Generating a Large Prime Factor of $p^4 \pm p^2 + 1$ in Polynomial Time

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 present a probabilistic polynomial-time algorithm for generating a large prime p such that $\Phi_m(p^2)$ has a large prime factor, where $\Phi_m(x)$ is the $m - th$ cyclotomic polynomial and $m = 3$ or $m = 6$. An unconditionally polynomial time algorithm for generating primes of the above form is not yet known. Generating primes of such form is essential for the GH and the CEILIDH Public Key Systems, since they are key parameters in these cryptosystems.

Keywords: The Gong-Harn Public Key System, CEILIDH Public Key System, Torus-Based Cryptography, primes of a special form.

1 Introduction and Background

Many new cryptosystems have been introduced in recent years which require generating primes of special forms as key parameters. For instance of interest is generating of a large prime p such that $\Phi_m(p^k)$ is divisible by a large prime q, where k is a fixed positive integer and $\Phi_m(x)$ is the m-th cyclotomic polynomial. From the security point of view it is essential to find a prime p such that $m \log p^k \approx 2048$ to obtain a level of security equivalent to factoring a positive integer having 2048 bits. The prime q should have at least 160 bits to make solving DLP in subgroup of order q of $\mathbf{F}^*_{p^k}$ impossible in practice. For $m = 3$, in 1998 Gong and Harn presented a public key system called GH [4], [5]. In 2003 Rubin and Silverberg introduced the idea of Torus-Based Cryptography [10]. In particular, they proposed a public key system called CEILIDH, which requires the generation of special primes p, q for $m = 6$. There exist two main approaches for generating primes of the above form. The first approach was proposed by Gong and Giuliani [6]. The second approach for generating desired primes was proposed by Lenstra and Verheul [9]. We next give an illustration of this algorithm in the case $m = 3$ and $k = 1$. The algorithm randomly selects a prime $q \equiv 7 \pmod{12}$ and computes r_i for $i = 1, 2$ roots of $\Phi_6(x) = x^2 - x + 1 \bmod q$. Alternatively the algorithm finds a positive integer r_3 such that $\Phi_6(r_3) = q$ is a prime. Next the algorithm selects a prime p such that $p \equiv r_i \pmod{q}$ for one

* Supported by Ministry of Science and Higher Education, grant N N201 1482 33.

R. Meersman and Z. Tari (Eds.): OTM 2008, Part II, LNCS 5332, pp. 1140–1149, 2008.

of r_i $i = 1, 2, 3$ (from this q divides $\Phi_6(p)$). It is worth pointing out that the above algorithm works perfectly well in practice. However in the general case, we can encounter some problems. For example let $k = 2$. Consider the naive way of computing the root of the polynomial $\Phi_6(x^2) = x^4 - x^2 + 1 \pmod{q}$, where q is a prime. Substituting $y = x^2$ we reduce the degree of $\Phi_6(x^2) \pmod{q}$ to 2. Next we compute y_1, y_2 roots of $y^2 - y + 1 \pmod{q}$, which requires computing $\sqrt{-3} \pmod{q}$. In the end we compute the square root $\pmod{q}$ of y_i for $i = 1$ or $i = 2$. There are two difficulties, which we can encounter in practice while computing the roots of $\Phi_6(x^2) \pmod{q}$. The first is that we have to use algorithm to compute the square root. Computing of the square root $\pmod{q}$ is basically simple, except for the case where $q \equiv 1 \pmod{8}$, which takes at most $O(\log^4 q)$ [2]. The second problem lies in the handling of square roots when these are not in $\mathbf{F}_q$ (they are then in $\mathbf{F}_{q^2}$ and $\mathbf{F}_{q^4}$ respectively). However the alternative method in the abovementioned algorithm, involving finding a positive integer r_3 such that $\Phi_6(r_3) = q$ is a prime, causes theoretical problem. We do not know if there exist infinitely many primes of the form $\Phi_6(r_3)$. This is an extremely hard, still unproven mathematical problem. The second part of the algorithm also seems problematic. When the modulus q is close to x there are not sufficiently many primes $p \leq x$, to warrant the equidistribution among the residue classes $a \pmod{q}$. To be more precise, let $\pi(x; a, q)$, $1 \leq a \leq q$, $(a, q) = 1$, denote the number of primes $p \equiv a \pmod{q}$ with $p \leq x$. By the Siegel-Walfisz theorem [3] we get that for any fixed $N > 0$, the formula $\pi(x; a, q) = x/(\phi(q) \log x)\{1 + o(1)\}$ holds uniformly throughout the range $q \leq (\log x)^N$ and $(a, q) = 1$. Therefore we cannot apply Siegel-Walfisz theorem to estimate the running time of the second procedure, when q is close to p. Analysis and theoretical estimation of computational complexity of the Lenstra and Verheul algorithm under the assumption of some unproven conjectures can be found in [7]. However an unconditionally polynomial time algorithm for generating desired primes p and q is not yet known.

