# Some steps in sieve theory

O. Ramaré

—

IMSc, Chennai

—

February 20, 2010

**Abstract**

File `LecturesEasyChennai.tex`.

## 1 First lecture: initiation to Brun pure sieve

Pure Brun sieve. It was very intricate before the invention of using Rankin's trick. Multiplicativity.

(Brun, 1919a), (Brun, 1919b), (Rankin, 1938), (Murty & Saradha, 1987). The Moebius function is defined by

$$\mu(d) = \begin{cases} (-1)^t & \text{when } d \text{ is a product of } t \text{ distinct prime factors,} \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

We have $\mu(1) = 1$. This function is very combinatorial in nature*. It appears in the inclusion-exclusion principle: we have, for any subset of integers $\mathcal{A}$,

$$\#\{a \in \mathcal{A} / \ \gcd(a, r) = 1\} = \sum_{d|r} \mu(d) \#\{a \in \mathcal{A} / \ d|a\}. \tag{2}$$

If you want elements of $\mathcal{A}$ that are coprime to $r = 6$, take all elements of $\mathcal{A}$ (this is the contribution for $d = 1$), remove from that the elements of $\mathcal{A}$ that are divisible by 2 (this is the contribution of $d = 2$) and the ones divisible by 3 (this is the contribution of $d = 3$). However you have removed twice

*And indeed has an equivalent in any ordered lattice satisfying some suitable finiteness hypothesis.

the elements of $\mathcal{A}$ that are divisible by 2 and by 3, i.e. by 6, and this is the contribution of $d = 6$. The general case is not more difficult than that. Note that $|\mu(r)|$ is a characteristic function, often written as $\mu^2(r)$.

When we do that for primes, the accumulated error term is too big. We look at an upper and a lower estimate.

**Lemma 1.1.** *We have, when $k \geq 1$*

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

Remark: we use the convention that

$$\binom{t}{s} = 0 \quad \text{when } t > s, \text{ or } t \leq 0 < s.$$

But $\binom{0}{0} = 1$.

*Proof.* We simply proceed by recursion on $r \geq 0$. When $r = 0$, both sides equal 1. Assume the property has been proved for $r$ and let us prove it for $r+1$. We find that the left hand expression equals

$$\begin{aligned}(-1)^r \binom{k-1}{r} + (-1)^{r+1}\binom{k}{r+1} &= (-1)^r \frac{(k-1)!}{(r+1)!(k-1-r)!}(r+1-k) \\ &= (-1)^{r+1}\frac{(k-1)!}{(r+1)!(k-1-(r+1))!}\end{aligned}$$

as required. $\square$

**Lemma 1.2.** *Let $r$ be an odd integer and let $m \geq 1$ be an integer. We have*

$$\sum_{\substack{d|m,\\ \omega(d)\leq r}} \mu(d) \leq 1\!\!1_{m=1}$$

*where $1\!\!1_{m=1}$ is 1 when $m = 1$ and vanishes otherwise.*

**Lemma 1.3.** *Let $r$ be an even integer and let $m \geq 1$ be an integer. We have*

$$1\!\!1_{m=1} \leq \sum_{\substack{d|m,\\ \omega(d)\leq r}} \mu(d)$$

*where $1\!\!1_{m=1}$ is 1 when $m = 1$ and vanishes otherwise.*

*Proof.* Indeed, let $k$ be the number of prime factors of $m$. When $k = 0$ (i.e. $m = 1$), both inequalities hold. Otherwise

$$\sum_{\substack{d|m,\\ \omega(d)\le r}} \mu(d) = \sum_{0\le \ell\le r} (-1)^\ell \binom{k}{\ell}$$

since there are $\binom{k}{\ell}$ divisors of $m$ that are squarefree and have exactly $\ell$ prime factors. $\square$

**Theorem 1.4** (Mertens, 1874)**.** *We have*

$$\prod_{p\le z}\Big(1-\frac{1}{p}\Big) = (1+\mathcal{O}(1/\operatorname{Log} z))e^{-\gamma}/\operatorname{Log} z.$$

(The error term may require the PNT).

**Theorem 1.5.** *Let $x \ge 10$ be a real number. The number of integers $n \le x$ that are such that $n(n+2)$ has no prime factors $\le z$ is equal to*

$$\frac{x}{2}\prod_{3\le p\le z}\Big(1-\frac{2}{p}\Big) + \mathcal{O}(xe^{-\sqrt{\operatorname{Log} x}})$$

*for any $z$ such that*

$$\operatorname{Log} z \le \sqrt{\operatorname{Log} x}.$$

This is not enough to prove Brun assertion: the sum of the reciproquals of the twin primes [is finite or] converges. But if you take better parameters in the proof that follows, you will be able to prove Brun's assertion.

