Ann. Sci. Math. Québec **33** (2009), no 2, 115–123

LEGENDRE TYPE FORMULA FOR PRIMES GENERATED BY QUADRATIC POLYNOMIALS

TAKASHI AGOH

Dedicated to Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. On en connaît très peu sur l'ensemble des entiers m tels que le polynôme quadratique $f(X) = aX^2 + bX + c$, avec a, b et c copremiers, est premier lorsqu'évalué en $X = m$. Dans cet article, basé sur le crible d'Ératosthène décalé, nous présentons une formule de type Legendre pour trouver explicitement la cardinalité des valeurs du polynôme $f(X)$ qui sont des nombres premiers ne dépassant pas t pour $t > 0$.

ABSTRACT. Very little is known about the set of integers m such that the quadratic polynomial $f(X) = aX^2 + bX + c$ with relatively prime integer coefficients has a prime value at $X = m$. In this paper, based on the shifted sieve of Eratosthenes, we introduce a Legendre type formula for counting explicitly the number of prime values taken by $f(X)$ that are less than or equal to t for any $t > 0$.

1. Introduction

Consider an irreducible quadratic polynomial f with integer coefficients:

$$f(X) := aX^2 + bX + c, \ \ a > 0, \ \ (a, b, c) = 1. \tag{1}$$

There are only few corroborative results on the set of integers m such that the polynomial $f(X)$ of (1) has a prime value for $X = m$; moreover, no quadratic polynomial producing infinitely many primes is known. However, Iwaniec [2] proved in 1978 that there are infinitely many integers n such that $n^2 + 1$ has at most 2 prime factors. For other interesting results and heuristic arguments including ample numerical computations see, *e.g.*, [5, 6].

Concerning the distribution of prime values of the polynomial $f(X)$, there is a conjecture posed by Hardy-Littlewood [1], which is firmly supported by ample numerical evidence. Let $\left(\frac{*}{p}\right)$ be the Legendre symbol. If $D := b^2 - 4ac$ is not a square and $a + b, c$ are not both even, then the number of prime values less than t taken by the

Reçu le 30 avril 2009 et, sous forme définitive, le 28 novembre 2009.

polynomial $f(X)$ is, asymptotically,

$$\pi_f(t) \;\sim\; \varepsilon\frac{C}{\sqrt{a}}\cdot\frac{\sqrt{t}}{\log t}\prod_{\substack{p>2\\ p|(a,b)}}\frac{p}{p-1},$$

where

$$\varepsilon := \begin{cases} 1 \text{ if } 2\nmid a+b,\\ 2 \text{ if } 2\mid a+b \end{cases} \quad \text{and } C := \prod_{\substack{p>2\\ p|a}}\left(1-\left(\frac{D}{p}\right)\frac{1}{p-1}\right)\cdot$$

We now introduce the Legendre formula to count the number of primes less than t for any real $t>0$. Let p_i be the i-th prime (*i.e.*, $p_1=2$, $p_2=3$, $p_3=5$, and so on), and

$$\begin{cases} \mathcal{P} := \{p_i \mid i=1,2,3,\ldots\} \text{ (the set of all primes)},\\ \mathcal{P}_m := \{p_1,p_2,\ldots,p_m\},\\ Q_m := p_1p_2\cdots p_m,\\ \pi(t) := \#\{p\in\mathcal{P}\mid p\le t\}. \end{cases}$$

Based on the sieve of Eratosthenes, Legendre, in 1808, showed the following formula for $\pi(x)$. Denoting $\mathcal{P}_m := \{p\in\mathcal{P}\mid p\le\sqrt{x}\}$ for $m=\pi(\sqrt{x})$ and

$$\Phi(x;\mathcal{P}_m) := \#\{n\in\mathbb{Z}\mid 1\le n\le x, (n,Q_m)=1\},$$

it follows that

$$\Phi(x;\mathcal{P}_m) = \sum_{d|Q_m}\mu(d)\left[\frac{x}{d}\right]$$

and hence

$$\pi(x) = m-1+\Phi(x;\mathcal{P}_m), \tag{2}$$

where μ is the Möbius function and $[x/d]$ is the greatest integer less than or equal to x/d.