In this paper we present a new probabilistic algorithm for generating large primes p and q such that $q|\Phi_6(p^2)$ or $q|\Phi_3(p^2)$, which is faster than those previously considered. We prove that the algorithm for finding such a primes is random and executes in polynomial time. We also present the developments and improvements of ideas proposed by Lenstra and Verheul. In particular, we improve the method of finding root of polynomials $\Phi_m(x^2) \pmod{q}$, where $m = 3, 6$ and q is a prime, by reducing the number of computed square roots. Our method require computing only $\sqrt{3} \pmod{q}$ in order to find the root of $\Phi_m(x^2) \pmod{q}$, which is a big improvement over the Lenstra-Verheul method [9]. Achieving the described goals is made possible by generating a prime q, which is a value of a primitive quadratic polynomial of two variables with integer coefficients. We prove that the procedure for finding such prime is random and executes in polynomial time. Moreover we prove Lemma 2, which is slightly weaker than the above Siegel-Walfisz result, but can be applied to estimate computational complexity of finding prime $p \equiv a \pmod{q}$, where p is close to q. Therefore we can prove that our algorithm executes in polynomial time.

2 Generating a Large Prime Factor of $\Phi_m(p^2)$

Our algorithm consists of two procedures. Let us fix $F(x,y) = 144x^2 + 144y^2 + 24y + 1 \in Z[x,y]$. The first procedure generates positive integers $a \in \left[\frac{n}{12\sqrt{2}}, \frac{cn}{12\sqrt{2}}\right]$ and $b \in \left[\frac{n-\sqrt{2}}{12\sqrt{2}}, \frac{cn-\sqrt{2}}{12\sqrt{2}}\right]$ such that $F(a,b) = q$ is a prime, where $n \in \mathbf{N}$ and c is some positive number. The second procedure computes $r \pmod q$ and next finds a positive integer $k \in \left[1, \left[\frac{n^6-r}{q}\right]\right]$ such that the number $qk + r$ is prime.

Algorithm 1. Generating primes p and q, such that $q|\Phi_m(p^2)$ and $m = 3, 6$

```
procedure FindPrimeQ($n$, $F(x,y)$)                      ▷ Input $n$ and $F(x,y)$
    $q \leftarrow 1$
    while not $IsPrime(q)$ do
        $a \leftarrow Random(n)$              ▷ Randomly select $a \in \left[\frac{n}{12\sqrt{2}}, \frac{cn}{12\sqrt{2}}\right]$
        $b \leftarrow Random(n)$              ▷ Randomly select $b \in \left[\frac{n-\sqrt{2}}{12\sqrt{2}}, \frac{cn-\sqrt{2}}{12\sqrt{2}}\right]$
        $q \leftarrow F(a,b)$
    end while
    return $(a,b,q)$
end procedure

procedure FindPrimePModuloQ($a,b,q,m$)                   ▷ Input $a,b,q$ and $m$
    $r \leftarrow (\sqrt{3}(12b+1) - 12a)(-2(12b+1))^{-1} \pmod q$
    if $m = 3$ then
        $r \leftarrow -r$
    end if
    $p \leftarrow 1$
    while not $IsPrime(p)$ do
        $k \leftarrow Random(n)$              ▷ Randomly select $k \in \mathbf{N}$, $k \in \left[1, \left[\frac{n^6-r}{q}\right]\right]$
        $p \leftarrow qk + r$
    end while
    return $(p)$
end procedure

return $(p,q)$
```

