COLLOQUIUM MATHEMATICUM

VOL. 103 2005 NO. 1

E-SYMMETRIC NUMBERS

BY

GANG YU (Columbia, SC)

Abstract. A positive integer n is called E-symmetric if there exists a positive integer m such that $|m-n| = (\phi(m), \phi(n))$, and n is called E-asymmetric if it is not E-symmetric. We show that there are infinitely many E-symmetric and E-asymmetric primes.

1. Introduction. Given any two distinct odd primes p and q, the well known quadratic reciprocity asserts

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Among the existing proofs, a most popular one that Gauss gave (cf., for example, proof of Theorem 98 in [3]) counts the lattice points inside the rectangle $\mathcal{R}(p,q)$ with sides parallel to the axes and two opposite vertices at the origin and $(p/2, q/2)$. In [1], P. Fletcher, W. Lindgren and C. Pomerance studied the so-called symmetric primes. A prime number p is called *symmetric* if it is one of the two members of a symmetric pair. Two distinct odd primes p and q form a *symmetric pair* if the number of lattice points in $\mathcal{R}(p,q)$ above the main diagonal is equal to the number of lattice points below it. In [1], the authors characterized symmetric pairs by the condition $|p-q| = (p-1, q-1)$ and, from this, they showed that almost all primes are not symmetric.

Generalizing the concept of symmetric pair, Fletcher calls $(m,n) \in \mathbb{N}^2$ an *E-symmetric pair* if $|m-n| = (\phi(m), \phi(n))$, and a positive integer *E-symmetric* if it belongs to an E-symmetric pair, where $\phi(\cdot)$ is the Euler totient function. A positive integer is called *E-asymmetric* if it is not E-symmetric.

At the 2002 Southeast Regional Meeting on Numbers, Peter Fletcher asked: Are there infinitely many (a) E-asymmetric numbers, (b) E-asymmetric primes, (c) E-symmetric primes?

It is clear that $(p, p+2)$ gives an E-symmetric pair if p and $p+2$ are both primes. Hence, there are infinitely many E-symmetric primes if we assume the twin prime conjecture. In fact, it is fairly easy to show that there are

2000 *Mathematics Subject Classification*: 11A41, 11N36.

Key words and phrases: E-symmetric numbers, sieve methods.

many more E-symmetric primes than twin primes. More precisely, we prove unconditionally

THEOREM 1.1. *There exists a constant* $c_1 > 0$ *such that, for every sufficiently large* N, *we have*

$$\#\{E\text{-}symmetric\ primes\ p \le N\} \ge \frac{c_1 N}{\log N \log\log\log N}.$$

With the same idea, we can also show that there are infinitely many E-asymmetric primes.

THEOREM 1.2. *There exists a constant* $c_2 > 0$ *such that, for every sufficiently large* N, *we have*

$$\#\{E\text{-}asymmetric\ primes\ p \le N\} \ge \frac{c_2 N}{(\log N)^{50}}. \tag{1.1}$$

We remark that, by making the argument tighter, it is easy to improve the lower bound (1.1). We shall not do so, however, since the method we use to prove the theorem does not seem to give the best bound that one can expect.

Throughout the paper, p, q, l and r always stand for primes; as usual, for given coprime integers k and a, we set $\pi(x;k,a) = \{p \le x : p \equiv a \pmod{k}\}$ and

$$E(x;k,a) = \pi(x;k,a) - \frac{\pi(x)}{\phi(k)}, \qquad E(x;k) := \max_{(a,k)=1} |E(x;k,a)|,$$

where $\pi(x) = \pi(x;1,1)$ is the number of primes up to x; moreover, $\mu(d)$ denotes the Möbius function, and $v(d)$ the number of distinct prime divisors of the integer d.

