Smooth Orders and Cryptographic Applications

Carl Pomerance[1] and Igor E. Shparlinski[2]

[1] Department of Fundamental Mathematics, Bell Laboratories
Murray Hill, NJ 07974-0636, USA
carlp@research.bell-labs.com
[2] Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract. We obtain rigorous upper bounds on the number of primes $p \le x$ for which $p-1$ is smooth or has a large smooth factor. Conjecturally these bounds are nearly tight. As a corollary, we show that for almost all primes p the multiplicative order of 2 modulo p is not smooth, and we prove a similar but weaker result for almost all odd numbers n. We also discuss some cryptographic applications.

1 Introduction

We recall that an integer $k \ge 1$ is called y-smooth if it is divisible only by primes $p \le y$. Here we obtain reasonably good upper bounds on the number of primes $p \le x$ for which $p-1$ is y-smooth and also for primes $p \le x$ for which $p-1$ has a large y-smooth factor.

We apply these bounds to show that for almost all primes p the multiplicative order $l(p)$ of 2 modulo p is not smooth. In particular, we show that for any function $\varepsilon(p) \to 0$, for almost all primes p, $l(p)$ has a prime divisor $q \ge p^{\varepsilon(p)}$. We also prove a similar statement for the multiplicative order $l(n)$ of 2 modulo almost all odd integers n.

Besides being a natural question, it also has some cryptographic motivations which we discuss in Section 4.

As usual, $\varphi(m)$ denotes the Euler function. We use log to denote the natural logarithm. Throughout the paper the implied constants in symbols 'O', '$\gg$' and '$\ll$' are absolute (the notations $U \ll V$ and $V \gg U$ are equivalent to $U = O(V)$ for positive functions U, V). The symbol '$\sim$' indicates the asymptotic relation is uniform over all parameters in their stated ranges.

2 Smooth Divisors of $p - 1$

Let $P(n)$ denote the largest prime divisor of the integer $n \ge 2$, and let $P(1) = 1$. Let $\pi(x, y)$ denote the number of primes $p \le x$ with $P(p-1) \le y$. Let $\psi(x, y)$ denote the number of positive integers $n \le x$ with $P(n) \le y$. It seems reasonable to conjecture that a random integer in the interval $[1, x]$ is about as likely to be

C. Fieker and D.R. Kohel (Eds.): ANTS 2002, LNCS 2369, pp. 338–348, 2002.

y-smooth as is a random integer of the form $p-1$ where p is a prime in $[1,x]$, at least if y is not too small. That is, it may be that

$$\frac{1}{x}\psi(x,y) \ \sim \ \frac{1}{\pi(x)}\pi(x,y), \tag{1}$$

for $y \le x$ and $y \to \infty$. This possibility is explicitly raised in [18], but the thought goes back at least to [6]. Through the years there has been progress towards the weaker assertion

$$\pi(x,y) \ \gg \ \psi(x,y)/\log x,$$

but only in the range $x^{\vartheta} \le y \le x$, where $\vartheta > 0$ is fixed. A recent paper of Baker and Harman [2] has the champion value of ϑ, namely 0.2961, but they have the inequality in the somewhat weaker form

$$\pi(x,y) \ \ge \ \psi(x,y)/(\log x)^{O(1)}.$$

Earlier papers on this subject are the already-cited [6] and [18], as well as papers by Wooldridge, Balog, Fouvry and Grupp, and Friedlander. In [1] there is a proof that $\pi(x,y)$ is proportional to $\pi(x)$ when $\log x/\log y$ is bounded, conditional on a reasonable hypothesis on the distribution of primes in arithmetic progressions. In addition, Granville (see [8]) has an unpublished argument that (1) holds when $\log x/\log y$ is bounded, conditional on the Elliott-Halberstam conjecture. In [15] a connection of (1) to a strong form of the generalized twin prime conjecture is demonstrated.

There are highly nontrivial *upper* bounds for $\pi(x,y)$ by Fouvry and others when $y > x^{1/2}$, and here the quest is to find the largest value of ϑ for which you can prove there is some $c > 0$ with $\pi(x,x^{\vartheta}) \le (1-c+o(1))\pi(x)$, or even just $\pi(x) - \pi(x,x^{\vartheta}) \to \infty$. Such a quest may be considered a back-door attack on the conjecture that there are infinitely many Sophie Germain primes, namely primes q where $2q+1$ is also prime. However, the results in our paper are more aimed at smaller values of y; we make no new contribution towards the problem of a nontrivial upper bound for $\pi(x,y)$ when y is large. Finally, we remark that there is at least one paper [16] (brought to our attention by the referee) that gives an upper bound for the number of primes up to x for which the order of a given element is y-smooth when $y > x^{1/2}$.