**Lemma 1.6.** *We have, when $d$ is squarefree,*

$$\sum_{\substack{n\le x,\\ d|n(n+2)}} 1 = h(d)x + \mathcal{O}^*(2^{\omega(d)})$$

*where*

$$h(d) = \prod_{\substack{p|d,\\ p\ne 2}}\frac{2}{p}\prod_{\substack{p|d,\\ p=2}}\frac{1}{2}. \tag{3}$$

The error term $\mathcal{O}^*(dh(d))$ would be enough.

*Proof.* Indeed,by the chinese remainder Theorem, the equation $n(n+2) \equiv 0[d]$ has $dh(d)$ solutions modulo $d$. $\square$

*Proof of Theorem 1.5.* We use the following inequality

$$S = \sum_{\substack{n\le x,\\ (n(n+2),P(z))=1}} 1 \ge S_r = \sum_{\substack{n\le x,\\ (n(n+2),P(z))=1}} \sum_{\substack{d|\gcd(n(n+2),P(z)),\\ \omega(d)\le r}} \mu(d) \tag{4}$$

valid for any odd integer $r$. Our aim is now to evaluate $S_r$, since, remember, the lower bound we have taken is because we said we would be able to evaluate the resulting sum $S_r$. As it turns out, the condition $d|\gcd(n(n+2), P(z))$ splits into $d|n(n+2)$ and $d|P(z)$. We invert summations, getting:

$$S_r = \sum_{\substack{d|P(z),\\ \omega(d)\le r}} \mu(d) \sum_{\substack{n\le x,\\ d|n(n+2)}} 1.$$

We appeal to Lemma 1.6 and reach our first ledge:

$$S_r = x \sum_{\substack{d|P(z),\\ \omega(d)\le r}} \mu(d)h(d) + \mathcal{O}^*\Bigg(\sum_{\substack{d|P(z),\\ \omega(d)\le r}} 2^{\omega(d)}\Bigg) = xS_r^\star + \mathcal{O}^*((2z)^r)$$

say. We have to evaluate both sums over $d$. Let us start with $S_r^\star$. We write

$$S_r^\star = \sum_{d|P(z)} \mu(d)h(d) + \mathcal{O}^*\Big(\sum_{\substack{d|P(z),\\ \omega(d)>r}} h(d)\Big) = \tfrac{1}{2}\prod_{3\le p\le z}\Big(1-\frac{2}{p}\Big) + \mathcal{O}^*\big(\overline{S}_r\big).$$

We now have to bound $\overline{S}_r$. We proceed as follows:

$$\overline{S}_r \le \sum_{\substack{d|P(z),\\ \omega(d)>r}} 2^{\omega(d)}y^{\omega(d)-r}/d \le y^{-r}\prod_{p\le z}(1+2y/p) \le \exp\Big(-r\operatorname{Log} y + 2y\sum_{p\le z}\frac{1}{p}\Big)$$

valid for any $y \ge 1$. We now have to choose $r$ and $y$. We first define

$$u = \frac{\operatorname{Log} x}{\operatorname{Log} z}. \tag{5}$$

We have $u \ge \sqrt{\operatorname{Log} x}$ which goes to infinity. This inequality also implies that $u \ge \operatorname{Log} z$. We take for $r$ the odd number that is immediately larger than $u/2$. We further select

$$y = \frac{u}{\operatorname{Log} u}.$$

The first error term $\mathcal{O}((2z)^r)$ is $\mathcal{O}(\sqrt{x})$. As for the second one, we have

$$-r\operatorname{Log} y + 2y\sum_{p\le z}\frac{1}{p} \le -\frac{u}{2}\operatorname{Log}\frac{u}{\operatorname{Log} u} + \frac{u}{2} + \frac{2u}{\operatorname{Log} u}(\operatorname{Log}\operatorname{Log} z + \mathcal{O}(1))$$
$$\le -\frac{u}{2}\operatorname{Log}\frac{u}{\operatorname{Log} u} + \frac{u}{2} + 2u + \mathcal{O}(1) \le -\frac{u\operatorname{Log} u}{3} \le -\sqrt{\operatorname{Log} x}$$

provided $x$ be large enough. We prove the upper bound in exactly the same way. □

**Further readings:**

(Iwaniec, 1977), (Daboussi & Rivat, 2001).

**More:**

the additive Rankin's method to get a lower bound for $n!$.

# 2 Second lecture: Vinogradov method made easy

**Theorem 2.1** (Dirichlet)**.** *Let $Q \ge 2$ be a real number. For every $\alpha \in [0,1]$, there exists un fraction $a/q$ such that $q \le Q$ and*

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{qQ}.$$

Take $Q = x/(\operatorname{Log} x)^6$. Let $\alpha$ be in $[0,1]$ and select $a/q$ as in Dirichlet's Theorem. We want to show that

$$\Big|\sum_{p\le x} e(\alpha p)\Big| \le Cx/(\operatorname{Log} x)^2$$

provided $q \ge (\operatorname{Log} x)^9$. So very few arcs are remaining.

