Final exam

December 14, 2017. 3 hours.

In the sequel we use the notation $e(z) = \exp(2i\pi z)$, for $z \in \mathbb{C}$.

Exercise 1. Let $p > 2$ be a prime number, let $a, b \in \mathbb{Z}$, and consider the *Kloosterman sum*

$$K(a, b; p) = \sum_{x=1}^{p-1} e\left(\frac{ax + bx^{-1}}{p}\right),$$

where x^{-1} denotes the inverse of the integer x mod p in the interval $[1, p-1]$.

1. For a not divisible by p, compute the exact value of $K(a, 0; p)$.
2. In this question we show that if $p \nmid ab$ then $|K(a, b; p| \leq 2p^{3/4}$. For this purpose we define the *k-th absolute moment* of the Kloosterman sums $K(a, b; p)$:

$$M_k = \sum_{a,b \in \mathbb{F}_p^\times} |K(a, b; p)|^{2k}$$

   (a) Noting that $K(a, b; p) = K(ac, bc^{-1}; p)$ for any $c \in \mathbb{F}_p^\times$, prove that if $M_k \leq M$ for some $M \geq 0$ then:

$$(p-1)|K(a, b; p)|^{2k} \leq M\,.$$

   (b) By considering the *complete* moment $\sum_{a,b \in \mathbb{F}_p} |K(a, b; p)|^{2k}$ (meaning that the indices a and b run over the full set $\mathbb{F}_p$ of residue classes modulo p), show that

$$M_k = p^2 N_k - 2(p-1) - (p-1)^{2k}\,,$$

   where N_k is the number of solutions $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ in $(\mathbb{F}_p^\times)^k$ to the system of equations:

$$\begin{cases} x_1 + \cdots + x_k = y_1 + \cdots + y_k \\ x_1^{-1} + \cdots + x_k^{-1} = y_1^{-1} + \cdots + y_k^{-1} \end{cases}$$

   (c) Compute N_1 and deduce $M_1 = p^3 - 2p^2 + 1$.

   (d) What is the contribution to N_2 of solutions $\{(x_1, x_2), (y_1, y_2)\}$ such that $(y_1, y_2) \in \{(x_1, x_2), (x_2, x_1)\}$?

   (e) What is the contribution to N_2 of solutions $\{(x_1, x_2), (y_1, y_2)\}$ **not already counted in the previous question** and such that $x_1 + x_2 = 0$?

   (f) Show that the system of equations

$$\begin{cases} x_1 + x_2 = y_1 + y_2 \\ y_1 y_2 (x_1 + x_2) = x_1 x_2 (y_1 + y_2) \end{cases}$$

   has no solutions other than those that have already been counted and deduce the value of N_2.

   (g) Conclude, using (a) with $k = 2$.

3. Next we investigate lower bounds for $|K(a, b; p)|$.

(a) Noting that $M_2 \leq (\max_{a,b\in\mathbb{F}_p^\times} |K(a,b;p|^2)M_1$, show that there exists (a,b) such that $p \nmid ab$ and

$$|K(a,b;p| > \sqrt{2p-3}\,.$$

(b) Let $\zeta_p = \exp(2i\pi/p)$. Recall that in the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\zeta_p)$ the prime number p is totally ramified: we have the factorization $p\mathcal{O} = \mathfrak{p}^{p-1}$ where the prime ideal $\mathfrak{p}$ of $\mathcal{O}$ is principal and generated by $1-\zeta_p$. By considering $K(a,b;p)(\mathrm{mod}\mathfrak{p})$, show that $K(a,b;p) \neq 0$ if $p \nmid ab$.

(c) Fix integers a, b such that $p \nmid ab$. For $\ell \in \{1,\dots,p-1\}$ let $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be defined by $\sigma_\ell(\zeta_p) = \zeta_p^\ell$. Show that $\sigma_\ell(K(a,b;p))$ is again a Kloosterman sum and use the norm map relative to $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ to prove that

$$|K(a,b;p)| \geq \left(\frac{1}{2p^{3/4}}\right)^{p-2}.$$

4. We now turn to an application of estimates for the modulus of Kloosterman sums. Fix a prime number p and an integer x not divisible by p. We want to find positive integers m, n *as small as possible* such that $mn \equiv x(\mathrm{mod}\,p)$. Let $M(x)$ denote the minimal value for $\max(m,n)$ in such a congruence. Of course $M(x) \leq p-1$ but we can get a better upper bound for $M(x)$ as we now show.

