Lecture 2. Average orders. Brun's sieve and Linnik's large sieve

M. Klazar

March 1, 2024

I continue my survey of G. Tenenbaum's book [12]. In the second lecture we cover Chapter I.3. *Average orders* and the first five sections of Chapter I.4. *Sieve methods*, up to page 82. The variables x and y range in $\mathbb{R}$ and $k, l, m, n \in \mathbb{N}$. $\mathbb{P}$ is the set of prime numbers and $p \in \mathbb{P}$. By A we denote the set of arithmetic functions, functions of the type $f\colon \mathbb{N} \to \mathbb{C}$. We remind the meaning of the asymptotic symbols O, $\ll$, $\sim$ and o (which we were using already in the last lecture). Let $f, g\colon M \to \mathbb{C}$, $M \subset \mathbb{R}$, be two complex-valued functions. Then $f(x) = O(g(x))$ for $x \in M$, or synonymously $f(x) \ll g(x)$ for $x \in M$, mean that

$$\exists\, c > 0\, \forall\, x \in M\, \big(|f(x)| \le c|g(x)|\big).$$

If $A \in \mathbb{R} \cup \{-\infty, +\infty\}$ is a limit point of the set $M \setminus Z(g)$, where $Z(g) = \{x \in M \mid g(x) = 0\}$, we write that $f(x) \sim g(x)$ for $x \to A$, resp. that $f(x) = o(g(x))$ for $x \to A$, if

$$\lim_{x\to A} \frac{f(x)}{g(x)} = 1,\ \text{ resp. }\ \lim_{x\to A} \frac{f(x)}{g(x)} = 0\ .$$

Chapter I.3. Average orders

The following is Theorem 3.1 (Dirichlet's hyperbola method) in [12]. If $f \in A$ then the *summatory function* $F\colon \mathbb{R} \to \mathbb{C}$ *of* f is defined by

$$F(x) := \textstyle\sum_{n\le x} f(n)$$

where $x \in \mathbb{R}$, $n \in \mathbb{N}$ and the empty sum is 0. Recall that for functions $f, g \in A$ their Dirichlet convolution $f * g \in A$ is given by

$$(f * g)(n) = \textstyle\sum_{kl=n} f(k)g(l).$$

Theorem 1 *Let $f, g \in A$, with respective summatory functions F, G. For $1 \le y \le x$, we have*

$$\sum_{n\le x} (f * g)(n) = \sum_{n\le y} g(n)F(x/n) + \sum_{m\le x/y} f(m)G(x/m) - F(x/y)G(y).$$

The following Theorem 3.2 in [12] is an application. By [11] it is due to P. L. Dirichlet in [6] in 1849. Recall that $\tau(n) = \sum_{kl=n} 1$ denotes the number of divisors of n and that $\gamma = \lim_{n\to\infty} \left(\sum_{i=1}^{n} \frac{1}{i} - \log n \right) \approx 0.577215$.

Theorem 2 *For $x \to +\infty$,*

$$\sum_{n \le x} \tau(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x})$$

where γ denotes Euler's constant.

Proof. We apply the previous theorem with $f = g = \mathbf{1}$, $F(x) = G(x) = \lfloor x \rfloor$ and $y = \sqrt{x}$, and get that

$$\sum_{n \le x} \tau(n) = 2 \sum_{m \le \sqrt{x}} \lfloor x/m \rfloor - \lfloor x \rfloor^2 = 2x \sum_{m \le \sqrt{x}} \frac{1}{m} - x + O(\sqrt{x}).$$

The initial key equality can be seen directly, by considering sets of lattice points $S = \{(k, l) \in \mathbb{N}^2 \mid kl \le x\}$, $T = \{(k, l) \in S \mid k \le y\}$ and $U = \{(k, l) \in S \mid l \le y\}$. Since $S = T \cup U$ and $|T| = |U|$, the first equality mirrors the PIE-type equality $|S| = |T| + |U| - |T \cap U|$. By Theorem 8 in the previous lecture, the last sum over m has asymptotics $\frac{1}{2} \log x + \gamma + O(1/\sqrt{x})$ and Dirichlet's result follows. $\square$

Let $\Delta(x) = \sum_{n \le x} \tau(n) - x \log x - (2\gamma - 1)x$ and let $D = \{\alpha > 0 \mid \Delta(x) = O(x^\alpha) \text{ for } x \ge 2\}$. The theorem says that $\inf(D) \le \frac{1}{2}$. It is conjectured that $\inf(D) = \frac{1}{4}$. M. Huxley proved in [7] in 2003 that $\inf(D) \le \frac{131}{416} \approx 0.314904$.