Let $\rho(u)$ denote the Dickman–de Bruijn function which is defined by

$$\rho(u) \ = \ 1, \qquad 0 \le u \le 1,$$

and

$$\rho(u) \ = \ 1 - \int_1^u \frac{\rho(v-1)}{v}dv, \qquad u > 1.$$

We recall that $\rho(u) = u^{-u+o(u)}$ as $u \to \infty$. For these and other properties of $\rho(u)$, see [25].

It is known that $\psi(x,y) \sim \rho(u)x$ in a wide range, and so, in light of the above comments, it seems appropriate to compare $\pi(x,y)$ with $\rho(u)\pi(x)$. In fact we give an upper bound for $\pi(x,y)$ that is nearly this sharp.

We begin with the following lemma which is perhaps of independent interest.

Lemma 1. *For* $\exp\left((\log\log x)^2\right) \le y \le x$, *we have*

$$\sum_{m\le x,\ P(m)\le y} \frac{m}{\varphi(m)} \ \sim\ \frac{\zeta(2)\zeta(3)}{\zeta(6)}\psi(x,y)$$

where $u = \log x/\log y$ *and where* $\zeta(s)$ *denotes the Riemann zeta function.*

Proof. Let $z = \log y$ and assume that $\exp\left((\log\log x)^2\right) \le y \le x$. We have

$$\begin{aligned}\sum_{m\le x,\ P(m)\le y} \frac{m}{\varphi(m)} \ &=\ \sum_{m\le x,\ P(m)\le y}\ \sum_{d\mid m}\frac{\mu^2(d)}{\varphi(d)}\\ &=\ \sum_{d\le x,\ P(d)\le y}\frac{\mu^2(d)}{\varphi(d)}\sum_{m\le x/d,\ P(m)\le y} 1\\ &=\ \sum_{d\le z,\ P(d)\le y}\frac{\mu^2(d)}{\varphi(d)}\psi(x/d,y)\ +\ \sum_{z<d\le x,\ P(d)\le y}\frac{\mu^2(d)}{\varphi(d)}\psi(x/d,y).\end{aligned}$$

Since $\psi(x,y)\sim\rho(u)x$ uniformly for $y\ge\exp\left((\log\log x)^{5/3+\varepsilon}\right)$, a result of Hildebrand (see [25], Chapter III.5, Corollary 9.3) and since

$$\rho(\log(x/d)/\log y)\ \sim\ \rho(u)$$

for $y\ge\exp\left((\log\log x)^2\right)$ and $d\le z$, we have

$$\begin{aligned}\sum_{d\le z,\ P(d)\le y}\frac{\mu^2(d)}{\varphi(d)}\psi(x/d,y) &\sim\ \rho(u)x\sum_{d\le z,\ P(d)\le y}\frac{\mu^2(d)}{d\varphi(d)}\ \sim\ \rho(u)x\sum_{P(d)\le y}\frac{\mu^2(d)}{d\varphi(d)}\\ &\sim\ \rho(u)x\sum_{d\ge1}\frac{\mu^2(d)}{d\varphi(d)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)}\rho(u)x.\end{aligned}$$

Let $j_0 = \lfloor\log z\rfloor$, so that

$$\begin{aligned}\sum_{z<d\le x,\ P(d)\le y}\frac{\mu^2(d)}{\varphi(d)}\psi(x/d,y) \ &\le\ \sum_{j_0\le j<\log x}\ \sum_{e^j<d\le e^{j+1},\ P(d)\le y}\frac{\mu^2(d)}{\varphi(d)}\psi(x/d,y)\\ &\ll x\sum_{j_0\le j<\log x}\ \sum_{e^j<d\le e^{j+1},\ P(d)\le y}\frac{\mu^2(d)}{d\varphi(d)}\rho\left(u-\frac{j+1}{\log y}\right)\\ &\ll\ x\sum_{j_0\le j<\log x} e^{-j}\rho\left(u-\frac{j+1}{\log y}\right)\\ &\ll\ xe^{-j_0}\rho\left(u-\frac{j_0+1}{\log y}\right)\ =\ o(\rho(u)x),\end{aligned}$$

by the choice of z. This completes the proof. □

Theorem 1. *For* $\exp\left(\sqrt{\log x \log\log x}\right) \le y \le x$, *we have*

$$\pi(x,y) \ll u\rho(u)\pi(x)$$

where $u = \log x/\log y$.

