Sieve Theory and Application to Brun's Theorem

u2213723

April 25, 2024

Contents

1 Introduction

Theorem 1.1 (Brun's Theorem)**.** The series

$$\sum_{p,\, p+2 \text{ prime}} \frac{1}{p}$$

of reciprocals of prime twins is convergent (or perhaps finite).[1]

In 1919, Viggo Brun published a paper providing a proof for the theorem above, which was but another step in understanding twin primes.[2] The proof made use of one of many techniques known a sieves to find an upper bound on the set $\mathcal{A} = \{n(n-2) : 1 \leq n \leq X\}$. Sieve Theory is the collection of these methods and techniques used in number theory to count or bound the number of primes (this need not be all the primes but a subset e.g. $\mathcal{P} = \{p : p \not\equiv 3(\text{mod}4)\}$) in any given set of positive integers.

The object of this essay is to discuss the construction of sieves and assess their effectiveness ultimately making use of certain sifting arguments of Brun to prove the above theorem. This will begin with the sieves of Eratosthenes and Legendre (the first and simplest modern sieve) following naturally on to Brun's pure sieve which is based on Legendre's sieve but lessens the trouble faced with the error term in the former. The thing all these sieves have in common is that they are known as combinatorial as they make use of inclusion-exclusion by way of the Möbius function. However, there exist other sieves such as the Selberg, Linear and Large sieves which produce more accurate results (in that the error term can be kept much smaller) and will be briefly discussed towards the end.

Sieves have many applications within analytic number theory, as they can be used to prove many results which can't easily be done with ordinary analytic methods as well as in more practical settings such as public-key cryptography which involves factorising large numbers into prime factors[3].

1.1 Motivation

Primes have for over 3000 years both intrigued and baffled many as people have tried to identify and prove patterns. Two such patterns that are yet to be proven are the twin prime conjecture (there are infinitely many primes, p s.t. $p+2$ is prime) and Goldbach's conjecture (every even integer can be expressed as the sum of 2 primes). When reading work done towards understanding these problems, I found that mathematicians frequently made use of sieve arguments in their proofs (notably Chen's theorem[4], a weaker

[1] As stated on pg. [8].

[2] Brun [2], alternative proofs given in Greaves [8] and [7].

[3] The role of sieves would be to obtain information on distribution of primes so that less computational power is used in searching for prime factors.

[4] Chen, 1966 [3] and 1973 [4].

form of Goldbach conjecture). The primary focus of this essay is to prove Brun's Theorem which is especially interesting as we know that the sum of the reciprocol of all primes diverges.

1.2 Sieve of Eratosthenes

Around 300 BCE Eratosthenes thought of a method sifting the set of positive integers up to X leaving only the primes $> \sqrt{X}$ with the end goal of counting the number of primes left over (Friedlander and Iwaniec, 2010 pg. xi [6]). Take a 6×6 grid of integers up to 36 (Table 1) (Greaves, 2001[5]). Starting at 2 sieve is done by crossing out all multiples of the integer then moving on to the next integer not crossed out. The process terminates once all multiples of the largest prime $\leq \sqrt{X}$ has been reached.

Table 1: End result of Eratosthenes sieve on number grid.

1	(2)	(3)	(4)	(5)	~~6~~
7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~
19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~

However, the goal was to count the number of primes in the set; ideally by taking the cardinality of the set and subtracting the number of crossed out numbers. However, there are multiple numbers crossed out more than once. In order to get around this we need to add back in the number of integers crossed out twice (when counting, we can only count the number of crosses so will count integers with two prime factors twice), but then we know that integers with 3 prime factors have been counted $C_1^3 - C_2^3 = 0$ times so we need to then subtract the number of integers crossed out thrice. This process, known as inclusion-exclusion, continues until we reach the number of primes $z \leq \sqrt{X}$ we wish to remove (in the case of the above example, 3).

2 Legendre's Sieve

Legendre revisited the idea of Eratosthenes in the 19th century and formalised this process (Friedlander and Iwaniec, 2010 pg. 35-37[6]) using the möbius function, $\mu(d)$, to perform the inclusion-exclusion.

[5]Table and explanation from pg. 8-9 in [8].