Using the fact that $\Phi(x;\mathcal{P}_m)=\Phi(x;\mathcal{P}_{m-1})-\Phi(x/p_m;\mathcal{P}_{m-1})$, Meissel [4] obtained a more efficient formula to compute $\pi(x)$. Letting $m=\pi(\sqrt{x})$ and $l=\pi(\sqrt[3]{x})$, it follows that

$$\pi(x)=\Phi(x;\mathcal{P}_l)+l(m-l+1)+\frac{(m-l)(m-l-1)}{2}-1-\sum_{i=l+1}^{m}\pi\left(\frac{x}{p_i}\right)\cdot$$

By means of this formula, Meissel himself obtained $\pi(10^8)=5\,761\,455$, and subsequently Lehmer [3] computed $\pi(10^{10})=455\,052\,512$ with an improved approach.

It is the main purpose of this paper to deduce a Legendre type formula analogous to (2) for explicitly counting the number of prime values taken by the polynomial $f(X)$ of (1). We should note beforehand that our method is very elementary and we will apply only the shifted sieve of Eratosthenes for finding primes.

2. Prime values of quadratic polynomials

For a real $t > 0$, we denote

$$\pi_f(t) := \#\{n \geq 1 \mid f(n) \in \mathcal{P},\ |f(n)| \leq t\}.$$

In what follows, we assume that $a + b$ and c are not simultaneously even and that $D = b^2 - 4ac$ is not a square. To simplify our discussion, we also assume that $0 < f(n) < f(n+1)$ for each integer $n \geq 0$, which is equivalent to $a > 0$, $a + b > 0$ and $c > 0$.

If a, b and c are integers that satisfy any one of the conditions

$$\text{(3)} \qquad \begin{cases} \text{(i)}\ \ a, b \text{ are even and } c \text{ is odd,} \\ \text{(ii)}\ \ \text{all of } a, b \text{ and } c \text{ are odd,} \end{cases}$$

then $f(X) \equiv 0 \pmod 2$ has no solution. Moreover, if $p \geq 3$ and $p \nmid a$, then we easily see that $f(X) \equiv 0 \pmod p$ has no solution if and only if $\left(\frac{D}{p}\right) = -1$.

Based on these observations, we have the following proposition.

Proposition 2.1. *Let f be the quadratic polynomial indicated above. Let a, b and c be such that they satisfy any one of the conditions in* (3) *and $\left(\frac{D}{p}\right) = -1$ for $p = p_2, \ldots, p_m$. Then f has prime values at $X = 0, 1, \ldots, n$, where n is the largest integer satisfying $\sqrt{f(n)} < p_{m+1}$.*

Proof. Indeed, if $0 \leq k \leq n$, then $f(k) \not\equiv 0 \pmod{p_i}$ for $i = 1, \ldots, m$ and this implies $f(k) \in \mathcal{P}$ as desired. □

Example 2.2. Consider the polynomial $f(X) = X^2 + 3X + 19$. In this case we have $D = -67$ and $\left(\frac{D}{p}\right) = -1$ for each $p = 3, 5, 7, 11, 13$, but $\left(\frac{D}{17}\right) = 1$. Since the largest integer n satisfying $\sqrt{f(n)} < 17$ is $n = 14$, $f(X)$ must have prime values at $X = 0, 1, \ldots, 14$. Indeed, these values are 19, 23, 29, 37, 47, 59, 73, 89, 103, 127, 149, 173, 193, 227 and 257 which are all primes, but $f(15) = 17^2$ is not a prime.

For a prime $q \in \mathcal{P}$, consider the congruence

$$\text{(4)} \qquad f(X) = aX^2 + bX + c \equiv 0 \pmod q, \quad 0 \leq X \leq q - 1,$$

where a, b and c satisfy the conditions stated above.

Here and in what follows, we shall use the following notations:

(i) $\rho(q)$ is the number of distinct solutions of (4), hence $\rho(q) = 0, 1$ or 2,

(ii) $\mathcal{S} := \{q \in \mathcal{P} \mid \rho(q) \neq 0\}$ is the infinite subset of $\mathcal{P}$ corresponding to f,

(iii) $\mathcal{S}_m := \{q_1, q_2, \ldots, q_m\}$ is the set of the first m primes in $\mathcal{S}$, hence $\rho(q_i) = 1$ or 2,

(iv) $Q_m := Q_m(\mathcal{S}_m) = q_1 q_2 \cdots q_m$ is the product of all primes in $\mathcal{S}_m$.