Proof. In the following the letter q runs over prime numbers. Let $\pi_q(x)$ denote the number of primes $p \le x$ with $P(p-1) = q$. Let $z = \exp\left((\log\log x)^2\right)$, and assume $z \le Y \le x$. We have

$$\begin{aligned}\pi(x,Y) - \pi(x,Y/e) &= \sum_{Y/e<q\le Y} \pi_q(x) = \sum_{Y/e<q\le Y} \sum_{\substack{m\le(x-1)/q,\, P(m)\le q\\ mq+1 \text{ prime}}} 1\\ &\le \sum_{\substack{m\le ex/Y\\ P(m)\le Y}} \sum_{\substack{Y/e<q\le Y\\ mq+1 \text{ prime}}} 1 \ll \sum_{\substack{m\le ex/Y\\ P(m)\le Y}} \frac{m}{\varphi(m)} \cdot \frac{Y}{\log^2 Y},\end{aligned}$$

where we use Brun's method (see [9], Theorem 2.2, page 68) for the last inequality. We thus have by Lemma 1,

$$\begin{aligned}\pi(x,Y) - \pi(x,Y/e) &\ll \rho\left(\frac{\log x - \log Y + 1}{\log Y}\right)\frac{x}{Y}\cdot\frac{Y}{\log^2 Y}\\ &\le \frac{x}{\log^2 Y}\rho\left(\frac{\log x}{\log Y} - 1\right).\end{aligned}$$

Now assume y is as in the theorem and let $i_0 = \lfloor \log z \rfloor$. Then, by the above estimate,

$$\begin{aligned}\pi(x,y) &\le \pi(x,z) + \sum_{i=0}^{i_0}\left(\pi(x,y/e^i) - \pi(x,y/e^{i+1})\right)\\ &\ll \psi(x,z) + x\sum_{i=0}^{i_0}\frac{1}{(\log y - i)^2}\rho\left(\frac{\log x}{\log y - i} - 1\right).\end{aligned}$$

The function $f(t) = \rho(\log x/(\log y - t) - 1)/(\log y - t)^2$ is decreasing for $0 \le t \le i_0$, so that

$$\begin{aligned}&\sum_{i=0}^{i_0}\frac{1}{(\log y - i)^2}\rho\left(\frac{\log x}{\log y - i} - 1\right)\\ &\le \frac{\rho(u-1)}{\log^2 y} + \int_0^{i_0}\frac{1}{(\log y - t)^2}\rho\left(\frac{\log x}{\log y - t} - 1\right)dt.\end{aligned}$$

The integral is equal to

$$\begin{aligned}\frac{1}{\log x}\int_{u-1}^{\frac{\log x}{\log y - i_0} - 1}\rho(s)\,ds &< \frac{1}{\log x}\int_{u-1}^{\infty}\rho(s)\,ds = -\frac{1}{\log x}\int_u^{\infty} t\rho'(t)\,dt\\ &= \frac{1}{\log x}\left(u\rho(u) + \int_u^{\infty}\rho(t)\,dt\right) \ll u\rho(u)/\log x.\end{aligned}$$

Thus,

$$\pi(x,y) \ \ll \ \psi(x,z) + \rho(u-1)x/\log^2 y + u\rho(u)x/\log x. \tag{2}$$

Note that $\rho(u-1) \sim \rho(u)u\log u$, see (61) in Chapter III.5 of [25]. We have then that $\rho(u-1)/\log^2 y \ll u\rho(u)/\log x$ in the stated range for y. In addition, by the choice of z, the term $\psi(x,z)$ is negligible in comparison to $u\rho(u)x/\log x$. This completes the proof of the theorem. □