[6]Notation taken from Chapter 5 of Opera de Cribro (pg. 35-37) on "Sieve Principles and Terminology" [6]

Definition 2.1 (The Möbius function)**.** (Greaves, 2001 pg. 9 [8], Friedlander and Iwaniec, 2010 pg. 2 [6]) For $d \in \mathbb{Z}$, $d > 0$ the Möbius function, $\mu(d)$, is defined by the formula,

$$\mu(d) = \begin{cases} 1 & \text{when } d = 1 \\ (-1)^{\nu(d)} & \text{when } d \text{ is the product of distinct primes} \\ 0 & \text{when } d \text{ has a repeated prime factor} \end{cases}$$

where $\nu(d) \geq 0$ counts the number of distinct prime factors of d.

The sieve is defined by a function (the sifting function), $S(\mathcal{A}, \mathcal{P}, z)$, where $\mathcal{A}$ is the sifting sequence (the sequence of non-negative integers to which the sieve is being applied), $\mathcal{P}$ is the sifting set (set of primes which are being sifted out of $\mathcal{A}$) and z is the sifting level. When formulating the sieve, z is used to define the sieving range which is the number of primes dividing,

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$$

which will frequently be shortened to P where z is not specified. This gives us the job of finding functions of the form,

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{\substack{n \leq x \\ (n, P(z))=1}} a_n.$$

Applying this to Eratosthenes' sifting idea in a more general case, we can state,

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}) &= [X] - \sum_{p<z} \left[\frac{X}{p}\right] + \sum_{p_1<p_2<z} \left[\frac{X}{p_1 p_2}\right] - \sum_{p_1<p_2<p_3<z} \left[\frac{X}{p_1 p_2 p_3}\right] - \ldots \\ &= \sum_{d|P} \mu(d) \left[\frac{X}{d}\right] \end{aligned}$$

where $\mathcal{A} = \{n \in \mathbb{Z} : 1 \leq n \leq X\}$, $\mathcal{P} = \{\text{all primes}\}$, $z = \sqrt{X}$ and the square brackets represent the floor function (maps a positive real number to the largest integer less or equal to the number). This appears to work. However it relies on the use of the floor function which isn't practical. To get around this, we separate the real number into integer and real number in the interval $[0, 1)$: $\frac{X}{d} = \left[\frac{X}{d}\right] + \left\{\frac{X}{d}\right\}$. Using big O notation we can then say $\frac{X}{d} = \left[\frac{X}{d}\right] + O(1)$ which can then be substituted into the formula for $S(\mathcal{A}, \mathcal{P})$ giving,

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}) &= \sum_{d|P} \mu(d) \frac{X}{d} + \sum_{d|P} O(1) = \sum_{d|P} \mu(d) \frac{X}{d} + O\left(\sum_{d|P} 1\right) \\ &= \sum_{d|P} \mu(d) \frac{X}{d} + O\left(2^{\pi(z)}\right) \end{aligned}$$

the last line coming from the fact that $d = p_1p_2p_3...$ is a product of distinct primes in the product $P(z)$ each of which are either factors of d or not (2 options).

2.1 Greater Generality

We start by redefining the sifting function S.

Definition 2.2. (Greaves, 2001 pg. 13 [8])

$$S(A) = \sum_{d|A} \mu(d)$$

We then write

$$S((a,P)) := S(a,P) = \sum_{d|(a,P)} \mu(d)$$

where P is defined as above and (x,y) is the greatest common divisor of x and y.

The following Lemma is also crucial in generalising this sieve for application.

Lemma 2.1 (Characteristic property of μ)**.** [7]

$$\sum_{d|(a,P)} \mu(d) = \begin{cases} 1 & \text{if } (a,P) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $(a,P) = 1$

$$\sum_{d|(a,P)} \mu(d) = \mu(1) = 1$$

as we know $d|1 \implies d = 1$.

Suppose $(a,P) \neq 1$,
we can say that $(a,P) = dm$ where $m \in \mathbb{N}$ P is a product of distinct primes so (a,P) must be a product of distinct primes. So we can write $(a,P) = p_1p_2...p_n$ for some $n \in \mathbb{N}$ where $p_1,...,p_n$ are distinct primes. We know that $\mu(d) = 1$ if n is even and $\mu(d) = -1$ if n is odd, so we want to show that there are an equal number of even subsets of $\{p_1,...,p_n\}$ as there are of odd subsets.
Case 1: n is even
There are $\binom{n}{k}$ subsets of size k so we want to show

$$\sum_{k=1}^{n/2} \binom{n}{2k} = \sum_{k=0}^{n/2-1} \binom{n}{2k+1}$$

[7] Stated as definition on pg. 13 of [8].

