Tatra Mt. Math. Publ. **20** (2000), 65–73

Tatra Mountains
Mathematical Publications

ON SOPHIE GERMAIN PRIMES

Takashi Agoh

ABSTRACT. A prime p is so called a SG (Sophie Germain) prime when $2p+1$ is also a prime. These primes were considered, in connection with the first case of Fermat's last theorem, in the paper of Sophie Germain. It is unknown whether there exist infinitely many such primes. In this paper we shall give the formula related to the number of SG primes not exceeding $t \geq 1$, which is analogous to the well-known Legendre formula for counting explicitly the number of primes $\leq t$. Further, we shall discuss SG prime chains and attempt another approach for counting the number of these primes $\leq t$.

1. Introduction

A prime p is so called a SG (Sophie Germain) prime when $2p+1$ is also a prime. These primes were considered, in connection with the first case of Fermat's last theorem, in the paper of Sophie Germain. Indeed, she proved that if p is a SG prime, then $x^p + y^p = z^p$ has no solutions in the case $p \nmid xyz$. We can find details related to Fermat's last theorem and these primes in Ribenboim's books [4, 6]. On the other hand, it is well-known as the divisor criterion of Euler for Mersenne numbers that if p is a prime with $p \equiv 3 \pmod 4$ and $M_p = 2^p - 1$ is a Mersenne number, then $2p+1 \mid M_p$ if and only if p is a SG prime. In spite of various efforts by many authors, it is unknown whether there exist infinitely many SG primes. We anticipate that this problem will be as difficult as the famous conjecture of twin primes.

Recently, the largest pair of twin primes (11713 decimal digits) and the largest SG prime (5847 decimal digits) were announced in the paper [1] by Indlekofer and Járai.

In what follows, let $\pi_{\mathrm{SG}}(t)$ be the number of SG primes not exceeding a fixed real number $t \geq 1$. Using the similar methods to the sieve of Brun sprung from

2000 Mathematics Subject Classification: 11A07, 11A41, 11N05, 11N36.
Keywords: Sophie Germain primes, the sieve of Eratosthenes, Legendre formula for the number of primes.

The author was supported in part by a grant of the Ministry of Education, Science and Culture of Japan.

attempts to estimate the number of twin primes, the following evaluation for $\pi_{\mathrm{SG}}(t)$ can be deduced (see, e.g., Ribenboim [5, Chapter 5]):

$$\pi_{\mathrm{SG}}(t) = O\left(\frac{t}{(\log t)^2}\right).$$

By the prime number theorem we see immediately that

$$\lim_{t\to\infty} \frac{\pi_{\mathrm{SG}}(t)}{\pi(t)} = 0\,,$$

where $\pi(t)$ is the prime counting function, i.e., $\pi(t)$ is the number of primes $\leq t$. In other words, we may say that the set of SG primes has primitive density 0. More generally, Powell [2] proved without the use of sieve methods that the set of primes p for which $kp + l$ is prime has primitive density 0, where k and l are integers such that $k \geq 1$, $l \neq 0$, not both odd and $(k, l) = 1$.

Let p_i be the ith prime (thus $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on), $\mathscr{P}$ the set of all primes, $\mathscr{P}_m := \{p_1, p_2, \dots, p_m\}$ the set of the first m primes, and $P_m := p_1 p_2 \cdots p_m$ the product of all primes in $\mathscr{P}_m$. As Legendre showed in 1808, if $\mathscr{P}_m$ is the set of all primes up to $\sqrt{t}$, then, using the sieve of Eratosthenes, $\pi(t)$ can be expressed as

$$\pi(t) = m - 1 + \sum_{d \mid P_m} \mu(d) \left[\frac{t}{d}\right],$$

where μ is the Möbius function, $[t/d]$ is the greatest integer $\leq t/d$ and the sum runs over all positive divisors d of P_m.

