

An Overview of Sieve Methods

R. A. Mollin

Department of Mathematics and Statistics
University of Calgary, Calgary, Alberta, Canada, T2N 1N4
URL: <http://www.math.ucalgary.ca/~ramollin/>
ramollin@math.ucalgary.ca

Abstract

We provide an overview of the power of Sieve methods in number theory meant for the non-specialist.

Mathematics Subject Classification: Primary: 11N35; Secondary: 11-02; 11N36

Keywords: Sieves, open problems

1 Sieves

Some of the following is adapted from [11]. Sieve methods are used in factoring, recognizing primes, finding natural numbers in arithmetic progression whose common difference are primes, or generally to estimate the cardinalities of various sets defined by the use of multiplicative properties. Recall that use of a sieve or *sieving* is a process whereby we find numbers via searching up to a prescribed bound and eliminate candidates as we proceed until only the desired solution set remains. In other words, sieve theory is designed to estimate the size of sifted sets of integers. For instance, sieves may be used to attack the following *open* problems, for which sieve methods have provided some advances.

(a) **(The Twin Prime Conjecture)**

There are infinitely many primes p such that $p + 2$ is also prime.

(b) **(The Goldbach Conjecture)**

Every even integer $n > 2$ is a sum of two primes.

(c) **(The $p = n^2 + 1$ Conjecture)**

There are infinitely many primes p of the form $p = n^2 + 1$.

(d) **(The $q = 4p + 1$ Conjecture)**

There are infinitely many primes p such that $q = 4p + 1$ is also prime.

(e) **(Artin's Conjecture)**

For any nonsquare integer $a \notin \{-1, 0, 1\}$, there exist infinitely many primes p such that a is a primitive root modulo p .

Indeed, in 1986, Heath-Brown [8] used sieving methods to advance the Artin conjecture to within a hair of a solution when he proved that with the possible exception of at most two primes, there are infinitely many primes q such that p is a primitive root modulo q . Thus, sieve methods are important to review for their practical use in number theory and the potential for solutions of outstanding problems such as the above.

The fundamental goal of sieve theory is to produce upper and lower bounds for cardinalities of sets of the type,

$$S(\mathcal{S}, \mathcal{P}, y) = \{n \in \mathcal{S} : p \mid n \text{ implies } p > y \text{ for all } p \in \mathcal{P}\}, \quad (1)$$

where \mathcal{S} is a finite subset of \mathbb{N} , \mathcal{P} is a subset of \mathbb{P} , the set of all primes, and y is a positive real number.

Example 1 Let

$$\mathcal{S} = \{n \in \mathbb{N} : n \leq x\} \text{ and } \sqrt{x} < y \leq x.$$

Then

$$|S(\mathcal{S}, \mathcal{P}, y)| = |\{n \leq x : p \mid n \text{ implies } p > y\}| = \pi(x) - \pi(y) + 1,$$

one more than the number of primes between x and y .

To illustrate (1) more generally, we begin with what has been called “the oldest nontrivial algorithm that has survived to the present day.” From antiquity, we have the Sieve of Eratosthenes, which is covered in a first course in number theory—see [10, Example 1.16, p. 31], which sieves to produce primes to a chosen bound. However, as discussed therein, this sieve is highly inefficient. Indeed, since in order to determine the primes up to some bound using this sieve for $n \in \mathbb{N}$, one must check for divisibility by all primes not exceeding \sqrt{n} , then the sieve of Eratosthenes has complexity $O(n \log_e n)(\log_e \log_e n)$,

which even using the world's fastest computers, this is beyond hope for large integers as a method for recognizing primes. Yet there is a formulation of this sieve that fits nicely into the use of arithmetic functions, and has applications as a tool for modern sieves, so we present that here for completeness and interests sake.

Recall that the Möbius function $\mu(d)$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not squarefree,} \\ (-1)^k & \text{if } n = \prod_{j=1}^k p_j \text{ where the } p_j \text{ are distinct primes.} \end{cases}$$

Also, let $\omega(d)$ denote the number of distinct prime divisors of d , and \mathbb{P} the set of all primes.