$$\begin{aligned}
\sum_{k=1}^{n/2}\binom{n}{2k} &= \sum_{k=1}^{n/2}\binom{n-1}{2k}+\binom{n-1}{2k-1}\\
&= \sum_{k=1}^{n/2}\binom{n-1}{2k}+\binom{n-1}{2k-1}\\
&= \sum_{k=1}^{n}\binom{n-1}{k}\\
&= \binom{n-1}{1}+\left(\binom{n-1}{2}+\binom{n-1}{3}\right)\\
&+ ...+\\
&+ \left(\binom{n-1}{k-2}+\binom{n-1}{k-1}\right)+\binom{n-1}{n}\\
&= \sum_{k=0}^{n/2-1}\binom{n}{2k+1}
\end{aligned}$$

with the last line coming from the identity, $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$ from Pascal's triangle.

Case 2: n is odd

Proof identical to proof for n even but with the limits of the sums altered i.e. to prove

$$\sum_{k=1}^{(n-1)/2}\binom{n}{2k} = \sum_{k=0}^{(n-1)/2}\binom{n}{2k+1}$$

□

We then define

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

and

$$S(\mathcal{A}, P) = \sum_{a\in\mathcal{A}} S(a, P)$$

From this, we can write,

$$S(\mathcal{A}, P) = \sum_{a\in\mathcal{A}}\sum_{d|a;d|P}\mu(d) = \sum_{d|P}\mu(d)|\mathcal{A}_d|$$

sometimes known as Legendre's identity (Greaves, 2001 pg. 13-14 [8]).

With this knowledge, we can now see how this sieve can be applied in the following example:

Example 2.1. (Greaves, 2001 pg. 14-15 [8]) We want to find an inequality approximating the number of primes in the interval $(Y - X, Y]$ (above, we used the sieve in the case where $Y = X$)

Let

$$\mathcal{A} = \{a \in \mathbb{Z} : Y - X < a \leq Y\}$$

We can then write,

$$|\mathcal{A}_d| = \left[\frac{Y}{d}\right] - \left[\frac{Y - X}{d}\right] = \frac{X}{d} + O(1)$$

with the last equality coming from the fact that $\left\{\frac{Y-X}{d}\right\} - \left\{\frac{Y}{d}\right\}$ lies in the interval $(-1, 1)$.

Applying Legendre's identity and the identity,

$$\sum_{d|P} \frac{\mu(d)}{d} = \prod_{p<z} \left(1 - \frac{1}{p}\right),$$

we get,

$$\begin{aligned} S(\mathcal{A}, P) &= X \sum_{d|P} \frac{\mu(d)}{d} + O(1) \\ &= X \prod_{p<z} \left(1 - \frac{1}{p}\right) + O\left(2^{\pi(z)}\right) \\ &= X \prod_{p<z} \left(\sum_{r=1}^{\infty} \frac{1}{p^r}\right)^{-1} + O\left(2^{\pi(z)}\right) \\ &\leq X \left(\sum_{n<z} \frac{1}{n}\right)^{-1} + O\left(2^{\pi(z)}\right) \\ &\leq \frac{X}{\log z} + O\left(2^{\pi(z)}\right) \end{aligned}$$

where the last line comes from the fact that the harmonic series is strictly less than the integral of $\frac{1}{n}$. Substituting $z = \log(X)$, we get,

$$\pi(Y) - \pi(Y - X) = O\left(\frac{X}{\log\log(X)}\right)$$

with $x \geq 3$ to ensure denominator is positive.

There is, however, a major problem with this sieve, so large that it can't really be used in any practical setting and can be seen in both examples. This is found in the remainder term, $O\left(2^{\pi(z)}\right)$ which gets larger than the $[X]$ as z gets large which isn't possible and will give us an erroneous result. This restricts the sieving range massively to $z = \log X$ (Greaves, 2001 pg

11, 71-72 [8]). This restriction is incovenient and doesn't allow for many results to be proven, a problem Brun managed to improve on by altering Legendre's sieve by truncating the each of the sums to limit the remainder terms.