To do that, we need to handle a summation over prime numbers. (Vinogradov, 1937) is the first one to have succeeded in this very difficult task. See also (Vinogradov, 2004). It has been thought as being extremely to follow, but we present now a very easy account of Vinogradov method, as presented in (Ramaré, 2006). The reader interested in the most powerful development of Vinogradov method should read (Harman, 1996, Theorem 2),

**Theorem 2.2.** *Let $z$ and $x$ be two real parameters such that $4 \le z^2 \le x$. Let $r(n)$ be the number of prime factors of $n$ that fall in the interval $(z, \sqrt{x}]$. We define next $\rho(n)$ by*

$$\rho(n) = \frac{\mathbb{1}_{(n,P(z))=1}}{1 + r(n)}. \tag{6}$$

*We have*

$$\sum_{z<p\le x} g(p) = \sum_{\substack{\ell \le x,\\ (\ell,P(z))=1}} g(\ell) - \sum_{\substack{z<p\le\sqrt{P},\\ d\le P/p}} \rho(d)g(dp) + R$$

*where $|R| \le 3x/z$ when $|g(n)| \le 1$ for all $n \ge 1$.*

*Proof.* We detect the prime numbers among the set of integers $\ell$ that have no prime factor $\le z$ by removing the ones that have a prime factor in $(z, \sqrt{x})$, i.e. that can be written as $\ell = dp$. We however have to divide by the number of such writings, and this is $r(dp)$. We have thus reached

$$\sum_{z<p\le x} g(p) = \sum_{\substack{\ell \le x,\\ (\ell,P(z))=1}} g(\ell) - \sum_{\substack{z<p\le\sqrt{x},\\ d\le x/p}} \frac{g(dp)}{r(dp)}.$$

Since $r(dp) = r(d) + 1$ when $d$ is not divisible by $p$, we can replace $r(dp)$ by $r(d) + 1$ provided we correct the resulting expression for the integers $dp$ of the shape $tp^2$. This gives us the claimed formula with

$$R = \sum_{z<p\le\sqrt{x}} \sum_{t\le x/p^2} \frac{\rho(tp^2)g(tp^2)}{r(tp^2)}. \tag{7}$$

In order to bound this remainder term, we put absolute values inside, extend the summation over $p$ to every integer, and simplify it by bounding $|g(tp^2)/r(tp^2)|$ above by 1, and $\rho(tp^2)$ by 1. We conclude by comparing the resulting expression to an integral. □

**Theorem 2.3** (Vinogradov)**.** *Let $\alpha \in [0,1]$ and $Q \ge 1$ be two real numbers. Let $a/q \in [0,1]$ be a rational, written in shortest terms and such that $q \le Q$. We assume that*

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{qQ}.$$

*We have*

$$\sum_{p\le x} e(\alpha p) \ll \frac{x}{\operatorname{Log} x}\Big(\frac{1}{\sqrt{q}} + \sqrt{\frac{q}{x}} + \frac{x}{qQ} + \exp\big(-\tfrac{1}{2}\sqrt{\operatorname{Log} x}\big)\Big)(\operatorname{Log} x)^2$$

*where $e(\beta) = \exp(2i\pi\beta)$.*

*Proof.* We want to use Theorem 2.2 with $g(p)$ being $e(p\alpha)$ when $p$ lies in $(x/2, x]$ and 0 otherwise. Let us first proceed to an initial reduction. We write $\alpha = (a/q) + \beta$ and readily check that we can assume $\beta = 0$ at a cost of an error term of size $\mathcal{O}(x^2/(qQ \operatorname{Log} x))$.

Concerning the bilinear part, we use a diadic decomposition in $p$. The part to handle is

$$\Big|\sum_{\substack{P<p\le P',\\ x/(2p)<d\le x/p}} \rho(d)\frac{e(adp/q)}{1+r(d)}\Big|^2 \ll \frac{x}{P}\sum_{x/(4P)<d\le x/P}\Big|\sum_{p\in I(d)} e(dap/q)\Big|^2$$

$$\ll \frac{x}{P}\sum_{p,p'\le P'}\sum_{d\in J(p,p')} e(da(p-p')/q)$$

$$\ll \frac{x}{P}\biggl(\Bigl(\frac{x}{P}+q\Bigr)\sum_{\substack{p,p'\le P',\\ p\equiv p'[q]}} 1 + \sum_{\substack{p,p'\le P',\\ p\not\equiv p'[q]}}\sum_{d\in K(p,p')} e(da(p-p')/q)\biggr)$$