Theorem 1 Eratosthenes' Sieve

Let $\mathcal{P} = \{p_1, p_2, \dots, p_n\} \subseteq \mathbb{P}$ be a set of distinct primes and let $\mathcal{S} \subseteq \mathbb{N}$ with $|\mathcal{S}| < \infty$. Denote by S the number of elements of \mathcal{S} not divisible by any of the p_j 's and by \mathcal{S}_d the number of elements of \mathcal{S} divisible by a given $d \in \mathbb{N}$. Then

$$S = \sum_{d|p_1 p_2 \cdots p_n} \mu(d) \mathcal{S}_d.$$

Moreover, For $m = 1, 2, \dots, \lfloor n/2 \rfloor$, we have

$$\sum_{\substack{d|p_1 p_2 \cdots p_n \\ \omega(d) \leq 2m-1}} \mu(d) \mathcal{S}_d \leq S \leq \sum_{\substack{d|p_1 p_2 \cdots p_n \\ \omega(d) \leq 2m}} \mu(d) \mathcal{S}_d,$$

where (1) is called Eratosthenes' sieve.

Proof. See [12, Corollary 2, p. 147]. □

For instance, an application of Theorem 1 is that it may be used to prove the following result on the number of primes less than a certain bound, first proved in 1919, by the Norwegian mathematician Viggo Brun (1882–1978).

Theorem 2 Brun's Theorem

If $n \in \mathbb{N}$ and $B_{2n}(x)$ denotes the number of primes $p \leq x$ for which $|p + 2n|$ is also prime, then

$$B_{2n}(x) = O(x(\log_e \log_e x)^2 \log_e^{-2} x).$$

Proof. See [12, Theorem 4.3, p. 148]. \square

Theorem 2 has as a special case, implications for the twin prime conjecture as follows.

Corollary 1 **Brun's Constant**

Let \mathcal{Q} be the set of all primes p such that $p + 2$ is also prime, then

$$\sum_{\substack{p \in \mathcal{Q} \\ p \leq x}} 1 \ll \frac{x(\log_e \log_e x)^2}{\log_e^2 x},$$

and the series

$$\sum_{p \in \mathcal{Q}} \frac{1}{p} = B \tag{2}$$

is convergent, where (2) is called Brun's constant.

Proof. See [12, Corollary, p. 152]. \square

Remark 1 We do not know if \mathcal{Q} in Corollary 1 is finite or not since its infinitude would be the twin prime conjecture. We *do know* that the sum of the reciprocals of *all* primes diverges, but since the series (2) converges, this is not a proof of the conjecture since we would need divergence to get the infinitude. The behaviour of the two series does tell us that, although the twin prime conjecture may be true, the twin primes must be appreciably less dense than the entire set of primes. Brun's result, that the reciprocals of twin primes converges, is one of the centerpiece achievements of sieve theory.

The value of Brun's constant is

$$B \approx 1.9021605824,$$

with an error within ± 0.000000003 , computed by Thomas R. Nicely in 1999. It is worth noting the now famous fact that, in 1995, Nicely was doing computations on Brun's constant which led him to discover a flaw in the floating-point arithmetic of the Pentium computer chip, costing literally millions of dollars to its manufacturer Intel—see <http://www.trnicely.net/twins/twins2.html>.

Theorem 1 tells us that the sieve of Eratosthenes investigates the function

$$S(\mathcal{S}, \mathcal{P}, x) = \sum_{\substack{n \in \mathcal{S} \\ \gcd(n, \Pi) = 1}} 1, \text{ where } \Pi = \prod_{\substack{p \in \mathcal{P} \\ p \leq x}} p$$

via the equality

$$S(\mathcal{S}, \mathcal{P}, x) = \sum_{n \in \mathcal{S}} \sum_{\substack{d|n \\ d|\Pi}} \mu(d) = \sum_{d|\Pi} \mu(d) \mathcal{S}_d.$$

