APPLICATIONS OF THE SELBERG SIEVE

GYUJIN OH

Contents

1. Selberg sieve: statement

We recall the statement of the Selberg sieve, slightly generalized to allow more general types of sieving primes. It can be derived by just using the exact same strategy we used before.

Theorem 1.1 (Selberg sieve)**.** *Let I be a set of N positive integers, and P be a finite product of distinct primes (In the previous lecture, we took $P=\prod_{p\leq z} p$). Assume the existence of a multiplicative function f such that, for $d|P$,*

$$|\{n\in I : d|n\}| = \frac{N}{f(d)} + R_d.$$

Let

$$f_1(a) = \sum_{d|a} \mu(d) f\left(\frac{a}{d}\right),$$

and, for $d|P$,

$$\lambda_d = \frac{1}{V^1_{z,P}} \frac{\mu(d)f(d)}{f_1(d)} \sum_{\substack{a\leq \frac{z}{d}\\ (a,d)=1\\ a|P}} \frac{\mu(a)^2}{f_1(a)}, \qquad V^1_{z,P} = \sum_{\substack{a\leq z\\ a|P}} \frac{\mu(a)^2}{f_1(a)}.$$

Then,

$$S(I,P) := |\{n\in I : (n,P)=1\}| \leq \frac{N}{V^1_{z,P}} + \sum_{d_1,d_2|P} \left|\lambda_{d_1}\lambda_{d_2} R_{[d_1,d_2]}\right|.$$

Remark 1.1. In our definition, it is implicit that $\lambda_d = 0$ for $d>z$ or $d\not| P$ (in particular when d is not squarefree). Also, in the definitions of λ_d and $V^1_{z,P}$, $\mu(a)^2=1$ is unnecessary; it is there to make it look similar to the previously stated Selberg sieve.

2. Brun–Titchmarsh

The first application we saw was the number of primes in an interval. We can ask a little bit more, that is we can ask the number of primes in an interval of arithmetic progression. The setup for the sieve would be as follows.

- Choose $(a, m) = 1$.
- $I = \{x < n \leq x + y : n \equiv a (\operatorname{mod} m)\}$, so that $N = \lfloor \frac{x+y-a}{m} \rfloor - \lfloor \frac{x-a}{m} \rfloor = \frac{y}{m} + O(1)$.
- We choose $z = \sqrt{\frac{y}{m}}$ and
$$P = \prod_{\substack{p \leq \sqrt{\frac{y}{m}} \\ (p,m)=1}} p.$$

Then,

$$S(I, P) = \left| \left\{ x < n \leq x + y : n \equiv a (\operatorname{mod} m),\ \text{any prime factor of } n \text{ is} > \sqrt{\frac{y}{m}} \right\} \right|.$$

Bounding this number from above will bound $\pi(x + y; m, a) - \pi(x; m, a)$ from above. Indeed, if $p \equiv a (\operatorname{mod} m)$ is a prime satisfying $x < p \leq x + y$, then either $p | P$ or $(p, P) = 1$, so

$$\pi(x + y; m, a) - \pi(x; m, a) \leq \omega(P) + S(I, P),$$

where $\omega(P)$ is the number of prime factors of P.

Now we use $z = \sqrt{\frac{y}{m}}$ and run the Selberg sieve machinery. We have a similar situation as the previous example of primes in an interval, namely $f(d) = d$ and $f_1(a) = \phi(a)$. Also, $|R_d| \leq 1$, and the same bound $\sum_{d \leq z} |\lambda_d| \ll \frac{z}{V^1_{z,P}}$ holds. Thus so far we have

$$\pi(x + y; m, a) - \pi(x; m, a) \leq \pi\left(\sqrt{\frac{y}{m}}\right) + \frac{\frac{y}{m} + O(1)}{V^1_{z,P}} + O\left(\frac{\frac{y}{m}}{(V^1_{z,P})^2}\right).$$

