

[Math Seminar] Brun's Combinatorial Sieve & Twin Primes

Connor Li, csl2192

March 20, 2024

1 Review of Sieves

1.1 Introduction

1.2 Conceptual Review

How Sieves work:

- Begin with some set \mathcal{A} of positive integers
- We are interested in the size of set after removing all the primes
- Remove elements that don't fit, but you have to make sure that you aren't overcounting
- Then, you have the desired set \mathcal{A}'

1.3 Connection to Brun's Sieve

Why it's different from Eratosthenes

- Brun's sieve is more about estimation, we are talking about specific sequences of primes like twin primes
- asymptotic approximation is much better and the error term is significantly less than the classical sieve

2 Brun's Sieve

2.1 Introduction

Brun's sieve is a combinatorial sieve that is used to estimate the number of twin primes up to a given number x .

A twine prime is a pair of prime numbers that differ by 2. For example, (3, 5) and (11, 13) are twin primes.

The goal of this sieve is to show that the twin primes are sparse compared to the prime numbers. From a result in last lecture, we know that the sum of reciprocals of prime numbers diverge.

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + B + O\left(\frac{1}{\log x}\right) \implies \lim_{x \rightarrow \infty} \sum_{p \leq x} \frac{1}{p} = \infty$$

Since twin primes are far less frequent than prime numbers, we can show

$$\lim_{x \rightarrow \infty} \sum_{\substack{p_1, p_2 \leq x \\ p_2 = p_1 + 2}} \frac{1}{p_1} + \frac{1}{p_2} < \infty$$

2.2 Inclusion-Exclusion

Like I mentioned before, Brun's sieve is based on the logic of inclusion-exclusion. As a result, we will prove a theorem to formalize that method of choosing. The combinatorial inequality that we will show is the simplest form of the Brun sieve.

Theorem: If $\ell \geq 1$ and $0 \leq m \leq \ell$, then

$$\sum_{k=0}^m (-1)^k \binom{\ell}{k} = (-1)^m \binom{\ell-1}{m}$$

Proof: We will prove this by induction. The base case is when $m = 0, 1, 2$. If $m = 0$, the case is trivial. If $m = 1$, then we have

$$\sum_{k=0}^1 (-1)^k \binom{\ell}{k} = 1 - \ell = (-1)^1 \binom{\ell-1}{1}$$

Similarly, for $m = 2$, we have the following.

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

Now, use induction on m . Assume the equation holds true for $m-1$, then we have

$$\begin{aligned} \sum_{k=0}^m (-1)^k \binom{\ell}{k} &= \sum_{k=0}^{m-1} (-1)^k \binom{\ell}{k} + (-1)^m \binom{\ell}{m} \\ &= (-1)^{m-1} \binom{\ell-1}{m-1} + (-1)^m \binom{\ell}{m} \\ &= (-1)^m \left(\binom{\ell}{m} - \binom{\ell-1}{m-1} \right) \\ &= (-1)^m \binom{\ell-1}{m} \end{aligned}$$

Thus, we have completed the proof.

2.3 The Brun Sieve

Now, we will use the above theorem to introduce the Brun sieve as a combinatorial argument.

Theorem: Let X be a nonempty, finite set where $|X| = N$. Now, let P_1, \dots, P_r be r distinct properties that elements of set X might have. Let N_0 denote the number of elements of X that have none of these properties.

For any subset $I = \{i_1, \dots, i_k\}$ of $\{1, 2, \dots, r\}$ let $N(I)$ denote the number of elements of X that have each of the properties $P_{i_1}, P_{i_2}, \dots, P_{i_k}$. And if $I = \emptyset$, then we assume that $N(\emptyset) = |X| = N$. If m is an even integer, then

$$N_0 \leq \sum_{k=0}^m (-1)^k \sum_{|I|=k} N(I)$$

If m is an odd integer, then

$$N_0 \geq \sum_{k=0}^m (-1)^k \sum_{|I|=k} N(I)$$

Note: The intuition behind this formula is to provide a bound on the number of elements of X . If you take the properties P_r to be “being divisible by some prime,” then we are able to construct bounds for a set N_0 that only consists of the prime numbers. Essentially, you should view this as a generalized method to pick and choose certain primes to construct your own set.