Theorem 1. *Let us fix $m = 3$ or $m = 6$. Then Algorithm 1 generates primes p and q such that q divides $\Phi_m(p^2)$. Moreover $q = F(a,b) = N(\gamma)$ and $\Phi_m(p^2) = N(\xi)$, where γ, $\xi \in \mathbf{Z}[i]$, $\gamma \,|\, \xi$ and $\gamma = 12a + (12b+1)i$ and $\xi = (p^2-1) + pi$.*

Proof. Let $\mathbf{Z}[i] = \{x + yi : x, y \in \mathbf{Z}, i = \sqrt{-1}\}$. Let $\mathbf{Q}(i)$ be the corresponding quadratic number field with the ring of integers $\mathbf{Z}[i]$. Let $\alpha \in \mathbf{Z}[i]$. We denote by $N(\alpha) = x^2 + y^2$ the norm of α relative to $\mathbf{Q}$. Assume that the procedure FindPrimeQ finds positive integers a, b such that $F(a,b) = q$ is prime. Then there exists $\gamma = 12a + (12b+1)i \in \mathbf{Z}[i]$ such that $F(a,b) = (12a)^2 - ((12b+1)i)^2 =$

$N(\gamma)$. Let $\xi \in \mathbf{Z}[i]$, $\xi = (p^2 - 1) + p\, i$, where p is a prime. We have $N(\xi) = \Phi_6(p^2)$. Assume that γ divides ξ. Then there exists $\delta \in \mathbf{Z}[i]$, $\delta = x + yi$, $x, y \in \mathbf{Z}$ such that

$$\gamma\delta = (12a + (12b + 1)i)(x + yi) = (p^2 - 1) + p = \xi, \tag{1}$$

and

$$N(\gamma)N(\delta) = N(\xi) = \Phi_6(p^2). \tag{2}$$

We show how one can find elements δ, $\xi \in \mathbf{Z}[i]$, and a prime p satisfying (1). By (1) it follows that

$$\begin{cases} 12ax - (12b + 1)y = p^2 - 1 \\ (12b + 1)x + 12ay = \quad p, \end{cases} \tag{3}$$

where $12a$, $12b + 1$ are given. Squaring the second equation and substituting to the first one we get

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + 1 = 0, \tag{4}$$

where

$$A = -(12b + 1)^2,\ B = -2(12a)(12b + 1), \tag{5}$$

$$C = -(12a)^2,\ D = 12a,\ E = -(12b + 1). \tag{6}$$

Now we find solutions of (4). We write $\Delta = B^2 - 4AC$. Trivial computation show that $\Delta = 0$. Multiplying (4) by $2A$ we obtain $(2Ax + By)^2 + 4ADx + 4AEy + 4A = 0$. Let $2Ax + By = T$ then $T^2 + 2(2AE - BD)y + 4A + 2DT = 0$ and $(T + D)^2 = 2(BD - 2AE)y + D^2 - 4A$. Consequently equation (4) is equivalent to

$$(2Ax + By + D)^2 + \alpha y = \beta, \tag{7}$$

where

$$\alpha = 2(BD - 2AE) = 4(12b + 1)((12a)^2 + (12b + 1)^2) = -4(12b + 1)q \tag{8}$$

