ACTA ARITHMETICA
179.4 (2017)

How strong can primes be

by

Ping Xi (Xi'an)

1. Introduction. In the RSA algorithm, one usually generates the modulus n by some primes p, q with certain properties which do not permit one to factorize n easily. Among the algebraic-group factorization algorithms, we would like to mention Pollard's $p-1$ algorithm [Po] and Williams' $p+1$ algorithm [Wi], which work well if $p-1$ and $p+1$ have only small prime factors. To defend against factoring attacks, it is suggested that one uses strong primes to construct RSA schemes (see [RS] for a nice survey).

A prime number p is said to be *strong* if $p+1$ has a large prime factor q, $p-1$ has a large prime factor q', and $q'-1$ has a large prime factor q''. More precisely, we call a prime p $(\theta_1, \theta_2, \theta_3)$-*strong* if

$$\begin{cases} p+1 \text{ has a large prime factor } q > p^{\theta_1}; \\ p-1 \text{ has a large prime factor } q' > p^{\theta_2}; \\ q'-1 \text{ has a large prime factor } q'' > p^{\theta_3}. \end{cases}$$

In practice, it is difficult to characterize the above three properties simultaneously and only a subset of such restrictions is usually required.

Gordon [Go] published an algorithm to find strong primes if the lengths of q and q' in bits are approximately half the length of p and the length of q'' is slightly less than that of q'. In particular, he showed that finding strong primes requires only 19% more work than the naive algorithm for finding random primes. Gordon's method is effective in practice; however, theoretically it is difficult to decide whether there exist such strong primes p of a given number of bits. If one accepts $\theta_3 = 0$, the answer is affirmative [Me]: the proportion of $(1/2, 1/2, 0)$-strong primes is at least $1/8$.

2010 *Mathematics Subject Classification*: 11Y05, 11N05, 11N13.
Key words and phrases: strong primes, greatest prime factor, Brun–Titchmarsh theorem.
Received 28 July 2016.
Published online 14 June 2017.

DOI: 10.4064/aa8578-5-2017

In this paper, we may capture primes which are *stronger* than [Me] theoretically by appealing to the Brun–Titchmarsh theorems on average (see Lemma 3.2 below).

THEOREM 1.1. *There are a positive proportion of primes that are* $\big(\frac{1}{2}, \frac{1}{2}, \frac{1}{14.18}\big)$*-strong.*

THEOREM 1.2. *There are a positive proportion of primes that are* $\big(\frac{1}{2}+\frac{1}{36}, \frac{1}{2}+\frac{1}{36}, 0\big)$*-strong.*

2. Chebyshev–Hooley method. We start from the evaluation of the weighted sum

$$H(X) = \sum_{p \le X} \log(p+1)\log(p-1).$$

The following proposition is an immediate consequence of the Prime Number Theorem.

LEMMA 2.1. *For sufficiently large* X*, we have*

$$H(X) = X \log X \,(1 + o(1)).$$

On the other hand, as in the Chebyshev–Hooley method, we invoke the identity

$$\sum_{m|n} \Lambda(m) = \log n, \tag{2.1}$$

so that

$$H(X) = \sum_{p \le X} \sum_{l_1 | p+1} \Lambda(l_1) \sum_{l_2 | p-1} \frac{\Lambda(l_2)}{\log(l_2 - 1)} \sum_{l_3 | l_2 - 1} \Lambda(l_3).$$

Here and in what follows, we may suppose l_2 is at least 3 so that the logarithm factor in the denominator does not vanish, and for $l_2 = 2$ the logarithm factor cancels out with the convolution of Λ.