The main aim of this paper is to deduce the Legendre type formula for $\pi_{\mathrm{SG}}(t)$ (Theorems 2.1 and 2.3 in Section 2 below), which is analogous to the above one for $\pi(t)$. For this, we shall utilize the inclusion-exclusion principle and the shifted sieve method of Eratosthenes. In addition, we would like to discuss SG prime chains (Cunningham prime chains of the first kind) in Section 3 and to attempt another approach for counting the number of these primes $\leq t$ in Section 4.

2. Legendre type formula

In this section we will derive the Legendre type formula relating to the number of SG primes. We first deduce a certain criterion for which both p and $2p+1$ are primes according to the definition of the SG prime, and subsequently we count the number of these primes in a given interval by means of this criterion.

Let $\mathscr{S}$ denote the set of SG primes. For a prime p, consider the polynomial

$$g_p(X) := \begin{cases} X & \text{for } p = p_1\,, \\ X\left(X - \frac{p-1}{2}\right) & \text{for } p \neq p_1\,. \end{cases}$$

We see from the sieve of Eratosthenes that if there exists a positive integer a such that $g_p(a) \not\equiv 0 \pmod p$ for all primes p not exceeding $\sqrt{2a+1}$, then the integers a and $2a+1$ are both prime, and so $a \in \mathscr{S}$. In this case, we can state that if p_m is the largest prime such that $p_m \le \sqrt{2a+1}$, then a satisfies

$$\begin{cases} a \not\equiv 0 \pmod p & \text{for } p = p_1\,, \\ a \not\equiv 0\,,\ \frac{p-1}{2} \pmod p & \text{for } p \in \mathscr{P}_m \backslash \{p_1\}\,. \end{cases} \tag{2.1}$$

Consequently, we are able to conclude that

$$a \in \mathscr{S} \iff a \text{ satisfies } (2.1)\,.$$

Let $x \ge 1$ be any real number. We want to extract integers a satisfying $g_p(a) \not\equiv 0 \pmod p$ (hence (2.1)) for all primes $p \in \mathscr{P}_m$ from the set of integers in the interval $[1, x]$. For this purpose, consider the system of congruences $g_p(X) \equiv 0 \pmod p$ for $p \in \mathscr{P}_m$, or equivalently, the system of congruences

$$\begin{cases} X \equiv 0 \pmod p & \text{for } p = p_1\,, \\ X \equiv 0\,,\ \frac{p-1}{2} \pmod p & \text{for } p \in \mathscr{P}_m \backslash \{p_1\}\,. \end{cases} \tag{2.2}$$

Now, we define $\nu(d)$ for each positive divisor d of P_m by

$$\nu(d) := \begin{cases} 2^{\#\mathscr{P}(d)-1} & \text{if } 2 \mid d\,, \\ 2^{\#\mathscr{P}(d)} & \text{if } 2 \nmid d\,, \end{cases}$$

where $\mathscr{P}(d)$ is the set of prime divisors of d and $\#\mathscr{P}(d)$ means its cardinality. Since there are two different congruences in (2.2) for each $p \in \mathscr{P}_m \backslash \{p_1\}$ and all divisors d of P_m are square-free, we see from the Chinese remainder theorem that if (2.2) holds, then there exist exactly $\nu(d)$ distinct integers $c(d)$ (common solutions of (2.2) for $p \in \mathscr{P}(d)$) such that $X \equiv c(d) \pmod d$, $0 \le c(d) \le d-1$. Here note that one of these equals 0. So, including cases for $d = 1$ and $d = p$ we write these integers as $0 = c_1(d) < c_2(d) < \cdots < c_{\nu(d)}(d) \le d-1$ in what follows.

Let $S(x; \mathscr{P}_1)$ be the number of integers a in $[1, x]$ satisfying only the first condition in (2.1), and let $S(x; \mathscr{P}_i)$ with $i \ge 2$ be the number of integers a in $[1, x]$ satisfying the both conditions in (2.1). Then $S(x; \mathscr{P}_m)$ can be formulated in the following theorem.

