

18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
Revisiting the sieve of Eratosthenes

This unit begins the second part of the course, in which we will investigate a class of methods in analytic number theory known as *sieves*. (For non-native speakers of English: in ordinary life, a *sieve* is a device through which you pour a powder, like flour, to filter out large impurities.) Whereas the first part of the course leaned heavily on methods from complex analysis, here the emphasis will be more combinatorial.

1 The Sieve of Eratosthenes

The original sieve is of course the Sieve of Eratosthenes for finding prime numbers. To find the prime numbers in $\{2, \dots, n\}$, you repeat the following operation as long as there are unmarked numbers: find the first unmarked number p , mark it as prime, then mark $2p, 3p, \dots$ as composite until you get to a number greater than n .

Of course, one need only sift out multiples of primes up to $n^{1/2}$ in order to leave only primes behind. More generally, if one is only able to sift out multiples of primes up to n^α , what remain are numbers with no prime factors less than n^α . In particular, any such number has at most $\lfloor \alpha^{-1} \rfloor$ prime factors, and so is in some sense “nearly prime”.

Of course, in the process of sieving, many numbers will be sifted out more than once. If one wants to draw any sort of quantitative conclusion from this process, one must keep track of the multiple counting; this suggests using inclusion-exclusion.

2 The principle of inclusion-exclusion

Let S be a finite set, and let P_1, \dots, P_n be subsets of S . Think of each P_i as containing the elements of S with a certain property.

Suppose we have some way to count the number of elements in the intersection of any subcollection of the P_i , but what we really want is to count the complement of the union of all of the P_i . The formula that computes this is:

$$\#(S \setminus (P_1 \cup \dots \cup P_n)) = \sum_{T \subseteq \{1, \dots, n\}} (-1)^{\#T} \# \left(\bigcap_{t \in T} P_t \right).$$

Proof: if $s \in S$ belongs to m of the subsets, then the number of times it gets counted on the right side is

$$\binom{m}{0} - \binom{m}{1} + \dots$$

which equals 1 if $m = 0$ and vanishes otherwise.

More generally, if $f : S \rightarrow \mathbb{C}$ is some function, and we want to compute the sum of f over the complement of the P_i , we have

$$\sum_{s \in S \setminus (P_1 \cup \dots \cup P_n)} f(s) = \sum_{T \subseteq \{1, \dots, n\}} (-1)^{\#T} \left(\sum_{s \in \bigcap_{t \in T} P_t} f(s) \right).$$

In number theory, we are often taking $S = \{1, \dots, N\}$ and taking the sets P_1, P_2, \dots to be the sets of multiples of certain small primes. It is convenient to rewrite the principle of inclusion-exclusion in terms of the arithmetic function μ , the Möbius function:

$$\mu(n) = \begin{cases} (-1)^d & n = p_1 \cdots p_d \quad (p_1, \dots, p_d \text{ distinct, } d \geq 0) \\ 0 & \text{otherwise.} \end{cases}$$

3 Smooth numbers

Before proceeding, I need a quick lemma concerning smooth numbers. A natural number is z -smooth if its prime factors are all less than or equal to z .

Lemma 1 (Rankin). *Let $\Phi(x, z)$ be the number of z -smooth numbers less than or equal to x . Then for any $\delta > 0$,*

$$\Phi(x, z) \leq x^\delta \prod_{p \leq z} (1 - p^{-\delta})^{-1}.$$

Proof. If we expand the right side as a product of geometric series, we get a term $(x/n)^\delta \geq 1$ for each z -smooth number $n \leq x$ (among other terms). This yields the claim. \square

4 Back to Eratosthenes

Here is a modern version of the Sieve of Eratosthenes, following Murty and Saradha. Let A be a set of natural numbers, and let P be a set of primes; also set

$$P(z) = \prod_{p \in P, p \leq z} p.$$

For each $p \in P$, choose a set R_p consisting of some number $\omega(p)$ of residue classes modulo p , and let A_p be the subset of A whose elements belong to the chosen residue classes. Put

$$W(z) = \prod_{p|P(z)} \left(1 - \frac{\omega(p)}{p} \right),$$

For d squarefree with all prime factors in P , put $\omega(d) = \prod_{p|d} \omega(p)$ and $A_d = \bigcap_{p|d} A_p$.

We wish to estimate $S(A, P, z)$, the number of elements of A not belonging to A_p for any $p \leq z$. For this, we must assume some good properties about the chosen residue classes. For starters, we want that for some $\kappa > 0$,

$$\sum_{p \leq z, p \in P} \frac{\omega(p) \log p}{p} \leq \kappa \log z + O(1), \quad (1)$$

where the big-O bound is for $z \rightarrow \infty$ and the constant depends on P, R_p, κ .