Set

$$L_j = X^{\theta_j}, \quad j = 1, 2, 3. \tag{2.2}$$

We wish to find a positive lower bound for the quantity

$$A(X) = \sum_{p \le X} \sum_{\substack{l_1 | p+1 \\ l_1 > L_1}} \Lambda(l_1) \sum_{\substack{l_2 | p-1 \\ l_2 > L_2}} \Lambda(l_2) \sum_{\substack{l_3 | l_2 - 1 \\ l_3 > L_3}} \Lambda(l_3).$$

In fact,

$$H(X) - A(X) \le A_1(X) + A_2(X) + A_3(X) - A_4(X), \tag{2.3}$$

where

$$A_1(X) = \sum_{p\le X} \sum_{\substack{l_1\mid p+1\\ l_1\le L_1}} \Lambda(l_1) \sum_{l_2\mid p-1} \frac{\Lambda(l_2)}{\log(l_2-1)} \sum_{l_3\mid l_2-1} \Lambda(l_3),$$

$$A_2(X) = \sum_{p\le X} \sum_{l_1\mid p+1} \Lambda(l_1) \sum_{\substack{l_2\mid p-1\\ l_2\le L_2}} \frac{\Lambda(l_2)}{\log(l_2-1)} \sum_{l_3\mid l_2-1} \Lambda(l_3),$$

$$A_3(X) = \sum_{p\le X} \sum_{l_1\mid p+1} \Lambda(l_1) \sum_{\substack{l_2\mid p-1\\ l_2> L_2}} \frac{\Lambda(l_2)}{\log(l_2-1)} \sum_{\substack{l_3\mid l_2-1\\ l_3\le L_3}} \Lambda(l_3),$$

$$A_4(X) = \sum_{p\le X} \sum_{\substack{l_1\mid p+1\\ l_1\le L_1}} \Lambda(l_1) \sum_{\substack{l_2\mid p-1\\ l_2\le L_2}} \frac{\Lambda(l_2)}{\log(l_2-1)} \sum_{l_3\mid l_2-1} \Lambda(l_3).$$

The following proposition collects the evaluations of $A_j(X)$, $j = 1, 2, 3, 4$.

PROPOSITION 2.2. *With the notation in* (2.2) *and for sufficiently large* X, *we have*

$$A_j(X) \le \left\{\frac{1}{2} + \int_{1/2}^{\theta_j} C(\theta)\, d\theta\right\} X \log X\,(1+o(1)), \qquad j = 1, 2,$$

$$A_3(X) \le \theta_3 \int_{\theta_2}^{1} \frac{C(\theta)}{\theta}\, d\theta \cdot X \log X\,(1+o(1)),$$

$$A_4(X) \ge \tfrac{1}{8} X \log X\,(1+o(1)),$$

where $C(\theta)$ *is defined later in Lemma* 3.2.

From Lemma 2.1, Proposition 2.2 and (2.3) one may derive a lower bound for $A(X)$ and one can see its dependence on the parameters $\theta_1, \theta_2, \theta_3$. In particular, we can take $\theta_1 = \theta_2 = 1/2$ and choose θ_3 as large as possible such that $A(X) \gg X \log X$. The details will be given in Sections 4 and 5. A sketch of the proof of Theorem 1.2 will be given in Section 6.

3. Primes in arithmetic progressions. Let q be a positive integer and $(a, q) = 1$. We are interested in the counting function of primes

$$\pi(x; q, a) = \sum_{\substack{p\le x\\ p\equiv a \bmod q}} 1.$$

The celebrated Bombieri–Vinogradov Theorem can be stated as follows:

LEMMA 3.1. *For any $A > 0$, there exists some constant $B = B(A) > 0$ such that*

$$\sum_{q \le x^{1/2}/(\log x)^B} \max_{(a,q)=1} \left| \pi(x;q,a) - \frac{1}{\varphi(q)} \pi(x;1,1) \right| \ll \frac{x}{(\log x)^A},$$

where the implied constant depends only on A.