Given $n \geq 1$, if q_m is the largest prime in $\mathcal{S}$ such that $q_m \leq \sqrt{f(n)}$, then it is obvious that $f(n)$ is prime if and only if $f(n) \not\equiv 0 \pmod{q}$ for all $q \in \mathcal{S}_m$. For a prime $q \in \mathcal{S}_m$, suppose that the solutions of (4) are

$$X \equiv \begin{cases} u_1(q) \pmod{q} & \text{when } \rho(q) = 1, \\ u_1(q), u_2(q) \pmod{q} & \text{when } \rho(q) = 2. \end{cases} \tag{5}$$

Let $d \geq 2$ be a divisor of Q_m. Since d is square-free and there are $\rho(q)$ distinct solutions of (4) for each $q \in \mathcal{S}_m$, we know from the Chinese Remainder Theorem that the number of non-negative common solutions less than or equal to $d-1$ modulo d is equal to

$$\rho(d) := \prod_{q|d} \rho(q).$$

Without loss of generality, we order all distinct solutions of the congruence

$$aX^2 + bX + c \equiv 0 \pmod{d}, \quad 0 \leq X \leq d-1, \tag{6}$$

as follows:

$$0 \leq u_1(d) < u_2(d) < \cdots < u_{\rho(d)}(d) \leq d-1.$$

Before discussing $\pi_f(t)$, we calculate, as a preliminary, the value of

$$\varepsilon_m := \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \delta_i(d), \tag{7}$$

where, for $i = 1, 2, \ldots, \rho(d)$,

$$\delta_i(d) := \begin{cases} 0 \ \text{ if } \ u_i(d) = 0, \\ 1 \ \text{ if } \ u_i(d) \neq 0. \end{cases} \tag{8}$$

Using the smallest solution $u_1(q)$ in (5), we define

$$k := \#\{q \in \mathcal{S}_m \mid \rho(q) = 1\} \quad \text{and} \quad s := \#\{q \in \mathcal{S}_m \mid u_1(q) = 0\}.$$

Then the above ε_m can be calculated as follows.

Lemma 2.3. *We have*

$$\varepsilon_m = \begin{cases} 0 & \text{if } k \neq 0 \text{ and } s \neq 0, \\ -1 & \text{if } k \neq 0 \text{ and } s = 0, \\ (-1)^m & \text{if } k = 0 \text{ and } s \neq 0, \\ (-1)^m - 1 & \text{if } k = 0 \text{ and } s = 0. \end{cases}$$

Proof. Since $\rho(q_i) \in \{1, 2\}$, we have

$$\sum_{d|Q_m} \mu(d)\rho(d) = \prod_{i=1}^{m} (1 - \rho(q_i)) = \begin{cases} 0 & \text{if } k \geq 1, \\ (-1)^m & \text{if } k = 0. \end{cases}$$

Now, let $\rho'(d) \in \{0,1\}$ denote the number of $u_i(d)$'s equal to 0. Then

$$\sum_{d|Q_m} \mu(d)\rho'(d) = \prod_{i=1}^{m}(1-\rho'(q_i)) = \begin{cases} 0 & \text{if } s \geq 1, \\ 1 & \text{if } s = 0. \end{cases}$$

Since $\varepsilon_m = \sum_{d|Q_m} \mu(d)(\rho(d) - \rho'(d))$, the result follows. □

For a real number $x \geq 1$ and an integer $m \geq 1$, put

$$\Phi(x;\mathcal{S}_m) := \#\{n \mid 1 \leq n \leq x,\ f(n) \not\equiv 0 \pmod{q} \text{ for all } q \in \mathcal{S}_m\}.$$

Based on the shifted sieve of Eratosthenes, we can easily deduce an explicit formula for $\Phi(x;\mathcal{S}_m)$.