Inclusion Exclusion

$$N_0 \leq N - \sum_{|I|=1} N(I) + \sum_{|I|=2} N(I) - \sum_{|I|=3} N(I) + \dots$$

Proof: The inequalities in the theorem count the elements of X as explained above. To prove the theorem, let's focus on the contribution from each individual element $x \in X$ to these inequalities.

Assume that x has exactly ℓ properties P_i . If $\ell = 0$, then x is counted once in N_0 and once in $N(\emptyset)$, but it is not counted in $N(I)$ if I is nonempty. If $\ell \geq 1$, then x is not counted in N_0 . But, since $\ell \geq 1$, we can renumber the properties P_1, \dots, P_ℓ such that x has those properties. Now, define some set of indexes of attributes $I \subset \{1, \dots, r\}$.

If $\exists i \in I$ such that $i > \ell$, then x is not counted in $N(I)$ because it is missing one of the properties of I . However, if $I \subset \{1, \dots, \ell\}$, then x is counted once in $N(I)$ since it contains all the properties. This means that for each $k = 0, 1, \dots, \ell$, there are exactly $\binom{\ell}{k}$ subsets I such that $|I| = k$. If $m \geq \ell$, the element x contributes

$$\sum_{k=0}^{\ell} (-1)^k \binom{\ell}{k} = 0$$

This is because of a property of the binomial theorem that allows you to express the left hand side with the summation as 0^n for some $n \in \mathbb{N}$, which evaluates to 0. However, if $m < \ell$, the binomial terms don't all cancel out and the element x contributes

$$\sum_{k=0}^m (-1)^k \binom{\ell}{k}$$

It's important to note that if ℓ is even, then the contribution is positive and we have an upper-bound. But if ℓ is odd, then the contribution is negative and we have a lower-bound as stated in the theorem.

3 Twin Primes

3.1 Introduction

3.2 Precursors to Theorem

Theorem: (Lemma 1) For $x \geq 1$ and for any congruence class $a \bmod m$, the number of positive integers not exceeding x that are congruent to $a \bmod m$ is $\frac{x}{m} + \theta$ where $|\theta| < 1$.

Proof: Although the actual proof requires skills from Algebra, the intuition is pretty simple. If you were to divide up the integers from 1 to x into m groups based on congruence classes, then each class would have $\frac{x}{m}$ elements. However, if x is not divisible by m , then there will be a remainder θ that is less than 1. This is the main idea behind the proof.

Theorem: (Lemma 2) Let $x \geq 1$, and let p_{i_1}, \dots, p_{i_k} be distinct odd primes. Let $N(i_1, \dots, i_k)$ denote the number of positive integers $n \leq x$ such that

$$n(n+2) \equiv 0 \bmod p_{i_1} \cdots p_{i_k}$$

Then, for $|\theta| < 1$,

$$N(i_1, \dots, i_k) = \frac{2^k x}{p_{i_1} \cdots p_{i_k}} + 2^k \theta$$

3.3 Brun's Theorem

Theorem: Let $\pi_2(x)$ denote the number of primes p not exceeding x such that $p+2$ is also prime. Then,

$$\pi_2(x) \ll \frac{x(\log \log x)^2}{(\log x)^2}$$

Proof: (Part 1) Let $5 \leq y < x$ and let $r = \pi(y) - 1$ represent the number of odd primes not exceeding y , which we will also enumerate as p_1, \dots, p_r . Now, let $\pi_2(y, x)$ denote the number of primes p such that $y < p \leq x$ and $p+2$ is also prime. If $y < n \leq x$ and both $n, n+2$ are prime numbers, then $n > p_i$ for all $i \in [1, r]$ and for all p_i ,

$$n(n+2) \not\equiv 0 \bmod p_i$$

Let $N_0(y, x)$ denotes the number of positive integers $n \leq x$ such that $n(n+2) \not\equiv 0 \bmod p_i$ for all $i \in [1, r]$. Then, we have a very simple upper-bound

$$\pi_2(y) \leq y + \pi_2(y, x) \leq y + N_0(y, x)$$

Now, we can simply use Brun's sieve and the lemmas above to find an upper-bound for $N_0(y, x)$.