The Bombieri–Vinogradov Theorem yields an asymptotic formula for $\pi(x;q,a)$ on average for $q \le x^{1/2}/(\log x)^B$. In many applications, one requires an asymptotic evaluation for $\pi(x;q,a)$ with q reasonably large, and sometimes numerical inequalities, instead of asymptotic formulae, offer a good choice. Setting $q = x^\theta$, one may expect, as $x \to +\infty$, that

$$\pi(x;q,a) \le \{C(\theta) + o(1)\} \frac{1}{\varphi(q)} \frac{x}{\log x} \tag{3.1}$$

for θ large with some $C(\theta) > 0$. This is called the *Brun–Titchmarsh theorem* since Titchmarsh was the first who proved the existence of such $C(\theta)$ via Brun's sieve. By a careful application of Selberg's sieve, van Lint & Richert [LR] showed that $C(\theta) = 2/(1-\theta)$ is admissible for $\theta \in (0,1)$, uniformly in $(a,q) = 1$. This was later sharpened in a series of papers of Motohashi, Iwaniec, Friedlander–Iwaniec [Mo, Iw, FI], and others.

On the other hand, motivated by the problem of greatest prime factors of shifted primes, Hooley [Ho1, Ho2, Ho3] initiated to bound $\pi(x;q,a)$ from above with an extra average over q. The subsequent improvement is due to Iwaniec [Iw], who combined Hooley's argument with his bilinear remainder terms in linear sieves. Thanks to the work of Deshouillers & Iwaniec [DI1] on the control of sums of Kloosterman sums, one can do much better on the level of linear sieves—see e.g. Deshouillers–Iwaniec [DI2], Fouvry [Fo1, Fo2], Baker–Harman [BH]. However, due to the use of the "switching-moduli" trick, the residue class a is usually assumed to be fixed.

Let w be the Buchstab function defined by

$$w(u) = \begin{cases} 0 & \text{for } 0 \le u < 1, \\ 1 & \text{for } 1 \le u \le 2, \end{cases} \qquad (u-1)w'(u) = w(u-1) \quad \text{for } u > 2.$$

We recall the Brun–Titchmarsh theorem *on average* as given in Fouvry [Fo2, Théorème 3] with corrections in [BH, Section 4].

LEMMA 3.2. *Let $A > 0$ and $a \ne 0$. For sufficiently large $Q = X^\theta$ with $\theta \in [1/2, 1)$, the inequality* (3.1) *holds for $q \in (Q, 2Q]$ with at most $O_A(Q(\log Q)^{-A})$ exceptions, where $C(\theta)$ satisfies*

$$C(\theta) = 1 + \Big(\int\limits_{\frac{3}{5}(1-\theta)}^{\max\{3/7,(5-3\theta)/8\}} + \int\limits_{1-\theta}^{1/2} \Big) \frac{w((1-t)/t)}{t(1-t)}\, dt$$
$$+ \iiint\limits_{\Omega(\theta)} \frac{w((1-t_1-t_2-t_3)/t_3)}{t_1t_2t_3(1-t_1-t_2-t_3)}\, dt_1\, dt_2\, dt_3$$

for $\theta \in [1/2, 17/32)$ *with* $\Omega(\theta) = \big\{(t_1,t_2,t_3) : (5-8\theta)/6 \le t_3 \le t_2 \le t_1 \le \frac{3}{5}(1-\theta)\big\}$, *and*

$$C(\theta) = \begin{cases} \frac{14}{12-13\theta} - \log\big(\frac{4(1-\theta)}{3\theta}\big) & \text{if } \theta \in [17/32, 4/7), \\ \frac{14}{12-13\theta} & \text{if } \theta \in [4/7, 3/5), \\ \frac{8}{3-\theta} & \text{if } \theta \in [3/5, 5/7), \\ \frac{6}{1+\theta} & \text{if } \theta \in [5/7, 3/4), \\ \frac{12}{5-12\theta} & \text{if } \theta \in [3/4, 5/6), \\ \frac{48}{15-2\theta} & \text{if } \theta \in [5/6, 9/10), \\ \frac{4}{2-\theta} & \text{if } \theta \in [9/10, 1). \end{cases}$$