We are left with finding a lower bound for $V^1_{z,P}$. The similar analysis applies, and we see that

$$V^1_{z,P} = \sum_{\substack{a \leq \sqrt{\frac{y}{m}} \\ a | P}} \frac{1}{\phi(a)} = \sum_{\substack{s(n) \leq \sqrt{\frac{y}{m}} \\ s(n) | P}} \frac{1}{n} \geq \sum_{\substack{n \leq \sqrt{\frac{y}{m}} \\ (n,m)=1}} \frac{1}{n} \geq \frac{\varphi(m) \log(y/m)}{2m}.$$

Thus,

$$\pi(x + y; m, a) - \pi(x; m, a) \leq O\left(\frac{\sqrt{\frac{y}{m}}}{\log\left(\frac{y}{m}\right)}\right) + \frac{2y + O(m)}{\varphi(m) \log\left(\frac{y}{m}\right)} + O\left(\frac{my}{\varphi(m)^2 \left(\log\left(\frac{y}{m}\right)\right)^2}\right).$$

We let the formula to be expressed this way as we may want m to be dependent on y. The RHS can be simplified whenever m is given an upper bound "not too close to y." To see what can go wrong, if we take, say, $m = \frac{y}{10}$, then one founds that the RHS really contains little information; the main term is subsumed in the error term as $2y + O(m) = O(m)$. If, on the other hand, one chooses small $\varepsilon > 0$ and asserts a bound $m < y^{1-\varepsilon}$, then the upper bound simplifies as follows:

Theorem 2.1 (Brun–Titchmarsh). *Choose $0 < \varepsilon < 1$. If $m < y^{1-\varepsilon}$, then*

$$\pi(x + y; m, a) - \pi(x; m, a) \leq \frac{2y}{\varphi(m) \log\left(\frac{y}{m}\right)} + O_\varepsilon\left(\frac{y}{\left(\log\left(\frac{y}{m}\right)\right)^2}\right).$$

Taking $x = 0$, one gets the Brun–Titchmarsh as stated in the Hint for Problem 4 of HW4:

Corollary 2.1. *If $m < y^{1-\varepsilon}$, then*

$$\pi(y; m, a) \ll_\varepsilon \frac{y}{\phi(m) \log y}.$$

This is the right order of magnitude.

3. $p + 2 = q$ (Twin primes)

Now we want the upper bound for the pairs of **twin primes** in an interval. The setup for the sieve is as follows.

- $I = \{n(n + 2) : x < n \le x + y\}$.
- $z \le \sqrt{y}$ to be determined later.
- $P = \prod_{p \le \sqrt{y}} p$.

Then,

$$S(I, P) = |\{x < n \le x + y : (n, P) = (n + 2, P) = 1\}|.$$

Let $u(x, y) = |\{x < n \le x + y : (n, n + 2) \text{ twin prime}\}|$. Then

$$u(x, y) \le \omega(P) + S(I, P) = O\left(\frac{\sqrt{y}}{\log y}\right) + S(I, P).$$

For an odd $p \le \sqrt{y}$,

$$|\{n \in I : p|n\}| = |\{x < n \le x + y : p|n \text{ or } p|n + 2\}| = \frac{y}{p/2} + R_p,$$

where $|R_p| \le 2$. So, f is a multiplicative function where $f(p) = p/2$ for $p \le \sqrt{y}$ odd and $f(2) = 2$. Thus, the Selberg sieve upper bound works.

We would like to first find a bound for $V^1_{z,P}$. First of all, $f_1(p) = \frac{p}{2} - 1$ (and $f_1(2) = 1$), and

$$V^1_{z,P} = \sum_{a<z} \frac{\mu(a)^2}{f_1(a)}.$$

This sum is a bit weird, so we want to compare this with a nicer sum. Note that for $p > 2$,

$$\frac{\mu(p)^2}{f_1(p)} = \frac{2}{p - 2},$$

and there is a multiplicative function that takes value $2/p$ at p; namely, $d(n)/n$ (recall $d(n)$ is the number of divisors of n). Thus we would like to express $\frac{\mu(a)^2}{f_1(a)}$ as a convolution of $\frac{d(n)}{n}$ with some fairly tame function $c(k)$. Namely, we would like to find $c(k)$ such that

$$\frac{\mu(a)^2}{f_1(a)} = \sum_{n|a} c\left(\frac{a}{n}\right) \frac{d(n)}{n}.$$

