# TOPICS IN NUMBER THEORY - EXERCISE SHEET II 

École Polytechnique Fédérale de Lausanne

Exercise 1 (The Pólya-Vinogradov inequality). - Let $q \geq 1$ be an integer and let $\chi$ be a non-trivial Dirichlet character modulo $q$. Let also $H, N \geq 1$. Prove that

$$
\sum_{n=N+1}^{N+H} \chi(n) \ll q^{1 / 2} \log q
$$

Steps. - (I) Prove that it suffices to deal with the case where $\chi$ is a primitive character modulo $q$.
(II) If $\chi$ is a primitive character modulo $q$, recall that

$$
\tau_{\chi}(n)=\tau_{\chi}(1) \overline{\chi(n)}
$$

where the Gauss sum $\tau_{\chi}(n)$ is defined by

$$
\tau_{\chi}(n)=\sum_{a(\bmod q)} \chi(a) e\left(\frac{a n}{q}\right)
$$

where $e(x)=e^{2 \pi i x}$.

Exercise 2 (On the least quadratic non-residue). - Let $q$ be prime and let $n(q)$ be the least quadratic non-residue modulo $q$. Prove that $n(q) \ll q^{1 / 2} \log q$.
To go further. - Recall that the Generalized Riemann Hypothesis implies that $n(q) \ll(\log q)^{4}$. Unconditionally, one can prove that $n(q) \ll q^{1 / 4 e^{1 / 2}+\varepsilon}$ for any fixed $\varepsilon>0$. What is the bound we obtain if we use Lemma 1 given in Exercise 5?

Exercise 3 (The Hadamard three-lines Theorem). - Let $\sigma_{1}, \sigma_{2}$ be two real numbers such that $\sigma_{1}<\sigma_{2}$. Let also $f$ be a holomorphic function of finite order in the strip $\left\{z \in \mathbb{C}, \sigma_{1} \leq \Re(z) \leq \sigma_{2}\right\}$. Suppose that the quantities

$$
M(\sigma)=\sup _{\Re(z)=\sigma}|f(z)|
$$

exist for $\sigma=\sigma_{1}$ and $\sigma=\sigma_{2}$. Then, for $\sigma_{1} \leq \sigma \leq \sigma_{2}$, $M(\sigma)$ is well-defined. Moreover, $\log M(\sigma)$ is a convex function on $\sigma_{1} \leq \sigma \leq \sigma_{2}$. In other words, for $0 \leq u \leq 1$, we have

$$
M\left(u \sigma_{1}+(1-u) \sigma_{2}\right) \leq M\left(\sigma_{1}\right)^{u} M\left(\sigma_{2}\right)^{1-u}
$$

Steps. - (I) By considering the function $z \mapsto m f(z) e^{\lambda z}$ where

$$
m=\left(\frac{M\left(\sigma_{2}\right)^{\sigma_{1}}}{M\left(\sigma_{1}\right)^{\sigma_{2}}}\right)^{1 /\left(\sigma_{2}-\sigma_{1}\right)}
$$

and

$$
\lambda=\frac{1}{\sigma_{2}-\sigma_{1}} \log \left(\frac{M\left(\sigma_{1}\right)}{M\left(\sigma_{2}\right)}\right),
$$

check that it suffices to prove the result for $M\left(\sigma_{1}\right)=M\left(\sigma_{2}\right)=1$.
(II) To deal with the case $M\left(\sigma_{1}\right)=M\left(\sigma_{2}\right)=1$, use the Maximum Modulus Principle.

## To go further (The Hadamard three-circles Theorem)

It is easy to check that the following result follows from Exercise 3.
Let $r_{1}, r_{2}$ be two real numbers such that $r_{1}<r_{2}$. Let also $f$ be a holomorphic function in the annulus $\left\{z \in \mathbb{C}, r_{1} \leq|z| \leq r_{2}\right\}$. For $r_{1} \leq r \leq r_{2}$, define

$$
M(r)=\sup _{|z|=r}|f(z)| .
$$

Then $\log M(r)$ is a convex function of $\log r$ on $r_{1} \leq r \leq r_{2}$.
To go further (The Phragmén-Lindelöf Principle). - In Exercise 4, we will make use of the following generalization of the result of Exercise 3.

Let $\sigma_{1}, \sigma_{2}$ be two real numbers such that $\sigma_{1}<\sigma_{2}$. Let also $f$ be a holomorphic function of finite order in the strip $\left\{z \in \mathbb{C}, \sigma_{1} \leq \Re(z) \leq \sigma_{2}\right\}$. Suppose that we have the bounds

$$
\left|f\left(\sigma_{j}+i t\right)\right| \leq M_{j}(1+|t|)^{\alpha_{j}}
$$

for $j=1,2$, and for some $M_{1}, M_{2} \in \mathbb{R}_{\geq 0}$ and $\alpha_{1}, \alpha_{2} \in \mathbb{R}$. Then, for $0 \leq u \leq 1$, we have

$$
\left|f\left(u \sigma_{1}+(1-u) \sigma_{2}+i t\right)\right| \leq M_{1}^{u} M_{2}^{1-u}(1+|t|)^{\alpha_{1} u+\alpha_{2}(1-u)}
$$

## Exercise 4 (Convexity bounds for Dirichlet $L$-functions)

Let $\chi$ be a Dirichlet character modulo $q$, and let $\delta, \varepsilon>0$ be fixed. Prove that we have

$$
L(\chi, \sigma+i t) \ll 1,
$$

uniformly in $q$ and $t$, in the region $\sigma \geq 1+\delta$. Prove that this bound implies that

$$
L(\chi, \sigma+i t) \ll(q(1+|t|))^{1 / 2-\sigma},
$$

for $\sigma \leq-\delta$. Deduce that

$$
L(\chi, \sigma+i t) \ll(q(1+|t|))^{1 / 2-\sigma / 2+\varepsilon},
$$

for $0 \leq \sigma \leq 1$.
To go further (Terminology). - The upper bounds

$$
L(\chi, \sigma+i t) \ll(q(1+|t|))^{1 / 2-\sigma / 2+\varepsilon},
$$

in the region $0 \leq \sigma \leq 1$, are called the convexity bounds for Dirichlet L-functions. Any bounds improving upon these are called subconvexity bounds. Exercise 5 gives examples of such bounds.

Exercise 5 (Subconvexity bounds for Dirichlet L-functions)
In this exercise, we assume that we know the following result.
Lemma 1. - Let $\varepsilon>0$ be fixed. Let $q \geq 1$ be an integer and let $\chi$ be a non-trivial Dirichlet character modulo $q$. Let also $H, N \geq 1$. We have the bound

$$
\sum_{n=N+1}^{N+H} \chi(n) \ll H^{1 / 2} q^{3 / 16+\varepsilon} .
$$

Let $\varepsilon>0$ be fixed. Prove that, for any fixed $T>0$ and $|t| \leq T$, we have the subconvexity bounds

$$
L(\chi, \sigma+i t) \ll q^{(4-5 \sigma) / 8+\varepsilon},
$$

for $0 \leq \sigma \leq 1 / 2$, and

$$
L(\chi, \sigma+i t) \ll q^{(3-3 \sigma) / 8+\varepsilon},
$$

for $1 / 2 \leq \sigma \leq 1$, where the constants involved in the notation $\ll$ may depend on $T$.

École Polytechnique Fédérale de Lausanne