Proposition 2.4. *We have* $\Phi(x;\mathcal{S}_m) = \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \left[\frac{x-u_i(d)}{d}\right] + \varepsilon_m.$

Proof. For each divisor $d \geq 1$ of Q_m, set

$$\eta(x;u(d)) := \#\{n \mid 1 \leq n \leq x,\ n \equiv u(d) \pmod{d}\}.$$

Then for $i = 1, 2, \ldots, \rho(d)$, we have

$$\eta(x;u_i(d)) = \left[\frac{x-u_i(d)}{d}\right] + \delta_i(d),$$

where $\delta_i(d) = 0$ or 1 as defined in (8). Therefore, it follows from the principle of inclusion-exclusion that

$$\begin{aligned} \Phi(x;\mathcal{S}_m) &= \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \eta(x;u_i(d)) \\ &= \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \left(\left[\frac{x-u_i(d)}{d}\right] + \delta_i(d)\right) \\ &= \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \left[\frac{x-u_i(d)}{d}\right] + \varepsilon_m, \end{aligned}$$

which completes the proof. □

Given $n \geq 1$, we assume that $\mathcal{S}_m$ is the set of all primes in $\mathcal{S}$ up to $\sqrt{f(n)}$. Then $\Phi(n;\mathcal{S}_m)$ expresses the number of prime values taken by $f(X) = aX^2 + bX + c$ in the interval $\left(\sqrt{f(n)}, f(n)\right]$. Using this function, we are able to deduce an explicit formula for $\pi_f(t)$.

For any $t \geq f(1) = a + b + c$, we first look for the largest prime $q_{m_1} \in \mathcal{S}$ such that $q_{m_1} \leq t^{1/2}$. Next, if $q_{m_1} \neq q_1$, then we look for the largest prime $q_{m_2} \in \mathcal{S}$ such that $q_{m_2} \leq t^{1/2^2}$. We repeat this procedure until we arrive at $q_{m_k} = q_1$ to obtain the sequence

$$q_1 = q_{m_k} \leq t^{1/2^k} < \cdots < q_{m_2} \leq t^{1/2^2} < q_{m_1} \leq t^{1/2} < t \tag{9}$$

and the descending chain of subsets

$$\{q_1\} = \mathcal{S}_{m_k} \subset \mathcal{S}_{m_{k-1}} \subset \cdots \subset \mathcal{S}_{m_2} \subset \mathcal{S}_{m_1} \subset \mathcal{S}.$$

With the above notations, we can state the following theorem.

Theorem 2.5. *We have* $\pi_f(t) = \sum_{i=1}^{k} \Phi\left(\sqrt{t^{1/2^{i-1}} - 1}; \mathcal{S}_{m_i}\right)$.

Proof. Since $\Phi\left(\sqrt{t^{1/2^{i-1}} - 1}; \mathcal{S}_{m_i}\right)$ is the number of integers n in the interval $\left[1, \sqrt{t^{1/2^{i-1}} - 1}\right]$ with $f(n) \not\equiv 0 \pmod{q}$ for all $q \in \mathcal{S}_{m_i}$, this expresses the number of prime values taken by $f(X)$ in the interval $\left(t^{1/2^i}, t^{1/2^{i-1}}\right]$. Connecting these intervals for $i = 1, 2, \ldots, k$, we obtain immediately the above formula. □

Proposition 2.6. *For any fixed* $m \geq 1$, *it follows that* $\lim_{x\to\infty} \Phi(x; \mathcal{S}_m) = \infty$.

Proof. Since $|\varepsilon_m| \leq 2$ by Lemma 2.3 and ρ is multiplicative for relatively prime divisors of Q_m, we obtain, for a fixed m,

$$\begin{aligned}
\Phi(x; S_m) &= \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \left[\frac{x - u_i(d)}{d}\right] + \varepsilon_m \\
&= \sum_{d|Q_m} \mu(d) \sum_{i=1}^{\rho(d)} \frac{x - u_i(d)}{d} + \varepsilon_m + O\left(\sum_{d|Q_m} \rho(d)|\mu(d)|\right) \\
&= x \sum_{d|Q_m} \frac{\mu(d)\rho(d)}{d} - \sum_{d|Q_m} \frac{\mu(d)}{d} \left(\sum_{i=1}^{\rho(d)} u_i(d)\right) + \varepsilon_m + O\left(4^m\right) \\
&= x \prod_{q\in\mathcal{S}_m} \left(1 - \frac{\rho(q)}{q}\right) + O(1).
\end{aligned}$$

The right-hand side diverges as x tends to infinity which, however, is absurd. □

We give here an example of how to compute $\pi_f(x)$ using the shifted sieve method of Eratosthenes.