and

$$\beta = D^2 - 4A = (12a)^2 + 4(12b + 1)^2. \tag{9}$$

Let

$$X = 2Ax + By + D, \quad Y = -\alpha y. \tag{10}$$

By (7)

$$X^2 - \beta = Y, \tag{11}$$

we see that a necessary condition for existence of integers solution of (7) is solubility of the congruence

$$Z^2 \equiv \beta \pmod{\alpha}. \tag{12}$$

Let z_0 be the solution of (12). From (8) and (9) it follows that

$$\begin{aligned} z_0 &\equiv 0 \pmod{4} \\ z_0 &\equiv 12a \pmod{(12b+1)} \\ z_0 &\equiv \sqrt{3}(12b+1) \pmod{q}. \end{aligned} \tag{13}$$

Since $q \equiv 1 \pmod 3$ then 3 is quadratic residue modulo q and, in consequence, $z_0 \pmod{\alpha}$ exists. It can be easily found by the Chinese Remainder Theorem. By (10), (11) we have $y = (z_0^2 - \beta)/(-\alpha)$, $y \in \mathbf{N}$. Now we prove that in this case x is integer as well. By (10) we have

$$z_0 - D = 2Ax + By \tag{14}$$

Since $q = F(a,b) = (12a)^2 + (12b+1)^2$ is a prime then $(2A, B) = 2(12b+1)$. Hence $z_0 - D \equiv 0 \pmod{2(12b+1)}$ and so (14) has integer solutions. Consequently, solutions of (7) are integers. This observation works for general solutions of (12) $z \equiv z_0 \pmod{\alpha}$. Our computation shows that integers solutions x, y of (7) have the form

$$x = \frac{z - By - D}{2A}, \quad y = \frac{z^2 - \beta}{-\alpha}, \quad x, y \in \mathbf{Z}, \tag{15}$$

where $z = \alpha t + z_0$, $t \in \mathbf{Z}$. Substituting the above x to the second equation of (3) we obtain

$$(12b+1)\left(\frac{\alpha t + z_0 - D}{2A}\right) + \left(12a - \frac{B(12b+1)}{2A}\right) y = p$$

Since $(12a - ((12b+1)B)/2A)y = 0$ then putting (8), (5) we get

$$2qt + \frac{z_0 - 12a}{-2(12b+1)} = p, \qquad t \in \mathbf{Z}.$$

Hence

$$p \equiv (z_0 - 12a)(-2(12b+1))^{-1} \pmod{q}$$

and consequently by (13)

$$p \equiv (\sqrt{3}(12b+1) - 12a)(-2(12b+1))^{-1} \pmod{q}, \tag{16}$$

Taking (compare steps 11-14 of procedure FindPrimePModuloQ)

$$r = (\sqrt{3}(12b+1) - 12a)(-2(12b+1))^{-1} \pmod{q}$$

then from (2) and (16) we get

$$\Phi_6(p^2) \equiv \Phi_6(r^2) \equiv 0 \pmod{q}.$$

Therefore if we find prime p in the arithmetic progression $p \equiv r \pmod{q}$ (compare steps 16-20 of procedure FindPrimePModuloQ), then $q | \Phi_6(p^2)$. Since $\Phi_6(r) = \Phi_3(-r)$ then if we find $p \equiv -r \pmod{q}$, then $q | \Phi_3(p^2)$. This finishes the proof.

3 Run-Time Analysis of the Algorithm

Let us adopt the standard notation used in the theory of primes. We denote by $\pi(x, q, a)$ the number of primes $p \equiv a \pmod{q}$ not exceeding x, where $x \geq 1$, $a, q \in \mathbf{N}$, $1 \leq a \leq q$, $(a, q) = 1$. We write also $\pi(x)$ in place of $\pi(x, 1, 1)$. Moreover we write

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \ (\bmod q)}} \Lambda(n),$$

where

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \\ 0, & \text{otherwise} \end{cases}$$

With the notation as above we recall some theorems which are related to distributions of primes.