3 Brun's Pure Sieve

Brun's pure Sieve was the first great development in Sieve Theory since Legendre developed the ideas of Eratosthenes. It is another combinatorial Sieve which as mentioned above involves truncating the sums of the Legendre sieve by only sifting out integers d such that $\nu(d) < k$ giving a bound on the value of $\pi(X)$, which can either be constructed using and extra condition in the limit of the sums or by replacing $\mu(d)$ with a sequence of functions $\Lambda = \lambda_d$ defined by,

$$\lambda_d = \begin{cases} \mu(d) & \text{if } \nu(d) < k \\ 0 & \text{if } \nu(d) \geq k \end{cases}.^{8}$$

Brun showed that whether this is a upper or lower bound is determined solely by whether k is odd or even corresponding to a lower and upper bounds respectively. The repeated truncation produces about a bound on $pi(z)$ for which, the remainder/error term can be controlled better as it contains fewer terms. As the error term is ultimately smaller when using this sieve, the sifting range, z, now satisfies $z \leq X^{1/c\kappa \log\log X}$ where $c \approx 3.591...$ is the positive constant for which

$$\left(\frac{c}{e}\right)^{c} = e.^{9}$$

and κ is the sifting density which, as the name suggests, is a weighted average of the number of residue classes sifted out by each prime (that is, $g(p)p$ equals κ on average where $g(p)$ is a sort of probability function giving the "chance of hitting" a multiple of a given prime p).[10]

3.1 Brun's Theorem

We restate Brun's Theorem,

Theorem 3.1 (Brun's Theorem)**.** The series

$$\sum_{p,\, p+2 \text{ prime}} \frac{1}{p}$$

converges (or terminates).

[8] Friedlander and Iwaniec, 2010 [6]
[9] Greaves, 2001 pg. 81 [8],
[10] Friedlander and Iwaniec, 2010 pg. 42 [6].

As mentioned in the Introduction, the proof (Gel'fond, A.O. and Linnik, Yu.V, 1966 p 101-105[11]) of this will involve finding an upper bound for $\pi_2(X)$ defined as being the number of twin primes not greater than X which we will find to be,

$$\pi_2(X) < c\frac{X}{\log^2 X}(\log\log X)^2$$

. We do this by sifting the set $\mathcal{A} = \{n(n-2) : 1 \leq n \leq X\}$, in an attempt to remove all primes $\leq z$ for some $z \leq \sqrt{X}$.

Proof. We can write as when starting with the sum of Eratosthenes

$$\pi_2(X) = X - \sum_{p|P,\, p\in\mathcal{A}} 1 + \sum_{p_1p_2|P,\, p_1,p_2\in\mathcal{A}} 1 - ...$$

We can obtain an upper bound on this by taking a partial sum stopping after an even number of terms[12] i.e.

$$\pi_2(X) \leq X - \sum_{p|P,\, p\in\mathcal{A}} 1 + \sum_{p_1p_2|P,\, p_1,p_2\in\mathcal{A}} 1 - ... + \sum_{p_1...p_{2k}|P,\, p_1,...,p_{2k}\in\mathcal{A}} 1$$

noting that each of the products of primes $p_1...p_l$ for $1 \leq l \leq 2k$ are counted exactly once.

Let $d = p_1p_2...p_l$ ($p_1, ..., p_l$ distinct $\implies \mu(d) \neq 0$). We wish to evaluate

$$S_d = \sum_{d\in\mathcal{A}} 1.$$

Case 1: $d \equiv 1 \pmod 2$

The sum,

$$S_d = \sum_{d\in\mathcal{A}} 1,$$

in this case counts the solutions of the congruence,

$$n(n+2) \equiv 0 \pmod d.$$

This quantity equals the number of solutions of the systems equations of the form,

$$\left.\begin{aligned} n &\equiv 0 \pmod{d_1} \\ n+2 &\equiv 0 \pmod{d_2} \end{aligned}\right\}$$

where $d = d_1d_2$. Each system will have,

$$\frac{X}{d} + \theta$$

[11] Proof heavily based on that given in [7].