4. Proof of Proposition 2.2

4.1. Upper bounds for $A_1(X)$ and $A_2(X)$. Recalling the convolution (2.1), we have

$$\begin{aligned} A_1(X) &= \sum_{p\le X} \sum_{\substack{l_1 \mid p+1 \\ l_1 \le L_1}} \Lambda(l_1) \sum_{l_2 \mid p-1} \Lambda(l_2) \\ &= \sum_{p\le X} \log(p-1) \sum_{\substack{l_1 \mid p+1 \\ l_1 \le L_1}} \Lambda(l_1) \\ &\le (\log X) \sum_{l_1 \le L_1} \Lambda(l_1)\pi(X; l_1, -1). \end{aligned}$$

Set $X^\flat = X^{1/2}\exp(-\sqrt{\log X})$. For $l_1 \le X^\flat$, we appeal to the Bombieri–Vinogradov Theorem, and for $X^\flat < l_1 \le L_1$, the Brun–Titchmarsh theorems are applied, so that

$$A_1(X) \le C_1 X \log X\,(1 + o(1)),$$

where

$$C_1 = \frac{1}{2} + \int\limits_{1/2}^{\theta_1} C(\theta)\, d\theta.$$

Similarly, we have

$$A_2(X)=\sum_{p\le X}\log(p+1)\sum_{\substack{l_2\mid p-1\\ l_2\le L_2}}\Lambda(l_2)\le(\log X+O(1))\sum_{l_2\le L_2}\Lambda(l_2)\pi(X;l_2,1).$$

Thus

$$A_2(X)\le C_2X\log X\,(1+o(1))\quad\text{with}\quad C_2=\frac{1}{2}+\int_{1/2}^{\theta_2}C(\theta)\,d\theta.$$

4.2. Upper bound for $A_3(X)$. Firstly, we may write

$$\begin{aligned}A_3(X)&=\sum_{p\le X}\log(p+1)\sum_{\substack{l_2\mid p-1\\ l_2>L_2}}\frac{\Lambda(l_2)}{\log(l_2-1)}\sum_{\substack{l_3\mid l_2-1\\ l_3\le L_3}}\Lambda(l_3)\\&\le(\log X+O(1))\sum_{l_3\le L_3}\Lambda(l_3)\sum_{\substack{L_2<l_2<X\\ l_2\equiv1\bmod l_3}}\frac{\Lambda(l_2)}{\log(l_2-1)}\pi(X;l_2,1).\end{aligned}$$

Let B be a reasonably large number. For $X/(\log X)^B\le L_2<X$, the Brun–Titchmarsh theorem, (3.1) say, yields

$$\begin{aligned}\log X\sum_{l_3\le L_3}\Lambda(l_3)&\sum_{\substack{X/(\log X)^B\le L_2<X\\ l_2\equiv1\bmod l_3}}\frac{\Lambda(l_2)}{\log(l_2-1)}\pi(X;l_2,1)\\&\ll X\sum_{l_3\le L_3}\Lambda(l_3)\sum_{\substack{X/(\log X)^B\le L_2<X\\ l_2\equiv1\bmod l_3}}\frac{\Lambda(l_2)}{\log(l_2-1)\varphi(l_2)}\\&\le X\sum_{X/(\log X)^B\le L_2<X}\frac{\Lambda(l_2)}{\varphi(l_2)}\ll X\log\log X,\end{aligned}$$

where we have used the Mertens Theorem in the last inequality. We now restrict l_2 to $L_2<l_2<X/(\log X)^B$. From Lemma 3.2 we derive that

$$\begin{aligned}A_3(X)\le X\sum_{l_3\le L_3}\Lambda(l_3)&\sum_{\substack{L_2<l_2<X/(\log X)^B\\ l_2\equiv1\bmod l_3}}\frac{\Lambda(l_2)}{\log(l_2-1)\varphi(l_2)}C\left(\frac{\log l_2}{\log X}\right)(1+o(1))\\&+O(X\log\log X).\end{aligned}$$