The following is Theorem 3.3 in [12]; recall that $\sigma(n) = \sum_{kl=n} k$.

Theorem 3 *For $x \to +\infty$,*

$$\sum_{n \le x} \sigma(n) = \frac{\pi^2}{12} \cdot x^2 + O(x \log x).$$

The constant in the asymptotics comes from the sum $\zeta(2) = \sum \frac{1}{n^2} = \frac{\pi^2}{6}$. By [12] the best error term known is $O(x(\log x)^{2/3})$ and is due to A. Walfisz [13, p. 99] in 1963.

The following is Theorem 3.4 in [12]; recall that φ is Euler's totient function.

Theorem 4 *For $x \to +\infty$,*

$$\sum_{n \le x} \varphi(n) = \frac{3}{\pi^2} \cdot x^2 + O(x \log x).$$

Proof. We know from the last Theorem 36 in the previous lecture that

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p} \right) = \sum_{km=n} \mu(k)m.$$

Thus for $x \geq 2$,

$$\begin{aligned}
\sum_{n \leq x} \varphi(n) &= \sum_{k \leq x} \mu(k) \sum_{m \leq x/k} m = \frac{1}{2} \sum_{k \leq x} \mu(k) \left\lfloor \frac{x}{k} \right\rfloor \left(\left\lfloor \frac{x}{k} \right\rfloor + 1 \right) \\
&= \frac{x^2}{2} \sum_{k \leq x} \frac{\mu(k)}{k^2} + O\bigg(x \sum_{k \leq x} \frac{1}{k} \bigg) \\
&= \frac{x^2}{2} \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} + O\bigg(x^2 \sum_{k > x} \frac{1}{k^2} \bigg) + O(x \log x) \\
&= \frac{x^2}{2} \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} + O(x) + O(x \log x)
\end{aligned}$$

where the O's follow easily by Theorem 4 in the previous lecture. It remains to show that the sum of the infinite series is $6/\pi^2$. Since $\sum_{k \mid n} \mu(k) = 1$ for $n = 1$ and is 0 for $n > 1$, by multiplying (in the way of Dirichlet convolution, not as in the Cauchy product) two absolutely convergent series we get the identity

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \cdot \sum_{k=1}^{\infty} \frac{1}{k^2} = \sum_{k=1}^{\infty} \bigg(\sum_{lm=k} \mu(l) \bigg) \frac{1}{k^2} = 1.$$

Now the famous result of L. Euler says that $\zeta(2) = \sum_{k \geq 1} 1/k^2 = \pi^2/6$. In [12] two proofs for this formula are suggested in Exercise 52. $\square$

Thus the constant in the asymptotics comes again from $\zeta(2)$. The best known error term $O(x(\log x)^{2/3}(\log \log x)^{4/3})$ is again obtained in the monograph [13, p. 144].

The following is Theorem 3.5 in [12]; recall that $(m, n) = 1$ means that m and n are coprime numbers.

Theorem 5 *For $x, y \geq 2$ and with $z = \min(\{x, y\})$,*

$$|\{(m,\, n) \in \mathbb{N}^2 \mid m \leq x,\, n \leq y,\, (m,\, n) = 1\}| = xy \bigg(\frac{6}{\pi^2} + O((\log z)/z) \bigg).$$

The following are Theorems 3.6 and 3.7 in [12]. We define functions $\omega, \Omega \in A$ by

$$\omega(n) = \sum_{p \mid n} 1 \ \text{ and } \ \Omega(n) = \sum_{p^\nu \| n} \nu.$$

Theorem 6 *For $x \to +\infty$,*

$$\sum_{n \leq x} \omega(n) = x \log \log x + c_1 x + O(x / \log x)$$

where $c_1 \approx 0.261497$ is the constant appearing in Theorem 1.10 (Theorem 20 in the previous lecture).