Proof: (Part 2) Define X to be the set of positive integers not exceeding x . For each odd prime $p_i \leq y$, we let P_i be the property that $n(n+2)$ is divisible by p_i . This means for any subset $I = \{i_1, \dots, i_k\}$ of $\{1, 2, \dots, r\}$, we have $N(I)$ denote the number of elements of X that have each of the properties $P_{i_1}, P_{i_2}, \dots, P_{i_k}$. In other words, $N(I)$ denotes the number of integers $n \in X$ such that $n(n+2)$ is divisible by each of the primes p_{i_1}, \dots, p_{i_k} or that $n(n+2)$ is divisible by $p_{i_1} \cdots p_{i_k}$.

Using our Lemma 2 from above, we have that

$$N(I) = N(i_1, \dots, i_k) = \frac{2^k x}{p_{i_1} \cdots p_{i_k}} + 2^k \theta$$

Now, let m be an even integer such that $1 \leq m \leq r$. Using our inequality from the Inclusion-Exclusion section, we have the following result.

$$\begin{aligned} N_0(y, x) &\leq \sum_{k=0}^m (-1)^k \sum_{|I|=k} N(I) \\ &\leq \sum_{k=0}^m (-1)^k \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \left(\frac{2^k x}{p_{i_1} \cdots p_{i_k}} + 2^k \theta \right) \\ &\leq x \sum_{k=0}^m \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}} + \sum_{k=0}^m (-1)^k \binom{r}{k} \mathcal{O}(2^k) \\ &\leq x \underbrace{\sum_{k=0}^r \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}}}_{S_1} - x \underbrace{\sum_{k=m+1}^r \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}}}_{S_2} + \underbrace{\mathcal{O}\left(\sum_{k=0}^m \binom{r}{k} 2^k\right)}_{S_3} \end{aligned}$$

As you can see, the above expression is composed of 3 parts, which we will evaluate separately. Using Merten's Formula, we can show the following bound for S_1 .

$$\begin{aligned} S_1 &= x \sum_{k=0}^r \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}} = x \prod_{2 < p \leq y} \left(1 - \frac{2}{p}\right) \\ &< x \prod_{2 < p \leq y} \left(1 - \frac{1}{p}\right)^2 \\ &\ll \frac{x}{(\log y)^2} \end{aligned}$$

Now, consider S_2 . Let $s_k(x_1, \dots, x_r)$ be the elementary symmetric polynomial of degree k in r variables. For any nonnegative real numbers x_1, \dots, x_r , we have

$$\begin{aligned} s_k(x_1, \dots, x_r) &= \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} x_{i_1} \cdots x_{i_k} \\ &\leq \frac{(x_1 + \cdots + x_r)^k}{k!} \\ &= \frac{(s_1(x_1, \dots, x_r))^k}{k!} \\ &< \left(\frac{e}{k}\right)^k (s_1(x_1, \dots, x_r))^k \end{aligned}$$

Using this fact, we have the following bound for S_2 .

$$\begin{aligned} |S_2| &= \left| x \sum_{k=m+1}^r \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}} \right| \leq x \sum_{k=m+1}^r \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \frac{2^k}{p_{i_1} \cdots p_{i_k}} \\ &\leq x \sum_{k=m+1}^r \sum_{\{i_1, \dots, i_k\} \subset \{1, \dots, r\}} \left(\frac{2}{p_{i_1}}\right) \cdots \left(\frac{2}{p_{i_k}}\right) \\ &= x \sum_{k=m+1}^r s_k\left(\frac{2}{p_1}, \dots, \frac{2}{p_r}\right) \\ &< x \sum_{k=m+1}^r \left(\frac{e}{k}\right)^k \left(s_1\left(\frac{2}{p_1}, \dots, \frac{2}{p_r}\right)\right)^k \\ &= x \sum_{k=m+1}^r \left(\frac{e}{k}\right)^k \left(\frac{2}{p_1} + \cdots + \frac{2}{p_r}\right)^k \\ &< x \sum_{k=m+1}^r \left(\frac{2e}{m}\right)^k \left(\sum_{p \leq y} \frac{1}{p}\right)^k \\ &< x \sum_{k=m+1}^r \left(\frac{c \log \log y}{m}\right)^k \\ &\leq x \underbrace{\sum_{k=m+1}^{\infty} \frac{1}{2^k}}_{m > 2c \log \log y} < \frac{x}{2^m} \end{aligned}$$