Lemma 2. *Assuming (1), we have*

$$\sum_{d < t, d|P(z)} \omega(d) = O\left(t(\log z)^\kappa \exp\left(-\frac{\log t}{\log z}\right)\right),$$

where the big-O bound is for $z \rightarrow \infty$ and the constant depends on P, R_p, κ .

Proof. Exercise. □

Lemma 3. *Fix $C > 0$. Assuming (1), we have*

$$\sum_{d > Cx, d|P(z)} \frac{\omega(d)}{d} = O\left((\log z)^{\kappa+1} \exp\left(-\frac{\log x}{\log z}\right)\right),$$

where the big-O bound is for $z \rightarrow \infty$ and the constant depends on P, R_p, κ, C .

Proof. Put $F_\omega(t, z) = \sum_{d < t, d|P(z)} \omega(d)$. Then

$$\sum_{d > Cx, d|P(z)} \frac{\omega(d)}{d} \leq \int_{Cx}^{\infty} \frac{F_\omega(t, z)}{t^2} dt \quad (2)$$

(exercise), so the result follows from Lemma 2. □

Theorem 4. *Fix P, R_p, κ satisfying (1), and also fix $C, c > 0$. Then for any set A and any $X, x > 0$ such that*

$$\left| \#A_d - \frac{\omega(d)}{d} X \right| \leq c\omega(d)$$

and $\#A_d = 0$ for $d > Cx$, we have

$$S(A, P, z) = XW(z) + O\left(x \log^{\kappa+1} z \exp\left(-\frac{\log x}{\log z}\right)\right),$$

where the big-O bound is for $z \rightarrow \infty$, uniformly in A, x, X .

Proof. Exercise. □

5 Motivation: the twin prime conjecture

The *twin prime conjecture* states that there are infinitely many primes p such that $p + 2$ is also prime. One can even guess the correct asymptotic up to a constant factor, by a very simple argument: since the probability of a random number in $[1, \dots, N]$ being prime is asymptotically $1/\log N$, the number of twin primes in $[1, \dots, N]$ should be asymptotic to $N/\log^2 N$. (Getting the constant right is a bit trickier; I won't deal with that just now.)

As a corollary of Theorem 4, we obtain the following result of Brun (with a slightly simpler proof).

Theorem 5. *The number of primes $p \leq x$ such that $p+2$ is also prime is $O(x(\log \log x)^2/(\log x)^2)$.*

Proof. We will apply Theorem 4 with $A = \{1, \dots, x\}$ and $P = \{p : 2 < p \leq z\}$. For each $p \in P$, let R_p consist of the residue classes of $0, -2$, so that $\omega(p) = 2$. For d odd squarefree, $\omega(d) = 2^{\nu(d)}$ for $\nu(d)$ the number of prime factors of d . One checks easily (exercise) that

$$\left| \#A_d - x \frac{\omega(d)}{d} \right| \leq 2^{\nu(d)}. \quad (3)$$

Since

$$\sum_{p \leq z} \frac{\log p}{p} = O(\log z)$$

from a prior homework, we can take $\kappa = 2$ in Theorem 4. This yields

$$S(A, P, z) = xW(z) + O\left(x \log^3 z \exp\left(-\frac{\log x}{\log z}\right)\right),$$

where the big-O constant does not depend on x or z . We now take

$$\log z = \frac{\log x}{A \log \log x}$$

for a suitable constant A . Since

$$W(z) \leq \prod_{3 \leq p \leq z} \left(1 - \frac{1}{p}\right)^2 = O((\log z)^{-2})$$

by a prior homework exercise, we deduce that $S(A, P, z) = O(x(\log \log x)^2/(\log x)^2)$.

To conclude, note that $S(A, P, z)$ includes all primes $z + 2 \leq p \leq x$ such that $p + 2$ is also prime. The number of twin primes up to x that we missed is at most $z = x^{1/(A \log \log x)}$, so this doesn't affect the claim. \square

We will get a sharper result using Selberg's sieve in a subsequent lecture.

Exercises

1. Prove Lemma 2 using Rankin's trick.
2. Prove (2).
3. Prove Theorem 4.
4. Prove (3).
5. (Brun) Prove that the sum of the reciprocals of the twin primes converges.
6. Prove that

$$\Phi(x, z) = O\left(x \log z \exp\left(-\frac{\log x}{\log z}\right)\right)$$

where the big-O bound is for $z \rightarrow \infty$, uniformly in x . (Hint: apply Rankin's lemma with $\delta = 1 - (\log z)^{-1}$.)

7. Prove that the number of squarefree integers in $\{1, \dots, N\}$ is

$$\frac{6}{\pi^2}N + O(N^{1-\epsilon})$$

for some explicit value of ϵ . (Hint: this is much easier than sieving over primes! Just make sure to round round no more than $O(N^{1-\epsilon})$ fractions off to the nearest integer. Also, don't forget that $6/\pi^2 = 1/\zeta(2) = \prod_p(1 - 1/p^2)$.)