J. Math. Crypt. **3** (2009), 265–271

DOI 10.1515 / JMC.2009.016

On the density of some special primes

John B. Friedlander and Igor E. Shparlinski

Communicated by Jaime Gutierrez

Abstract. We show, under the Generalized Riemann Hypothesis, that a certain set of primes which is of importance for the theory of pseudorandom sequences is of positive relative density. We also use an unconditional result of H. Mikawa, which in turn is based on the results of E. Bombieri, J. B. Friedlander and H. Iwaniec on primes in arithmetic progressions, which go beyond the range of the Generalized Riemann Hypothesis.

Keywords. Pseudorandom numbers, Artin's conjecture, primes in arithmetic progressions.

AMS classification. 11K45, 11T23, 11Y16.

1 Introduction

Let $\mathcal{R}$ be the set of primes r such that 2 is a primitive root modulo r. It has been demonstrated in [4, 9] that prime powers q for which $q-1$ has a large prime divisor $r \in \mathcal{R}$ are of special interest in the theory of pseudorandom sequences.

For example, let us fix a primitive root g of the field $\mathbb{F}_q$ of q elements, and define the sequence a_n, $n = 0, \ldots, q-2$ as

$$a_n = \begin{cases} 1 & \text{if } g^n + 1 \text{ is a quadratic non-residue in } \mathbb{F}_q, \\ 0 & \text{otherwise.} \end{cases}$$

Then W. Meidl and A. Winterhof, [9, Proposition 3] have shown that if $q-1$ has a prime divisor $r \in \mathcal{R}$ with $r \geq q^{1/2} + 1$, then the polynomial

$$A(X) = \sum_{n=0}^{q-2} a_n X^n \in \mathbb{F}_2[X]$$

is relatively prime to the rth cyclotomic polynomial $1 + X + \ldots + X^{r-1}$ over $\mathbb{F}_2$. This result has been generalized by N. Brandstätter and A. Winterhof [4, Proposition 1], where it is shown that if

$$r \geq q^{1/2} + 2k + 1$$

for some integer $k \geq 0$, then the co-primality property is preserved for any polynomial which differs from A in at most k coefficients. Furthermore, the result of [4, Proposition 1], also covers the case of arbitrary g (that is, when g is not necessary a primitive root of $\mathbb{F}_q$). In turn, such co-primality results are important in studying the linear complexity of the sequences introduced by V. M. Sidel'nikov [11] (and also in [8]) as well as their generalizations, see, for example, [4, Corollary 1]. Further references to other works on Sidel'nikov sequences can be found in [4, 9].

We note that although numerical calculations have confirmed that such prime powers p are quite common, no rigorous results about their existence and distribution have been known prior to this paper. Furthermore, since squares and higher powers of primes form a very sparse sequence, we mainly concentrate on the distribution of primes p for which $p-1$ has a large prime divisor $r \in \mathcal{R}$.

Clearly there are two main difficulties in studying such prime powers:

- One stems from the fact that r needs to have a prescribed primitive root, namely 2. This however can be handled with the help of the result of C. Hooley [6] who, under the *Generalized Riemann Hypothesis* (GRH) has established an asymptotic formula for the number of such primes $r \le x$.
- The other obstacle is the fact that any "interesting" $q \equiv 1 \pmod r$ needs to be bounded by $(r-1)^2$ (or even by a smaller quantity for the results of [4, Corollary 1]). This range is too short even for the GRH to be useful. However, here we use the result of H. Mikawa [10], which in turn is based on the results of E. Bombieri, J. B. Friedlander and H. Iwaniec [1, 2, 3] to break through the barrier imposed by the limits of the GRH.

The results which we obtain seem to be new and not previously discussed in the literature. Apart from this, we hope that this work will also exhibit some very powerful tools that have never been used for cryptographic applications.

2 Main result

For real $x \ge y \ge 1$ we denote by $\mathcal{P}(x,y)$ the set of primes $p \in [x, 2x]$ such that $p-1$ has a prime divisor $r \in \mathcal{R}$ with $r \ge y$. In view of the aforementioned potential applications, we are primarily interested in the case $y > (2x)^{1/2}$.

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$.

Let

$$A = \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) = 0.373955\ldots \tag{2.1}$$

be the *Artin constant*.

Theorem 2.1. *Assume the GRH, then for any fixed α with*

$$\alpha < \frac{17}{32}$$

and $x^{1/2} \le y = x^{\alpha}$, we have

$$\#\mathcal{P}(x,y) \ge \left(A\frac{\log(17/32\alpha)}{100} + o(1)\right)\frac{x}{\log x}.$$

Note that, when we refer to the GRH we specifically mean the Riemann Hypothesis for the Dedekind zeta-functions of the Kummer extensions $\mathbb{Q}(\sqrt[k]{2}, \sqrt[k]{1})$.

