THE ARITHMETIC LARGE SIEVE WITH AN APPLICATION TO THE LEAST QUADRATIC NON-RESIDUE

1. The least quadratic non-residue

Given a large prime p how large can the least quadratic non-residue be? Let

$$n_p = \min\left\{1 \le m \le (p+1)/2 : \left(\frac{m}{p}\right) = -1\right\}.$$

Vinogradov conjectured that

$$n_p \ll p^{\varepsilon}.$$

From the Polya-Vinogradov inequality it follows that $n_p \ll p^{1/2+o(1)}$ and this estimate was subsequently improved by Vinogradov who showed $n_p \ll p^{\frac{1}{2\sqrt{e}}+o(1)}$. In the 1960's Burgess gave the estimate

$$n_p \ll p^{\frac{1}{4\sqrt{e}}+o(1)},$$

which up to the $p^o(1)$ factor is the best known result today. Conjecturally, Ankeny showed that GRH gives an even better estimate than Vinogradov conjectured, showing GRH implies

$$n_p \ll (\log p)^2.$$

We will prove a result of Linnik which shows that Vinogradov's conjecture holds for all but very few primes.

Theorem 1.1 (Linnik)**.** *Let $\varepsilon > 0$. Then the number of primes $p \le N$ such that $n_p > N^{\varepsilon}$ is $\ll_{\varepsilon} 1$ as $N \to \infty$.*

2. The arithmetic large sieve

We begin by describing a sieving problem. Suppose we are given the following

- $\mathcal{A}$ a set of integers with $\#\mathcal{A} = X$.
- $\mathcal{P}$ a subset of primes $\le z$
- for each $p \in \mathcal{P}$ a set $\Omega_p \subset \{h \pmod p\}$ of "excluded" residue classes with $\omega(p) := \#\Omega_p$

The problem is to estimate

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) = \#\{a \in \mathcal{A} : a \notin \Omega_p \text{ for each } p \in \mathcal{P}\}$$

For square-free $n = p_1 \cdots p_r$ define $\omega(n) = \omega(p_1) \cdots \omega(p_r)$.

Date: June 4, 2015.

Theorem 2.1 (The arithmetic large sieve). *In the above notation*

$$\mathcal{S}(\mathcal{A},\mathcal{P},\Omega) \leq \frac{X+z^2}{S(z)}$$

where

$$S(z) = \sum_{\substack{n\leq z\\ n-\text{square-free}}} \frac{\omega(n)}{n\prod_{p|n}(1-\frac{\omega(p)}{p})}$$

Remark. *If $\omega(p)$ is typically large, say, $> cp$ then the sieve bound is typically effective. That is, the sieve works well if one excludes a "large" number of residue classes* $\pmod p$. *This is the reason for the name "the large sieve".*

A trivial lower bound for $S(z)$, which we will use later, is

$$S(z) \geq \sum_{p\leq z} \frac{\omega(p)}{p}.$$

Definition. *An integer n is called Y-**smooth** if $p|n \Rightarrow p \leq Y$.*

Before proving Theorem 1.1 we first require the following auxilliary lemma for a lower bound on the number of N^{ε}-smooth numbers $\leq N$.

Lemma 2.2. *Let $\varepsilon > 0$. Then*

$$\sum_{\substack{n\leq N\\ p|n\Rightarrow p<N^{\varepsilon}}} 1 \gg_{\varepsilon} N.$$

Proof. We claim that the set of N^{ε}-smooth numbers $\leq N$ contains the set

$$B := \{m \leq N : m = np_1\cdots p_k \text{ where } N^{\varepsilon-\varepsilon^2} \leq p_j \leq N^{\varepsilon} \text{ for } j=1,\ldots,k\}$$

where $k = 1/\varepsilon$ (it suffices to prove the lemma for $\varepsilon^{-1} \in \mathbb{Z}$). To see this note that for $m \in B$, $m = np_1\cdots p_k$ with $N^{\varepsilon-\varepsilon^2} < p_j \leq N^{\varepsilon}$. We need to show that n is N^{ε}-smooth. This is clear since

$$n \leq \frac{N}{p_1\cdots p_k} \leq \frac{N}{N^{k(\varepsilon-\varepsilon^2)}} = N^{\varepsilon}.$$