We remark that but for the factor u in Theorem 1, the estimate is likely to be best possible. It is reasonable to conjecture that $\pi(x,y) = o(\psi(x,y))$ uniformly for $x \to \infty$ and $y \ge 2$. Theorem 1 implies this result for $y \ge \exp\left(\sqrt{\log x \log\log x}\right)$, and (2) does so in the wider range $y \ge \exp\left((\log x)^{1/3+\varepsilon}\right)$. That $\pi(x,2) = o(\psi(x,2))$ is essentially due to Fermat, but already for $y = 3$, the conjecture that $\pi(x,3) = o(\psi(x,3))$ seems difficult. Hooley [11] has shown, under assumption of several unproved hypotheses, including the Generalised Riemann Hypothesis, that the set of integers n with $2^n - 3$ prime has density 0. It is likely the same proof would go through for primes of the form $3 \cdot 2^n + 1$. Thus, there may be a conditional proof that $\pi(x,3) = o(\psi(x,3))$, and if so, it is likely that a similar proof would work for $\pi(x,y) = o(\psi(x,y))$ with y fixed or growing slowly.

There is another approach to Theorem 1 through direct sieving. That is, for any parameter z with $1 \le z \le y$ we have

$$\pi(x,y) - \pi(z) \ \le \ \sum_{P(d)\le z} \mu(d) \sum_{\substack{n\le x,\ P(n)\le y \\ n\equiv -1 \pmod d}} 1.$$

The inner sum has been studied somewhat, see [7], and using such results, plus sieve methods, may yield a larger range of validity in Theorem 1.

Now, let $\pi(x,y,w)$ denote the number of primes $p \le x$ such that $p-1$ has a divisor $m > w$ with $P(m) \le y$.

Theorem 2. *For* $\exp\left(\sqrt{\log x \log\log x}\right) \le y \le w \le x$, *we have*

$$\pi(x,y,w) \ \ll \ \frac{u\rho(v)}{\log(2v)}\pi(x) + u\rho(u)\pi(x),$$

where $u = \log x/\log y$, *and* $v = \log w/\log y$.

Proof. Let $Q(n)$ denote the least prime factor of n, if the integer $n > 1$, and let $Q(1) = +\infty$. For a positive integer m, let $\pi_m(x,y)$ denote the number of primes $p \le x$ such that $m|p-1$ and such that all prime factors of $(p-1)/m$ exceed y, that is, $Q((p-1)/m) > y$. Note that

$$\pi(x,y,w) \ = \ \sum_{m>w,\ P(m)\le y} \pi_m(x,y).$$

Therefore, by Brun's method, see [9],

$$\pi(x,y,w) - \pi(x,y) \ \le \ \sum_{w<m<x/y,\ P(m)\le y} \pi_m(x,y)$$

$$\begin{aligned}
&\leq \sum_{w<m<x/y,\, P(m)\leq y} \; \sum_{\substack{n\leq (x+1)/m,\, Q(n)>y \\ nm+1 \text{ prime}}} 1 \\
&\ll \sum_{w<m<x/y,\, P(m)\leq y} \frac{x/m}{\log y \log(x/m)} \cdot \frac{m}{\varphi(m)} \\
&\leq \frac{x}{\log^2 y} \sum_{w<m<x/y,\, P(m)\leq y} \frac{1}{\varphi(m)}.
\end{aligned}$$

Now,

$$\begin{aligned}
\sum_{w<m<x,\, P(m)\leq y} \frac{1}{\varphi(m)} &= \sum_{w<m<x,\, P(m)\leq y} \frac{1}{m} \cdot \frac{m}{\varphi(m)} \\
&= \frac{1}{x} \sum_{w<m<x,\, P(m)\leq y} \frac{m}{\varphi(m)} + \int_w^x \frac{1}{t^2} \sum_{w<m\leq t,\, P(m)\leq y} \frac{m}{\varphi(m)}\, dt.
\end{aligned}$$

Using Lemma 1, we have

$$\sum_{w<m\leq t,\, P(m)\leq y} \frac{m}{\varphi(m)} \;\leq\; \sum_{m\leq t,\, P(m)\leq y} \frac{m}{\varphi(m)} \;\ll\; \rho\left(\frac{\log t}{\log y}\right) t,$$

so that

$$\begin{aligned}
\sum_{w<m<x,\, P(m)\leq y} \frac{1}{\varphi(m)} &\ll \rho(u) + \int_w^\infty \frac{1}{t}\, \rho\left(\frac{\log t}{\log y}\right) dt \\
&= \rho(u) + \log y \int_v^\infty \rho(s)\, ds \\
&\ll \frac{\log y}{\log(2v)} \rho(v).
\end{aligned}$$

The last estimate follows from a similar integral calculation in the proof of Theorem 1, and from the fact that $\rho(s)/\rho(s+1) \sim s \log s$ as $s \to \infty$.