Theorem 2.1. *Given $\mathscr{P}_m$ for $m \ge 1$, it follows that*

$$S(x; \mathscr{P}_m) = \sum_{d \mid P_m} \mu(d) \sum_{i=1}^{\nu(d)} \left[\frac{x - c_i(d)}{d} \right].$$

Proof. Given but fixed divisor d of P_m, let $\rho\big(x; c(d)\big)$ be the number of solutions of the congruence $X \equiv c(d) \pmod d$ in the interval $[1, x]$. It is clear that if $c(d)=0$, then $\rho(x;0)=[x/d]$. If $c(d)\neq 0$, then the integers in $[1,x]$ satisfying $X\equiv c(d) \pmod d$ are

$$c(d)+kd, \qquad k=0,1,\ldots,\left[\tfrac{x-c(d)}{d}\right],$$

hence we have $\rho\big(x;c(d)\big)=\big[\big(x-c(d)\big)/d\big]+1$. Here we remark that this evaluation is available even if $x-c(d)\le 0$, because $-1<\big(x-c(d)\big)/d\le 0$ in this case. Therefore we obtain from the inclusion-exclusion principle that

$$\begin{aligned}
S(x;\mathscr{P}_m) &= \sum_{d|P_m}\mu(d)\sum_{i=1}^{\nu(d)}\rho\big(x;c_i(d)\big)\\
&= \sum_{d|P_m}\mu(d)\sum_{i=1}^{\nu(d)}\left(\left[\frac{x-c_i(d)}{d}\right]+\delta_i(d)\right) \qquad (2.3)\\
&= \sum_{d|P_m}\mu(d)\sum_{i=1}^{\nu(d)}\left[\frac{x-c_i(d)}{d}\right]+\sum_{d|P_m}\mu(d)\sum_{i=1}^{\nu(d)}\delta_i(d),
\end{aligned}$$

where $\delta_i(d)=0$ if $c_i(d)=0$, and $\delta_i(d)=1$ if $c_i(d)\neq 0$. We will now show that the second sum on the right-hand side vanishes. Since $c_1(d)=0$ and $c_i(d)\neq 0$ $(i\ge 2)$ for all divisors d of P_m, we have $\delta_1(d)=0$ and $\delta_i(d)=1$ for $i\ge 2$, so that

$$\sum_{i=1}^{\nu(d)}\delta_i(d)=\nu(d)-1.$$

The number of divisors d of P_m such that $\#\mathscr{P}(d)=j\ge 1$ is equal to $\binom{m-1}{j-1}$ if $2|d$, and to $\binom{m-1}{j}$ if $2\nmid d$. Noting that the term for $d=1$ vanishes, we have

$$\begin{aligned}
\sum_{d|P_m}\mu(d)\sum_{i=1}^{\nu(d)}\delta_i(d) &= \sum_{j=1}^{m}(-1)^j\sum_{\substack{d|P_m\\ \#\mathscr{P}(d)=j}}\big(\nu(d)-1\big)\\
&= \sum_{j=1}^{m}(-1)^j\left\{\sum_{\substack{2|d|P_m\\ \#\mathscr{P}(d)=j}}\big(\nu(d)-1\big)+\sum_{\substack{2\nmid d|P_m\\ \#\mathscr{P}(d)=j}}\big(\nu(d)-1\big)\right\}\\
&= \sum_{j=1}^{m}(-1)^j\binom{m-1}{j-1}(2^{j-1}-1)+\sum_{j=1}^{m-1}(-1)^j+\binom{m-1}{j}(2^j-1)\\
&= 0
\end{aligned}$$

as desired. This deduces immediately the result from (2.3). □

We should comment that $S(x;\mathscr{P}_1)$ is the number of odd integers in the interval $[1,x]$. Also, if $p_m \geq p_2 = 3$ is the largest prime such that $p_m \leq \sqrt{2x+1}$, then $S(x;\mathscr{P}_m)$ represents the number of SG primes in the interval $(p_m, x]$.