(a) Let $q \in \mathbb{Z}_{\geq 1}$ and let $(A_n)_{n\geq 0}$ be any q-periodic sequence of complex numbers. Set $\hat{A}_m = \sum_{k=1}^q A_k e(mk/q)$. Show that for any integers $a < b$ one has

$$\left|\sum_{a<n\leq b} A_n - \frac{b-a}{q}\hat{A}_0\right| \leq (\log q) \max_{1\leq m<q} |\hat{A}_m|\,.$$

(b) Fix an integer $1 \leq M \leq p-1$ and consider the sequence (A_n) defined by $A_n = 1$ if $mn \equiv x(\mathrm{mod}\,p)$ has a solution m with $1 \leq m \leq M$, and $A_n = 0$ otherwise. Apply the previous question with $q = p$, $a = 0$, $b = M$ to show

$$\left|\#\{m,n \leq M : mn \equiv x(\mathrm{mod}\,p)\} - \frac{M^2}{p}\right| \leq (\log p) \max_{1\leq k<p} |\hat{A}_k|\,.$$

(c) Using again 4(a) to show that for $1 \leq k < p$ one has

$$|\hat{A}_k| \leq (1+\log p) \max_{1\leq m\leq p} |K(m,k;p)|\,.$$

(d) Conclude that $M(x) \leq 2p^{7/8}\log p$.

Exercise 2. In this exercise, the letter p always denotes a prime number. Let $q \geq 1$ be an integer and let a be an integer coprime to q. We consider the counting function

$$S_{a,q}(x) = \sum_{\substack{p\leq x\\ p\equiv a(\mathrm{mod}\,q)}} \frac{1}{p} \qquad (x \geq 2)\,.$$

The goal of the exercise is to prove a weak form of the prime number theorem in arithmetic progressions:

$$S_{a,q}(x) = \frac{1}{\varphi(q)}\log\log x + O_q(1) \qquad (x \geq 3)\,, \tag{1}$$

where φ is the Euler indicator function and "$O_q(1)$" is a constant depending only on q. To do so we first introduce the following series:

$$F_{a,q}(s) = \sum_{\substack{p\\ p\equiv a(\mathrm{mod}\,q)}} \frac{1}{p^s}\,, \qquad F_\chi(s) = \sum_p \frac{\chi(p)}{p^s}\,,$$

that are defined for $\sigma = \mathrm{Re}(s) > 1$ and for a fixed Dirichlet character χ modulo q.

1. In this question we show that it suffices to prove:

$$F_{a,q}(\sigma) = \frac{1}{\varphi(q)} \log \frac{1}{\sigma - 1} + O_q(1) \qquad (\sigma > 1)\,, \tag{2}$$

to deduce (1).

   (a) Let Λ denote the von Mangoldt function, which we recall can be defined using Dirichlet convolution: $\log = \Lambda * \mathbf{1}$. Use (without proof) the fact that $\sum_{1 \le n \le x} \log n = x \log x + O(x)$ to prove that $\sum_{1 \le n \le x} \frac{\Lambda(n)}{n} = \log(x) + O(1)$. Deduce that $\sum_{p \le x} \frac{\log p}{p} = \log(x) + O(1)$. (The three implied constants are absolute.)

   (b) Fix $x \ge 3$ and $\sigma_x = 1 + (\log x)^{-1}$. Explain that one can write $S_{a,q}(x) - F_{a,q}(\sigma_x)$ as $\Sigma_1 - \Sigma_2$ where Σ_1 is a sum over a subset of primes $\le x$ and Σ_2 is a sum over a subset of primes $> x$ satisfying

$$\Sigma_1 \ll 1\,, \qquad \Sigma_2 \ll 1\,.$$

   [For Σ_1 you may use the fact that $1 - \exp(-y) \le y$ for $y \in \mathbb{R}$. For Σ_2, use Abel's summation and the fact that $\pi(u) \ll u/\log u$ for $u \ge 2$.]

   (c) Conclude that (2) implies (1).

2. We next reduce (2) to the study of $F_\chi(s)$.

   (a) Explain why for $\sigma > 1$, one has $\varphi(q) F_{a,q}(\sigma) = \sum_\chi \overline{\chi(a)} F_\chi(\sigma)$, where in the sum χ runs over the set of Dirichlet characters modulo q.

   (b) Prove that for every Dirichlet character χ modulo q one has

$$F_\chi(s) = \log L(s, \chi) + O(1) \qquad (\mathrm{Re}(s) = \sigma > 1)\,,$$

   with an absolute implied constant.

3. Let χ_0 denote the principal character modulo q.

   (a) Use the analytic properties of $L(s, \chi_0)$ at $s = 1$ to show that there exists $\sigma_0(q) > 1$ such that $L(\sigma, \chi_0) > 0$ if $1 < \sigma \le \sigma_0(q)$ and

$$\log L(\sigma, \chi_0) = \log \frac{1}{\sigma - 1} + O_q(1) \qquad (1 < \sigma \le \sigma_0(q))\,.$$

   (b) Deduce $F_{\chi_0}(\sigma) = \log \dfrac{1}{\sigma - 1} + O_q(1)$ for all $\sigma > 1$.

4. Let χ be a **non-principal** Dirichlet character modulo q.

   (a) Use the analytic properties of $L(s, \chi)$ to show that for any given $\sigma_1 > 1$ we have for every σ such that $1 < \sigma \le \sigma_1$,

$$F_\chi(\sigma) = O(1)\,.$$

   (b) Extend $F_\chi(\sigma) = O(1)$ to every $\sigma > 1$.

5. Conclude that (2) (and hence (1)) holds.