Theorem 2 (de la Vallée Poussin). *For some positive number A*

$$\pi(x) = \text{li } x + O(x \exp(-A\sqrt{\log x})).$$

Proof. see [3].

Theorem 3 (Bombieri-Vinogradov). *Let $A > 0$ be fixed. Then*

$$\sum_{q \leq Q} \max_{y \leq x} \max_{\substack{a \\ (a,q)=1}} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ll x^{\frac{1}{2}} Q (\log x)^5,$$

provided that $x^{\frac{1}{2}} (\log x)^{-A} \leq Q \leq x^{\frac{1}{2}}$.

Proof. see [3].

Theorem 4 (Iwaniec). *Let $P(x, y) = ax^2 + bxy + cy^2 + ex + fy + g \in Z[x, y]$,* deg $P = 2$, *$(a, b, c, e, f, g) = 1$, $P(x, y)$ be irreducible in $\mathbf{Q}[x, y]$, represent arbitrary large number and depend essentially on two variables. Then $\frac{N}{\log N} \ll \sum_{\substack{q \leq N \\ q = P(x,y)}} 1$, if $D = af^2 - bef + ce^2 + (b^2 - 4ac)g = 0$ or $\Delta = b^2 - 4ac$ is a perfect square.*

Proof. see [8].

3.1 Analysis of the Procedure FindPrimeQ

We denote by $\mathcal{PT}$ the number of bit operations necessary to carry out the deterministic primality test [1]. For simplicity, assume that $\mathcal{PT} \gg \log^4 n$.

Theorem 5. *Let $F(x,y) = 144x^2 + 144y^2 + 24y + 1 \in Z[x,y]$. Then there exist constants c and $b_0 = b_0(c,n)$, n_0 such that for every integer $n \geq n_0$ and an arbitrary real $\lambda \geq 1$, the procedure* FindPrimeQ *finds $a \in \left[\frac{n}{12\sqrt{2}}, \frac{cn}{12\sqrt{2}}\right]$ and $b \in \left[\frac{n-\sqrt{2}}{12\sqrt{2}}, \frac{cn-\sqrt{2}}{12\sqrt{2}}\right]$ such that $q = F(a,b)$ is a prime, $q \in [n^2, (cn)^2]$, with probability greater than or equal to $1-e^{-\lambda}$ after repeating $[b_0 \lambda \log n]$ steps 3– 7 of the procedure. Every step of the procedure takes no more than $\mathcal{PT}$ bit operations.*

Proof. We start with an estimate for the number of primes in the interval $[n^2, cn^2]$ which are of the form $F(a,b)$, where $F(x,y) = 144x^2+144y^2+24y+1 \in Z[x,y]$. We apply the Theorem 4. We say that F depends essentially on two variables if $\partial F/\partial x$ and $\partial F/\partial y$ are linearly independent. We use the Lemma

Lemma 1. *Let $F(x,y) = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbf{Z}[x,y]$, $\Delta = b^2 - 4ac$, $\alpha = bf - 2ce$, $\beta = be - 2af$. Then $\partial F/\partial x$ and $\partial F/\partial y$ are linearly dependent if and only if $\Delta = \alpha = \beta = 0$.*

Proof. see [8]