The general basic sieve problem emanates from this, namely find arithmetic functions $\lambda_\ell(d) : \mathbb{N} \mapsto \mathbb{R}$ and $\lambda_u(d) : \mathbb{N} \mapsto \mathbb{R}$ with

$$\sum_{\substack{d|n \\ d|\Pi}} \lambda_\ell(d) \leq \begin{cases} 1 & \text{if } \gcd(n, \Pi) = 1, \\ 0 & \text{if } \gcd(n, \Pi) > 1, \end{cases}$$

and

$$\sum_{\substack{d|n \\ d|\Pi}} \lambda_u(d) \geq \begin{cases} 1 & \text{if } \gcd(n, \Pi) = 1, \\ 0 & \text{if } \gcd(n, \Pi) > 1, \end{cases}$$

such that

$$\sum_{d|\Pi} \lambda_\ell(d) \mathcal{S}_d = \sum_{n \in \mathcal{S}} \sum_{\substack{d|n \\ d|\Pi}} \lambda_\ell(d) \leq S(\mathcal{S}, \mathcal{P}, x) \leq \sum_{n \in \mathcal{S}} \sum_{\substack{d|n \\ d|\Pi}} \lambda_u(d) = \sum_{d|\Pi} \lambda_u(d) \mathcal{S}_d. \quad (3)$$

Now we interpret the above in terms of what Selberg did to create his famous sieve and how Theorem 1 comes into play. With the notation of Theorem 1 still in force, we add that P denotes the product of the primes in \mathcal{P} , $|\mathcal{S}| = N$, and call the following *Selberg's condition* on \mathcal{S} .

There exists a multiplicative function $f(d)$ such that if $d \mid P$, then

$$\mathcal{S}_d = \frac{f(d)}{d} N + R(d), \quad (4)$$

where $|R(d)| \leq f(d)$ and $d > f(d) > 1$. With the Selberg condition plugged into the right-hand side of (3), we have

$$\begin{aligned} |S(\mathcal{S}, \mathcal{P}, x)| &\leq \sum_{d|\Pi} \frac{\lambda_u(d) f(d) N}{d} + \sum_{d|\Pi} \lambda_u(d) R(d) \\ &= N \sum_{d|\Pi} \frac{\lambda_u(d) f(d)}{d} + O\left(\sum_{d|\Pi} |\lambda_u(d) R(d)|\right). \end{aligned} \quad (5)$$

Selberg's sieve arose from his attempts to minimize (5) subject to Selberg's condition (4). Theorem 1 comes into play again in that it is used in the proof of the following, first proved by Selberg [13] in 1947. The following is considered to be the fundamental theorem concerning Selberg's sieve, which for the above-cited reasons, is often called *Selberg's upper bound sieve*.

Theorem 3 Selberg's Sieve

Let \mathcal{P} be a finite set of primes, P denoting their product, $\mathcal{S} \subseteq \mathbb{N}$ with $|\mathcal{S}| = N \in \mathbb{N}$, such that \mathcal{S} satisfies Selberg's condition (4), and let $S = S(\mathcal{S}, \mathcal{P}, x)$ be the number of elements of \mathcal{S} not divisible by primes $p \in \mathcal{P}$ with $p \leq x$ where $x > 2$. If for $p \mid P$, we have that $f(p) > 1$,

$$g(n) = \prod_{d|n} \frac{\mu(n/d)d}{f(d)},$$

and

$$Q_x = \sum_{\substack{d|P \\ d \leq x}} g^{-1}(d),$$

then

$$S \leq \frac{N}{Q_x} + x^2 \prod_{\substack{p \in \mathcal{P} \\ p \leq x}} \left(1 - \frac{f(p)}{p}\right)^{-2}.$$

Proof. See [12, Theorem 4.4, p. 158]. □

An application of Theorem 3 is the following, where $\pi(x; k, \ell)$ denotes the number of primes $p \leq x$ such that $p \equiv \ell \pmod{k}$. In the notation of Theorem 3, we have that

$$\mathcal{P} = \{p \in \mathbb{P} : p \nmid k \text{ and } p \leq \sqrt{x}\}.$$

Also,

$$\mathcal{S} = \{y = kn + \ell : n \in \mathbb{N} \text{ and } y \leq x\}.$$

Then $N = \lfloor x/k \rfloor$,

$$S(\mathcal{S}, \mathcal{P}, x) = \pi(x; k, \ell) - \pi(\sqrt{x}; k, \ell) = \pi(x; k, \ell) + O(\sqrt{x}).$$

It follows that $f(d) = 1$, $S_d = \lfloor N/d \rfloor + R_d$ with $|R_d| \leq 1$, $g(n) = \phi(n)$, and $Q_x = \sum_{x \geq d|P} \phi^{-1}(d)$.