2. Preliminaries. In this section, we give some simple sieve results that we need in the proofs of the theorems.

Let $\mathcal{A}$ be a finite sequence of positive integers (not necessarily distinct), and, for any given integer d,

$$\mathcal{A}_d := \{a \in \mathcal{A} : a \equiv 0 \pmod{d}\}.$$

Suppose $X := |\mathcal{A}| > 1$, and for each positive integer d, let $|\mathcal{A}_d|$ be approximated by a "main term" $(\omega(d)/d)X$, where $\omega(d)$ is a multiplicative function with $\omega(1) = 1$. Let

$$R_d := |\mathcal{A}_d| - \frac{\omega(d)}{d}X,$$

and, for a given real number $z > 1$,

$$S(\mathcal{A}, z) := |\{a \in \mathcal{A} : l \mid a \Rightarrow l \ge z\}|.$$

LEMMA 2.1. *Let* $\xi \geq z$ *and* $\tau = \log\xi/\log z$. *Suppose there exist some constants* $A_0 > 0$, $0 < \delta < 1$ *such that*, *for every prime* p,

$$0 \leq \omega(p) \leq \min\{(1-\delta)p, A_0\}. \tag{2.1}$$

Then

$$S(\mathcal{A}, z) = XW(z)(1 + O(e^{-\tau(\log\tau+1)})) + \theta \sum_{d<\xi^2} \mu^2(d)3^{v(d)}|R_d|, \tag{2.2}$$

where $|\theta| \leq 1$ *and*

$$W(z) := \prod_{p<z}\biggl(1 - \frac{\omega(p)}{p}\biggr).$$

Proof. This is essentially a special case ($g = 1$) of Theorem 7.1 in [2]. ∎

We now make use of Lemma 2.1 to deduce a lower bound sieve result. Let $A > 0$ be a fixed number, and $\varepsilon > 0$ be a constant which is sufficiently small such that, if we let C be the constant involved in the O-symbol in (2.2), then $C\exp(-(1-\log(100\varepsilon))/100\varepsilon) < 1/2$. Suppose N is sufficiently large, $Q, R, S \leq (\log N)^A$, and $2 < D \leq N^\varepsilon$, where Q, R and S are odd integers, pairwise coprime and $3 \nmid S$. Let $\mathcal{P}(Q, R, S, D, N)$ be the set

$$\biggl\{p \leq N : p \equiv f \pmod{2QRS} \text{ and } l \;\biggl|\; \frac{p-1}{2Q} \Rightarrow l \geq D\biggr\},$$

where $f \pmod{2QRS}$ is determined by the following three congruences:

$$p \equiv 1 \pmod{2Q}, \quad p \equiv 2 \pmod{R}, \quad p \equiv -2 \pmod{S}.$$

LEMMA 2.2. *There is a constant* $c > 0$ *such that*, *for large* N,

$$|\mathcal{P}(Q, R, S, D, N)| \geq \frac{cN}{QRS\log N\log D}.$$

Proof. Let

$$\mathcal{A} = \mathcal{A}(Q, R, S, D, N) := \biggl\{\frac{p-1}{2Q} : p \leq N \text{ and } p \equiv f \pmod{2QRS}\biggr\}.$$

Then $|\mathcal{P}(Q, R, S, D, N)| = S(\mathcal{A}, D)$. We also note that, for any integer $d \geq 1$, we have

$$|\mathcal{A}_d| = \begin{cases} \pi(N; 2QRSd, g) & \text{if } (d, RS) = 1, \\ 0 & \text{if } (d, RS) > 1, \end{cases}$$

where $g \pmod{2QRSd}$ is the intersection of the residue classes

$$1 \pmod{2Qd}, \quad 2 \pmod{R}, \quad -2 \pmod{S}.$$

Let $X := |\mathcal{A}| = \pi(N; 2QRS, f)$, and

$$\omega(d) = \begin{cases} \dfrac{d\phi(2Q)}{\phi(2Qd)} & \text{if } (d, RS) = 1, \\ 0 & \text{if } (d, RS) > 1. \end{cases}$$