Thus, to finish the proof we use Mertens' theorem to get

$$\begin{aligned}
\#B = & \sum_{\substack{np_1\cdots p_k \le N \\ N^{\varepsilon-\varepsilon^2} \le p_1,\ldots,p_k \le N^{\varepsilon}}} 1 \\
= & \sum_{N^{\varepsilon-\varepsilon^2} \le p_1,\ldots,p_k \le N^{\varepsilon}} \left\lfloor \frac{N}{p_1\cdots p_k} \right\rfloor \\
\gg & N \sum_{N^{\varepsilon-\varepsilon^2} \le p_1,\ldots,p_k \le N^{\varepsilon}} \frac{1}{p_1\cdots p_k} \\
= & N \left(\sum_{N^{\varepsilon-\varepsilon^2} \le p \le N^{\varepsilon}} \frac{1}{p} \right)^k \\
= & N \left(\log \frac{\log(N^{\varepsilon})}{\log(N^{\varepsilon-\varepsilon^2})} + O(1/(\varepsilon \log N)) \right)^k \gg_{\varepsilon} N.
\end{aligned}$$

□

Proof of Theorem 1.1. Let

$$\mathcal{A} = \{1, \ldots, N\}, \qquad \mathcal{P} = \left\{ p \le N^{1/2} : \left(\frac{n}{p}\right) = 1 \text{ for all } n \le N^{\varepsilon} \right\}$$

and

$$\Omega_p = \left\{ h \pmod p : \left(\frac{h}{p}\right) = -1 \right\},$$

so $\omega(p) = \#\Omega_p = (p-1)/2$, $p > 2$. The large sieve gives that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) \le \frac{2N}{S(z)}$$

where

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) = \#\{n \le N : n \notin \Omega_p \text{ for all } p \in \mathcal{P}\}$$

and

$$S(z) \ge \sum_{p \le z} \frac{\omega(p)}{p} = \frac{1}{2} \sum_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right).$$

We now proceed in a slightly unusual way. We will derive a **lower bound** for $\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega)$ and then use this and the sieve estimate above to get an **upper bound** for

$$\sum_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right).$$

This will imply that the cardinality of the set $\mathcal{P}$ is small, which means there are very few primes $\le N$ for which $n_p > N^{\varepsilon}$.

To obtain a lower bound on $\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega)$ we claim that the set

$$\{n \le N : n \notin \Omega_p \text{ for all } p \in \mathcal{P}\}$$

contains the set of $n \le N$ such that n is N^{ε}-smooth. To see this note that if n is N^{ε}-smooth and $n = p_1 \cdots p_r$ (not necessarily distinct) it follows by the definition of $\mathcal{P}$ that for $p \in \mathcal{P}$

$$\left(\frac{n}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right) \neq -1,$$

i.e. $n \notin \Omega_p$ for all $p \in \mathcal{P}$. Thus, by Lemma 2.2

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) \gg_{\varepsilon} N$$

so that

$$\#\{p \le N^{1/2} : n_p > N^{\varepsilon}\} = \sum_{p \in \mathcal{P}} 1 \ll \frac{N}{S(z)} \ll_{\varepsilon} 1.$$

□

3. Proof of the arithmetic large sieve

The arithmetic large sieve is a consequence of the analytic large sieve which we will discuss in the following lecture. Let

$$L(\alpha) = \sum_{n \in \mathcal{S}} e(\alpha n)$$

where $e(x) = e^{2\pi i x}$ and $\mathcal{S} \subset [M+1, M+N]$. (For us $\#\mathcal{S} = L(0) = \mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega)$ so $\mathcal{S}$ is the remaining set after the sifting has been carried out.)

Let a_n be complex numbers and let

$$\mathcal{L}(\alpha) = \sum_{M < n \le M+N} a_n e(\alpha n).$$

Theorem 3.1 (The analytic large sieve)**.** *In the above notation*

$$\sum_{q \le Q} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\ q)} \left| \mathcal{L}\left(\frac{a}{q}\right)\right|^2 \le \left(Q^2 + N - 1\right) \sum_{M < n \le N+M} |a_n|^2$$

We now require a few additional lemmas.