Theorem 4 The Brun-Titchmarsh Theorem

There exists a $C = C(\varepsilon) \in \mathbb{R}^+$ such that for $1 \leq q < x$ and $\gcd(k, \ell) = 1$, we have

$$\pi(x; k, \ell) \leq \frac{Cx}{\phi(k) \log_e(x/q)}.$$

Proof. See [12, Corollary, p. 161]. □

Remark 2 Theorem 4 is known to hold when the constant $c = 2$. Moreover, if $1 \leq q \leq x^{1-\varepsilon}$ for $\varepsilon > 0$, then the upper bound is at the expected order of magnitude.

Another interpretation of Theorem 4 is that if x, y are positive reals, and $k, \ell \in \mathbb{Z}$ with $y/k \rightarrow \infty$, then

$$\pi(x + y, k, \ell) - \pi(x, k, \ell) < \frac{(2 + o(1))y}{\phi(k) \log_e(y/k)}.$$

Yet another formulation is given as follows. There exists an effective constant $k > k_0(\varepsilon)$ such that

$$\pi(x + ky, k, \ell) - \pi(x, k, \ell) < \frac{(2 + \varepsilon)y}{\phi(k) \log_e y},$$

for all y, x, ℓ with $y > k$. The amazing aspect of Brun-Titchmarsh is that if we could replace 2 by $2 - \delta$ for any $\delta > 0$, then Landau-Siegel zeros cannot exist.

Selberg's sieve also has applications to some other classical problems. For instance, the twin-prime conjecture may be interpreted as follows. Suppose that $f(d)$ represents the number of elements of

$$\{n(n+2) : d \mid n(n+2) \text{ where } 1 \leq n \leq d\}$$

which are divisible by d and for some $m \in \mathbb{N}$,

$$\mathcal{S} = \{j(j+2) : j = m, m+1, \dots, m+N-1\}.$$

Let $\pi_2(N)$ be the number of twin primes less than N , from which it follows that

$$\pi_2(N) \leq |S(\mathcal{S}, \mathcal{P}, N^{1/3})| + N^{1/3}$$

because if $p \leq N$ has a twin prime, then either $p \leq N^{1/3}$ or else $p(p+2)$ has no prime factor $\leq N^{1/3}$. Thus, using Selberg's sieve to estimate $|S(\mathcal{S}, \mathcal{P}, N^{1/3})|$, we have $f(2) = 1$ and $f(p) = 2$ for odd primes p . We claim that

$$\prod_{p \leq N^{1/3}} \left(1 - \frac{f(p)}{p}\right)^{-1} \ll (\log_e N)^2.$$

This follows from the fact that for $p > 3$,

$$\left(1 - \frac{2}{p}\right)^{-1} \leq \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p^2}\right)^{-1}$$

and the fact that

$$\prod_{p \leq N^{1/3}} \left(1 - \frac{1}{p}\right)^{-1} \ll \log_e N^{1/3},$$

which, in turn, follows from Merten's Theorem, keeping in mind that $\prod_{p \leq N^{1/3}} (1 - 2p^{-2})^{-1}$ converges. (Recall that Merten's theorem says:

$$\sum_{p \leq x} \frac{1}{p} = \log_e \log_e x + M + o(1),$$

and

$$M = \gamma + \sum_{p=\text{prime}} \left(\log_e \left(1 - \frac{1}{p}\right) + \frac{1}{p} \right),$$

where γ is Euler's constant and M is called *Merten's constant*.) One may also deduce a lower bound as follows,

$$\sum_{\substack{d \leq N^{1/3} \\ d \text{ odd}}} \frac{f(d)}{d} \geq (\log_e N)^2.$$

Putting this all together via Theorem 3, we get the following.