Theorem 7 *For $x \to +\infty$,*

$$\sum_{n \le x} \Omega(n) = x \log\log x + c_2 x + O(\tfrac{x}{\log x}) \ \textit{ with } \ c_2 = c_1 + \sum_p \frac{1}{p(p-1)} \approx 1.034653.$$

The following Theorem 3.8 and Corollary 3.9 in [12] deal with equivalent forms of PNT (the Prime Number Theorem). Recall that μ is the Möbius function, $\Lambda(n) = 0$ if n is not a prime power and $\Lambda(p^\nu) = \log p$, $\psi(x) = \sum_{n \le x} \Lambda(n)$, $\vartheta(x) = \sum_{p \le x} \log p$ and $\pi(x) = \sum_{p \le x} 1$.

Theorem 8 *For $x \to +\infty$ the next three claims are elementarily equivalent,*

$$\lim \frac{\psi(x)}{x} = 1 \iff M(x) := \sum_{n \le x} \mu(n) = o(x) \iff \sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

The first claim is in fact written as $\psi(x) \sim x$ and, as we know, the second one means that $\lim M(x)/x = 0$.

Corollary 9 *For $x \to +\infty$ the next three claims are elementarily equivalent to those in Theorem* 3.8 *(here Theorem 8).*

$$\pi(x) \sim \frac{x}{\log x} \iff \vartheta(x) \sim x \iff \sum_{n \le x} \frac{\Lambda(n)}{n} = \log x - \gamma + o(1).$$

Here γ is Euler's constant.

In the following Theorems 3.10 and 3.11 in [12],

$$Q(x) = \sum_{n \le x} \mu(n)^2$$

is the number of square-free numbers not exceeding x. Recall that $n \in \mathbb{N}$ is *square-free* if it is a product of distinct primes. These numbers include the empty product $n = 1$ and primes $\mathbb{P}$.

Theorem 10 *For $x \to +\infty$,*

$$Q(x) = \frac{6}{\pi^2} \cdot x + O(\sqrt{x}).$$

The next theorem is due to E. Landau [8] in 1909.

Theorem 11 *For $x \to +\infty$,*

$$M(x) = \sum_{n \le x} \mu(n) = o(x) \Rightarrow Q(x) = \frac{6}{\pi^2} \cdot x + o(\sqrt{x}).$$

Thus under the assumption that $M(x) = o(x)$, which is equivalent with PNT, one can deduce that the error term in asymptotics for $Q(x)$ is o as well. The constant comes again from $\zeta(2)$. The best known error term in the asymptotics for $Q(x)$ is $O\big(\sqrt{x} \exp(-c(\log x)^{3/5}/(\log\log x)^{1/5})\big)$ in [13], for some constant $c > 0$.

The next Theorem 3.12 in [12] is quite general.

Theorem 12 *Let $f\colon \mathbb{N} \to [0,1]$ be multiplicative and*

$$M(f) := \prod_p \left(1 - \frac{1}{p}\right) \sum_{\nu \geq 0} \frac{f(p^\nu)}{p^\nu}.$$

Then

$$\sum_{n \leq x} f(n) = xM(f) + o(x) \quad (x \to +\infty).$$

We explain how the constant $M(f) \in [0,1]$ is defined. Since $f(p^\nu) \in [0,1]$, the inner series over $\nu \in \mathbb{N}_0$ (absolutely) converges and has the sum

$$s(p,\, f) := \sum_{\nu \geq 0} \frac{f(p^\nu)}{p^\nu} \in [0,\, p/(p-1)]\ .$$

If $(p_n) = (2, 3, 5, 7, 11, \dots)$ is the sequence of prime numbers, one has that

$$M(f) = \lim_{n \to \infty} \prod_{i=1}^{n} \frac{(p_i - 1)s(p_i,\, f)}{p_i} =: \lim_{n \to \infty} \prod_{i=1}^{n} t_i\ .$$

Since $t_i \in [0,1]$ for every $i \in \mathbb{N}$, it holds that $t_1 \geq t_1 t_2 \geq t_1 t_2 t_3 \geq \cdots \geq 0$ and the limit $M(f)$ exists (and lies in $[0,1]$) by the theorem on limits of monotone sequences.