Such function in fact does exist. We defer its calculation at the moment and proceed. Then we have

$$V^1_{z,P} = \sum_{a<z} \frac{\mu(a)^2}{f_1(a)} = \sum_{a<z} \sum_{n|a} c\left(\frac{a}{n}\right) \frac{d(n)}{n} = \sum_{k<z} c(k) \sum_{n \le \frac{z}{k}} \frac{d(n)}{n}.$$

It is an elementary exercise to show that

$$\sum_{n \le N} \frac{d(n)}{n} = \frac{1}{2}(\log N)^2 + O(\log N),$$

so

$$\begin{aligned} V^1_{z,P} &= \sum_{k<z} c(k) \left(\frac{1}{2} \left(\log \left(\frac{z}{k} \right) \right)^2 + O \left(\log \left(\frac{z}{k} \right) \right) \right) \\ &= \frac{1}{2}(\log z)^2 \sum_{k \le z} c(k) + O \left((\log z) \sum_k |c(k)| \log k \right) + O \left(\sum_k |c(k)| (\log k)^2 \right). \end{aligned}$$

Now we calculate $c(k)$. By taking the Dirichlet series generating series, we see that

$$\sum_n \frac{\mu(n)}{f_1(n)} n^{-s} = \left(\sum_n c(n) n^{-s} \right) \cdot \left(\sum_n \frac{d(n)}{n} n^{-s} \right).$$

In terms of Euler products, we have

$$(1 + 2^{-s}) \prod_{p>2} \left(1 + \frac{2}{(p-2)p^s} \right) = \left(\sum_n c(n) n^{-s} \right) \prod_p \left(1 - \frac{1}{p^{s+1}} \right)^{-2},$$

so

$$\sum_n c(n) n^{-s} = (1 + 2^{-s}) \prod_{p>2} \left(1 + \frac{2}{(p-2)p^s} \right) \prod_p \left(1 - \frac{1}{p^{s+1}} \right)^2.$$

This Euler product absolutely converges for $\operatorname{Re} s > -\frac{1}{2}$, so $\sum_k |c(k)| \log k$ and $\sum_k |c(k)| (\log k)^2$ are convegent. So,

$$V^1_{z,P} = \frac{1}{2} c (\log z)^2 + O(\log z),$$

where $c = \sum_n c(n) = \frac{1}{2} \prod_{p>2} \left(1 + \frac{2}{p-2} \right) \left(1 - \frac{1}{p} \right)^2$.

Now we bound the error term. In general, for $d|P$, $|R_d| \le \frac{d}{f(d)}$ (namely $|R_{p_1 \cdots p_k}| \le 2^k$ for distinct odd primes $p_1, \cdots, p_k \le z$). So the error term is $\ll \left(\sum_{d \le z} \frac{d}{f(d)} |\lambda_d| \right)^2$. Now we have

$$\sum_{d \le z} \frac{d}{f(d)} |\lambda_d| = \sum_{d \le z} \frac{d \mu(d)^2}{f_1(d) V^1_{z,P}} \sum_{\substack{a \le \frac{z}{d} \\ (a,d)=1}} \frac{\mu(a)^2}{f_1(a)} = \frac{1}{V^1_{z,P}} \sum_{m \le z} \frac{\sigma(m) \mu(m)^2}{f_1(m)},$$

by multiplicativity. Now a sum of multiplicative function has a nice estimate:

Theorem 3.1 (Vaughan–Montgomery, Theorem 2.14)**.** *Let g be a nonnegative multiplicative function such that there is a constant A such that for all x,*

$$\sum_{p \le x} g(p) \log p \le Ax,$$

$$\sum_{\substack{p^k \\ k \ge 2}} \frac{g(p^k) k \log p}{p^k} \le A.$$

Then,

$$\sum_{n\le x} g(n) \ll \frac{x}{\log x}\prod_{p\le x}\left(1+\frac{f(p)}{p}+\frac{f(p^2)}{p^2}+\cdots\right).$$

