Abstract

This is a translation from French of an ENS exam which I particularly loved as a student.

It gives an elementary proof, due to Selberg, of Dirichlet's theorem on primes in arithmetic progressions: Whenever a and b are coprime positive integers (why do we require that?), there exist infinitely many prime numbers of the form $ak + b$.

All it requires is basic group theory and basic material about series, as well as some skill and courage!

Dirichlet's theorem is obtained at the end of part V; part VI is an application to cyclotomic polynomials, which may be left aside.

First Mathematics Composition (Common exam ENS Ulm / Lyon, 1993) Duration: 6 hours

Nicolas Mascot*

Trinity College, Dublin

June 2, 2022

Candidates may answer any part by admitting results stated in the previous parts. It should be noted that once the results of part V have been admitted, the final part is independent from the previous parts.
The symbols m, n (respectively, x) will denote integers (respectively, a real number) $\geqslant 1$. The symbol p will always denote a *prime number*.
We denote by $v_p(n)$ the highest power[1], possibly 0, of p which divides n.
The integer $[x]$ denotes the floor[2] of x.
Whenever f, g are real-valued functions defined on a neighbourhood of $+\infty$, the notation $f = O(g)$ means that f is the product of g by a function which is bounded in a neighbourhood of $+\infty$. Similarly, whenever u_n, v_n are complex-valued sequences, the notation $u_n = O(v_n)$ means that the sequence u_n is the product of the sequence v_n and of a sequence which is bounded in a neighbourhood of $+\infty$.
The notation $\displaystyle\sum_{d|n} u_d$ denotes the sum of the u_d ranging over the integers $d \geqslant 1$ that divide n.
We denote by log the natural logarithm.
We fix once and for all a positive integer N.
We denote by $G(N)$ the multiplicative group of invertible elements of the ring $\mathbb{Z}/N\mathbb{Z}$.

Preliminary

1. Let $\sum_{n\geqslant 1} u_n$ and $\sum_{n\geqslant 1} v_n$ be two series of complex numbers. Let $U_n = \sum_{k=1}^{n} u_k$ be the partial sum. Check the identity

$$\sum_{k=1}^{n} u_k v_k = U_n v_n + \sum_{k=1}^{n-1} U_k (v_k - v_{k+1}).$$

*mascotn@tcd.ie

[1]Translator's note: Actually, the *exponent* of this highest power, so that $p^{v_p(n)} \mid n$.

[2]Translator's note: This means the largest integer $\leqslant x$.

I

Let G be a finite Abelian group whose operation is written multiplicatively. We say that a homomorphism from G to the multiplicative group $\mathbb{C}^\times$ is a *character* of G. Let χ and χ' be two characters of G. The product $\chi\chi'$ is defined by the formula

$$\chi\chi'(g) = \chi(g)\chi'(g) \text{ for } g \in G.$$

We denote by 1 the constant character of value 1. The set $\widehat{G}$ of characters of G is thus endowed with a group law whose identity element is 1.

We denote by $\widehat{\widehat{G}}$ the group of characters of $\widehat{G}$.

Finally, we denote by $\overline{\chi}$ the character which maps $g \in G$ to the conjugate $\overline{\chi(g)}$ of $\chi(g)$.

For all $x \in G$, consider the map $\phi_x \in \widehat{\widehat{G}}$:

$$\begin{array}{ccc} \widehat{G} & \longrightarrow & \mathbb{C}^\times \\ \chi & \longmapsto & \chi(x). \end{array}$$

Our first goal is to prove that the morphism

$$(*) \quad \begin{array}{ccc} G & \longrightarrow & \widehat{\widehat{G}} \\ x & \longmapsto & \phi_x \end{array}$$

is injective.

1. Let $x \in G$, $x \neq 1$, and let $\langle x \rangle$ be the subgroup of G spanned by x. Prove that there exists a character χ of $\langle x \rangle$ such that $\chi(x) \neq 1$.