Chapter I.4. Sieve methods

In contrast to the previous chapters, in this chapter (on sieves) statements of results, especially the intermediate ones, may be complicated and at first not easy to understand. Recall the principle of inclusion and exclusion (PIE) which we used in the last proof at the end of the previous lecture: If $A_1, \dots, A_n \subset U$, $n \in \mathbb{N}$, are finite sets then

$$\left| U \setminus \bigcup_{i=1}^{n} A_i \right| = \sum_{X \subset [n]} (-1)^{|X|} \left| \bigcap_{i \in X} A_i \right|$$

where $[n] = \{1, 2, \dots, n\}$ and for $X = \emptyset$ the intersection is defined to be U. This is an exact formula but the number of summands on the right side, which is 2^n, is too large. For example, to compute or estimate $\pi(x)$ for $x > 0$ and going to $+\infty$, we write $P \in \mathbb{N}$ for the product of all primes $p \leq \sqrt{x}$, set $U = [\lfloor x \rfloor]$ and $A_p = p\mathbb{Z} \cap U$, and get this instance of the above displayed formula:

$$\pi(x) = \sum_{d \,|\, P} \mu(d) \lfloor x/d \rfloor.$$

Using the trivial estimate $\lfloor x/d \rfloor = x/d + O(1)$ we get the formula

$$\pi(x) = x \prod_{p \leq \sqrt{x}} \big(1 - 1/p\big) + O\big(2^{\pi(\sqrt{x})}\big).$$

But, by Chebyshev's estimates, $2^{\pi(\sqrt{x})} \gg \exp(c\sqrt{x}/\log x)$ for some constant $c > 0$. This is much larger than the main term and the formula is useless.

Nevertheless, it is an easy exercise to show that for any $h \in \mathbb{N}_0$ the following truncations of the above displayed general PIE formula yield lower and upper bounds on the unknown quantity:

$$\sum_{\substack{X\subset[n] \\ |X|\le 2h+1}} (-1)^{|X|}\Big|\bigcap_{i\in X} A_i\Big| \le \Big|U \setminus \bigcup_{i=1}^{n} A_i\Big| \le \sum_{\substack{X\subset[n] \\ |X|\le 2h}} (-1)^{|X|}\Big|\bigcap_{i\in X} A_i\Big|.$$

Now the sums have only $\binom{n}{0} + \cdots + \binom{n}{2h+1}$, resp. $\binom{n}{0} + \cdots + \binom{n}{2h}$, terms. These are so called Bonferroni inequalities. In *Brun's sieve* they are the main tool for obtaining nontrivial results on prime numbers.

The following is Theorem 4.1 (Brun) in [12]. "Brun" refers to the Norwegian mathematician Viggo Brun (1885–1978) who in 1917–24 founded in the pioneering works [1, 2, 3, 4, 5] the discipline of sieve methods in number theory. Recall that $\omega(n) = |\{p \mid p \,|\, n\}|$, μ is the Möbius function, $*$ denotes the Dirichlet convolution, $\mathbf{1} \in A$ is constantly 1 and $1_A \in A$ has values $1_A(1) = 1$ and $1_A(n) = 0$ for $n > 1$. As we know,

$$\mu * \mathbf{1} = 1_A \; .$$

The *square-free kernel* $\mathrm{sq}(n) \in \mathbb{N}$ of $n \in \mathbb{N}$ is the product of all prime factors of n; we set $\mathrm{sq}(1) = 1$. Brun's idea is embodied in the next theorem.