where $I(d)$ is an interval of length $\le P$, $J(p,p')$ is an interval of length $\le x/P$ and $K(p,p')$ is an interval of length $< q$: we obtaining it by removing as many times as possible $q$ consecutive integers from the interval $J(p,p')^*$. In this last sum, the primes such that $p \equiv p'[q]$ contribute at most $q(\operatorname{Log} q)\sum_{\substack{p,p'\le P',\\ p\equiv p'[q]}} 1$. Hence

$$\Big|\sum_{\substack{P<p\le P',\\ x/(2p)<d\le x/p}} \rho(d)\frac{e(adp/q)}{1+r(d)}\Big|^2$$

$$\ll \frac{x}{P}\Bigl((P+q)^2\operatorname{Log} q + P^2 q\operatorname{Log} q\Bigr) \ll \Bigl(xPq + \frac{xq^2}{P}\Bigr)\operatorname{Log} q.$$

We now have to handle the linear part, namely

$$S = \sum_{\substack{\ell\le x,\\ (\ell,P(z))=1}} e(a\ell/q).$$

We have seen how to handle this summation when the function we are summing (here $e(\alpha\ell)$) is non-negative. Here is how we reduce the problem to this case. We consider

$$\sum_{\substack{\ell\le x,\\ (\ell,P(z))=1}} \bigl(1+\Re e(a\ell/q)\bigr) \quad\text{and}\quad \sum_{\substack{\ell\le x,\\ (\ell,P(z))=1}} \bigl(1+\Im e(a\ell/q)\bigr)$$

---

*Starting from its least integer for instance.

for which we give asymptotic bounds. We proceed as in the proof of Theorem 1.5. The main difference is that we will have to handle the summation

$$\sum_{\substack{d|P'(z),\\ \omega(d)\le r,\\ q\nmid d}} \mu^2(d)/\|da/q\| + \sum_{\substack{x/2<\ell\le x,\\ q|d|\ell,\\ d|P(z),\\ \omega(d)\le r}} \mu(d)$$

where $\|\theta\|$ denotes the distance to the nearest integer. It is not more than

$$\sum_{\substack{d\le z^r,\\ (d,q)=1}} 1/\|ad/q\| + \sum_{q|\ell\le x} \tau(\ell/q) \ll z^r \operatorname{Log} q + \frac{x}{q}\operatorname{Log} x.$$

This way, we compute

$$\sum_{\substack{\ell\le x,\\ (\ell,P(z))=1}} \big(1+\Re e(a\ell/q)\big)$$

and

$$\sum_{\substack{\ell\le x,\\ (\ell,P(z))=1}} 1.$$

By substraction, the main terms cancel out!. Operating similarly for the imaginary part, we get the Theorem we sought. □

**Further readings:**

(Iwaniec & Jutila, 1979), (Harman, 1982), (Iwaniec & Kowalski, 2004).

# 3 Third lecture: Initiation to Selberg upper bound sieve

(Levin & Fainleib, 1967), (Ramaré, 2009, Theorem 21.1). Convolution method: folklore but can be found in (Ramaré, 1995).

**Theorem 3.1.** *Let $g$ be a non-negative multiplicative function. Let $\kappa$, $L$ and $A$ be three non-negative real parameters such that*

$$\begin{cases} \displaystyle\sum_{\substack{p\ge 2,\nu\ge 1,\\ w<p^\nu\le Q}} g\big(p^\nu\big)\operatorname{Log}\big(p^\nu\big) = \kappa\operatorname{Log}(Q/w) + \mathcal{O}^*(L), \quad (Q>w\ge 1),\\ \displaystyle\sum_{p\ge 2}\sum_{\nu,k\ge 1} g\big(p^\nu\big)g\big(p^k\big)\operatorname{Log}\big(p^\nu\big) \le A. \end{cases}$$

*Then, when* $D \geq \exp(2(L+A))$*, we have*

$$\sum_{d\leq D} g(d) = C(\operatorname{Log} D)^\kappa (1 + \mathcal{O}^*(B/\operatorname{Log} D))$$

*with*

$$\begin{cases} C = \dfrac{1}{\Gamma(\kappa+1)} \displaystyle\prod_{p\geq 2}\biggl\{\Bigl(1-\frac{1}{p}\Bigr)^\kappa \sum_{\nu\geq 0} g(p^\nu)\biggr\}, \\ B = 2(L+A)(1+2(\kappa+1)e^{\kappa+1}). \end{cases}$$

Here is a simpler version:

**Theorem 3.2.** *Let* $g$ *be a non-negative multiplicative function. Let* $\kappa$*,* $L'$ *and* $A$ *be three non-negative real parameters such that*

$$\begin{cases} \displaystyle\sum_{\substack{p\geq 2, \nu\geq 1,\\ p^\nu \leq Q}} g\bigl(p^\nu\bigr) \operatorname{Log}\bigl(p^\nu\bigr) = \kappa \operatorname{Log} Q + \mathcal{O}^*(L'), \quad (Q \geq 1), \\ \displaystyle\sum_{p\geq 2} \sum_{\nu,k\geq 1} g\bigl(p^\nu\bigr) g\bigl(p^k\bigr) \operatorname{Log}\bigl(p^\nu\bigr) \leq A. \end{cases}$$

*Then, when* $D \geq \exp(4(L'+A))$*, we have*

$$\sum_{d\leq D} g(d) = C(\operatorname{Log} D)^\kappa (1 + \mathcal{O}^*(B'/\operatorname{Log} D))$$

*with*

$$\begin{cases} C = \dfrac{1}{\Gamma(\kappa+1)} \displaystyle\prod_{p\geq 2}\biggl\{\Bigl(1-\frac{1}{p}\Bigr)^\kappa \sum_{\nu\geq 0} g(p^\nu)\biggr\}, \\ B' = 4(L'+A)(1+2(\kappa+1)e^{\kappa+1}). \end{cases}$$

As an application, let us evaluate

$$G(z) = \sum_{d\leq z} \mu^2(d) g(d) \tag{8}$$

where $g$ is the multiplicative function defined on the primes by

$$g(2) = 1, \quad g(p) = 2/(p-2) \quad (p \geq 3) \tag{9}$$

and $g(p^k) = 0$ for $k \geq 2$ and any prime $p$. The condition are easily verified with $\kappa = 2$, so that the constant reads here

$$\prod_{p\geq 3}\biggl\{\Bigl(1-\frac{1}{p}\Bigr)^2 \frac{p}{p-2}\biggr\}.$$

We want to evaluate

$$\sum_{\substack{p\le x,\\ p+2\text{ prime}}} 1.$$

We first select a sieving parameter $z$ and limit our search to primes $> z$, at a cost of at most $\mathcal{O}^*(z)$. The idea of Selberg has then been to consider

$$S = \sum_{n\le x}\Bigl(\sum_{\substack{d|n(n+2),\\ d\le z}} \lambda_d\Bigr)^2$$

with $\lambda_1 = 1$. This sum is indeed larger than the number of prime twins in $(z, x]$. Indeed, the coefficients we sum is equal to 1 on such a prime twin and non-negative otherwise. Let us now try to choose the $\lambda_d$'s to the best of our interests. Our choice will have $|\lambda_d| \le 1$. We have

$$\begin{aligned} S &= \sum_{d_1,d_2\le z} \lambda_{d_1}\lambda_{d_2} \sum_{\substack{[d_1,d_2]|n(n+2),\\ n\le x}} 1 = x\sum_{d_1,d_2\le z} \lambda_{d_1}\lambda_{d_2} h([d_1,d_2]) + \mathcal{O}(\sum_{d\le z} 2^{\omega(z)}) \\ &= x\sum_{d_1,d_2\le z} \frac{\lambda_{d_1}\lambda_{d_2} h(d_1)h(d_2)}{h((d_1,d_2))} + \mathcal{O}(z^2(\operatorname{Log} z)^2) \end{aligned}$$

where $h$ is defined by (3). Notice next that when $(d_1, d_2)$ is squarefree:

$$\frac{1}{h((d_1,d_2))} = \sum_{\substack{\delta|d_1,\\ \delta|d_2}} h^\star(\delta)$$

where $h^\star$ is the multiplicative function defined on prime numbers by

$$h^\star(2) = 1, \quad h^\star(p) = \frac{p}{2} - 1 \quad (p \ge 3) \tag{10}$$

and the values on prime powers will not intervene, so we do not have to define $h^\star$ there. The reader will check that $h^\star$ is in fact $1/g$, with $g$ being defined in (9). We get

$$S = \sum_{\delta\le z} h^\star(\delta)\Bigl(\sum_{\delta|d\le z} \lambda_d h(d)\Bigr)^2 + \mathcal{O}((z\operatorname{Log} z)^2).$$

Let us define the new variables

$$y_\delta = \sum_{\delta|d\le z} h(d)\lambda_d. \tag{11}$$

It is readily checked that

$$h(d)\lambda_d = \sum_{d|\delta} \mu(\delta/d) y_\delta. \tag{12}$$

*Proof.* Indeed, put (11) inside the right hand side of (12). We get

$$\sum_{d|\delta} \mu(\delta/d) \sum_{\delta|\ell\le z} h(\ell)\lambda_\ell = \sum_{d|\ell\le z} h(\ell)\lambda_\ell \sum_{d|\delta|\ell} \mu(\delta/d) = h(d)\lambda_d.$$

□

Our condition $\lambda_1 = 1$ reads

$$\sum_{\delta\ge 1} \mu(\delta) y_\delta = 1$$

condition uder which we seek to minimize the quadratic form $\sum_{\delta\le z} h^\star(\delta) y_\delta^2$. It is readily checked that such a minimum is reached with the choice

$$y_\delta = \frac{\mu(\delta)}{h^\star(\delta)G(z)}$$

where $G(z)$ has been defined in (8). Let us only check that the linear condition holds.