Theorem 5 **Selberg's Sieve on Twin Primes**

The number $\pi_2(N)$ of twin primes less than N satisfies

$$\pi_2(N) \ll \frac{N}{(\log_e N)^2}.$$

Remark 3 With the above application of Selberg's sieve, it is certainly worth mentioning another highlight of sieve theory with respect to the twin-prime conjecture, namely *Chen's Theorem*, which shows that there are infinitely many primes p such that $p+2$ is either prime or a product of two primes. Again, sieve methods allowed a result that is within a hair of the affirmation of another classical conjecture.

Another of the list of conjectures from our discussion at the outset is the Goldbach conjecture. Now we look at applications of Selberg's sieve to this classical problem. To this end, let $N = 2m$ for $m \in \mathbb{N}$, and for some $k \in \mathbb{N}$,

$$\mathcal{S} = \{j(N - j) : j = k, k + 1, \dots, k + N - 1\},$$

and let $\mathfrak{r}(N)$ be the number of representations of N as a sum of two primes. Also, $f(d)$ is the number of elements of

$$\{n(N - n) : n = 1, 2, \dots, d\}$$

divisible by d . It follows that

$$\mathfrak{r}(N) \leq |S(\mathcal{S}, \mathcal{P}, N^{1/3})| + 2N^{1/3}.$$

Thus, $f(p) = 2$ if $p \nmid N$ and $f(p) = 1$ if $p \mid N$. Applying Theorem 3, and arguing in a similar fashion to the above, we get the following, a complete proof of which may be found in [12, Theorem 4.6, p. 162].

Theorem 6 **Selberg's Sieve on the Goldbach Conjecture**

For $N \in \mathbb{N}$,

$$\mathfrak{r}(N) \ll \frac{N}{(\log_e N)^2} \prod_{p|d} \left(1 + \frac{2}{p}\right).$$

We have amply illustrated the applications of Selberg's sieve to a variety of classical problems. It is now time to look at other sieves and their contributions. One of these is due to Linnik [9] first produced in 1941. To understand what it says, we provide a preamble that takes into account what we have learned thus far. Brun's result Theorem 2 may be interpreted as a generalization of Eratosthenes sieve as follows. Take $1, 2, \dots, n$ and for each prime $p \leq \sqrt{n}$, we eliminate k residue classes modulo p , then the number remaining does not exceed $C(k)N/(\log_e^k n)$, where $C(k) > 0$ depends on k . Linnik considered a more general situation by considering for each prime $p \leq \sqrt{n}$, we eliminate $f(p)$ classes modulo p where $f(p)$ gets large as p does. Linnik called this the *large sieve*. This is formalized in terms of the notation we have developed herein as follows.

Theorem 7 **The Large Sieve Inequality**

Suppose that $N \in \mathbb{N}$ and for every prime $p \leq \sqrt{N}$, let $f(p)$ residue classes modulo p be given, where $0 \leq f(p) < p$. If I_N is any interval of natural numbers of length N , then in I_N there are at most

$$\frac{(1 + \pi)N}{\sum_{p \leq \sqrt{N}} f(p)/(p - f(p))}$$

integers not lying in any of the given residue classes.

Proof. See [12, Corollary 2, p. 170]. □

The large sieve can be applied to Artin's conjecture, one of the classical problems from our list at the outset. From the large sieve Theorem 7, we have the following.