Since $\Delta = 288^2$ and $(144, 144, 24, 1) = 1$ then $F(x,y)$ satisfies assumptions of Theorem 4. We define the set

$$\mathcal{Q} = \{n^2 \leq q \leq (cn)^2 : F(x,y) = q - prime,\ x, y \in \mathbf{N}\},$$

where $c > 0$. Denote by $|\mathcal{Q}|$ the number of the elements of $\mathcal{Q}$. Since Δ is a perfect square then by Theorem 4 there exists $c_0 > 0$ such that $|\mathcal{Q}| \geq (c_0(cn)^2)(2\log n)^{-1} - \pi(n^2)$. By Theorem 2 and the above there exists c_1 such that for sufficiently large n we have

$$|\mathcal{Q}| \geq c_1 \frac{n^2}{\log n} + O\left(\frac{n^2}{\log^2 n}\right), \tag{17}$$

where $c_1 = (c_0c^2-1)/2$ with $c \geq \sqrt{3/c_0}$. Denote by A_F the event that a randomly chosen pair of natural numbers a and b satisfying

$$a \in \left[\frac{n}{12\sqrt{2}}, \frac{cn-\sqrt{2}}{12\sqrt{2}}\right], \qquad b \in \left[\frac{n-\sqrt{2}}{12\sqrt{2}}, \frac{cn-\sqrt{2}}{12\sqrt{2}}\right]$$

is such that the number $F(a,b) \in [n^2, (cn)^2]$ is a prime. Hence by (17) there exists $c_2 = c_1 - \varepsilon(n)$, where $\varepsilon \longrightarrow 0$ as $n \longrightarrow \infty$ such that for sufficiently large n, the probability that in l trials A_F does not occur is

$$\left(1 - \frac{c_2}{\log n}\right)^l = \exp\left(l \log\left(1 - \frac{c_2}{\log n}\right)\right) \leq \exp\left(\frac{-c_2 l}{\log n}\right) \leq e^{-\lambda}$$

for an arbitrary real $\lambda \geq 1$ and $l = b_0 \lambda \log n$, where $b_0 = c_2^{-1}$. Hence the probability that in l trials A_F does occur is greater or equal to $1 - e^{-\lambda}$. So after repeating $[b_0 \lambda \log n]$ steps, the procedure finds integers a and b and primes $q = F(a,b)$ with probability greater than or equal to $1 - e^{-\lambda}$. The most time-consuming step of the algorithm is the deterministic primality test for number q which takes no more than $\mathcal{PT}$ operations. This finished the proof.

3.2 Analysis of the Procedure FindPrimePModuloQ

Theorem 6. *Let q be the output of the procedure* FindPrimeQ. *The procedure* FindPrimePModuloQ *with the input consisting of the prime q and a, b has the following properties. There exists b_1 and n_1 such that for every integer $n \geq n_1$ and an arbitrary real $\lambda \geq 1$, the procedure finds a positive integer $k \in \left[1, \left[\frac{n^6 - r}{q}\right]\right]$ such that $p = qk + r$ is prime, $q \ll p \ll n^6$, with probability greater than or equal to $1 - e^{-\lambda}$ after repeating $[b_1 \lambda \log n]$ steps of the procedure with the possible exception of at most $O(n^2 (\log n)^{-C_0 - 1}))$ values of q. Every step of the procedure takes no more than $\mathcal{PT}$ bit operations.*

Proof. We use the lemma

Lemma 2. *Let $q \leq (cn)^2$ be a positive integer. Then there exist constants $0 < C_0 < B < 1$ and n_0 such that for every $n > n_0$ and for all residue classes a* (mod q)

$$\pi(n^6; q, a) = \frac{n^6}{6\phi(q) \log n} + O\left(\frac{n^6}{\phi(q)(\log n)^{B - C_0 + 1}}\right)$$

with the possible exception of at most $O(n^2 (\log n)^{-C_0 - 1}))$ values of q.