Using Theorem 2.1 one can state

Proposition 2.2. *Given $\mathscr{P}_m$ for $m \geq 1$, it follows that*

$$\lim_{x\to\infty} S(x;\mathscr{P}_m) = \infty .$$

P r o o f. It is enough to prove that there exists a real number $x \geq 1$ such that $S(x;\mathscr{P}_m) > n$ for any positive integer n. Assume that $S(x;\mathscr{P}_m) = n$ with x sufficiently large. Then, since m is fixed, we obtain from Theorem 2.1 that

$$\begin{aligned}
n &= \sum_{d\mid P_m} \mu(d) \sum_{i=1}^{\nu(d)} \left[\frac{x-c_i(d)}{d}\right] \\
&= \sum_{d\mid P_m} \mu(d) \sum_{i=1}^{\nu(d)} \frac{x-c_i(d)}{d} + O\left(\sum_{d\mid M_m} |\mu(d)|\right) \\
&= x\sum_{d\mid P_m} \frac{\mu(d)\nu(d)}{d} - \sum_{d\mid P_m} \frac{\mu(d)}{d} \sum_{i=1}^{\nu(d)} c_i(d) + O(2^m) \\
&= x\prod_{p\in\mathscr{P}_m} \left(1 - \frac{\lambda(p)}{p}\right) + O(1),
\end{aligned}$$

where $\lambda(p) = 1$ if $p = p_1$ and $\lambda(p) = 2$ otherwise. The right-hand side diverges to infinity as x tends to infinity, which is a contradiction. So the result follows. □

Next, by making use of Theorem 2.1 we will formulate $\pi_{\mathrm{SG}}(t)$ (the number of SG primes in the interval $[1,t]$).

For brevity, we put $f(x) := \sqrt{2x+1}$ for $x > 0$. Since $p_1 (= 2)$ is the smallest prime in $\mathscr{S}$, assume that $t \geq 2$. First find the largest prime p_{m_1} such that $p_{m_1} \leq f(t)$. If $p_{m_1} \neq p_1$, then find the largest prime p_{m_2} such that $p_{m_2} \leq f(p_{m_1})$. Repeating this procedure until we arrive at the prime $p_{m_k} = p_1$, we have the sequence

$$p_1 = p_{m_k} \leq f(p_{m_{k-1}}) < p_{m_{k-1}} \leq f(p_{m_{k-2}}) < \cdots < p_{m_2} \leq f(p_{m_1}) < p_{m_1} \leq f(t),$$

hence the strictly descending chain of subsets of $\mathscr{P}$:

$$\mathscr{P}_1 = \mathscr{P}_{m_k} \subset \mathscr{P}_{m_{k-1}} \subset \cdots \subset \mathscr{P}_{m_2} \subset \mathscr{P}_{m_1} \subset \mathscr{P}.$$

Using these subsets $\mathscr{P}_{m_i}$ $(i = 1, 2, \ldots, k)$ the number of SG primes not exceeding t can be explicitly computed by the formula in the following theorem.

Theorem 2.3. *Let $t \geq 2$ be a real number. With above notations, it follows that*

$$\pi_{\mathrm{SG}}(t) = S\big(t; \mathscr{P}_{m_1}\big) + \sum_{i=1}^{k-1} S\big(p_{m_i}; \mathscr{P}_{m_{i+1}}\big).$$