Theorem 13 *Let $t \in \mathbb{N}_0$ and the function $\chi_t \colon \mathbb{N} \to \{0, 1\}$ be given by $\chi_t(n) = 1 \iff \omega(n) \le t$. For $h \in \mathbb{N}_0$ and $i \in \{0, 1\}$ we set*

$$\mu_i(n) := \mu(n) \cdot \chi_{2h+i}(n) \; .$$

Then for any $n \in \mathbb{N}$,

$$(\mu_1 * \mathbf{1})(n) \le 1_A(n) \le (\mu_0 * \mathbf{1})(n) \; .$$

Proof. First we prove by induction on l the identity that for any $k, l \in \mathbb{N}_0$,

$$\sum_{j=0}^{l} (-1)^j \binom{k}{j} = (-1)^l \binom{k-1}{l} \; .$$

For $l = 0$ both sides equal 1. For $l > 0$ we get by induction and the basic recurrence for binomial coefficients that indeed

$$\begin{aligned} \sum_{j=0}^{l} (-1)^j \binom{k}{j} &= \sum_{j=0}^{l-1} (-1)^j \binom{k}{j} + (-1)^l \binom{k}{l} = (-1)^{l-1} \binom{k-1}{l-1} + \\ &\quad + (-1)^l \left(\binom{k-1}{l} + \binom{k-1}{l-1} \right) = (-1)^l \binom{k-1}{l} \; . \end{aligned}$$

Let $h \in \mathbb{N}_0$. It is easy to see that if $m, n \in \mathbb{N}$ have $\mathrm{sq}(m) = \mathrm{sq}(n)$ then $(\mu_i * \mathbf{1})(m) = (\mu_i * \mathbf{1})(n)$ for $i = 0, 1$. Thus it suffices to consider only squarefree $n \in \mathbb{N}$, $\mathrm{sq}(n) = n$ and $\omega(n) = k \in \mathbb{N}_0$. Then for $i = 0, 1$ the identity gives that

$$(\mu_i * \mathbf{1})(n) = \sum_{d \mid n} \mu(d) \cdot \chi_{2h+i}(d) = \sum_{j=0}^{2h+i} (-1)^j \binom{k}{j} = (-1)^{2h+i} \binom{k-1}{2h+i} .$$

For $n = 1$ and $i = 0, 1$ the definition of μ_i yields that $(\mu_i * \mathbf{1})(1) = 1 = 1_A(1)$ and both stated inequalities hold as equalities. Let $n > 1$ and $k = \omega(n) \geq 1$. For $i = 1$, resp. $i = 0$, we indeed have $(\mu_1 * \mathbf{1})(n) = -\binom{k-1}{2h+1} \leq 0 = 1_A(n)$, resp. $(\mu_0 * \mathbf{1})(n) = \binom{k-1}{2h} \geq 0 = 1_A(n)$. □

The following is Corollary 4.2 in [12]; $\mathbb{P} = \{2, 3, 5, \dots\}$ is the set of primes, $(m, n) = 1$ says that m and n are coprime and μ is the Möbius function.

Corollary 14 *$y \geq 2$, $\mathcal{A} \subset \mathbb{Z}$ is a finite set of integers, $P \subset \mathbb{P}$, $A_d = |d\mathbb{Z} \cap \mathcal{A}|$ (for $d \in \mathbb{N}$), $P(y)$ is the product of the primes $p \in P$ with $p \leq y$ and*

$$S(\mathcal{A}, P, y) = |\{a \in \mathcal{A} \mid (a, P(y)) = 1\}|.$$

Then for every $h \in \mathbb{N}_0$,

$$\sum_{\substack{d \mid P(y) \\ \omega(d) \leq 2h+1}} \mu(d) A_d \leq S(\mathcal{A}, P, y) \leq \sum_{\substack{d \mid P(y) \\ \omega(d) \leq 2h}} \mu(d) A_d.$$

Proof. These are instances of the above mentioned Bonferroni inequalities. □

The following is Theorem 4.3 in [12]. In it $P^-(n)$ denotes the smallest prime dividing n; $P^-(1) := +\infty$.