Proof. See section 3.3

Denote by A_p the event that a randomly chosen positive integer $k \in \left[1, \frac{n^6 - r}{q}\right]$ is such that the number $qk + r$ is a prime. It follows by Lemma 2 that there exist $0 < C_0 < B < 1$ and n_1 such that for every $n > n_1$ we have $A_p \geq (6 \log n)^{-1} + O((\log n)^{-B + C_0 - 1})$ for all q with the possible exception of at most $O(n^2 (\log n)^{-C_0 - 1}))$ values of q. Hence there exists $c_1 = \frac{1}{6} - \varepsilon(n)$, where $\varepsilon \longrightarrow 0$ as $n \longrightarrow \infty$ such that for sufficiently large n the probability that in l trials A_p does not occur is

$$\left(1 - \frac{c_1}{\log n}\right)^l = \exp\left(l \log\left(1 - \frac{c_1}{\log n}\right)\right) \leq \exp\left(\frac{-l c_1}{\log n}\right) \leq e^{-\lambda}$$

for an arbitrary real $\lambda \geq 1$ and $l = b_1 \lambda \log n$, where $b_1 = c_1^{-1}$. Hence the probability that in l trials A_P does occur is greater than or equal to $1 - e^{-\lambda}$. So after repeating $[b_1 \lambda \log n]$ steps, the procedure finds a positive integer k such that $p = qk + r$ is prime with probability greater than or equal to $1 - e^{-\lambda}$ for all q with the possible exception of at most $O(n^2 (\log n)^{-C_0 - 1}))$ values of q. The most time-consuming step of the algorithm is the deterministic primality test for number p which takes no more than $\mathcal{PT}$ operations. This finishes the proof.

3.3 Proof of Lemma 2

Proof. We apply Theorem 3 with $x = n^6$ and $A = 2B + 6$, $0 < B < 1$

$$\sum_{q \ll n^3(\log n)^{-2B-6}} \max_{y \le n^6} \max_{\substack{a \\ (a,q)=1}} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ll \frac{n^6}{(\log n)^{2B+1}}. \tag{18}$$

Let

$$\widetilde{\mathcal{Q}} = \left\{ q \le (cn)^2 : \exists_{n^6(\log n)^{-C} \le y \le n^6} \exists_{\substack{a \\ (a,q)=1}} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ge \frac{y}{\phi(q)(\log n)^B} \right\},$$

where $C > 0$. Then

$$\frac{n^6}{(\log n)^{2B+1}} \ge \sum_{q \in \widetilde{\mathcal{Q}}} \frac{y}{\phi(q)(\log n)^B} \gg \frac{n^6}{(\log n)^{B+C}} \sum_{q \in \widetilde{\mathcal{Q}}} \frac{1}{\phi(q)} \gg \frac{n^6 |\widetilde{\mathcal{Q}}|}{n^2(\log n)^{B+C}}.$$

Hence

$$|\widetilde{\mathcal{Q}}| \ll \frac{n^2}{(\log n)^{B-C+1}} = \frac{n^2}{(\log n)^{C_0+1}}, \tag{19}$$

where $C = B - C_0$ and $B < 2C_0$. Consequently

$$\max_{\frac{n^6}{(\log n)^{B-C_0}} \le y \le n^6} \max_{\substack{a \\ (a,q)=1}} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \le \frac{n^6}{(\log n)^B}.$$

and

$$\psi(y; q, a) = \frac{y}{\phi(q)} \left(1 + O((\log n)^{-C_0}\right) \tag{20}$$

for all reduced residue classes $a \pmod q$, and for all $q \le (cn)^2$ with the possible exception of at most $O(n^2(\log n^{-C_0-1}))$ values of q. We have

$$\begin{aligned} \pi(n^6; q, a) &= \sum_{\substack{m \le n^6 \\ m \equiv a \,(\bmod\, q)}} \frac{\Lambda(m)}{\log m} - \sum_{t \ge 2} \sum_{\substack{p^t \le n^6 \\ p^t \equiv a \,(\bmod\, q)}} \frac{1}{t} \\ &= \sum_{\substack{m \le n^6 \\ m \equiv a \,(\bmod\, q)}} \frac{\Lambda(m)}{\log m} + O\left(\frac{n^3}{\log n}\right) \end{aligned}$$