Proof. The first term on the right-hand side of the formula expresses the number of integers a in the interval $[1, t]$ satisfying (2.1) for $p \in \mathscr{P}_{m_1}$, so it is equal to the number of SG primes in $\big(p_{m_1}, t\big]$. Similarly, the term $S\big(p_{m_i}; \mathscr{P}_{m_{i+1}}\big)$ for each $i = 1, 2, \dots, k-2$ expresses the number of SG primes in the interval $\big(p_{m_{i+1}}, p_{m_i}\big]$. The last term $S\big(p_{m_{k-1}}; \mathscr{P}_{m_k}\big)$ with $\mathscr{P}_{m_k} = \mathscr{P}_1$ is the number of odd integers in the interval $\big[1, p_{m_{k-1}}\big]$. In this case, since $2 \leq f\big(p_{m_{k-1}}\big) < 3$, we have $p_{m_{k-1}} = p_2 = 3$, so that $S\big(p_{m_{k-1}}; \mathscr{P}_{m_k}\big) = 2$. Noticing that p_1 and p_2 both are the SG primes, we understand that this value is exactly equal to the number of SG primes in $[1, 3]$. This completes the proof of the theorem. □

By making faithfully use of Theorems 2.1 and 2.2 we can compute the number of SG primes in a given interval. However, when t is large, it is quite a troublesome work to find common solutions $c_i(d)$ $\big(i = 1, 2, \dots, \nu(d)\big)$ of (2.2) for all divisors d of P_m (the product of all primes up to $f(t)$) and to calculate all terms in the formula stated in Theorem 2.3. It would be therefore better to use directly the shifted sieve method of Eratosthenes avoiding the use of such common solutions. To clarify the procedure we will give an example below.

Example 2.4. We count here the number of SG primes in the interval $[1, 100]$. The largest prime p_{m_1} satisfying $p_{m_1} \leq f(100)$ is $p_6(= 13)$, and similarly we get $p_{m_2} = p_3(= 5)$, $p_{m_3} = p_2(= 3)$ and $p_{m_4} = p_1(= 2)$, so that $k = 4$. The solutions of $g_p(X) \equiv 0 \pmod{p}$ for $p \in \mathscr{P}_6$ are given by $c_1(p) = 0$ for all $p \in \mathscr{P}_6$, $c_2(p_2) = 1$, $c_2(p_3) = 2$, $c_2(p_4) = 3$, $c_2(p_5) = 5$ and $c_2(p_6) = 6$. First write the positive integers up to 100 and efface integers X satisfying (2.2) for all $p \in \mathscr{P}_6$. Then we get $H_1 = \{23, 29, 41, 53, 83, 89\}$ as the set of integers survived. Similarly, by extracting integers a from the intervals $[1, 13]$, $[1, 5]$ and $[1, 3]$ satisfying (2.1) for $p \in \mathscr{P}_3, \mathscr{P}_2$ and $\mathscr{P}_1$, respectively, we have the sets $H_2 = \{11\}$, $H_3 = \{5\}$ and $H_4 = \{1, 3\}$. We therefore know that $\pi_{\mathrm{SG}}(100) = \#\,(H_1 \cup H_2 \cup H_3 \cup H_4) = 10$ by Theorem 2.3. In fact, the set of SG primes up to 100 is $H_1 \cup H_2 \cup H_3 \cup \{2, 3\} = \{2, 3, 5, 11, 23, 29, 41, 53, 83, 89\}$.

3. SG prime chains

Let $l = l(q)$ be length of a SG prime chain (a Cunningham prime chain of the first kind) for a prime q. That is, for a prime $q = q_1$, l integers q_1, $q_2 = 2q_1 + 1$,

$q_3 = 2q_2 + 1$, ..., $q_l = 2q_{l-1} + 1$ are primes, but $q_{l+1} = 2q_l + 1$ is not. For example, if $q = 2$, then we have the SG prime chain $2 < 5 < 11 < 23 < 47$, where $95 = 2 \cdot 47 + 1$ is not a prime. So we have $l(2) = 5$.

For an odd prime p we denote by $\mathrm{ord}_p(2)$ the order of 2 mod p, i.e., $\mathrm{ord}_p(2)$ is the least positive exponent such that $2^{\mathrm{ord}_p(2)} \equiv 1 \pmod{p}$. Then we can easily show the following proposition.