[12] By similar logic, a lower bound could be found by stopping after an odd number of terms.

solutions where $|\theta| \leq 1$. Denoting the number of systems by $\tau(d)$ gives,

$$S_d = X\frac{\tau(d)}{d} + \theta\tau(d).$$

Case 2: $d \equiv 0 \pmod 2$
The sum,

$$S_d = \sum_{d\in\mathcal{A}} 1$$

now counts the solutions of the congruence,

$$n(n+1) \equiv 0 \quad \left(\text{mod } \frac{d}{2}\right)$$

for integers $n \leq \frac{X}{2}$ giving,

$$S_d = X\frac{\tau\left(\frac{d}{2}\right)}{d} + \theta\tau\left(\frac{d}{2}\right).$$

We can then write,

$$S_d = X\frac{\tau'(d)}{d} + \theta\tau'(d).$$

where

$$\tau'(d) = \begin{cases} \tau, & \text{if } d \equiv 1 \pmod 2 \\ \tau, & \text{if } d \equiv 0 \pmod 2 \end{cases}$$

Now returning to the upper bound on $\pi_2(X)$, we have,

$$\begin{aligned}\pi_2(X) \leq X \Bigg(1 - \sum_{p|P}\frac{\tau'(p)}{p} + \sum_{p_1p_2|P}\frac{\tau'(p_1p_2)}{p_1p_2} \\ -... + \sum_{p_1...p_{2k}|P}\frac{\tau'(p_1...p_{2k})}{p_1...p_{2k}}\Bigg) + \sum_{p|P}\tau'(p) + \sum_{p_1p_2|P}\tau'(p_1p_2) \\ + ... + \sum_{p_1...p_{2k}|P}\tau'(p_1...p_{2k})\end{aligned}$$

where the final $2k$ sums come from the fact that $|\theta| \leq 1$.

We then want to show the result:

$$\sum_{p_1...p_r|P}\tau'(p_1...p_r) \leq 2^r C_r^{\pi(z)} < 2^r\frac{\pi^r(z)}{r!}$$

where C_b^a is a choose b. The first inequality comes from considering the number of ways of composing a number $d := p_1...p_r$ consisting of r distinct

prime factors. So the sum $\sum_{p_1...p_r|P} 1$ evaluates to $C_r^{\pi(z)}$. If we then consider the number of ways of partitioning the set $\{p_1, ..., p_r\}$ into to two parts, we see that each p_i is either in the first part or the second part ($\tau(d)$ gives the number of systems of equations, each containing two equations, so we must factorise d into two factors each a product of distinct prime factors). This gives that $\tau'(p_1...p_r) = 2^r \ \forall p_1...p_r|P$ from which we can state the first inequality.

The second inequality follows directly from the definition of the binomial coefficient in that $C_k^n = \frac{n!}{k!(n-k)!} < \frac{n^k}{k!}$ for all non-negative integers $k \leq n$.

Using this and assuming $z > 2 \implies \pi(z) \neq 1$ we can deduce,

$$\sum_{p|P} \tau'(p) + \sum_{p_1p_2|P} \tau'(p_1p_2) + ... + \sum_{p_1...p_{2k}|P} \tau'(p_1...p_{2k}) < \pi^{2k}(z) \sum_{r \leq 2k} \frac{2^r}{r!} \leq 9\pi^{2k}(z)$$

with the last inequality coming from the fact that $\lim_{k\to\infty} \sum_{r\leq 2k} \frac{2^r}{r!} = e^2$. Next we need to address the rest of the sum defining $\pi_2(x)$ i.e.

$$- \sum_{p_1...p_{2k+1}|P} \frac{\tau(p_1...p_{2k+1})}{p_1...p_{2k+1}} + \sum_{p_1...p_{2k+2}|P} \frac{\tau(p_1...p_{2k+2})}{p_1...p_{2k+2}} - ... = T_{2k}$$

If we add T_{2k} to the first term of the sum,

$$\begin{aligned} X \Bigg(1 - \sum_{p|P} \frac{\tau'(p)}{p} + \sum_{p_1p_2|P} \frac{\tau'(p_1p_2)}{p_1p_2} \\ - ... + \sum_{p_1...p_{2k}|P} \frac{\tau'(p_1...p_{2k})}{p_1...p_{2k}} \Bigg) + \sum_{p|P} \tau'(p) + \sum_{p_1p_2|P} \tau'(p_1p_2) \\ + ... + \sum_{p_1...p_{2k}|P} \tau'(p_1...p_{2k}), \end{aligned}$$

the term ends up equal to

$$\left(1 - \frac{1}{2}\right) \prod_{3\leq p\leq z} \left(1 - \frac{2}{p}\right).$$

This can be shown by noticing that $\tau'(d) = 2^{\nu(d)}$ where ν, as before, is defined as being the number of prime factors of d ($\nu(d) = 0$ if d has repeated prime factors).