Apply this for $g(m) = \frac{\sigma(m)\mu(m)^2}{f_1(m)}$ (the existence of A follows easily from the Prime Number Theorem), and we get

$$\sum_{m\le z}\frac{\sigma(m)\mu(m)^2}{f_1(m)} \ll \frac{z}{\log z}\prod_{p\le z}\left(1+\frac{2(p+1)}{p(p-2)}\right) = \frac{z}{\log z}\prod_{p\le z}\frac{p^2+2}{p(p-2)} \ll \frac{z}{\log z}\prod_{p\le z}\frac{p}{p-2} \ll z\log z,$$

where at the last part we used Mertens' third theorem. Therefore, the error is bounded by $O\left(\frac{z^2}{(\log z)^2}\right)$. Thus, we have

$$\begin{aligned} u(x,y) &\le O\left(\frac{\sqrt{y}}{\log y}\right) + \frac{y}{\frac{1}{2}c(\log z)^2 + O(\log z)} + O\left(\frac{z^2}{(\log z)^2}\right) \\ &= \frac{2y}{c(\log z)^2} + O\left(\frac{\sqrt{y}}{\log y} + \frac{y}{(\log z)^3} + \frac{z^2}{(\log z)^2}\right). \end{aligned}$$

We now take $z = \sqrt{\frac{y}{\log y}}$. Then $\log z = \frac{1}{2}\log y + O(\log\log y)$, so

$$\begin{aligned} u(x,y) &= \frac{2y}{c(\frac{1}{4}(\log y)^2 + O(\log y\log\log y))} + O\left(\frac{\sqrt{y}}{\log y} + \frac{y}{(\log y)^3} + \frac{y}{(\log y)^3}\right) \\ &= \frac{8y}{c(\log y)^2} + O\left(\frac{y\log\log y}{(\log y)^3}\right) + O\left(\frac{y}{(\log y)^3}\right) = \frac{8y}{c(\log y)^2} + O\left(\frac{y\log\log y}{(\log y)^3}\right). \end{aligned}$$

We record this as the following

Theorem 3.2. *The number of twin primes $x < p \le x + y$ is bounded above by*

$$\frac{8y}{c(\log y)^2} + O\left(\frac{y\log\log y}{(\log y)^3}\right), \qquad c = \frac{1}{2}\prod_{p>2}\frac{(p-1)^2}{p(p-2)}.$$

Corollary 3.1 (Brun)**.** *The sum of reciprocals of twin primes is convergent.*

Proof. The number of twin primes $2^k < p \le 2^{k+1}$ is bounded above by $\ll \frac{2^k}{k^2}$. So,

$$\sum_{\substack{p \text{ twin prime} \\ 2^k < p \le 2^{k+1}}} \frac{1}{p} \ll \frac{2^k}{k^2}\cdot\frac{1}{2^{k+1}} \ll \frac{1}{k^2}.$$

Adding up, we get a convergent sum. □

Remark 3.1. For any $a, b \in \mathbb{Z}$, almost the same strategy gives a similar upper bound for the number of primes p in an interval where $ap + b$ is a prime. Note that a can be negative, so this can give an upper bound for the number of expressions $2n = p + q$. One can also do a similar game for k-tuple of linear equations.

4. n^2+1

More generally, for any $f(X)$ a polynomial with integer coefficients, one can take $I = \{f(n) : x < n \leq x+y\}$. For appropriately chosen P, $S(I,P)$ would be close to

$$\#\{x < n \leq x+y : f(n) \text{ is the least factorizable}\}.$$

More precisely, if $f(X) = f_1(X)\cdots f_k(X)$ for irreducible polynomials $f_1(X), \cdots, f_k(X)$, then $f(n)$ being the least factorizable means the condition of $f_1(n), f_2(n), \cdots, f_k(n)$ all being prime. One can run the Selberg sieve, and one can calculate the major term of the upper bound as long as one knows well about the problems $f(X) \equiv 0 (\operatorname{mod} p)$ for each prime p.