3 Auxiliary tools

We denote by $\Pi(z)$ the set of $r \in \mathcal{R}$ with $r \le z$. We recall the result of C. Hooley [6]:

Lemma 3.1. *Assuming the GRH, for any real* $z > 1$, *we have*

$$\Pi(z) = A\frac{z}{\log z} + O\left(z(\log z)^{-2}\right),$$

where A *is given by* (2.1).

Using standard arguments, we now obtain

Lemma 3.2. *Assuming the GRH, for any real* $z > 3$, *we have*

$$\sum_{\substack{r \le z \\ r \in \mathcal{R}}} \frac{1}{r} = A \log\log z + B + O\left(1/\log z\right),$$

where A *is given by* (2.1) *and* B *is some absolute constant.*

Proof. We consider the function

$$\Theta(z) = \sum_{\substack{r \le z \\ r \in \mathcal{R}}} \frac{\log r}{r}.$$

By partial summation and Lemma 3.1,

$$\sum_{\substack{r \le z \\ r \in \mathcal{R}}} \frac{\log r}{r} = \frac{\Pi(z)\log z}{z} + \int_2^z \frac{\log t - 1}{t^2}\Pi(t)\,dt = A\int_2^z \frac{\log t - 1}{t\log t}\,dt + O\left(1\right).$$

The same arguments also imply that

$$\sum_{r \le z} \frac{\log r}{r} = \int_2^z \frac{\log t - 1}{t \log t}\,dt + O\left(1\right).$$

The *Mertens theorem*, see [5, Sections 22.7 and 22.8] or [12, Sections I.1.4 and I.1.5], now yields

$$\Theta(z) = \sum_{\substack{r \le z \\ r \in \mathcal{R}}} \frac{\log p}{p} = A\log z + \Delta(z),$$

where $\Delta(z) = O(1)$. Applying partial summation again, we derive

$$\begin{aligned}\sum_{\substack{r \le z \\ r \in \mathcal{R}}} \frac{1}{r} &= \frac{\Theta(z)}{\log z} + \int_2^z \frac{\Theta(t)}{t\log^2 t}\,dt \\ &= \frac{A\log z + \Delta(z)}{\log z} + \int_2^z \frac{A\log t + \Delta(t)}{t\log^2 t}\,dt\end{aligned}$$

$$= A\log\log z - A\log\log 2 + A + \int_2^x \frac{r(t)}{t\log^2 t}\,dt + O\left(1/\log z\right)$$
$$= A\log\log z - A\log\log 2 + A + \int_2^\infty \frac{\Delta(t)}{t\log^2 t}\,dt + O\left(1/\log z\right)$$

(here the existence of the improper integral follows from $\Delta(t) = O(1)$). Thus putting

$$B = -A\log\log 2 + A + \int_2^\infty \frac{\Delta(t)}{t\log^2 t}\,dt,$$

we conclude the proof. □

As usual, for a real $z \ge 1$ and integers $k > a > 0$, we use $\pi(z;k,a)$ to denote the number of primes $p \le z$ with $p \equiv a \pmod k$. We also put

$$\varpi(x;k,a) = \pi(2x;k,a) - \pi(x;k,a).$$

Our next result follows immediately from much more general estimates due to H. Mikawa [10, Bounds (4) and (5)].

Lemma 3.3. *For any fixed $\beta < 17/32$ and $u \le x^\beta$*

$$\sum_{\substack{u\le r<2u\\ r\in\mathcal{R}}} \varpi(x;r,1) \ge \left(\frac{1}{100} + o(1)\right)\frac{x}{\log x}\sum_{\substack{u\le r<2u\\ r\in\mathcal{R}}}\frac{1}{r}.$$

4 Proof of Theorem 2.1

Since for a prime $p \in [x,2x]$ the congruence $p \equiv 1 \pmod r$ is possible for at most one odd prime divisor $r \ge y \ge x^{1/2}$, we obtain

$$\#\mathcal{P}(x,y) = \sum_{\substack{r\ge y\\ r\in\mathcal{R}}} \varpi(x;r,1). \tag{4.1}$$

We now fix an arbitrary β with $\alpha < \beta < 17/32$ and put

$$J = \left\lfloor (\beta-\alpha)\frac{\log x}{\log 2}\right\rfloor.$$

Then we derive from (4.1)

$$\#\mathcal{P}(x,y) \ge \sum_{\substack{2^J y>r\ge y\\ r\in\mathcal{R}}} \varpi(x;r,1) \ge \sum_{j=0}^{J-1}\sum_{\substack{2^{j+1}y>r\ge 2^j y\\ r\in\mathcal{R}}} \varpi(x;r,1).$$

Using Lemma 3.3, we obtain

$$\begin{aligned}\#\mathcal{P}(x,y) &\geq \sum_{\substack{2^J y > r \geq y \\ r \in \mathcal{R}}} \varpi(x;r,1) \geq \Big(\frac{1}{100}+o(1)\Big)\frac{x}{\log x}\sum_{j=0}^{J-1}\sum_{\substack{2^{j+1}y>r\geq 2^j y \\ r\in\mathcal{R}}}\frac{1}{r} \\ &= \Big(\frac{1}{100}+o(1)\Big)\frac{x}{\log x}\sum_{\substack{2^J y>r\geq y \\ r\in\mathcal{R}}}\frac{1}{r}.\end{aligned} \tag{4.2}$$