PROPOSITION 3.1. *Given any odd $q \in \mathscr{S}$, it follows that $l(q) \le \mathrm{ord}_q(2)$.*

Proof. Let $q_1 = q$ and $q_{i+1} = 2q_i + 1$ for $i \ge 1$. If $k = \mathrm{ord}_q(2)$, then we have $q_{k+1} = 2q_k + 1 = 2^2 q_{k-1} + 2^2 - 1 = \cdots = 2^k q_1 + 2^k - 1 \equiv 0 \pmod{q_1}$, which shows that q_{k+1} is not a prime. Hence we have $l(q) \le \mathrm{ord}_q(2)$. □

Suppose that the odd prime $q = q_1 \in \mathscr{S}$ has length $l(q) \ge n$ for $n \ge 2$. Since $q_i = 2^{i-1} q_1 + (2^{i-1} - 1) \in \mathscr{S}$ for $i = 1, 2, \dots, n-1$ and $q_n \in \mathscr{P}$, each q_i $(1 \le i \le n-1)$ must satisfy condition (2.1) for all $p \in \mathscr{P}_{m(i)}$, where $\mathscr{P}_{m(i)}$ is the set of all primes up to $f(q_i)$. Here the following question arises naturally:

For every $n \ge 1$, is there always $q \in \mathscr{S}$ having length $l(q) \ge n$?

If the answer of this question is affirmative, then it is of course possible to state that there exist infinitely many SG primes. However, we may declare that this problem will present serious difficulties to solve. For numerical data of long such prime chains, see Löh's paper [2].

4. Another approach for computing $\pi_{\mathrm{SG}}(t)$

In this section we shall attempt another approach for counting the number of SG primes in the interval $[1, t]$.

By the density result for $\pi_{\mathrm{SG}}(t)$ with respect to $\pi(t)$ stated in the introduction, it is obvious that there are infinitely many primes which are not SG primes. We are able to confirm this fact in a very simple and elementary way.

For an odd prime p, consider the set

$$A(p) := \left\{ kp + \tfrac{p-1}{2} : k = 1, 2, 3, \dots \right\}.$$

It is clear that any prime in $A(p)$ cannot be the SG. Indeed, if $q = kp + (p-1)/2 \in A(p)$ is a prime, then $2q + 1 = (2k+1)p \equiv 0 \pmod{p}$, so that $q \notin \mathscr{S}$. Since there are infinitely many primes in $A(p)$ by Dirichlet's prime number theorem on arithmetic progressions, we are able to say that there are infinitely many primes not belonging to the set $\mathscr{S}$.

Further one can state

PROPOSITION 4.1. *There holds*

$$\mathscr{P}\Big\backslash \bigcup_{i=2}^{\infty} A(p_i) = \mathscr{S}\,.$$

P r o o f. Let $q \in \mathscr{P}\backslash\mathscr{S}$. Since $q \notin \mathscr{S}$, $2q+1$ is a composite, and so there is an odd prime p dividing $2q+1$, i.e., $2q+1 = kp$ with some odd integer $k \geq 3$. Here we see $q = \big((k-1)/2\big)p + (p-1)/2 \in A(p)$, which proves the proposition. □

If there are only finitely many SG primes, then we can say that for every prime q greater than the largest prime in $\mathscr{S}$ there exists an odd prime p such that $q \in A(p)$, or equivalently, that there exists $x_0 \geq 1$ such that $S(x; \mathscr{P}_m) = 0$ for any $x \geq x_0$, where $\mathscr{P}_m$ is the set of all primes up to $f(x)$. We cannot insist now strongly, but it seems that such a situation is unsatisfactory. However, this may be nothing but a mere wishful thinking.

Next, we would like to evaluate again $\pi_{\mathrm{SG}}(t)$ from the point of view of the fact stated in Proposition 4.1. Letting $d \geq 3$ be an odd and square-free integer, consider the set $A(d) := \bigcap_{p|d} A(p)$. By the Chinese remainder theorem an element in $A(d)$ can be expressed in the form $k'd + r(d)$ with some $k' \geq 0$, where $r(d)$ is the least positive common solution modulo d of the congruences $X \equiv (p-1)/2 \pmod{p}$ for all $p \in \mathscr{P}(d)$. So we may write this set as

$$A(d) = \{k'd + r(d) \colon k' = 0, 1, 2, \ldots\}\,.$$

Here note that $(p-1)/2 \notin A(p)$ for an odd prime p, but $r(d) \in A(d)$ for a composite number d.