It is easy to see that $\omega(d)$ is multiplicative and satisfies (2.1) with $A_0 = 2$ and $\delta = 1/2$. We also note that $R_d = 0$ if $(d, RS) > 1$ and

$$R_d = E(N; 2QRSd, g) - \frac{\phi(2Q)}{\phi(2Qd)} E(N; 2QRS, f) \tag{2.3}$$
$$\ll E(N; 2QRSd) + \frac{N \exp(-\kappa\sqrt{\log N})}{\phi(d)}$$

if $(d, RS) = 1$, where the estimate for the term $\frac{\phi(2Q)}{\phi(2Qd)} E(N; 2QRS, f)$ in (2.3) is from the Siegel–Walfisz Theorem, and $\kappa > 0$ is a certain constant. Applying Lemma 2.1 with $\xi = N^{1/5}$ and noticing the restriction on ε, we get

$$|\mathcal{P}(Q, R, S, D, N)| \geq \tfrac{1}{2} X W(D) - O(\mathcal{E}(Q, R, S, D, N))$$

where the error term $\mathcal{E}(Q, R, S, D, N)$ is given by the sum in (2.2). By the Siegel–Walfisz Theorem and the Mertens Theorem, the term $\frac{1}{2} X W(D)$ is

$$\frac{1}{2}\pi(N; 2QRS, f) \prod_{p|2Q} \left(1 - \frac{1}{p}\right) \prod_{\substack{p\nmid 2QRS \\ p \leq D}} \left(1 - \frac{1}{p-1}\right) \gg \frac{N}{QRS \log N \log D}.$$

The sum of the terms $N \exp(-\kappa\sqrt{\log N})/\phi(d)$ in (2.3) over d gives a contribution $O(N \exp(-(\kappa/2)\sqrt{\log N}))$, which is obviously negligible. Then, from Lemma 3.3 of [2], we have

$$\mathcal{E}(Q, R, S, D, N) \ll \frac{N}{(\log N)^B}$$

for any given $B > 0$. We have thus proved the lemma. ∎

We also state an upper bound result here.

LEMMA 2.3. *Let g be a natural number, a_i, b_i $(i = 1, \ldots, g)$ be pairs of integers satisfying*

$$(a_i, b_i) = 1, \qquad i = 1, \ldots, g,$$

and

$$E := \prod_{i=1}^{g} a_i \prod_{1 \leq i < j \leq g} (a_i b_j - a_j b_i) \neq 0.$$

For prime p, let $\varrho(p)$ be the number of solutions of

$$\prod_{i=1}^{g} (a_i n + b_i) \equiv 0 \pmod{p}.$$

Then for any fixed constant $\delta \in (0,1)$ and $D \le x^\delta$, we have

$$\#\Big\{n \le x : p \mid \prod_{i=1}^{g}(a_i n + b_i) \Rightarrow p > D\Big\} \ll \prod_{p\mid E}\Big(1-\frac{1}{p}\Big)^{\varrho(p)-g}\frac{x}{(\log D)^g},$$

where the constant involved in the $\ll$-symbol depends on δ only.

Proof. This is a straightforward corollary of Theorem 2.2 in [2]. ■

3. Infinitude of E-symmetric primes. In this section, we prove Theorem 1.1. Suppose N is sufficiently large. Let

$$\mathcal{P}_1(N) = \Big\{p \le N : l \;\Big|\; \frac{p-1}{2} \Rightarrow l \ge (\log\log N)^2\Big\}.$$

Then from Lemma 2.2 (with $Q = R = S = 1$ and $D = (\log\log N)^2$), we have

$$|\mathcal{P}_1(N)| \ge \frac{c_3 N}{\log N \log\log\log N}$$

for some constant $c_3 > 0$.

We claim that, for almost all $p \in \mathcal{P}_1(N)$,

$$(\phi(p), \phi(p+2)) = 2. \tag{3.1}$$

Assume $p \in \mathcal{P}_1(N)$ and (3.1) does not hold. Then there is a prime $q \ge (\log\log N)^2$ such that $2q$ divides $(\phi(p), \phi(p+2))$, thus $p+2$ is divisible by a prime $l \equiv 1 \pmod{2q}$.