Example 2.7. For the special polynomial $f(X) = X^2 + 1$, we see that there exists a solution of $X^2 + 1 \equiv 0 \pmod{q}$, $0 \leq X \leq q - 1$, if and only if $q = 2$ and $\left(\frac{-1}{q}\right) = 1$ for an odd $q \in \mathcal{P}$. Hence we have $\mathcal{S} = \{2\} \cup \{q \in \mathcal{P} \mid q \equiv 1 \pmod{4}\}$ and all the solutions of this congruence are given, for each $q \in \mathcal{S}$, as

$$X = \begin{cases} u_1(q) = 1 & \text{for } q = q_1 = 2, \\ u_1(q), u_2(q) & \text{for } q \equiv 1 \pmod{4}. \end{cases}$$

Here note that if $q \neq 2$, then $u_1(q) \neq u_2(q)$ and $u_1(q) + u_2(q) = q$.

As a practical application, we will now compute $\pi_{X^2+1}(t)$ for $t = 10^4$. First find the sequence of all primes $q_{m_i} \in \mathcal{S}$, $i = 1, 2, \ldots, k$, given in (9). Then we have $q_{m_1} = q_{12} = 97$, $q_{m_2} = q_2 = 5$, $q_{m_3} = q_1 = 2$, and so $k = 3$. Therefore, consider the following chain of subsets of $\mathcal{S}$:

$$\mathcal{S}_1 = \{2\} \subset \mathcal{S}_2 = \{2, 5\} \subset \mathcal{S}_{12} = \{2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97\}.$$

We enumerate all solutions $u_i(q)$ of $X^2 + 1 \equiv 0 \pmod q$ for each $q \in \mathcal{S}_{12}$ in the following table:

q	2	5	13	17	29	37	41	53	61	73	89	97
$u_1(q)$	1	2	5	4	12	6	9	23	11	27	34	22
$u_2(q)$	–	3	8	13	17	31	32	30	50	46	55	75

Write all positive integers less than or equal to $99 = \left[\sqrt{10^4 - 1}\right]$ and cross out integers n such that $n \equiv u_1(q), u_2(q) \pmod q$ for all $q \in \mathcal{S}_{12}$. Then we get the set of integers that survive:

$$M_1 := \{10, 14, 16, 20, 24, 26, 36, 40, 54, 56, 66, 74, 84, 90, 94\}.$$

Hence the number of primes in $(10^2, 10^4]$ of the form $X^2 + 1$ is

$$\Phi\left(\sqrt{10^4 - 1}; \mathcal{S}_{12}\right) = \# M_1 = 15.$$

Similarly, we have $M_2 := \{4, 6\}$ and $M_3 := \{2\}$, which are the sets of integers in the intervals $[1, \sqrt{99}]$ and $[1, 3]$, respectively, not satisfying (4). Hence

$$\Phi\left(\sqrt{99}; \mathcal{S}_2\right) = \# M_2 = 2, \quad \Phi(3; \mathcal{S}_1) = \# M_3 = 1.$$

Noticing that $1^2 + 1 = 2$ is a prime, we finally have

$$\pi_{X^2+1}(10^4) = \#\left(M_1 \cup M_2 \cup M_3\right) + 1 = 19.$$

Indeed, the set $\mathcal{M}$ of primes in the interval $[1, 10^4]$ of the form $f(X) = X^2 + 1$ is precisely given by

$$\mathcal{M} = \left\{n^2 + 1 \mid n \in \{2\} \cup M_1 \cup M_2 \cup M_3\right\}.$$

The next proposition seems to be trivial, but its proof gives us a certain piece of information about the value of each term in the function $\Phi(x; \mathcal{S}_m)$.