Let $\pi_{A(1)}(t) := \pi(t)$ and $\pi_{A(d)}(t)$ (with $d \geq 3$ odd) be the number of primes $\leq t$ in the set $A(d)$, including the case when d is an odd prime. Further let $h(t) := (2t+1)/3$, p_m be the largest prime satisfying $p_m \leq h(t)$ for $t \geq 4$ and put $Q_m := P_m/p_1 = p_2 p_3 \cdots p_m$. We note that if $t \geq 4$, then the smallest element $z = p_m + (p_m - 1)/2$ in $A(p_m)$ satisfies $z \leq t$, hence $A(p_i) \cap [1, t] \neq \emptyset$ for all $i = 2, 3, \ldots, m$.

With these preparations, we can state the following theorem:

THEOREM 4.2. *Let $t \geq 4$ be a real number. Then*

$$\pi_{\mathrm{SG}}(t) = \sum_{d|Q_m} \mu(d)\,\pi_{A(d)}(t)\,.$$

P r o o f. First we remark that $h(t) \geq 3$ if $t \geq 4$, hence $Q_m \geq 3$. This implies $\mathscr{P}(Q_m) \neq \emptyset$. By means of the inclusion-exclusion principle the theorem clearly follows from Proposition 4.1. □

Applying de la Vallée Poussin's result on the number of primes $\leq t$ in arithmetic progression, one gets

$$\pi_{A(d)}(t) \sim \frac{1}{\varphi(d)} \cdot \frac{t}{\log t},$$

where φ is the Euler totient function. On the other hand, noticing that Q_m is odd and square-free, we obtain for $t \geq 4$

$$L(t) := \sum_{d \mid Q_m} \frac{\mu(d)}{\varphi(d)} = \prod_{p \mid Q_m} \left(1 - \frac{1}{p-1}\right) = \prod_{\substack{p \text{ odd} \\ p \leq h(t)}} \left(\frac{p-2}{p-1}\right),$$

where the product on the right-hand side are taken over all odd primes p with $p \leq h(t)$. Based on Theorem 4.2, we may expect the following formula:

$$\pi_{SG}(t) = O\Big(L(t)\frac{t}{\log t}\Big).$$

At last, we would like to mention that by similar methods to those stated in this paper it is also possible to formulate the number of primes of the form $ap + b$ (where p is a prime and a, b are fixed integers prime to each other with $a \geq 1$, $b \neq 0$ and a, b not both odd) in a given interval. We hope to deduce the Legendre type formula for the number of primes $\leq t$ having this form and to discuss the distribution of these primes in another paper.

REFERENCES

[1] INDLEKOFER, K. H.—JÁRAI, A.: *Largest known twin primes and Sophie Germain primes*, Math. Comp. **68** (1999), 1317–1324.

[2] LÖH, G.: *Long chains of nearly doubled primes*, Math. Comp. **53** (1989), 751–759.

[3] POWELL, B. J.: *Primitive densities of certain sets of primes*, J. Number Theory **12** (1980), 210–217.

[4] RIBENBOIM, P.: 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, Berlin, Heidelberg, New York, 1979.

[5] RIBENBOIM, P.: *The New Book of Prime Number Records*, Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[6] RIBENBOIM, P.: *Fermat's Last Theorem for Amateurs*, Springer-Verlag, Berlin, Heidelberg, New York, 1999.

Received October 29, 1999

Department of Mathematics
Science University of Tokyo
Noda, Chiba 278–8510
JAPAN

E-mail: agoh@ma.noda.sut.ac.jp