By induction, we can show

$$\sum_{p_1...p_r|P} \frac{1}{p_1...p_r} \leq \frac{\left(\sum_{p\leq z} \frac{1}{p}\right)^r}{r!}.$$

Since we know that $\sum_{p\leq z}\frac{1}{p}=\log\log z+c$, we can write

$$\sum_{p_1...p_r|P}\frac{1}{p_1...p_r}<\frac{(\log\log z+c)^r}{r!}.$$

From this we deduce that,

$$T_{2k}\leq\sum_{r\geq 2k+1}\frac{(2\log\log z+2c)^r}{r!}.$$

Using

$$r!>\left(\frac{r}{e}\right)^r,$$

we can then state (substitution),

$$T_{2k}\leq\sum_{r\geq 2k+1}\left(\frac{2e\log\log z+2ec}{r}\right)^r.$$

From here, we can set $k=2e\log\log z+2ec$ as well as note that $T_{2k}\leq 2^{-2k}<\frac{1}{\log^4 z}$.[13] We can therefore write, starting with the sums of before,

$$\begin{aligned}1-\sum_{p|P}\frac{\tau'(p)}{p}+\sum_{p_1p_1|P}\frac{\tau'(p)}{p}+...+\sum_{p_1...p_{2k}|P}\frac{\tau'(p_1...p_{2k})}{p_1...p_{2k}}\\ =\sum_{d|P}\mu(d)\frac{\tau'(d)}{d}-T_{2k}\leq\prod_{p\leq z}\left(1-\frac{\tau'(p)}{p}\right)+\frac{1}{\log^4 z}\\ =\frac{1}{2}\prod_{3\leq p\leq z}\left(1-\frac{2}{p}\right)+\frac{1}{\log^4 z}\end{aligned}$$

where the last equality comes from using $\tau(d)=2^{\nu(d)}$ which equals 2 when d is prime.

We finally return to our orginal upper bound inequality (after having substituted τ' function in) and substitute the above result in addition to the fact that $\sum_{p|P}\tau'(p)+\sum_{p_1p_2|P}\tau'(p_1p_2)+...+\sum_{p_1...p_{2k}|P}\tau'(p_1...p_2k)<9\pi^{2k}(z)$. This gives,

$$\pi_2(X)<\frac{X}{2}\prod\left(1-\frac{2}{p}\right)+\frac{X}{\log^4 z}+9\pi^{2k}(z).$$

We need to satisfy $\pi^{2k}(z)<\frac{X}{\log^4 z}$ and it ends up being enough to take $z=X^{1/2k}$. We can show that

$$\prod_{3\leq p\leq z}\left(1-\frac{2}{p}\right)<\frac{c_0}{\log^2 z}$$

[13]The first inequality can be proven through the substitution of k followed by induction. The second inequality isn't as obvious and it's proof has been omitted.

where c_0 is an absolute constant, using Merten's third theorem (Hardy, Wright, 1975 pg. 351 [9]),

$$\prod_{p\leq z}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}}{\log z}\implies\prod_{p\leq z}\left(1-\frac{1}{p}\right)<\frac{e^{-\gamma}}{\log z}$$

for some constant b and where $\gamma\approx 0.561459...$ is the Euler-Mascheroni constant. To do this, we take the square of both sides of the second inequality and compare term wise,

$$\prod_{p\leq z}\left(1-\frac{2}{p}\right)<\prod_{p\leq z}\left(1-\frac{2}{p}+\frac{1}{p^2}\right)<\frac{c_0}{\log^2 z}$$

by setting $e^{-2\gamma}=c_0$. Using the inequality, $\prod_{3\leq p\leq z}\left(1-\frac{2}{p}\right)<\frac{c_0}{\log^2 z}$, and that $\pi_2(X)<\frac{X}{2}\prod\left(1-\frac{2}{p}\right)+\frac{X}{\log^4 z}+9\pi^{2k}(z)$, we can show $\pi_2(X)<c\frac{X}{\log^2 X}(\log\log X)^2$. The proof of this has been omitted as it is merely the result of repeated substitution and algebraic manipulation based on results already given.