*Proof.*

$$\sum_{\delta\ge 1} \mu(\delta) y_\delta = \sum_{\delta\ge 1} \frac{\mu(\delta)^2}{h^\star(\delta)G(z)} = \frac{G(z)}{G(z)} = 1$$

as required. □

The minimum is then

$$\sum_{\delta\le z} h^\star(\delta) y_\delta^2 = \sum_{\delta\le z} \frac{\mu^2(\delta)}{h^\star(\delta)G(z)^2} = 1/G(z). \tag{13}$$

Since we have already evaluated the main term, this gives us

$$\sum_{\substack{p\le x,\\ p+2 \text{ prime}}} 1 \le \frac{x}{G(z)} + z + \mathcal{O}((z \operatorname{Log} z)^2)$$

and we choose $z = \sqrt{x}/(\operatorname{Log} x)^2$ to get

**Theorem 3.3.** *The number of prime twins in* $[1, x]$ *is not more than*

$$(1 + o(1))\frac{x}{2}\prod_{p\geq 3}\left(1 - \frac{1}{(p-1)^2}\right) \times 8.$$

Note : this is valid as an upper bound for the number of twin primes in *any* interval of length $x$. (Siebert, 1976) gives a completely explicite version of this result. It may be possible to improve on it in the spirit of (Ramaré & Schlage-Puchta, 2008).

We now should check that $|\lambda_d| \leq 1$.

**Further readings:**

(Halberstam & Richert, 1974), (Ramaré, 2005).

# 4 Fourth lecture: the parity principle in sieve methods

What is a sieve? One answer is: it is a machine that extracts informations from an over-sequence $\mathcal{A}$, for instance the integer of interval, to get properties of a smaller sequence, for instance the one of primes in this interval, or the one of prime twins in this interval. What kind of informations? Well, usually only information on how this sequence is distributed in some specific arithmetic progressions. And, if you look closely, only at information concerning the main terms in the form*:

$$\forall d \leq D, \quad \sum_{\substack{a\in\mathcal{A},\\ d|a}} 1 = \sigma(d)X + R_d.$$

We want to extract information from $\sigma(d)$.

The fact is that these processi are usually very general, as we have seen. This implies that they are flexible and give information even in very tricky situation. But this should also imply that they have limitations!

## Following Selberg

We rely on (Selberg, 1949), (Selberg, 1949) and (Selberg, 1991, Lectures on sieve).

*When sieving to get prime numbers

Let us follow Selberg on the subject and consider the Liouville function $\lambda(d)$ defined by

$$\lambda(d) = (-1)^{\Omega(d)} = (-1)^{\text{number of prime factors of } d\text{, counted with multiplicity}}.$$

This function is completely multiplicative, Let us assume for simplicity the Riemann Hypothesis, though we could do without. This hypothesis tells us that

$$\forall \varepsilon > 0, \quad \sum_{n \le x} \lambda(n) \ll x^{\frac{1}{2}+\varepsilon}.$$

Let us now consider two sequences: $\mathcal{A}_{\mathrm{even}}$ is the sequence of integers in $[1, x]$ that have an even number of prime factors and $\mathcal{A}_{\mathrm{odd}}$ is the sequence of integers in $[1, x]$ that have an odd number of prime factors. An integer $n \in [1, x]$ is in $\mathcal{A}_{\mathrm{even}}$ if and only if $(1 + \lambda(n))/2 = 1$, and this function takes value 0 otherwise. As a consequence

$$\forall d, \forall \varepsilon > 0, \quad \sum_{\substack{n \le x,\\ d|n}} \frac{1 + \lambda(n)}{2} = \frac{x}{2d} + \mathcal{O}_\varepsilon\big((x/d)^{\frac{1}{2}+\varepsilon}\big).$$

This means that for this sequence, the main term is the same as when sieving the whole interval! If we had a sieve that would extract from this information that the number of primes in such a sequence is indeed $> 0$, then it would do so in $\mathcal{A}_{\mathrm{even}}$ also. But this sequence does not contain any primes at all!

Looking at $\mathcal{A}_{\mathrm{odd}}$, we see that the best a sieve could do is produce $\delta X = (1 + o(1))x/\operatorname{Log} x$ primes, i.e. $\delta = 2/\operatorname{Log} x$, which when applied to the sequence of primes in *any* interval or length $x$, implies that this kind of process cannot give any better than

$$2x/\operatorname{Log} x$$

in this interval.