From the Bombieri–Vinogradov Theorem, it follows that

$$A_3(X) \le X \sum_{l_3 \le L_3} \frac{\Lambda(l_3)}{\varphi(l_3)} \sum_{\substack{L_2 < l_2 < X/(\log X)^B \\ (l_2,l_3)=1}} \frac{\Lambda(l_2)}{\log(l_2-1)\varphi(l_2)} C\left(\frac{\log l_2}{\log X}\right)(1+o(1))$$
$$+ O(X \log\log X)$$
$$= \theta_3 \int_{\theta_2}^{1} \frac{C(\theta)}{\theta}\, d\theta \cdot X \log X\,(1+o(1))$$

as stated.

4.3. Lower bound for $A_4(X)$. We have

$$A_4(X) = \sum_{p \le X} \sum_{\substack{l_1 \mid p+1 \\ l_1 \le L_1}} \Lambda(l_1) \sum_{\substack{l_2 \mid p-1 \\ l_2 \le L_2}} \Lambda(l_2)$$
$$= \sum_{l_1 \le L_1} \sum_{l_2 \le L_2} \Lambda(l_1)\Lambda(l_2) \sum_{\substack{p \le X \\ p \equiv -1 \bmod l_1 \\ p \equiv 1 \bmod l_2}} 1$$
$$\ge \sum_{\substack{l_1 \le L_1 \\ (l_1,l_2)=1}} \sum_{l_2 \le L_2} \Lambda(l_1)\Lambda(l_2)\pi(X, l_1 l_2, \delta(l_1,l_2)),$$

where $\delta(l_1,l_2) \equiv -1 \bmod l_1$ and $\equiv 1 \bmod l_2$. As in [Me], we conclude from the Bombieri–Vinogradov Theorem that

$$A_4(X) \ge \tfrac{1}{8} X \log X\,(1+o(1)).$$

5. Proof of Theorem 1.1. We now assume $\theta_1 = \theta_2 = 1/2$. From Lemma 2.1 and Proposition 2.2, one has

$$H(X) - A(X) \le CX \log X\,(1+o(1)),$$

where

$$C = \frac{7}{8} + \theta_3 \int_{1/2}^{1} \frac{C(\theta)}{\theta}\, d\theta.$$

Theorem 1.1 then follows by choosing θ_3 as large as possible such that $C < 1$.

For $1/2 \le \theta < 17/32$, we borrow the evaluations of Fouvry [Fo2, p. 405]:

$$C(\theta) \le 1 + \log 2 + \int_{2}^{\frac{2+3\theta}{3-3\theta}} \frac{1+\log(t-1)}{t}\, dt - C^*(\theta)$$
$$+ \frac{3}{5-8\theta}\left(1 + \left(1 - \log\left(\frac{18(1-\theta)}{5(5-8\theta)}\right)\right)^2\right) - \frac{5}{3(1-\theta)},$$

where

$$C^*(\theta)=\begin{cases}\log\big(\frac{3(1+\theta)(1-\theta)}{\theta(5-3\theta)}\big), & 1/2\le\theta<11/21,\\ \log\big(\frac{4(1-\theta)}{3\theta}\big), & 11/21\le\theta<17/32.\end{cases}$$

Hence

$$\begin{aligned}\int_{1/2}^{17/32}\frac{C(\theta)}{\theta}\,d\theta &\le (1+\log 2)\int_{1/2}^{17/32}\frac{d\theta}{\theta}+\int_{1/2}^{17/32}\frac{d\theta}{\theta}\int_{2}^{\frac{2+3\theta}{3-3\theta}}\frac{1+\log(t-1)}{t}\,dt\\ &\quad-\int_{1/2}^{11/21}\log\Big(\frac{3(1+\theta)(1-\theta)}{\theta(5-3\theta)}\Big)\frac{d\theta}{\theta}-\int_{11/21}^{17/32}\log\Big(\frac{4(1-\theta)}{3\theta}\Big)\frac{d\theta}{\theta}\\ &\quad+\int_{1/2}^{17/32}\frac{3}{\theta(5-8\theta)}\bigg(1+\bigg(1-\log\Big(\frac{18(1-\theta)}{5(5-8\theta)}\Big)\bigg)^2\bigg)\,d\theta-\int_{1/2}^{17/32}\frac{5\,d\theta}{3\theta(1-\theta)}\\ &=0.124593\ldots.\end{aligned}$$