Putting this estimate into our earlier estimate, and using $\log x = u \log y$, we have that

$$\pi(x, y, w) - \pi(x, y) \;\ll\; \frac{\rho(v)}{\log(2v)} \cdot \frac{x}{\log y} \;=\; \frac{u\rho(v)}{\log(2v)} \cdot \frac{x}{\log x}.$$

This estimate, combined with Theorem 1, completes the proof. □

3 Smooth Orders of 2

For an odd integer n, let $l(n)$ denote the multiplicative order of 2 modulo n.

Let $\mathcal{L}(x, y)$ denote the set of odd primes $p \leq x$ with $l(p)$ being y-smooth, and let $L(x, y) = |\mathcal{L}(x, y)|$ be the cardinality of $\mathcal{L}(x, y)$.

Theorem 3. *For* $\exp\left(\sqrt{\log x \log\log x}\right) \le y \le x$, *we have*

$$L(x,y) \ \ll \ \frac{u\rho(u/2)}{\log(2u)}\pi(x),$$

where $u = \log x/\log y$.

Proof. Let $z = \log y$. We first consider only primes p with $l(p) > x^{1/2}/z$. Note that if $p \le x$ is such that $l(p)$ is y-smooth and $l(p) > x^{1/2}/z$, then $p-1$ has a y-smooth divisor which exceeds $x^{1/2}/z$. But, by Theorem 2, we have

$$\pi(x,y,x^{1/2}/z) \ \ll \ \frac{u\rho(u/2-\log z/\log y)}{\log(2u)}\pi(x) + u\rho(u)\pi(x) \ \sim \ \frac{u\rho(u/2)}{\log(2u)}\pi(x),$$

by our choice of z. Now let us estimate L_0, the number of primes p with $l(p)$ a y-smooth integer bounded by $x^{1/2}/z$. For each integer j, the number of primes p with $l(p) = j$ is evidently at most j, so that

$$L_0 \ \le \sum_{j \le x^{1/2}/z,\, P(j) \le y} j \ \le \ \frac{x^{1/2}}{z}\psi\left(\frac{x^{1/2}}{z}, y\right) \ \sim \ \frac{x}{z^2}\rho(u/2).$$

Since $x/z = xu/\log x \sim u\pi(x)$, and $\log(2u) = o(z)$ in the stated range for y, we have

$$L_0 \ \ll \ x\rho(u/2)/z^2 \ = \ o\left((u\rho(u/2)/\log(2u))\pi(x)\right),$$

which, with our earlier calculation, completes the proof. □

In particular, we see that for any function $\varepsilon(x) \to 0$, the number of primes $p \le x$ for which $l(p)$ is $x^{\varepsilon(x)}$-smooth is $o(\pi(x))$.

Now we show that Theorem 3 combined with known sieve estimates implies that the order of 2 modulo n is not smooth for almost all integer n.

Let $\mathcal{N}(x,y)$ denote the set of odd integers $n \le x$ with $l(n)$ being y-smooth, and let $N(x,y) = |\mathcal{N}(x,y)|$ be the cardinality of $\mathcal{N}(x,y)$.

Theorem 4. *For* $\exp\left(\sqrt{\log x \log\log x}\right) \le y \le x$, *we have*

$$N(x,y) \ \ll \ x/u$$

where $u = \log x/\log y$.

Proof. If $l(n)$ is y-smooth, then clearly each prime factor p of n must have $l(p)$ being y-smooth. By Brun's method (Theorem 2.2, p. 68 of [9])

$$\begin{aligned} N(x,y) \ &\ll \ x \prod_{p \le x,\, p \notin \mathcal{L}(x,y)} \left(1 - \frac{1}{p}\right) \ \ll \ \frac{x}{\log x} \prod_{p \in \mathcal{L}(x,y)} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \ \frac{x}{u} \prod_{p \in \mathcal{L}(x,y),\, p > y} \left(1 + \frac{1}{p}\right). \end{aligned}$$