## Hand waving

Here is how one can summarize what has been observed:

The sieve alone is not able to distinguish between an even and an odd number of primes factors.

In particular it cannot produce primes. This is vague, and true only if the notion of sieve is understood in a proper general context. In Theorem 2.2, the reader may have noticed that in applies only to the primes between 1 and $x$. Though this is not a sieve, it is surely akin to a sieving process.

## Selberg's identity

$$\Lambda \operatorname{Log} + \Lambda \star \Lambda = \mu \star \operatorname{Log}^2 . \tag{14}$$

This leads to:

**Theorem 4.1.** *We can prove elementarily that*

$$\sum_{n \le x} \Lambda(n) \operatorname{Log} n + \sum_{n_1 n_2 \le x} \Lambda(n_1)\Lambda(n_2) = 2x \operatorname{Log} x + \mathcal{O}(x).$$

**Lemma 4.2.** *We can prove elementarily that*

$$\sum_{d \le x} \frac{\mu(d)}{d} \ll 1, \quad \sum_{d \le x} \frac{\mu(d)}{d} \operatorname{Log}(x/d) \ll 1$$

*and that*

$$\sum_{d \le x} \frac{\mu(d)}{d} \operatorname{Log}^2(x/d) = 2 \operatorname{Log} x + \mathcal{O}(1).$$

*Proof.* Let us start with the difficult one which is the third one. The reader will check on using Dirichlet hyperbola formula that

$$\sum_{m \le M} \frac{d(m)}{m} = \frac{(\operatorname{Log} M)^2}{2} + c_1 \operatorname{Log} M + c_2 + \mathcal{O}(M^{-2/3}). \tag{15}$$

(even better is available). This gives us

$$\begin{aligned}
&\sum_{d \le x} \frac{\mu(d)}{d} \operatorname{Log}^2(x/d) \\
&\quad = \sum_{d \le x} \frac{\mu(d)}{d} \biggl( 2 \sum_{m \le x/d} \frac{d(m)}{m} - 2c_1 \operatorname{Log}(x/d) + 2c_2 + \mathcal{O}((d/x)^{2/3}) \biggr) \\
&\qquad = 2 \sum_{dm \le x} \frac{\mu(d) d(m)}{dm} + \mathcal{O}(1) = 2 \operatorname{Log} x + \mathcal{O}(1).
\end{aligned}$$

□

*Proof of Theorem 4.1.* We have

$$\begin{aligned}
S &= \sum_{d \le x} \mu(d) \Bigl( \frac{x}{d} \operatorname{Log}^2 \frac{x}{d} - \frac{2x}{d} \operatorname{Log} \frac{x}{d} + \frac{2x}{d} + \mathcal{O}(\sqrt{x/d}) \Bigr) \\
&= x \sum_{d \le X} \frac{\mu(d)}{d} \Bigl( \operatorname{Log}^2 \frac{x}{d} - 2 \operatorname{Log} \frac{x}{d} + 2 \Bigr) + \mathcal{O}(x) = 2x \operatorname{Log} x + \mathcal{O}(x)
\end{aligned}$$

by the previous Lemma. □

It is worth mentionning that the part with the primes and the part without it have the same contribution, namely that

$$\sum_{n\le x}\Lambda(n)\operatorname{Log} n = x\operatorname{Log} x+\mathcal{O}(x)=\sum_{p_1p_2\le x}\Lambda(p_1)\Lambda(p_2).$$

In (Bombieri, 1976), (Friedlander & Iwaniec, 1996) and (Friedlander & Iwaniec, 1998), the sum

$$\sum_{n\le x}\Lambda(n)\operatorname{Log} n f(n)+\sum_{p_1p_2\le x}\Lambda(n_1)\Lambda(n_2)f(n_1n_2)$$

is computed for a wide variety of functions $f$. This is made possible by the fact that the treatment above is elementary. In (Ramaré, 2010), we compute

$$\sum_{n\le x}\frac{\Lambda(n)(\operatorname{Log} n)^{2\nu-1}}{(2\nu-1)!}f(n)+\sum_{n_1n_2\le x}\frac{\Lambda(n_1)(\operatorname{Log} n_1)^{\nu-1}\Lambda(n_2)(\operatorname{Log} n_2)^{\nu-1}}{(\nu-1)!^2}f(n_1n_2)$$

for about the same class of functions. We get a better error term when $\nu$ (any integer $\ge 1$) grows. This is so, while in fact the coefficient

$$\frac{\Lambda(n_1)(\operatorname{Log} n_1)^{\nu-1}\Lambda(n_2)(\operatorname{Log} n_2)^{\nu-1}}{(\nu-1)!^2}$$

enables a better localization of $n_1$ and $n_2$ as this quantity will be larger when $n_1$ and $n_2$ are close to $\sqrt{x}$. This phenomenom increases as $\nu$ increases.