From this statement, Brun's Theorem follows as we can write (Greaves, 2001 p 85[14]),

$$\sum_{\substack{2^k<p\leq 2^{k+1}\\ p+2\text{ prime}}}\frac{1}{p}\ll 2\left(\frac{\log\log 2^{k+1}}{\log 2^{k+1}}\right)^2.$$

□

4 Conclusion

Brun's theorem was an interesting leap in the understanding of twin primes (of course if the twin prime conjecture doesn't hold, we get that the series terminates), but it was only the beginning of sieves being used to prove otherwise challenging results in analytic number theory, the most notable example being Chen's theorem (an additive result stating that every even integer can be expressed as the sum of a prime and an integer with at most 2 prime factors) – essentially a weaker form of the Goldbach Conjecture.

As mentioned before, all sieves discussed in the essay are of combinatorial type meaning that they make use of inclusion-exclusion. However, sieves do not have to use inclusion-exclusion in this way and the results suggest that these approaches tend to produce more accurate bounds. The first sieve created in one of these new ways was the Selberg sieve developed in 1947. The fundamental idea is that the function $\mu(d)$ is replaced by a

[14]Final step in proof given in [8].

pair of functions $\lambda_D^{\pm}$ satisfying the inequality $\sum_{d|A} \lambda_D^-(d) \leq \sum_{d|A} \mu(d) \leq \sum_{d|A} \lambda_D^+(d)$ where $A|P$. It is essentially an upper bound sieve satisfying,

$$S(\mathcal{A}, P(z)) \leq \sum_{d|(A,P(z)} \lambda_D^+(d).$$

Care must be taken to keep $d < D$ sufficiently small to avoid the error terms faced in previous sieves. In order to do this, Selberg ensured that the λ_D^+ function satisfied[15]

$$\sum_{d|A} \lambda_D^+(d) = \left(\sum_{d_1 < \sqrt{D}} \lambda(d_1) \right)^2.$$

What followed were a series of new more effective sieves which continue to be used both within number theory and in areas such as cryptography, in particular public-key cryptography as the primes dealt with are very large and the aim is to decrease the computing power required for instance to find such primes. Despite this, within sieve theory, there lie many unsolved problems. For instance, applying the ideas of the Selberg sieve to find a lower bound

$$S(\mathcal{A}, P(z)) \geq \sum_{d|(A,P(z)} \lambda_D^+(d)$$

has yet to be given a complete solution. Another problem within sieve theory is the Parity problem. This states:

"If A is a set whose elements are all products of an odd number of primes (or are all products of an even number of primes), then (without injecting additional ingredients), sieve theory is unable to provide non-trivial lower bounds on the size of A. Also, any upper bounds must be off from the truth by a factor of 2 or more." (Tau, Terence, 2007 [1])

Work has been done by Iwaniec and Friedlander since 1996 to find "parity- sensitive" sieves which aim to lower the barrier of the parity problem something they succeeded in doing when they proved Friedlander-Iwaniec Theorem, that is there are infinitely many primes of the form $x^2 + y^4$ using these new methods. These advances are but glimpse of what is to come in our understanding of prime numbers (Friedlander, Iwaniec, 1997 [5]).

[15](Greaves, 2001 pg. 41 [8])

5 Bibliography

References

[1] Open question: The parity problem in sieve theory. https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory, June 2007. Accessed on 25 April 2024.

[2] Viggo Brun. La série 1/5+1/7+1/11+1/13+1/17+1/19+1/29+1/31 +1/41+1/43+1/59+1/61+..., où les dénominateurs sont nombres premiers jumeaux est convergente ou finie. Bulletin des Sciences Mathématiques, 43:124–128, 1919.

[3] J.R. Chen. On the representation of a large even integer as the sum of a prime and the product of at most two primes. Kexue Tongbao, 11(9):385–386, 1966.

[4] J.R. Chen. On the representation of a larger even integer as the sum of a prime and the product of at most two primes. Sientia Sinica, 16(2):157–176, 1973.

[5] John Friedlander and Henryk Iwaniec. Using a parity-sensitive sieve to count prime values of a polynomial. PNAS, 94(4):1054–1058, 1997.

[6] John Friedlander and Henryk Iwaniec. Opera de Cribro. Colloquium Publications, Rhode Island, NY, 2010.

[7] A.O. Gel'fond and Yu.V. Linnik. Elementary methods in the analytic theory of numbers. M.I.T., Cambridge, Massachusetts, 1966. (Translated from Russian).

[8] G.R.H. Greaves. Sieves in Number Theory. Springer Berlin, Heidelberg, 2001.

[9] G.H. Hardy and E.M. Wright. An Introduction to the Theory of Numbers, 4th ed. Oxford University Press, Oxford, England, 1975. 4th ed with corrections.