Lemma 3.2. *For complex numbers a_n supported on $\mathcal{S}$ we have*

$$\sum_{h \,(\mathrm{mod}\ p)} \left| \sum_{\substack{n \in \mathcal{S} \\ n \equiv h \,(\mathrm{mod}\ p)}} a_n \right|^2 = \frac{1}{p} \sum_{a \,(\mathrm{mod}\ p)} \left| \mathcal{L}\left(\frac{a}{p}\right)\right|^2.$$

Proof. Let

$$Z(p, h) = \sum_{\substack{n \in \mathcal{S} \\ n \equiv h \,(\mathrm{mod}\ p)}} a_n.$$

Observe that

$$\mathcal{L}\left(\frac{a}{p}\right) = \sum_{n \in \mathcal{S}} a_n e(an/p) = \sum_{h \,(\mathrm{mod}\ p)} e(ah/p) Z(p, h).$$

Thus,

$$\begin{aligned}\sum_{a \,(\mathrm{mod}\ p)} \left|\mathcal{L}\left(\frac{a}{p}\right)\right|^2 &= \sum_{a \,(\mathrm{mod}\ p)} \left|\sum_{h \,(\mathrm{mod}\ p)} e(ah/p) Z(p,h)\right|^2 \\ &= \sum_{h \,(\mathrm{mod}\ p)} \sum_{k \,(\mathrm{mod}\ p)} Z(p,h)\overline{Z(p,k)} \sum_{a \,(\mathrm{mod}\ p)} e\left(\frac{a(h-k)}{p}\right).\end{aligned}$$

One has that

$$\sum_{a \,(\mathrm{mod}\ p)} e\left(\frac{a(h-k)}{p}\right) = \begin{cases} p \text{ if } h \equiv k \,(\mathrm{mod}\ p) \\ 0 \text{ otherwise.}\end{cases}$$

So that

$$\sum_{a \,(\mathrm{mod}\ p)} \left|\mathcal{L}\left(\frac{a}{p}\right)\right|^2 = p \sum_{h \,(\mathrm{mod}\ p)} |Z(p,h)|^2$$

as claimed.

□

Lemma 3.3. *For complex numbers a_n supported on $\mathcal{S}$ we have*

$$|\mathcal{L}(0)|^2 \frac{\omega(p)}{p-\omega(p)} \leq \sum_{h \,(\mathrm{mod}\ p)}^{*} |\mathcal{L}(a/p)|^2.$$

Proof. Let

$$Z(p,h) = \sum_{\substack{n \in \mathcal{S} \\ n \equiv h \,(\mathrm{mod}\ p)}} a_n.$$

Applying Cauchy-Schwarz and Lemma 3.2 gives

$$\begin{aligned}|\mathcal{L}(0)|^2 &= \left|\sum_{h \,(\mathrm{mod}\ p)} Z(p,h)\right|^2 \\ &\leq \left(\sum_{\substack{h \,(\mathrm{mod}\ p) \\ Z(p,h)\neq 0}} 1\right)\left(\sum_{h \,(\mathrm{mod}\ p)} |Z(p,h)|^2\right) \\ &= \left(\sum_{\substack{h \,(\mathrm{mod}\ p) \\ Z(p,h)\neq 0}} 1\right) \frac{1}{p} \sum_{a \,(\mathrm{mod}\ p)} \left|\mathcal{L}\left(\frac{a}{p}\right)\right|^2.\end{aligned}$$

Note that $Z(p,h) = 0$ if $h \in \Omega_p$ so that

$$\sum_{\substack{h \,(\mathrm{mod}\ p) \\ Z(p,h)\neq 0}} 1 \leq p - \omega(p).$$

Also note

$$\sum_{a \,(\mathrm{mod}\, p)} \left|\mathcal{L}\left(\frac{a}{p}\right)\right|^2 = \sum_{a \,(\mathrm{mod}\, p)}{}^{*} \left|\mathcal{L}\left(\frac{a}{p}\right)\right|^2 + |\mathcal{L}(0)|^2.$$