Let $l = 2sq + 1$ for some $s \ge 1$. Then

$$p + 2 = (2sq+1)(2tq+3)$$

for some $t \ge 1$. (Note that $t = 0$ is impossible since $p \equiv 1 \pmod{2q}$ and $3 \nmid (p+2)$.) Thus the number of such primes $p \in \mathcal{P}_1(N)$ with $q > (\log N)^3$ is bounded by

$$\sum_{(\log N)^3 < q \le \sqrt{N}} \; \sum_{st \le N/q^2} 1 \ll \sum_{q} \sum_{m \le N/q^2} d(m) \ll \frac{N}{(\log N)^2} \ll \frac{\mathcal{P}_1(N)}{\sqrt{\log N}}. \tag{3.2}$$

The number of those $p \in \mathcal{P}_1(N)$ with $D \le q \le (\log N)^3$ and $l > \sqrt{N}$ is bounded by

$$\sum_{D \le q \le (\log N)^3} \; \sum_{t \le \sqrt{N}/2q} \; \sum_{\substack{s \le N/4tq^2 \\ l \mid (2sq+1)((2sq+1)(2tq+3)-2) \Rightarrow l \ge N^{1/4}}} 1 \tag{3.3}$$

(for which we appeal to Lemma 2.3 with $g = 2$) and has upper bound

$$\sum_{D\le q\le(\log N)^3}\ \sum_{t\le\sqrt{N}/2q}\frac{N}{q^2t(\log N)^2}\prod_{p\mid 2q(2tq+3)}\Big(1-\frac{1}{p}\Big)^{-1} \ll \frac{N\log\log N}{D\log N} \ll \frac{|\mathcal{P}_1(N)|}{\sqrt{\log\log N}}, \tag{3.4}$$

where we have used the fact that $n/\phi(n)\ll\log\log n$ for $n\ge 3$. By the Brun–Titchmarsh inequality (cf. Theorem 3.8 in [2], for example), we have the upper bound for the number of primes with $D\le q\le(\log N)^3$ and $l\le\sqrt{N}$:

$$\begin{aligned}
&\ll \sum_{D\le q\le(\log N)^3}\ \sum_{\substack{l\le\sqrt{N}\\ l\equiv 1\ (\mathrm{mod}\ 2q)}}\ \sum_{\substack{p\le N\\ p\equiv 1\ (\mathrm{mod}\ 2q)\\ p\equiv -2\ (\mathrm{mod}\ l)}} 1 \\
&\ll \frac{N}{\log N}\sum_{D\le q\le(\log N)^3}\frac{1}{q}\sum_{\substack{l\le\sqrt{N}\\ l\equiv 1\ (\mathrm{mod}\ 2q)}}\frac{1}{l} \\
&\ll \frac{N}{\log N}\sum_{D\le q\le(\log N)^3}\Big(\frac{1}{q^2}+\frac{1}{q}\int_{4q}^{\sqrt{N}}\frac{1}{t}\,d\pi(t;2q,1)\Big) \\
&\ll \frac{N}{D\log N} \\
&\quad + \frac{N}{\log N}\sum_{D\le q\le(\log N)^3}\frac{1}{q}\Big(\frac{1}{q\log(\sqrt{N}/2q)}+\frac{1}{q}\int_{4q}^{\sqrt{N}}\frac{1}{t\log(t/2q)}\,dt\Big) \\
&\ll \frac{N\log\log N}{D\log N} \ll \frac{|\mathcal{P}_1(N)|}{\sqrt{\log\log N}}.
\end{aligned} \tag{3.5}$$

From (3.2)–(3.5), we have shown that

$$|\{p\in\mathcal{P}_1(N):(\phi(p),\phi(p+2))\ne 2\}| \ll \frac{|\mathcal{P}_1(N)|}{\sqrt{\log\log N}};$$

we have thus proved Theorem 1.1.

4. Infinitude of E-asymmetric primes. We now prove Theorem 1.2. Let $\varepsilon>0$ be sufficiently small, as required in Lemma 2.2. Suppose N is sufficiently large. We let $q\asymp(\log N)^4$ be a fixed prime. From Heath-Brown's work [4], we can further fix two distinct primes l_1,l_2 satisfying $l_1,l_2\equiv 1\ (\mathrm{mod}\ 2q)$ and $l_1,l_2\ll q^{5.5}$.

Let $\mathcal{P}_2(N)$ be the set of primes $p\le N$ satisfying

$$p\equiv 1\ (\mathrm{mod}\ 2q),\qquad p\equiv 2\ (\mathrm{mod}\ l_1),\qquad p\equiv -2\ (\mathrm{mod}\ l_2), \tag{4.1}$$

and

$$l \mid \frac{p-1}{2q} \Rightarrow l \geq N^{\varepsilon}.$$

Directly from Lemma 2.2, we have

$$|\mathcal{P}_2(N)| \geq \frac{c_4 N}{q l_1 l_2 (\log N)^2}$$

for some constant $c_4 > 0$.

