. *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, 2004.

[9] Borevich Z. and Shafarevich I. *Number Theory*. Academic Press, 1966.

Maciej Grześkowiak received the M.Sc. degree in Informatics from Adam Mickiewicz University University, Poznań, Poland in 1999, and Ph.D degree in Mathematics from same institution in 2004. He is currently an assistant professor at the Department of Algebra and Number Theory in Adam Mickiewicz University, Poznań, Poland. His current research interests are computational number theory and cryptography.