Combining estimates gives

$$|\mathcal{L}(0)|^2 \frac{\omega(p)}{p-\omega(p)} \leq \sum_{a \,(\mathrm{mod}\, p)}{}^{*} \left|\mathcal{L}\left(\frac{a}{p}\right)\right|^2.$$

□

Proof of Theorem 2.1. Let $\mathcal{A} \subset [M+1, N+M]$ and

$$\mathcal{S} = \{n \in \mathcal{A} : n \notin \Omega_p \text{ for all } p \in \mathcal{P}\},$$

also let

$$L(\alpha) = \sum_{n \in \mathcal{S}} e(\alpha n),$$

so that

$$L(0) = \mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega).$$

By Lemma 3.3

$$L(0)^2 \frac{\omega(p)}{p-\omega(p)} \leq \sum_{a \,(\mathrm{mod}\, p)}{}^{*} \left|L\left(\frac{a}{p}\right)\right|^2.$$

Our goal is to establish a similar bound for square-free q. First consider the case $q = p_1 p_2$ and observe

$$\sum_{a \,(\mathrm{mod}\, q)}{}^{*} \left|L\left(\frac{a}{q}\right)\right|^2 = \sum_{a_1 \,(\mathrm{mod}\, p_1)}{}^{*} \sum_{a_2 \,(\mathrm{mod}\, p_2)}{}^{*} \left|L\left(\frac{a_1}{p_1} + \frac{a_2}{p_2}\right)\right|^2.$$

To see this write $a = a_1 p_2 \overline{p_2} + a_2 p_1 \overline{p_1}$, where $\overline{p_1}$ and $\overline{p_2}$ denote the multiplicative inverses of p_1 modulo p_2 and p_2 modulo p_1 (resp.). By construction $a \equiv a_1 \pmod{p_1}$ and $a \equiv a_2 \pmod{p_2}$. The CRT implies that a runs over all residue classes $\pmod{p_1 p_2}$ as a_1, and a_2 run over the residue classes $\pmod{p_2}$ and $\pmod{p_2}$ (resp.). At this point it is not hard to deduce the above identity.

Now take $a_n = e(na_1/q_1)$ for $n \in S$ and $a_n = 0$ otherwise so that by Lemma 3.3

$$\begin{aligned}\sum_{a_2 \,(\mathrm{mod}\, p_2)}{}^{*} \left|L\left(\frac{a_1}{p_1} + \frac{a_2}{p_2}\right)\right|^2 &= \sum_{a_2 \,(\mathrm{mod}\, p_2)}{}^{*} \left|\sum_{M<n\leq N+M} a_n e(na_2/q_2)\right|^2 \\ &\geq \frac{\omega(p_2)}{p_2-\omega(p_2)} \left|L(a_1/q_1)\right|^2.\end{aligned}$$

Also by Lemma 3.3

$$\sum_{a_1 \,(\mathrm{mod}\, p_1)}{}^{*} |L(a_1/q_1)|^2 \geq \frac{\omega(p_1)}{p_1-\omega(p_1)} |L(0)|^2$$

Thus, for $q = p_1 p_2$ we have

$$\sideset{}{^*}\sum_{a \,(\mathrm{mod}\ q)} \left| L\left(\frac{a}{q}\right)\right|^2 \geq \frac{\omega(q)}{q \prod_{p|q}\left(1 - \frac{\omega(p)}{p}\right)} |L(0)|^2.$$

By induction on the number of prime factors of q this holds for all square free q as well.

Summing over all square-free $q \leq z$ and applying the analytic large sieve, Theorem 3.1 we get that

$$\begin{aligned} |L(0)|^2 \sum_{\substack{q \leq z \\ q-\text{square-free}}} \frac{\omega(q)}{q \prod_{p|q}\left(1 - \frac{\omega(p)}{p}\right)} &\leq \sum_{q \leq z} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\ q)} \left| L\left(\frac{a}{q}\right)\right|^2 \\ &\leq |L(0)|(N + z^2). \end{aligned}$$

So that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, \Omega) = L(0) \leq \frac{N + z^2}{S(z)}.$$

□