We shall show that almost all $p \in \mathcal{P}_2(N)$ are E-asymmetric. Namely, for almost all $p \in \mathcal{P}_2(N)$,

$$(\phi(p), \phi(p \pm 2k)) \neq 2k$$

for all $2k \mid p-1$.

We discuss this case by case.

• $k = 1$. Note that $2q \mid (\phi(p), \phi(p \pm 2))$, thus $(\phi(p), \phi(p \pm 2)) \neq 2$.

• $k = q$. If $p \in \mathcal{P}_2(N)$ satisfies $2q \mid \phi(p+2q)$, then $p + 2q$ is divisible by a prime $l(q) \equiv 1 \pmod{2q}$.

(1) $l(q) = p + 2q$. In this case, $(p+2q)(p-1)/2q$ is free of prime divisors $\leq N^{\varepsilon}$, and $p \equiv f(q) \pmod{2ql_1l_2}$. Thus the number of such primes is bounded by the number of integers $n \leq N$ such that each such n satisfies the congruences (4.1) and $n(n+2q)(n-1)/2q$ is free of prime divisors $\leq N^{\varepsilon}$. This is equal to the number of integers $k \in (-f/2ql_1l_2, (N-f)/2ql_1l_2]$ such that

$$(2ql_1l_2k + f)(2ql_1l_2k + 2q + f)\left(l_1l_2k + \frac{f-1}{2q}\right)$$

is free of prime divisors $\leq N^{\varepsilon}$. By Lemma 2.3, the number of such integers k is bounded by

$$\ll \frac{N}{ql_1l_2(\log N)^3} \cdot \frac{2q+1}{\phi(2q+1)} \ll \frac{|\mathcal{P}_2(N)|}{\sqrt{\log N}}.$$

(2) $l(q) < p + 2q$. Then there is an integer $a > 0$ such that $p + 2q = l(q)(aq+1)$; the number of such $p \in \mathcal{P}_2(N)$ is bounded by

$$\sum_{\substack{(aq+1)(bq+1) \leq N \\ (aq+1)(bq+1) \equiv f(q)+2q \pmod{l_1l_2}}} 1. \tag{4.2}$$

Note that $f(q) + 2q$ is obviously prime to l_1l_2, so this sum is

$$\ll \sum_{a \leq \sqrt{N}/q} \frac{N}{aq^2l_1l_2} \ll \frac{N}{ql_1l_2(\log N)^3} \ll \frac{|\mathcal{P}_2(N)|}{\log N}. \tag{4.3}$$

Therefore,

$$|\{p \in \mathcal{P}_2(N) : (\phi(p), \phi(p+2q)) = 2q\}| \ll \frac{|\mathcal{P}_2(N)|}{\sqrt{\log N}}.$$

Similarly, we can show that

$$|\{p \in \mathcal{P}_2(N) : (\phi(p), \phi(p-2q)) = 2q\}| \ll \frac{|\mathcal{P}_2(N)|}{\sqrt{\log N}}.$$

- $k > q$. Suppose there is a prime $l > N^\varepsilon$ such that

$$(\phi(p), \phi(p+2ml)) = 2ml,$$

where m satisfies

(I) if $q \mid m$, then $m/q = 1$ or $r \mid m/q \Rightarrow r \geq N^\varepsilon$;
(II) if $q \nmid m$, then $m = 1$ or $r \mid m \Rightarrow r \geq N^\varepsilon$.

We estimate the number of such primes $p \in \mathcal{P}_2(N)$ in dependence on whether $p + 2ml$ is a prime.

(1) *$p + 2ml$ is a prime.* The two cases ($q \mid m$ or $q \nmid m$) can be treated similarly.