Theorem 15 *If $x^{1/(10 \log \log x)} \geq y \geq 2$ then*

$$|\{n \leq x \mid P^-(n) > y\}| = x\big(1 + O(1/(\log y)^2)\big) \prod_{p \leq y} \left(1 - \frac{1}{p}\right).$$

The following is Theorem 4.4 (Fundamental lemma of the combinatorial sieve) in [12]. It is obtained by Brun's method with the above weights μ_i. The notation y, $\mathcal{A}$, P, $P(y)$, A_d and $S(\mathcal{A}, P, y)$ is as in Corollary 14.

Theorem 16 *Let $w \colon \mathbb{N} \to [0, +\infty)$ be multiplicative, $X \in \mathbb{R}$, let $\kappa, \lambda > 0$ and for any $d \mid P(y)$ let $R_d := A_d - Xw(d)/d$. If for any $\xi \geq \eta \geq 2$ one has that*

$$\prod_{\eta \leq p \leq \xi} \frac{1}{1 - w(p)/p} < \left(\frac{\log \xi}{\log \eta}\right)^{\kappa} \left(1 + \frac{\lambda}{\log \eta}\right)$$

then the asymptotics

$$S(\mathcal{A},\, P,\, y) = X \prod_{\substack{p\in P \\ p\le y}} \left(1 - \frac{w(p)}{p}\right)\bigl(1 + O(u^{-u/2})\bigr) + O\biggl(\sum_{d\le y^u,\, d\,|\,P(y)} |R_d|\biggr)$$

holds uniformly in $\mathcal{A}$*,* X*,* y *and* $u \ge 1$.

The following are Theorem 4.5 (Brun) and Corollary 4.6 in [12].

Theorem 17 *There is a constant* $c > 0$ *such that for every* $x \ge 3$*,*

$$|\{p \le x \mid p+2 \text{ is prime}\}| \le \frac{cx(\log\log x)^2}{(\log x)^2}.$$

Corollary 18 *We have*

$$\sum_{p,\, p+2\in\mathbb{P}} \frac{1}{p} < \infty.$$

In contrast, $\sum_p \frac{1}{p} = \infty$ because $\sum_{p\le x} \frac{1}{p} = \log\log x + O(1)$ by Theorem 20 in the previous lecture. But V. Brun is more precise in the title of his article [3], the series of reciprocals of prime twins is convergent or finite. To this day nobody was able to confirm the conjecture that the set of prime twins $p, p+2 \in \mathbb{P}$ is infinite.

We leave Brun's sieve and proceed to so called *large sieve* (bol'shoe resheto) which was invented by Yuri V. Linnik (1915–1972) in [9] in 1941. We begin with the analytic form of the large sieve. The following is Theorem 4.7 (Montgomery & Vaughan; Selberg) in [12]; the first reference is to the article [10]. First we introduce some notation. With $\alpha \in \mathbb{R}$, $M, N \in \mathbb{N}_0$ and $(a_n) \subset \mathbb{C}$ $(n = 0, 1, \dots)$, we consider the trigonometric polynomial

$$S(\alpha) := \sum_{M<n\le M+N} a_n \cdot \mathrm{e}(n\alpha)$$

where $\mathrm{e}(u) = \exp(2\pi i u)$, $u \in \mathbb{R}$. For $\delta > 0$ a tuple of real numbers is δ*-spaced* if any two distinct elements of it have distance $\ge \delta$.

Theorem 19 *Let* $\delta > 0$ *and* $(\alpha_1, \dots, \alpha_R) \subset \mathbb{R}$*,* $R \in \mathbb{N}$*, be a* δ*-spaced tuple. Then, with the above notation,*

$$\sum_{i=1}^{R} |S(\alpha_i)|^2 \le \bigl(N + \delta^{-1} - 1\bigr) \sum_{M<n\le M+N} |a_n|^2.$$

The following Lemmas 4.8 and 4.9, Corollary 4.10 and Lemma 4.11 in [12] are tools used in the proof of Theorem 4.7 (here Theorem 19).