On the other hand, we find

$$\int_{17/32}^{1}\frac{C(\theta)}{\theta}\,d\theta=1.64682\ldots.$$

Therefore,

$$C\le 7/8+1.77142\theta_3,$$

which is smaller than 1 if we take $\theta_3=\frac{1}{14.18}\approx 0.070522$.

6. A sketch of the proof of Theorem 1.2. To prove Theorem 1.2, we write

$$H(X)=\sum_{p\le X}\sum_{l_1\mid p+1}\Lambda(l_1)\sum_{l_2\mid p-1}\Lambda(l_2)$$

and seek a positive lower bound for

$$B(X):=\sum_{p\le X}\sum_{\substack{l_1\mid p+1\\ l_1>L_1}}\Lambda(l_1)\sum_{\substack{l_2\mid p-1\\ l_2>L_2}}\Lambda(l_2).$$

The inclusion-exclusion principle implies

$$H(X)-B(X)=B_1(X)+B_2(X)-B_3(X),$$

where

$$B_1(X) = \sum_{p\le X} \sum_{\substack{l_1\mid p+1\\ l_1\le L_1}} \Lambda(l_1) \sum_{l_2\mid p-1} \Lambda(l_2),$$

$$B_2(X) = \sum_{p\le X} \sum_{l_1\mid p+1} \Lambda(l_1) \sum_{\substack{l_2\mid p-1\\ l_2\le L_2}} \Lambda(l_2),$$

$$B_3(X) = \sum_{p\le X} \sum_{\substack{l_1\mid p+1\\ l_1\le L_1}} \Lambda(l_1) \sum_{\substack{l_2\mid p-1\\ l_2\le L_2}} \Lambda(l_2).$$

Note that $B_j(X) = A_j(X)$ for $j = 1, 2$ and $B_3(X) = A_4(X)$. Recalling the notation in (2.2), we then have

$$B_j(X) \le \left\{\frac{1}{2} + \int_{1/2}^{\theta_j} C(\theta)\, d\theta\right\} X \log X\,(1 + o(1)), \qquad j = 1, 2,$$

and

$$B_3(X) \ge \tfrac{1}{8} X \log X\,(1 + o(1)).$$

It now follows that

$$H(X) - B(X) \le \left\{\frac{7}{8} + \int_{1/2}^{\theta_1} C(\theta)\, d\theta + \int_{1/2}^{\theta_2} C(\theta)\, d\theta\right\} X \log X\,(1 + o(1)).$$

For $\theta_1 = \theta_2 = 1/2 + 1/36$, one may check

$$\frac{7}{8} + \int_{1/2}^{\theta_1} C(\theta)\, d\theta + \int_{1/2}^{\theta_2} C(\theta)\, d\theta \le \frac{7}{8} + 0.1249 < 1.$$

This proves Theorem 1.2.