For example, let's take the simplest non-linear irreducible polynomial, $f(X) = X^2+1$. The Selberg sieve works more or less in the same fashion, except that every prime we consider needs to be $\equiv 1(\operatorname{mod} 4)$. As a result, the estimates we use in the process get changed; for example,

$$\prod_{\substack{p\leq N\\ p\equiv 1(\operatorname{mod} 4)}} \frac{p}{p-k} = \Theta\left((\log N)^{k/2}\right) \qquad \text{(“Mertens’ theorem for arithmetic progressions”)},$$

$$\sum_{\substack{n\leq N\\ \text{prime factors of } n \text{ are all } \equiv 1(\operatorname{mod} 4)}} \frac{d(n)}{n} = \Theta(\log N),$$

etc. In turn, one induces the

Proposition 4.1. *The number of primes of form n^2+1, $x < n \leq x+y$ is bounded above by $\frac{Cy}{\log y}(1+o(1))$ for an explicit constant C.*

Proof. We take

- $I = \{n^2+1 : x < n \leq x+y\}$,
- $z = \sqrt{y}$,
- $P = \prod_{p\leq\sqrt{y}, p\equiv 1(\operatorname{mod} 4)} p$.

Then,

$$\#\{x < n \leq x+y :\ n^2+1 \text{ is a prime}\} \leq \omega(P) + S(I,P) = O\left(\frac{\sqrt{y}}{\log y}\right) + S(I,P).$$

We have $f(p) = \frac{p}{2}$ and $f_1(p) = \frac{p}{2} - 1$ for $p \leq \sqrt{y}$, $p \equiv 1(\operatorname{mod} 4)$.

We estimate $V^1_{z,P}$. In this case

$$V^1_{z,P} = \sum_{k<\sqrt{y}} c(k) \sum_{\substack{n\leq\frac{\sqrt{y}}{k}\\ \text{any prime factor of } n \text{ is } \equiv 1(\operatorname{mod} 4)}} \frac{d(n)}{n},$$

where

$$\sum_n c(n)n^{-s} = \prod_{p\equiv 1(\operatorname{mod} 4)} \left(1 + \frac{2}{(p-2)p^s}\right)\left(1 - \frac{1}{p^{s+1}}\right)^2.$$

Note that $\sum_{\substack{n\leq N\\ n\equiv 1(\operatorname{mod} 4)}} \frac{d(n)}{n}$ can be estimated via Wiener–Ikehara (see Appendix); the Dirichlet series for $\{d(n)\}_{\text{prime factors} \equiv 1(\operatorname{mod} 4)}$ is $\prod_{p\equiv 1(\operatorname{mod} 4)}(1-p^{-s})^{-2}$, and this should have a pole at $s=1$

of order 1 (see Appendix). So $\sum_{n\leq N,\text{prime factors}\,\equiv\,1(\text{mod}\,4)} d(n) \sim AN$ where $A > 0$ is the residue of the Dirichlet series at $s = 1$. By partial sum,

$$\sum_{n\leq N,\text{prime factors}\,\equiv 1(\text{mod}\,4)} \frac{d(n)}{n} \sim A\left(\sum_{n\leq N}\frac{1}{n+1}\right) \sim A\log N.$$

So,

$$V^1_{z,P} \sim Ac'\log z = \frac{Ac'}{2}\log y,$$

where $c' = \prod_{p\equiv 1(\text{mod}\,4)} \frac{(p-1)^2}{p(p-2)}$. For the error term, by the same argument,

$$\text{Error term of Selberg sieve} \ll \left(\frac{z}{\log z}\prod_{p\leq z, p\equiv 1(\text{mod}\,4)}\frac{p}{p-2}\right)^2 \ll z^2 = y,$$

by Mertens' for arithmetic progressions (see Appendix). Thus

$$\#\{x < n \leq x+y : n^2+1 \text{ prime}\} \leq \frac{2y}{Ac'\log y + o(\log y)} + O\left(\frac{\sqrt{y}}{\log y} + \frac{y}{(\log y)^2}\right) = \frac{2y}{Ac'\log y}(1+o(1)).$$

□

5. Appendix: Useful tools for estimating $\sum_{n\leq N} f(n)$

Theorem 5.1 (Mertens' first theorem). *For any $n \geq 2$,*

$$\left|\sum_{p\leq n}\frac{\log p}{p} - \log n\right| \leq 2.$$

Theorem 5.2 (Mertens' second theorem). *For any $n \geq 2$,*

$$\left|\sum_{p\leq n}\frac{1}{p} - \log\log n - M\right| \leq \frac{4}{\log(n+1)} + \frac{2}{n\log n},$$

where M is some absolute constant.