Lemma 20 *Let* $N, R \in \mathbb{N}$*,* $(c_{nr}) \in \mathbb{C}^{N\times R}$ *and* $D \in \mathbb{R}$*. The following claims are equivalent.*

1. *For any* $(x_n) \in \mathbb{C}^N$*,* $\sum_r |\sum_n c_{nr} x_n|^2 \le D \sum_n |x_n|^2$*.*
2. *For any* $(x_n) \in \mathbb{C}^N$ *and* $(y_r) \in \mathbb{C}^R$*,* $|\sum_{n,r} x_n y_r|^2 \le D \sum_n |x_n|^2 \sum_r |y_r|^2$*.*
3. *For any* $(y_r) \in \mathbb{C}^R$*,* $\sum_n |\sum_r c_{nr} y_r|^2 \le D \sum_r |y_r|^2$*.*

The trigonometric polynomials $S(\alpha)$ and their arguments α and coefficients a_n are as above.

Lemma 21 *Let* $(\alpha_r) \in \mathbb{R}^R$ *with* $R \in \mathbb{N}$ *and let* $b_n > 0$ *for* $M < n \le M+N$ *with* $M, N \in \mathbb{N}_0$ *and* $B > 0$ *be real numbers. The following claims are equivalent.*

1. *For any* $a_n \in \mathbb{C}$*,* $\sum_{r=1}^R |S(\alpha_r)|^2 \le B \sum_{M<n\le M+N} |a_n|^2/b_n$*.*
2. *For any* $y_r \in \mathbb{C}$*,* $\sum_{M<n\le M+N} b_n \big| \sum_{r=1}^R y_r \cdot \mathrm{e}(n\alpha_r)\big|^2 \le B \sum_{r=1}^R |y_r|^2$*.*

Corollary 22 *Suppose that* $b_n \ge 0$ *for* $n \in \mathbb{Z}$*, and even* $b_n > 0$ *for* $M < n \le N$ *with* $M, N \in \mathbb{N}_0$*, and* $B > 0$ *are real numbers and that* $B(\alpha) = \sum_{n\in\mathbb{Z}} b_n \cdot \mathrm{e}(n\alpha)$ *is a convergent Fourier series. Let* $R \in \mathbb{N}$*. If for any* $y_r \in \mathbb{C}$ *the inequality*

$$\sum_{r,s=1}^{R} y_r \overline{y_s} B(\alpha_r - \alpha_s) \le B \sum_{r=1}^{R} |y_r|^2$$

holds, then for any $a_n \in \mathbb{C}$ *also the inequality*

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \le B \sum_{M<n\le M+N} |a_n|^2/b_n$$

holds.

Recall that a function $F\colon \mathbb{C} \to \mathbb{C}$ is called *entire* if for every $z_0 \in \mathbb{C}$ the derivative

$$F'(z_0) = \lim_{z\to z_0} \frac{F(z) - F(z_0)}{z - z_0} \in \mathbb{C}$$

exists. The function $\mathrm{sgn}\colon \mathbb{R} \to \{-1, 0, 1\}$ has values $\mathrm{sgn}(x) = -1$ for $x < 0$, $\mathrm{sgn}(0) = 0$ and $\mathrm{sgn}(x) = 1$ for $x > 0$. By $\mathrm{im}(z) = b$ we denote the imaginary part of $z = a + bi \in \mathbb{C}$.

Lemma 23 $F(z) = (\frac{1}{\pi}\sin(\pi z))^2 \big(\sum_{n\ge 0}(z-n)^{-2} - \sum_{n\ge 1}(z+n)^{-2} + \frac{2}{z}\big)$ *is an entire function with the properties that* $F(0) = 1$*,* $F(x) \ge \mathrm{sgn}(x)$ *for* $x \in \mathbb{R}$*,* $F(z) \ll \exp(2\pi \cdot |\mathrm{im}(z)|)$ *(for* $z \in \mathbb{C}$*) and*

$$\int_{-\infty}^{+\infty} \big(F(x) - \mathrm{sgn}(x)\big)\, \mathrm{d}x = 1.$$

We proceed to the arithmetic form of the large sieve. The following are Theorem 4.12 and Corollary 4.13 (Arithmetic large sieve) in [12]. As before we have trigonometric polynomials