Proposition 2.8. *Let $n \geq 2$, $m \geq 1$ and $u(q)$ be a solution of (4). If $n \not\equiv u(q) \pmod q$ for all $q \in \mathcal{S}_m$, then $\Phi(n; \mathcal{S}_m) = \Phi(n-1; \mathcal{S}_m) + 1$.*

Proof. By the division algorithm we have

$$(n-1) - u(q) = \left[\frac{(n-1) - u(q)}{q}\right] q + r_q(n-1), \; 0 \leq r_q(n-1) < q. \tag{10}$$

If we choose especially an integer $n \geq 2$ satisfying $n \not\equiv u(q) \pmod q$ for all $q \in \mathcal{S}_m$, then $r_q(n-1) \neq q - 1$, *i.e.*, $0 \leq r_q(n-1) \leq q - 2$. Indeed, if $r_q(n-1) = q - 1$, then $n \equiv u(q) \pmod q$, which is contrary to the assumption. From (10) we obtain

$$n - u(q) = \left[\frac{(n-1) - u(q)}{q}\right] q + r_q(n-1) + 1,$$

where $1 \leq r_q(n-1)+1 \leq q-1$. This implies $r_q(n) = r_q(n-1)+1$ and hence

$$[(n-u(q))/q] = [((n-1)-u(q))/q], \quad \text{for all } q \in \mathcal{S}_m.$$

Since the condition $n \not\equiv u(q) \pmod q$ for all $q \in \mathcal{S}_m$ yields $n \not\equiv u(d) \pmod d$ for all divisors $d > 0$ of Q_m, we also have

$$[(n-u(d))/d] = [((n-1)-u(d))/d].$$

Consequently, it follows from Proposition 2.4 that

$$\begin{aligned}\Phi(n;\mathcal{S}_m) &= n + \sum_{\substack{d|Q_m \\ d\neq 1}} \mu(d) \sum_{i=1}^{\rho(d)} \left[\frac{n-u_i(d)}{d}\right] + \varepsilon_m \\ &= (n-1) + \sum_{\substack{d|Q_m \\ d\neq 1}} \mu(d) \sum_{i=1}^{\rho(d)} \left[\frac{(n-1)-u_i(d)}{d}\right] + \varepsilon_m + 1 \\ &= \Phi(n-1;\mathcal{S}_m) + 1,\end{aligned}$$

which completes the proof. □

To conclude this paper, we would like to mention that all above discussions can be extended to a polynomial $f(X)$ with arbitrary degree ≥ 2. Indeed, let $\mathcal{S}$ and $\mathcal{S}_m$ be the sets of primes corresponding to f, similarly to the quadratic case. Then it will be possible to compute $\Phi(x;\mathcal{S}_m)$ and $\pi_f(t)$ without difficulty by the same method as above, except for a treatment of the number $\rho(q)$ (where $q \in \mathcal{S}$) of distinct solutions of the congruence

$$f(X) \equiv 0 \pmod q, \quad 0 \leq X \leq q-1. \tag{11}$$

It is easy to show that the value of ε_m in this case is formally given by $\varepsilon_m = g(1)$ (with $0^0 = 1$) for the polynomial

$$g(X) := \prod_{q \in \mathcal{S}m} (X - \rho(q)) - X^{m-s}(X-1)^s,$$

where $s := \#\{q \in \mathcal{S}_m \mid u_1(q) = 0\}$ and $u_1(q)$ is the smallest solution of (11).

Acknowledgements. The author would like to express his gratitude to the anonymous referee for the useful suggestions which led to various improvements of this paper. This research was supported in part by the Grant-in-Aid for Scientific Research (C), No.21540026, Japan Society for the Promotion of Science.

REFERENCES

[1] G.H. Hardy and J.E. Littlewood, *Some problems of 'Partitio Numerorum', III: On the expression of a number as a sum of primes*, Acta Math. **44**, 1923, 1–70. Collected papers of G.H. Hardy, I, Clarendon Press, Oxford, 1966, 561–588.

[2] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47**, 1978, 171–188.

[3] D.H. Lehmer, *On the exact number of primes less than a given limit*, Illinois J. Math. **3**, 1959, 381–388.

[4] E. Meissel, *Über die Bestimmung der Primzahlmenge innerhalb gegebener Grenzen*, Math. Ann. **2**, 1870, 636–642.

[5] P. Ribenboim, *The new book of prime number records* (3rd ed.), Springer-Verlag, New York, 1995.

[6] P. Ribenboim, *The little book of bigger primes* (2nd ed.), Springer-Verlag, New York, 2004.

T. AGOH, DEPT. OF MATH., TOKYO U. OF SCIENCE, NODA, CHIBA 278-8510, JAPAN
agoh_takashi@ma.noda.tus.ac.jp