Theorem 8 **The Large Sieve on Artin's Conjecture**

Let I_N be an interval of natural numbers of length $N \in \mathbb{N}$ and let

$$\mathfrak{C}(N) = \left| \left\{ n \in I_N : n \text{ is not a primitive root modulo for any prime } p \leq \sqrt{N} \right\} \right|.$$

Then

$$\mathfrak{C}(N) \ll \sqrt{N} \log_e(N).$$

Proof. See [12, Theorem 4.8, p. 171]. □

Corollary 2 *Almost every $n \in \mathbb{N}$ is a primitive root for some prime.*

Using the large sieve, Bombieri [1] and Vinogradov [15] independently found a result on distribution of primes in arithmetic progression that is quite pleasant. In the next result, we use the following. The (basic) *Mangoldt function* is given by

$$\Lambda(n) = \log_e p \text{ if } n = p^a \text{ for some prime and } p, a \in \mathbb{N}, \text{ and } \Lambda(n) = 0 \text{ otherwise.}$$

In the

Theorem 9 **The Bombieri-Vinogradov Theorem**

For any real number $A > 0$, there is a constant $B = B(A)$ such that, for $Q = \sqrt{x}(\log_e x)^{-B}$,

$$\sum_{q \leq Q} \max_{y \leq x} \max_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ll \frac{x}{(\log_e x)^A}, \quad (6)$$

where

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n).$$

In keeping with the above, we now show how some classical problems can be tackled with Theorem 9. If $\tau(x)$ is the number of divisors function, and $n \in \mathbb{N}$, is fixed, then the *Titchmarsh divisor problem* is to compute the order of the function

$$S(x) = \sum_{p \leq x} \tau(p + n).$$

Theorem 9 can be applied to this problem to get the following—see [12, Theorem 5.11, p. 202] for a related result.

Theorem 10 **Bombieri-Vinogradov Applied to Titchmarsh**

For any $n \in \mathbb{N}$, there exists a constant $c \in \mathbb{R}^+$ such that

$$S(x) = cx + O\left(\frac{x \log_e \log_e x}{\log_e x}\right).$$

This establishes more than that proved by Titchmarsh [14] in 1930, wherein he showed that $S(x) = O(x)$.

Bombieri also provided a sieve, essentially generalizing the Selberg sieve, that was highly useful in establishing another highlight of sieve theory. To describe this and the application, we need the following notions. If (6) holds for any $A > 0$ and any $\varepsilon > 0$ with $Q = x^{\nu-\varepsilon}$, then we say the primes have *level of distribution* ν . Thus, according to Theorem 9, the primes are known to have level of distribution $\nu = 1/2$. The *Elliott-Halberstam conjecture* says the primes have level of distribution $\nu = 1$. This remains open.

The *generalized Mangoldt function* is given by

$$\Lambda_k(n) = \sum_{d|n} \mu(d) \log_e^k(n/d).$$

Also, let $\{a_n\}_{n=1}^\infty$ be a sequence of positive real numbers,

$$A(x) = \sum_{n \leq x} a_n, \text{ and } H = \prod_p (1 - f(p))(1 - 1/p)^{-1},$$

for a multiplicative function f . Then the following, proved by Bombieri in 1976—see [3]—under the assumption of the validity of the Elliott-Halberstam conjecture, is called the *asymptotic sieve*, where $k \geq 2$:

$$\sum_{n \leq x} a_n \Lambda_k(n) \sim kHA(x)(\log_e x)^{k-1}. \quad (7)$$

The case $k = 2$ and $a_n = 1$ for all n is essentially Selberg's sieve.

The most striking application to date of (7) was achieved by Friedlander and Iwaniec in 1998—see [4]–[5]—when they proved the following.

Theorem 11 **The Friedlander-Iwaniec Theorem**

There are infinitely many primes of the form $a^2 + b^4$.

We have covered an overview of some of the successes of sieve methods, but there are weaknesses. In particular, sieve methods cannot, in general, distinguish between numbers with an even number of prime factors and an odd number of prime factors, which is called the *parity problem*. Bombieri's

sieve clarified some of this issue in [2]–[3], by showing that, assuming the validity of the Elliot-Halberstam conjecture, his sieve implies an asymptotic formula for

$$\sum_{n \leq x} a_n F(n)$$

precisely when a function F provides what is called *equal weight* to integers with an even number of prime factors and those with an odd number of prime factors. It turns out that the generalized Mangoldt functions have exactly this property for $k > 1$. Of course, the parity problem remains, but the above strides and applications are indicative of the power of sieve methods.