When $q \mid m$, the corresponding prime $p \in \mathcal{P}_2(N)$ satisfies the following conditions:

(i) $p = 2qst + 1$, $r \mid st \Rightarrow r \geq N^\varepsilon$;
(ii) $2qst + 2qs + 1$ is a prime;
(iii) $st \equiv g(q) \pmod{l_1 l_2}$ for some $(s,t) \in \mathbb{N}^2$, where $g(q) = (f(q) - 1)/2q$.

The number of such primes is bounded by

$$\sum_{\substack{st \leq N/2q,\, s > N^\varepsilon \\ st \equiv g(q) \pmod{l_1 l_2} \\ r \mid st(2qst+1)(2qst+2qs+1) \Rightarrow r \geq N^\varepsilon}} 1.$$

From Lemma 2.3, this sum is bounded by

$$\sum_{\substack{t \leq N^{1-\varepsilon}/2q \\ (t, l_1 l_2) = 1 \\ r \mid t \Rightarrow r \geq N^\varepsilon}} \sum_{\substack{s \leq N/2qt \\ s \equiv g(q)\bar{t} \pmod{l_1 l_2} \\ r \mid s(2qst+1)(2qst+2qs+1) \Rightarrow r \geq N^\varepsilon}} 1$$

$$\ll \sum_{\substack{t \leq N^{1-\varepsilon}/2q \\ (t, l_1 l_2) = 1 \\ r \mid t \Rightarrow r \geq N^\varepsilon}} \frac{N}{q l_1 l_2 t (\log N)^3} \prod_{l \mid q l_1 l_2} \left(1 - \frac{3}{l}\right)^{-1} \prod_{3 < l \mid t(t+1)} \left(\frac{1 - 2/l}{1 - 3/l}\right)$$

$$\ll \frac{N}{q l_1 l_2 (\log N)^3} \sum_{\substack{t \leq N^{1-\varepsilon}/2q \\ r \mid t \Rightarrow r \geq N^\varepsilon}} \frac{t+1}{\phi(t(t+1))}.$$

Taking $(\log\log N)^2/t(t+1)$ as an upper bound of $1/\phi(t(t+1))$, by the

Mertens Theorem, this sum is bounded by

$$\frac{N(\log\log N)^2}{ql_1l_2(\log N)^3}\sum_{\substack{t\le N\\ r|t\Rightarrow r\ge N^\varepsilon}}\frac{1}{t}\ll\frac{N(\log\log N)^2}{ql_1l_2(\log N)^3}\prod_{N^\varepsilon\le r\le N}\left(1+\frac{1}{r}\right)$$
$$\ll\frac{N(\log\log N)^2}{ql_1l_2(\log N)^3}\ll\frac{|\mathcal{P}_2(N)|}{\sqrt{\log N}}.$$

We can similarly deal with the case when $q\nmid m$ and get the same upper bound.

(2) $p+2ml$ *is not a prime.* Then $p+2ml$ is (strictly) divisible by a prime $r(l)\equiv 1\pmod{l}$. This is similar to the case when $p+2q$ is divisible by a prime $r(q)\equiv 1\pmod{2q}$. With the same argument as in (4.2)–(4.3), the number of these $p\in\mathcal{P}_2(N)$ is bounded by $O(N^{1-\varepsilon})$.

We have thus shown that

$$|\{p\in\mathcal{P}_2(N):(\phi(p),\phi(p+2k)=2k\text{ for some }k>q\}|\ll\frac{|\mathcal{P}_2(N)|}{\sqrt{\log N}}.$$

Similarly, we have

$$|\{p\in\mathcal{P}_2(N):(\phi(p),\phi(p-2k)=2k\text{ for some}k>q\}|\ll\frac{|\mathcal{P}_2(N)|}{\sqrt{\log N}}.$$

Collecting all these estimates together, we have shown that almost all primes in $\mathcal{P}_2(N)$ are E-asymmetric, and thus Theorem 1.2 follows.

REFERENCES

[1] P. Fletcher, W. Lindgren and C. Pomerance, *Symmetric and asymmetric primes*, J. Number Theory 58 (1996), 89–99.

[2] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, London, 1968.

[4] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64 (1992), 265–338.

Department of Mathematics
LeConte College
University of South Carolina
1523 Greene Street
Columbia, SC 29208, U.S.A.
E-mail: yu@math.sc.edu

Received 1 September 2004 (4493)