7. Concluding remarks. Based on Pollard's $p-1$ and Williams' $p+1$ algorithms, Bach and Shallit developed techniques for factorizations by assuming that any kth cyclotomic polynomial $\Phi_k(p)$ has no large prime factors. Note that the first several cyclotomic polynomials are given by $\Phi_1(p) = p - 1, \Phi_2(p) = p + 1, \Phi_3(p) = p^2 + p + 1$ and $\Phi_4(p) = p^2 + 1$. In the spirit of Theorems 1.1 and 1.2, one should consider the greatest prime factors of $\Phi_k(p)$ with p satisfying some other difficult factorizations. Quite recently, in a joint work with Wu [WX2], we have been able to prove that there are a positive proportion of primes p such that $\Phi_4(p)$ has a prime factor at least $p^{0.847}$, and the method also applies to other quadratic irreducible polynomials; this is based on our previous work on a quadratic extension of Brun–Titchmarsh theorems [WX1]. It would be quite interesting to extend Theorems 1.1 and 1.2 to the cases of cyclotomic polynomials

by appealing to the Brun–Titchmarsh theorem developed in [WX1], as well as its generalizations.

Acknowledgements. The author is grateful for the financial support of CPSF (No. 2015M580825) and NSF (No. 11601413) of P.R. China.

References

[BS] E. Bach and J. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. 52 (1989), 201–219.

[BH] R. C. Baker and G. Harman, *The Brun–Titchmarsh theorem on average*, in: Analytic Number Theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math. 138, Birkhäuser Boston, Boston, MA, 1996, 39–103.

[DI1] J.-M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms*, Invent. Math. 70 (1982/83), 171–188.

[DI2] J.-M. Deshouillers and H. Iwaniec, *On the Brun–Titchmarsh theorem on average*, in: Topics in Classical Number Theory, Vols. I, II (Budapest, 1981), Colloq. Math. Soc. János Bolyai 34, North-Holland, Amsterdam, 1984, 319–333.

[Fo1] É. Fouvry, *Sur le théorème de Brun–Titchmarsh*, Acta Arith. 43 (1984), 417–424.

[Fo2] É. Fouvry, *Théorème de Brun–Titchmarsh: application au théorème de Fermat*, Invent. Math. 79 (1985), 383–407.

[FI] J. B. Friedlander and H. Iwaniec, *The Brun–Titchmarsh theorem*, in: Analytic Number Theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser. 247, Cambridge Univ. Press, Cambridge, 1997, 85–93.

[Go] J. Gordon, *Strong primes are easy to find*, in: Advances in Cryptology (Paris, 1984), Lecture Notes in Comput. Sci. 209, Springer, Berlin, 1985, 216–223.

[Ho1] C. Hooley, *On the Brun–Titchmarsh theorem*, J. Reine Angew. Math. 255 (1972), 60–79.

[Ho2] C. Hooley, *On the largest prime factor of $p+a$*, Mathematika 20 (1973), 135–143.

[Ho3] C. Hooley, *On the Brun–Titchmarsh theorem. II*, Proc. London Math. Soc. 30 (1975), 114–128.

[Iw] H. Iwaniec, *On the Brun–Titchmarsh theorem*, J. Math. Soc. Japan 34 (1982), 95–123.

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[LR] J. H. van Lint and H.-E. Richert, *On primes in arithmetic progressions*, Acta Arith. 11 (1965), 209–216.

[Me] X. M. Meng, *On the number of strong primes*, Acta Math. Hungar. 145 (2015), 505–515.

[Mo] Y. Motohashi, *On some improvements of the Brun–Titchmarsh theorem. III*, J. Math. Soc. Japan 27 (1975), 444–453.

[Po] J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. 76 (1974), 521–528.

[RS] R. Rivest and R. Silverman, *Are 'strong' primes needed for RSA?*, Cryptology ePrint Archive: Report 2001/007, http://eprint.iacr.org/2001/007.

[Wi] H. C. Williams, *A $p+1$ method of factoring*, Math. Comp. 39 (1982), 225–234.

[WX1] J. Wu and P. Xi, *Arithmetic exponent pairs for algebraic trace functions and applications*, arXiv:1603.07060 [math.NT].

[WX2] J. Wu and P. Xi, *Quadratic polynomials at prime arguments*, Math. Z. 285 (2017), 631–646.

Ping Xi
Department of Mathematics
Xi'an Jiaotong University
Xi'an 710049, P.R. China
E-mail: ping.xi@xjtu.edu.cn