$$S(\alpha) = \sum_{M<n\le M+N} a_n \cdot \mathrm{e}(n\alpha)$$

where $\alpha \in \mathbb{R}$, $M, N \in \mathbb{N}_0$ and $a_n \in \mathbb{C}$. For any prime p let $w(p)$ be the number of $h \in \mathbb{N}_0$ with $h < p$ and such that $a_n = 0$ for any $n \equiv h \pmod p$. We define for any $q \in \mathbb{N}$ the quantity

$$g(q) := \mu(q)^2 \prod_{p\,|\,q} \frac{w(p)}{p - w(p)}$$

(we assume that $S(\alpha)$ is not identically 0 and thus $w(p) < p$ for every p).

Theorem 24 *With this notation we have for any $q \in \mathbb{N}$ that*

$$\Bigg|\sum_{M<n\le M+N} a_n\Bigg|^2 \cdot g(q) \le \sum_{\substack{a=1\\(a,\,q)=1}}^{q} |S(a/q)|^2.$$

Corollary 25 *Let $Q \in \mathbb{N}$, $L = \sum_{q=1}^{Q} g(q)$ where $g(q)$ is as above and let $a_n \in \mathbb{C}$ for $M < n \le M + N$ with $M, N \in \mathbb{N}_0$. Then*

$$\Bigg|\sum_{M<n\le M+N} a_n\Bigg|^2 \le \frac{N - 1 + Q^2}{L} \sum_{M<n\le M+N} |a_n|^2.$$

Finally, the following is Theorem 4.14 in [12].

Theorem 26 *Let $M, N \in \mathbb{N}_0$, $a_n \in \mathbb{C}$ for $M < n \le M + N$ and for any prime p and $h \in \mathbb{N}_0$ with $h < p$ let*

$$S(p,\,h) = \sum_{\substack{M<n\le M+N\\ n\equiv h \pmod p}} a_n \quad \text{and} \quad S(0) = \sum_{h=0}^{p-1} S(p,\,h).$$

Then for any $Q \in \mathbb{N}$,

$$\sum_{p\le Q} p \sum_{h=0}^{p-1} \big|S(p,\,h) - S(0)/p\big|^2 \le (N - 1 + Q^2) \sum_{M<n\le M+N} |a_n|^2.$$

In the next lecture we will continue with applications of the large sieve and with Selberg's sieve.

References

[1] V. Brun, Sur les nombres premiers de la forme $ap + b$, *Arkiv for Math. og Naturvid.* B **34** (1917), n° 14, 9 pp.

[2] V. Brun, Le crible d'Ératosthène et le théorème de Goldbach, *C. R. Acad. Sci. Paris* **168** (1919), 544–546

[3] V. Brun, La série $1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + 1/41 + 1/43 + 1/59 + 1/61 + \ldots$ où les dénominateurs sont nombres premiers jumeaux est convergente ou finie, *Bull. Sci. Math.* **43** (1919), 100–104; 124–128

[4] V. Brun, Das Sieb des Eratosthenes, *5 Scand. Math. Kongr., Helsingfors* (1922), 197–203

[5] V. Brun, Untersuchungen über das Siebverfahren des Eratosthenes, *Jahresber. Deutsch. Math.-Verein* **33** (1924), 81–96

[6] L. Dirichlet, Über die Bestimmung der mittleren Werthe in der Zahlentheorie, *Math. Abhandl. Königl. Akad. Wiss.* Berlin (1849), 69–83

[7] M. N. Huxley, Exponential sums and lattice points, *Proc. London Math. Soc* **87** (2003), 591–609

[8] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig 1909

[9] Ju. V. Linnik, Bol'shoe "resheto", *Dokl. Akad. Nauk* **30** (1941), 292–294 (Large "sieve")

[10] H. L. Montgomery and R. C. Vaughan, On the large sieve, *Mathematika* **20** (1973), 119–134

[11] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge University Press, Cambridge, UK 2007

[12] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, AMS, Providence, RI 2015 (Third Edition)

[13] A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin 1963