It is worth pointing out, before we turn to another topic, that the Elliot-Halberstam conjecture implies some fascinating recent results for gaps between primes as well as implications for the twin-prime conjecture. These were found by Goldston, Pintz, and Yildirim in 2005—see [6]–[7]. For the following statement recall that the *infimum of a set* S is the greatest lower bound of S and is denoted $\inf(S)$. Also, the *limit inferior*, denoted by \liminf , is given by

$$\liminf_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} (\inf_{m \geq n} a_m)$$

for a sequence $\{a_n\}$.

The first result is unconditional.

Theorem 12 **Unconditional Goldston-Pintz-Yildirim**

If p_n denotes the n -th prime, then

$$\liminf_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\sqrt{\log_e p_n (\log_e \log_e p_n)^2}} < \infty.$$

Also, if $\{a_n\}$ is a sequence of natural numbers satisfying that

$$|\{a_n : n \leq N\}| > C(\log_e N)^{1/2} (\log_2 N)^2$$

for all sufficiently large N , then infinitely many of the differences of two elements of $\{a_n\}$ can be expressed as the difference of two primes.

The following is the conditional result.

Theorem 13 **The Conditional Goldston-Pintz-Yildirim Theorem**

If the Elliott-Halberstam conjecture is true, then

$$\liminf_{n \rightarrow \infty} p_{n+1} - p_n \leq 16.$$

Remark 4 It is worth noting that, in joint work with S. Graham, Goldston, Pintz, and Yildirim proved that if q_n is the n -th natural number with exactly two prime factors, then under the assumption of a generalized Elliot-Halberstram conjecture:

$$\liminf_{n \rightarrow \infty} q_{n+1} - q_n \leq 6$$

–see: <http://www.math.boun.edu.tr/instructors/yildirim/yildirim.htm>.

Acknowledgements: The author’s research is supported by NSERC Canada grant # A8484.

References

- [1] E. Bombieri, *On the large sieve*, *Mathematika* **12**, 201–225 (1965).
- [2] E. Bombieri, *On twin-almost primes*, *Acta Arith.* **28** (1975), 177–193, 457–461.
- [3] E. Bombieri, *The asymptotic sieve*, *Mem. Acad. Naz. dei XL* (1976), 243–269.
- [4] J. Friedlander and H. Iwaniec, *The polynomial X^2+Y^4 captures its primes*, *Annals of Math.* **148** (1998), 945–1040.
- [5] J. Friedlander and H. Iwaniec, *Asymptotic sieve for primes*, *Annals of Math.* **148** (1998), 1041–1065.
- [6] D.A. Goldston, J. Pintz, and C.Y. Yilidrim, *Primes in tuples I*, (preprint (2005)-19 of <http://aimath.org/preprints.html>; to appear in *Ann. of Math.*
- [7] D.A. Goldston, J. Pintz, and C.Y. Yilidrim, *The path to recent progress on small gaps between primes*, *Clay Math. Proceed.* **7** (2007).
- [8] D.R. Heath-Brown, *Artin’s conjecture for primitive roots*, *Quart. J. Math. Oxford* **37** (1986), 27–38.
- [9] Yu. V. Linnik, *The large sieve*, *Dokl. AN USSR* **30** (1941), 290–292.[Russian]

- [10] R.A. Mollin, **Fundamental Number Theory with Applications**, *Second Edition*, CRC, Taylor and Francis Group, Boca Raton, London, New York (2008).
- [11] R.A. Mollin, **Advanced Number Theory with Applications**, CRC, Taylor and Francis Group, Boca Raton, London, New York (2009).
- [12] W. Narkiewicz, **Number Theory**, World Scientific Publishers, Singapore (1983).
- [13] A. Selberg, *On an elementary method in the theory of primes*, , Norske Vid. Selsk. Forh. Trondhjem **19**, 64-67, (1947).
- [14] E.C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo **54** (1930), 414–429.
- [15] A.I. Vinogradov, *On the denseness hypothesis for Dirichlet L-series*, Izv. AN SSSR, Ser. Matem. **29** (1965), 903–934.[Russian]

Received: May, 2009