It is now enough to show that

$$\sum_{p \in \mathcal{L}(x,y),\, p>y} \frac{1}{p} \ll 1.$$

By Theorem 3 and partial summation, we have

$$\begin{aligned}\sum_{p \in \mathcal{L}(x,y),\, p>y} \frac{1}{p} &= \frac{1}{x}\left(L(x,y) - \pi(y)\right) + \int_y^x \frac{1}{t^2}\left(L(t,y) - \pi(y)\right)\, dt \\ &\ll \int_y^x \frac{1}{t \log y} \rho\left(\frac{\log t}{2 \log y}\right)\, dt \\ &= \int_{1/2}^{u/2} 2\rho(s)\, ds \ll 1,\end{aligned}$$

which completes the proof. □

In particular, we see that for any function $\varepsilon(x) \to 0$, the number of odd integers $1 \le n \le x$ for which $l(n)$ is $x^{\varepsilon(x)}$-smooth is $o(x)$.

4 Cryptographic Applications

We remark that it is well known that primes p for which $p-1$ is smooth are not suitable for cryptographic applications which rely on the hardness of the discrete logarithm problem modulo p. Our Theorem 1 implies that there are very few such primes. This fact has never been doubted in practice but our results provide its rigorous confirmation and a quantitative form of this statement. Unfortunately it also means that the polynomial factorization algorithm of [23] almost never runs in polynomial time. A similar remark pertains to integer factorization via the $p-1$ method of Pollard (cf. [20]). Both of these applications to smooth values of $p-1$ are actually to *very* smooth values, and so the more delicate calculations of the current paper are not really necessary to deduce that usually the algorithms are not polynomial.

It is clear to see that using 2 as the generator for exponentiation-based cryptographic constructions, such as the Diffie-Hellman key exchange scheme, the El Gamal cryptosystem, the Digital Signature Algorithm and so on (these and many other examples can be found in [14,24]) reduces the cost of exponentiation. Indeed using repeated squaring type algorithms to compute $g^a \pmod p$ requires a substantial number of multiplications by g, see Section 9.3 of [5] or Chapter 14 of [14]. Thus using $g = 2$ reduces this stage to merely one bit-shift and, possibly, one subtraction of the modulus (only in 50% of the cases), for example, see Section 14.81 of [14].

We remark that it is often recommended to work in groups of prime order, which 2 may not necessarily generate. In this case one can select a large prime divisor q of the order $l(p)$ of 2 modulo p and then compute $g \equiv 2^r \pmod p$,

where $r = l(p)/q$. Obviously g generates a group of order q. Now, to compute $g^x \pmod p$ one just computes $y \equiv rx \pmod q$ and then

$$g^x \equiv 2^y \pmod p.$$

There is also one more reason to use 2 as the base. It has been shown in [4] that in this case a slight modification of the corresponding Diffie-Hellman key exchange scheme has a very important property of bit security (provided the whole scheme is secure in the traditional sense). More precisely, it has been shown in [4] that recovering even a certain bit of information about the modified secret Diffie-Hellman key modulo p (deciding whether it belongs to the interval $[0, (p-1)/2]$) is as hard as the recovering the whole key.

On the other hand, if the multiplicative order of 2 modulo p is smooth then the Pohlig–Hellman algorithm can be used to efficiently solve the discrete logarithm problem in base 2, see Section 3.6.4 of [14] or Section 5.1 of [24]. We recall that based on our current knowledge we may conclude that the hardness of the discrete logarithm problem modulo p in base g, for an integer g, is majorised

1. by $q^{1/2}$ where q is the largest prime divisor of the multiplicative order of g modulo p, see [14,24];
2. by $\mathbf{L}_p(1/2, 2^{1/2})$ for a rigorous unconditional algorithm, see [19];
3. by $\mathbf{L}_p\left(1/3, (64/9)^{1/3}\right)$ for the heuristic number field sieve algorithm, see [21,22],

where as usual we denote by $\mathbf{L}_m(\alpha, \gamma)$ any quantity of the form

$$\mathbf{L}_m(\alpha, \gamma) \;=\; \exp\left((\gamma + o(1))(\log m)^{\alpha}(\log\log m)^{1-\alpha}\right),$$

with the "$o(1)$" expression tending to 0 as the variable m tends to ∞.

The problem is: If the prime p is selected at random, what are the chances that the running time $q^{1/2}$ of the Pohlig–Hellman algorithm 1 is smaller than the running time of, say, algorithm 2? It follows from Theorem 3 that the chances of this occurring are vanishingly small. Thus, our result implies that for $g = 2$ and a randomly selected prime p, with probability exponentially close to 1, the security of the discrete logarithm to base $g = 2$ is as high as when a "safe" prime p is deliberately chosen (namely, a prime p where $p - 1$ is twice a prime).

