TOPICS IN NUMBER THEORY - EXERCISE SHEET III

École Polytechnique Fédérale de Lausanne

***Exercise 1* (The Arithmetic Large Sieve).** — *Let $N \geq 1$ and $\mathcal{M}$ be a set of integers contained in $[1, N]$. Let also $\mathcal{P}$ be a finite set of prime numbers. For each $p \in \mathcal{P}$, let $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$ be a set of residue classes modulo p and set $\Omega = (\Omega_p)_{p\in\mathcal{P}}$. Define*

$$S(\mathcal{M}, \mathcal{P}, \Omega) = \{m \in \mathcal{M}, \forall p \in \mathcal{P} \;\; m \pmod{p} \notin \Omega_p\},$$

and

$$Z(a) = \sum_{n\in S(\mathcal{M},\mathcal{P},\Omega)} a_n,$$

for any sequence $a = (a_n)_{n\leq N}$ of complex numbers. Assume that $\omega(p) = |\Omega_p| < p$ for every $p \in \mathcal{P}$. Prove that for any $Q \geq 1$, we have

$$|Z(a)|^2 \leq (N + Q^2)H^{-1} \sum_{n\in S(\mathcal{M},\mathcal{P},\Omega)} |a_n|^2,$$

where

$$H = \sum_{q\leq Q} h(q),$$

where h is the multiplicative function supported on squarefree integers with prime divisors in $\mathcal{P}$ which is defined by

$$h(p) = \frac{\omega(p)}{p - \omega(p)}.$$

Steps. — (I) For $\alpha \in \mathbb{R}$, let

$$S(\alpha) = \sum_{n\in S(\mathcal{M},\mathcal{P},\Omega)} a_n e(\alpha n),$$

where $e(x) = e^{2\pi ix}$. Start by proving that for any squarefree integer q, we have

$$h(q)|S(0)|^2 \leq \sideset{}{^*}\sum_{a \pmod{q}} \left| S\left(\frac{a}{q}\right)\right|^2,$$

where the symbol $*$ indicates that the summation is restricted to residue classes a which are coprime to q. Reason by induction on the number of prime factors of q.

(II) Use the additive large sieve inequality to conclude.

***Exercise 2* (On Twin Primes).** — *Let $\mathcal{P}_2$ be the set of prime numbers p such that $p-2$ is also prime and let $\pi_2(x)$ be the number of $p \in \mathcal{P}_2$ such that $p \leq x$. Prove that*

$$\pi_2(x) \ll \frac{x}{(\log x)^2}.$$

Deduce that

$$\sum_{p \in \mathcal{P}_2} \frac{1}{p} \ll 1.$$

***Exercise 3* (A Theorem of Linnik on least quadratic non-residues)**

For q a prime number, let $n(q)$ be the least quadratic non-residue modulo q. Let $\varepsilon > 0$ be fixed and $N \geq 1$. Prove that the number of primes $q \leq N$ such that $n(q) > N^{\varepsilon}$ is bounded by a constant depending only on ε.

***To go further* (A Theorem of Serre on rational points on diagonal conics)**

The following statement is also a consequence of the Arithmetic Large Sieve. For $a, b, c \geq 1$, let $\mathcal{C}_{a,b,c}$ be the conic defined in $\mathbb{P}^2(\mathbb{Q})$ by the equation

$$ax^2 + by^2 = cz^2,$$

and for $B \geq 1$, let

$$N(B) = \#\{(a,b,c) \in \mathbb{Z}^3 \cap [1,B]^3, \mathcal{C}_{a,b,c}(\mathbb{Q}) \neq \emptyset\}.$$

We have

$$N(B) = o(B^3).$$

***Exercise 4* (The Bombieri-Vinogradov Theorem for the Möbius function)**

Let $A > 0$ be fixed. Prove that there exists a constant $B > 0$ depending on A such that

$$\sum_{q \leq x^{1/2}/(\log x)^B} \max_{a \pmod q} \left| \sum_{\substack{n \leq x \\ n = a \pmod q}} \mu(n) \right| \ll \frac{x}{(\log x)^A},$$

where the maximum is taken over integers a coprime to q, and where the constant involved in the notation $\ll$ may depend on A.

Steps. — (I) Start by proving that the Möbius function satisfies the following Siegel-Walfisz condition. For any $A > 0$, and for $a, q \geq 1$ two coprime integers,

$$\sum_{\substack{n \leq x \\ n = a \pmod q}} \mu(n) \ll \frac{x}{(\log x)^A}.$$

(II) Prove that for $y, z \geq 1$ and for $n > \max(y,z)$, we have

$$\mu(n) = -\sum_{\substack{ab|n \\ a \leq y, b \leq z}} \mu(a)\mu(b) + \sum_{\substack{ab|n \\ a > y, b > z}} \mu(a)\mu(b).$$

(III) Follow the steps of the proof of the Bombieri-Vinogradov Theorem.

***Exercise 5* (The Barban-Davenport-Halberstam Theorem)**
For $a, q \geq 1$ two coprime integers, we set as usual

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n = a \pmod q}} \Lambda(n).$$

Let $A > 0$ be fixed. Prove that there exists a constant $B > 0$ depending on A such that

$$\sum_{q \leq x/(\log x)^B} \sideset{}{^*}\sum_{a \pmod q} \left(\psi(x; q, a) - \frac{x}{\varphi(q)} \right)^2 \ll \frac{x^2}{(\log x)^A},$$

where the constant involved in the notation $\ll$ may depend on A.

Steps. — (I) Rewrite the left-hand side using Dirichlet characters.

(II) Use the Siegel-Walfisz Theorem and the multiplicative large sieve inequality to conclude.

***Exercise 6* (The Titchmarsh divisor problem).** — *Let τ denote the divisor function. Prove that there exists a constant $c > 0$ such that*

$$\sum_{p \leq x} \tau(p-1) = cx + O\left(\frac{x \log \log x}{\log x} \right).$$

Steps. — (I) Start by using the fact that if $n \geq 1$ is not a square then

$$\tau(n) = 2 \sum_{\substack{d \mid n \\ d \leq \sqrt{n}}} 1.$$

(II) Use the Brun-Titchmarsh Theorem and the Bombieri-Vinogradov Theorem to conclude.

Pierre Le Boudec - *Fall 2014*

École Polytechnique Fédérale de Lausanne