**Further readings:**

# References


Bombieri, E. 1976. The asymptotic sieve. *Rend., Accad. Naz. XL, V. Ser. 1-2*, 243–269.

Brun, V. 1919a. La série $\frac15+\frac17+\frac1{11}+\frac1{13}+\frac1{17}+\frac1{19}+\frac1{29}+\frac1{31}+\frac1{41}+\frac1{43}+\frac1{59}+\frac1{61}+\cdots$ où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie. *Darboux Bull.*, **43**(2), 100–104, 124–128.

Brun, V. 1919b. Le crible d'Erathosthène et le théorème de Goldbach. *C.R.*, **168**, 544–546.

Daboussi, H., & Rivat, J. 2001. Explicit upper bounds for exponential sums over primes. *Math. Comp.*, **70**(233), 431–447.

Friedlander, J., & Iwaniec, H. 1996. Bombieri's sieve. *Pages 411–430 of:* Berndt, Bruce C. (ed.) et al. (ed), *Analytic number theory. Vol. 1. Proceedings of a conference in honor of Heini Halberstam, May 16-20, 1995, Urbana, IL, USA. Boston, MA.* Birkhäuser. Prog. Math., vol. 138.

Friedlander, J., & Iwaniec, H. 1998. Asymptotic sieve for primes. *Ann. of Math. (2)*, **148**(3), 1041–1065.

Halberstam, H., & Richert, H.E. 1974. Sieve methods. *Academic Press (London)*, 364pp.

Harman, G. 1982. Primes in short intervals. *Math. Z.*, **180**(3), 335–348.

Harman, G. 1996. On the distribution of $\alpha p$ modulo one. II. *Proc. London Math. Soc. (3)*, **72**(2), 241–260.

Iwaniec, H. 1977. The sieve of Eratosthenes-Legendre. *Ann. Sc. Norm. Super. Pisa, Cl. Sci., IV. Ser. 4*, 257–268.

Iwaniec, H., & Jutila, M. 1979. Primes in short intervals. *Ark. Mat.*, **17**(1), 167–176.

Iwaniec, H., & Kowalski, E. 2004. *Analytic number theory.* American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI. xii+615 pp.

Levin, B.V., & Fainleib, A.S. 1967. Application of some integral equations to problems of number theory. *Russian Math. Surveys*, **22**, 119–204.

Murty, M.Ram, & Saradha, N. 1987. On the sieve of Eratosthenes. *Can. J. Math.*, **39**(5), 1107–1122.

Ramaré, O. 1995. On Snirel'man's constant. *Ann. Scu. Norm. Pisa*, **21**, 645–706. `http://math.univ-lille1.fr/~ramare/Maths/Article.pdf`.

Ramaré, O. 2005. Le théorème de Brun-Titchmarsh : une approche moderne. 1–10. `http://math.univ-lille1.fr/\~{}ramare/Maths/Nantes.pdf`.

Ramaré, O. 2006. *Variations modernes sur la suite des nombres premiers. De la densité des sin(p) lorsque p parcourt l'ensemble des nombres premiers.* Lulu.com. 105pp.

Ramaré, O. 2009. *Arithmetical aspects of the large sieve inequality.* Harish-Chandra Research Institute Lecture Notes, vol. 1. New Delhi: Hindustan Book Agency. With the collaboration of D. S. Ramana.

Ramaré, O. 2010. On Bombieri's asymptotic sieve. *J. Number Theory*, 40pp.

Ramaré, O., & Schlage-Puchta, J.-C. 2008. Improving on the Brun-Titchmarsh theorem. *Acta Arith.*, **131**(4), 351–366.

Rankin, R.A. 1938. The difference between consecutive prime numbers. *J. Lond. Math. Soc.*, **13**, 242–247.

Selberg, A. 1949. An elementary proof of the prime-number theorem. *Ann. Math.*, **50**(2), 305–313.

Selberg, A. 1949. On elementary problems in prime number-theory and their limitations. *C.R. Onzième Congrès Math. Scandinaves, Trondheim, Johan Grundt Tanums Forlag*, 13–22.

Selberg, A. 1991. Collected Papers. *Springer-Verlag*, **II**, 251pp.

Siebert, H. 1976. Montgomery's weighted sieve for dimension two. *Monatsh. Math.*, **82**(4), 327–336.

Vinogradov, I. M. 2004. *The method of trigonometrical sums in the theory of numbers.* Mineola, NY: Dover Publications Inc. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.

Vinogradov, I.M. 1937. Representation of an odd number as a sum of three primes. *Dokl. Akad. Nauk SSSR*, **15**, 291–294.