For the suggested modifications in [4] of the ElGamal public key cryptosystem, it is also important that the order of 2 modulo p is not smooth and thus the discrete logarithm problem in the corresponding group is hard. On the other hand, as in [4], we have to warn that small generators are not suitable for using with the ElGamal signature scheme, see [3]. However, the results of this paper can be extended to multiplicative orders of any fixed integer $g \geq 2$.

5 Remarks

We remark that it is likely to be true that $L(x, y) \ll \rho(u)\pi(x)$ in the stated range for y. The slightly weaker estimate $L(x, y) \ll u\rho(u)\pi(x)$ is likely to be provable

assuming the Generalised Riemann Hypothesis, using the tools that Hooley [10] has used to prove Artin's conjecture on the Generalised Riemann Hypothesis.

Studying other arithmetic properties of $l(p)$, for example, the number of prime and integer divisors, is of interest as well. A recent paper on this subject is [17] (also see [13]).

Finally, having in mind applications to elliptic curve cryptography, one can ask how often a given elliptic curve defined over $\mathbb{Q}$ has a smooth order modulo a prime p. This subject is considered in [12], the paper of Lenstra where elliptic curve factoring is first introduced.

References

1. W. R. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers,' *Annals Math.* **140** (1994), 703-722.
2. R. C. Baker and G. Harman, 'Shifted primes without large prime factors,' *Acta Arith.* **83** (1998), 331–361.
3. D. Bleichenbacher, 'Generating ElGamal signatures without knowing the secret key,' *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1070** (1996), 10–18.
4. D. Boneh and R. Venkatesan, 'Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes,' *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.
5. R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, Springer-Verlag, New York, 2001.
6. P. Erdős, 'On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's ϕ-function,' *Quart. J. Math. (Oxford Ser.)* **6** (1935), 205–213.
7. A. Granville, 'Integers without large prime factors, in arithmetic progressions. II,' *Philos. Trans. Roy. Soc. London Ser. A* **345** (1993), 349–362.
8. A. Granville, 'Smooth numbers: computational number theory and beyond,' *Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Berkeley, 2000*, J. Buhler and P. Stevenhagen, eds., Cambridge University Press, to appear.
9. H. Halberstam and H.–E. Richert, *Sieve methods*, Academic Press, London, 1974.
10. C. Hooley, 'On Artin's conjecture,' *J. Reine Angew. Math.* **225** (1967), 209–220.
11. C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Mathematics, No. 70, Cambridge University Press, Cambridge-New York-Melbourne, 1976.
12. H. W. Lenstra, Jr., 'Factoring integers with elliptic curves,' *Ann. of Math.* **2** (1987), 649–673.
13. S. Li and C. Pomerance, 'On generalizing Artin's conjecture on primitive roots to composite moduli,' *Preprint*, 2001.
14. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.
15. G. Martin, 'An asymptotic formula for the number of smooth values of a polynomial,' *J. Number Theory* **93** (2002), 108–182.
16. P. Moree, 'A note on Artin's conjecture,' *Simon Stevin* **67** (1993), 255–257.
17. M. R. Murty and F. Saidak, 'Non-abelian generalizations of the Erdős–Kac theorem,' *Preprint*, 2001.

18. C. Pomerance, 'Popular values of Euler's function,' *Mathematika* **27** (1980), 84–89.
19. C. Pomerance, 'Fast, rigorous factorization and discrete logarithm algorithms,' *Discrete Algorithms and Complexity*, Academic Press, 1987, 119–143
20. C. Pomerance and J. Sorenson, 'Counting the integers factorable via cyclotomic methods,' *J. Algorithms* **19** (1995), 250–265.
21. O. Schirokauer, 'Discrete logarithms and local units,' *Philos. Trans. Roy. Soc. London, Ser. A* **345** (1993), 409–423.
22. O. Schirokauer, D. Weber and T. Denny, 'Discrete logarithms: The effectiveness of the index calculus method,' *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1122** (1996), 337–362.
23. V. Shoup, 'Smoothness and factoring polynomials over finite fields,' *Inform. Proc. Letters*, **38** (1991), 39–42.
24. D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL, 1995.
25. G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, University Press, Cambridge, UK, 1995.