Theorem 5.3 (Mertens' third theorem).

$$\lim_{n\to\infty}\log n\prod_{p\leq n}\left(1-\frac{1}{p}\right) = e^{-\gamma},$$

where γ is the Euler constant.

Theorem 5.4 (Mertens' third theorem for arithmetic progressions; Williams). *For $(a, m) = 1$,*

$$\prod_{\substack{p\leq x\\ p\equiv a(\text{mod}\,m)}}\left(1-\frac{1}{p}\right) = \Omega\left((\log x)^{-\frac{1}{\phi(m)}}\right).$$

More precisely,

$$\prod_{\substack{p\leq x\\ p\equiv a(\text{mod}\,m)}}\left(1-\frac{1}{p}\right) = A(\log x)^{-\frac{1}{\phi(m)}} + O\left((\log x)^{-\frac{1}{\phi(m)}-1}\right),$$

where

$$A=\left(e^{-\gamma}\frac{m}{\phi(m)}\prod_{\chi\neq\chi_0 \textit{ modulus } m}\prod_{p}\left(1-\frac{1}{p}\right)^{\chi(pa^{-1})}\right)^{\frac{1}{\phi(m)}}.$$

Theorem 5.5 (Wiener–Ikehara tauberian theorem; Wiener–Ikehara, Delange, Kable)**.** *Let* $\{a_n\}$ *be a sequence of nonnegative real numbers. Suppose that*

$$L(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s},$$

is absolutely convergent for $\operatorname{Re} s > d$*, and has a pole of order* $u\in\mathbb{Q}_{>0}$ *at* $s=d$ *with* $L(s)\sim A(s-d)^{-u}$ *for* $A>0$ *around* $s=d$*. Then,*

$$\sum_{n\leq N}a_n\sim\frac{A}{d\Gamma(u)}N^d(\log N)^{u-1}.$$

For example, having a pole of order $\frac{3}{2}$ means that $L(s)^2$ has a pole of order 3 at $s=d$ with $A^2=\lim_{s\to d}L(s)^2(s-d)^3$.

Theorem 5.6 (Takloo-Bighash)**.** *Let* $K/\mathbb{Q}$ *be Galois, and* $C\subset\operatorname{Gal}(K/\mathbb{Q})$ *be a conjugacy class. Then*

$$L_C(s)=\prod_{p \textit{ unramified in } K,\, \operatorname{Frob}_p\in C}(1-p^{-s})^{-1},$$

is absolutely convergent for $\operatorname{Re}(s)>1$ *and has a pole of order* $\frac{|C|}{|\operatorname{Gal}(K/\mathbb{Q})|}$ *at* $s=1$*.*

It's fine if you don't know algebraic number theory; for example, this implies that the partial Euler product $\prod_{p\equiv 1 \pmod 4}(1-p^{-s})^{-1}$ has a pole of order $1/2$ at $s=1$ (the case of $K=\mathbb{Q}(i)$ and C being the identity).

Theorem 5.7 (Vaughan–Montgomery, Theorem 2.14)**.** *Let* g *be a nonnegative multiplicative function such that there is a constant* A *such that for all* x*,*

$$\sum_{p\leq x}g(p)\log p\leq Ax,$$

$$\sum_{\substack{p^k\\k\geq 2}}\frac{g(p^k)k\log p}{p^k}\leq A.$$

Then,

$$\sum_{n\leq x}g(n)\ll\frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{f(p)}{p}+\frac{f(p^2)}{p^2}+\cdots\right).$$