Proof: (Part 3) Finally, we have the following bound for S_3 . Since r is the number of odd primes less than or equal to y , it follows that $2r \leq y$, so we can bound S_3 as follows.

$$S_3 = \sum_{k=0}^m \binom{r}{k} 2^k \leq \sum_{k=0}^m r^k 2^k \ll (2r)^m \leq y^m$$

Thus, if we backtrack to our original estimate for $\pi_2(y)$, we have the following for any $5 \leq y < x$ and $m > 2c \log \log y$ where c is fixed.

$$\pi_2(y) \leq y + N_0(y, x) \leq y + S_1 - S_2 + S_3 \ll \frac{x}{(\log y)^2} + \frac{x}{2^m} + y^m$$

Let $c' = \max\{2c, \frac{1}{\log 2}\}$ and define y as follows.

$$y = \exp\left(\exp\left(\frac{\log x}{3c' \log \log x}\right)\right) \quad m = 2c' \log \log x$$

This definition for y satisfies the necessary bounding conditions for x sufficiently large. And since $\log y = \frac{\log x}{3c' \log \log x}$, we can bound S_1 .

$$\frac{x}{(\log y)^2} \ll \frac{x(\log \log x)^2}{(\log x)^2}$$

For S_2 , use our same definitions of y, m to show the following.

$$\frac{x}{2^m} < \frac{4x}{2^{2c' \log \log x}} \leq \frac{4x}{(\log x)^{2c' \log 2}} \ll \frac{4x}{(\log x)^2}$$

For S_3 , do the same and we get the following.

$$y^m \leq y^{2c' \log \log x} = \exp\left(\frac{2c' \log \log x \log x}{3c' \log \log x}\right) = x^{\frac{2}{3}}$$

Finally, if we combine these three estimates, we get the following result.

$$\pi_2(x) \ll \frac{x(\log \log x)^2}{(\log x)^2} + \frac{4x}{(\log x)^2} + x^{\frac{2}{3}} \ll \frac{x(\log \log x)^2}{(\log x)^2}$$

This completes our proof.

3.4 Twin Primes

This is the famous conjecture about twin primes and their reciprocals converging.

Theorem: Let p_1, p_2, \dots be a sequence of prime numbers p such that $p+2$ is also prime. Then,

$$\sum_{n=1}^{\infty} \left(\frac{1}{p_n} + \frac{1}{p_n+2} \right) = \left(\frac{1}{3} + \frac{1}{5} \right) + \left(\frac{1}{5} + \frac{1}{7} \right) + \left(\frac{1}{11} + \frac{1}{13} \right) + \dots$$

$$< \infty$$

Proof: From the above Brun's Theorem, we know the following for $x \geq 2$.

$$\pi_2(x) \ll \frac{x(\log \log x)^2}{(\log x)^2} \ll \frac{x}{(\log x)^{\frac{3}{2}}}$$

Thus, we also have that for some $n = \pi_2(p_n)$.

$$n = \pi_2(p_n) \ll \frac{p_n}{(\log p_n)^{\frac{3}{2}}} \leq \frac{p_n}{(\log n)^{\frac{3}{2}}}$$

If we rearrange the terms on both sides, we can get the following inequality.

$$n(\log n)^{\frac{3}{2}} \ll p_n \implies \frac{1}{p_n} \ll \frac{1}{n(\log n)^{\frac{3}{2}}}$$

Thus, we can prove that the series converges.

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \frac{1}{3} + \sum_{n=2}^{\infty} \frac{1}{p_n} \ll \frac{1}{3} + \sum_{n=2}^{\infty} \frac{1}{n(\log n)^{\frac{3}{2}}} < \infty$$