By (20) and Abel's summation formula

$$\begin{aligned} \sum_{\substack{2 \le m \le n^6 \\ m \equiv a \,(\bmod\, q)}} \frac{\Lambda(m)}{\log m} &= \frac{\psi(n^6; q, a)}{6 \log n} + \int_2^{n^6} \frac{\psi(y; q, a) dy}{y \log^2 y} = \frac{\psi(n^6; q, a)}{6 \log n} + J_1 + J_1 \\ &= \frac{n^6}{6\phi(q) \log n} + O\left(\frac{n^6}{\phi(q)(\log n)^{C_0+1}}\right) + J_1 + J_2, \end{aligned}$$

where

$$J_1 = \int_{2}^{\frac{n^6}{(\log n)^{B-C_0}}} \frac{\psi(y;q,a)dy}{y\log^2 y}, \quad J_2 = \int_{\frac{n^6}{(\log n)^{B-C_0}}}^{n^6} \frac{\psi(y;q,a)dy}{y\log^2 y}.$$

Since

$$\psi(y;q,a) = \sum_{\substack{2\le m\le y\\ m\equiv a \ (\bmod q)}} \Lambda(m) \ll \log y \sum_{\substack{2\le m\le y\\ m\equiv a \ (\bmod q)}} 1 \ll \frac{y\log y}{q} + O(\log y)$$

Hence there exists n_1 such that for every positive integer $n \ge n_1$

$$J_1 \ll \frac{1}{q} \int_{2}^{\frac{n^6}{(\log n)^{B-C_0}}} \frac{dy}{\log y} + \int_{2}^{\frac{n^6}{(\log n)^{B-C_0}}} \frac{dy}{y\log y} \ll \frac{1}{q}\frac{n^6}{(\log n)^{B-C_0+1}}.$$

By (20) there exists n_2 such that for every positive integer $n \ge n_2$

$$J_2 \ll \frac{1}{\phi(q)} \int_{\frac{n^6}{(\log n)^{B-C_0}}}^{n^6} \frac{dy}{\log^2 y} + \frac{1}{\phi(q)} \int_{\frac{n^6}{(\log n)^{B-C_0}}}^{n^6} \frac{dy}{(\log y)^{C_0+2}} \ll \frac{n^6}{\phi(q)\log^2 n}.$$

This finishes the proof.

References

1. Agrawal, M., Kayal, K., Saxena, N.: Primes is P. Ann. of Math. 160, 781–793 (2004)
2. Cohen, H.: A Course in Computational Algebraic Number Theory. Springer, New York (1993)
3. Davenport, H.: Multiplicative Number Theory. Springer, New York (1980)
4. Gong, G., Harn, L.: Public-Key Cryptosystems Based on Cubic Finite Field Extension. IEEE Transactions on Information Theory 45, 2601–2605 (1999)
5. Gong, G., Harn, L.: A New Approach on Public-key Distribution. In: Proceedings of China - Crypto, Chengdu, China, pp. 50–55 (1998)
6. Giuliani, K., Gong, G.: Generating Large Instances of the Gong-Harn Cryptosytem. In: Proceedings of Cryptography and Coding: 8th International Conference Cirencester. LNCS, vol. 2261, pp. 111–133. Springer, Heidelberg (2002)
7. Grześkowiak, M.: Analysis of Algorithms of Generating Key Parameters for the XTR Cryptosystem. In: Proceedings of Wartacrypt 2004, pp. 1–12. Tatra Mountains Mathematical Publications (2006)
8. Iwaniec, H.: Primes Represented by Quadratic Polynomials in Two Variables. Acta Arith. 24, 435–459 (1974)
9. Lenstra, A.K., Verhuel, E.R.: The XTR Public Key System. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 1–19. Springer, Heidelberg (2000)
10. Rubin, K., Silverberg, A.: Torus-based cryptography. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 349–365. Springer, Heidelberg (2003)