Now by Lemma 3.2, we deduce

$$\begin{aligned}\sum_{\substack{2^J y>r\geq y \\ r\in\mathcal{R}}}\frac{1}{r} &\geq A\Big(\log\log 2^J y - \log\log y + O\Big(\frac{1}{\log x}\Big)\Big) \\ &= A\Big(\log\log x^{\beta+o(1)} - \log\log x^{\alpha+o(1)} + O\Big(\frac{1}{\log x}\Big)\Big) \\ &= A\frac{\log(\beta/\alpha)}{100} + o(1).\end{aligned}$$

Substituting this bound in (4.2), we obtain

$$\#\mathcal{P}(x,y) \geq \Big(A\frac{\log(\beta/\alpha)}{100}+o(1)\Big)\frac{x}{\log x}.$$

Since $\alpha < \beta < 17/32$ are arbitrary, the result follows.

5 Comments

For $\alpha = 1/2$, which is the first case interesting for applications, Theorem 2.1 implies that the set of suitable primes is of density at least

$$A\frac{\log(17/16)}{100} = 0.0002267\ldots.$$

This is certainly below what is heuristically expected. For example, under the *Elliott–Halberstam Conjecture*, see [7, Section 17.1], which asserts that for any fixed $\varepsilon > 0$ and $C > 1$

$$\sum_{k\leq z^{1-\varepsilon}}\max_{\gcd(a,k)=1}\left|\pi(z;k,a)-\frac{\pi(z)}{\varphi(k)}\right| \ll z(\log z)^{-C}$$

where as usual $\pi(z)$ is the number of primes $p \leq z$ and $\varphi(k)$ is the Euler function, one can derive from (4.1) that

$$\#\mathcal{P}(x,y) = (A\log(1/\alpha)+o(1))\,\frac{x}{\log x}$$

for $x^{1/2} \le y \le x^{\alpha+o(1)}$ with any fixed $\alpha < 1$. In particular, for $\alpha = 1/2$ we believe that the expected density of suitable primes is about

$$A \log 2 = 0.2592\ldots.$$

We note that the threshold $17/32$ in Lemma 3.3 might be very hard to improve, but improving the denominator 100 seems to be a more feasible task and this will immediately lead to better rigorous estimates.

Acknowledgments. The authors are grateful to Arne Winterhof for attracting our attention to this problem, literature pointers and useful discussions. The second author thanks Jaime Gutierrez and the other organizers of the 2nd Workshop on Mathematical Cryptology, Santander, October 2008, where the idea of this work appeared.

During the preparation of this paper, the first author was supported in part by NSERC Grant A5123, and the second by ARC Grant DP0881473.

References

[1] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. 156 (1986), pp. 203–251.

[2] ______, *Primes in arithmetic progressions to large moduli, II*, Math. Ann. 277 (1987), pp. 361–393.

[3] ______, *Primes in arithmetic progressions to large moduli, III*, J. Amer. Math. Soc. 2 (1989), pp. 215–224.

[4] N. Brandstätter and A. Winterhof, *Subsequences of Sidelnikov sequences*. Proceedings of the 8th Conference on Finite Fields and Applications, pp. 33–46. Contemporary Mathematics 461, Amer. Math. Soc., Providence, RI, 2008.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford Univ. Press, Oxford, 1979.

[6] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), pp. 209–220.

[7] H. Iwaniec and E. Kowalski, *Analytic Number Theory*. Amer. Math. Soc., Providence, RI, 2004.

[8] A. Lempel, M. Cohn, and W. L. Eastman, *A class of balanced binary sequences with optimal autocorrelation properties*, IEEE Trans. Inform. Theory 23 (1977), pp. 38–42.

[9] W. Meidl and A. Winterhof, *Some notes on the linear complexity of Sidel'nikov–Lempel–Cohn–Eastman sequences*, Des. Codes Cryptogr. 38 (2006), pp. 159–178.

[10] H. Mikawa, *On primes in arithmetic progressions*, Tsukuba J. Math. 25 (2001), pp. 121–153.

[11] V. M. Sidel'nikov, *Some k-valued pseudo-random sequences and nearly equidistant codes*, Problemy Peredachi Inform. 5(1) (1969), pp. 16–22 (in Russian).

[12] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*. Cambridge University Press, 1995.

Received 8 December, 2008; revised 18 September, 2009

Author information

John B. Friedlander, Department of Mathematics, University of Toronto,
Toronto, Ontario M5S 3G3, Canada.
Email: frdlndr@math.toronto.edu

Igor E. Shparlinski, Department of Computing, Macquarie University,
Sydney, NSW 2109, Australia.
Email: igor@comp.mq.edu.au