2. Let F be the set of subgroups H of G containing $\langle x \rangle$ such that χ may be extended into a character of H. Prove that F contains an element G' of maximal order. Suppose $G' \neq G$. Let y be an element of G which does not lie in G'. By considering the smallest $n \geqslant 1$ such that $y^n \in G'$, whose existence you must justify, prove that χ may be extended to the subgroup spanned by G' and y. What can you conclude from this?

3. Let $\chi' \in \widehat{G}$ and $x \in G$. Compare the sums

   $$\sum_{\chi \in \widehat{G}} \chi(x) \text{ and } \sum_{\chi \in \widehat{G}} \chi\chi'(x).$$

   By suitably choosing χ', prove the formulae

   $$\sum_{\chi \in \widehat{G}} \chi(x) = 0 \text{ if } x \neq 1,$$

   $$\sum_{\chi \in \widehat{G}} \chi(x) = |\widehat{G}| \text{ if } x = 1.$$

   Similarly, prove the formulae

   $$\sum_{x \in G} \chi(x) = 0 \text{ if } \chi \neq 1,$$

   $$\sum_{x \in G} \chi(x) = |G| \text{ if } \chi = 1.$$

4. By considering the sum $\sum_{\chi,x} \chi(x)$, prove that $|G| = |\widehat{G}|$. What can you conclude about the morphism $G \longrightarrow \widehat{\widehat{G}}$ described at $(*)$?

II

You are reminded that the symbol p denotes a *prime number*.
Recall the formula $\log n! = n \log n - n + O(\log n)$.

1. Prove the identity

$$v_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right].$$

Deduce the bounds

$$\frac{n}{p} - 1 < v_p(n!) \leqslant \frac{n}{p} + \frac{n}{p(p-1)}.$$

2. By considering the expression $(1+1)^{2m+1}$, prove that $\binom{2m+1}{m} \leqslant 4^m$. Deduce the upper bound

$$\prod_{m+1<p\leqslant 2m+1} p \leqslant 4^m.$$

3. Prove the upper bound

$$\prod_{p\leqslant n} p \leqslant 4^n$$

by induction on n.

4. By considering $\log n!$, prove the estimate

$$\sum_{p\leqslant x} \frac{\log p}{p} = \log x + O(1).$$

III

From now on, by character, we mean character of $G(N)$. We say that a character $\chi \neq 1$ is *nontrivial.* We still denote by χ the map from $\mathbb{N}$ to $\mathbb{C}$ defined by $\chi(m) = \chi(m \bmod N)$ if m and N are coprime and $\chi(m) = 0$ else. We have the identity $\chi(ab) = \chi(a)\chi(b)$ for all a, b.

1. Let χ be a nontrivial character. Prove that series $\sum_{n\geqslant 1} \frac{\chi(n)}{n}$ (respectively, $\sum_{n\geqslant 1} \frac{\chi(n)\log n}{n}$) converges. We denote its sum by $L(\chi)$ (respectively, by $L_1(\chi)$).

In this part, from now on, χ is a nontrivial *real-valued* character.

2. Let $f(n) = \sum_{d|n} \chi(d)$. Prove that $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$. Deduce the lower bounds

$$f(n) \geqslant 1 \text{ if } n \text{ is a square, and } f(n) \geqslant 0 \text{ else.}$$

For $x \geqslant 0$, define $g(x) = \sum_{n\leqslant x} \frac{f(n)}{\sqrt{n}}$. How does g behave when $x \to +\infty$?

3. Prove very carefully the identity

$$g(x) = \sum_{d' \leqslant \sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x} < d \leqslant \frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{d' \leqslant \frac{x}{d}} \frac{1}{\sqrt{d'}}.$$

By a thorough analysis of the two terms of this sum, prove that the difference $g(x) - 2\sqrt{x}L(\chi)$ is bounded.

4. Prove that $L(\chi)$ does not vanish in this case.

IV

1. We denote by $\mu(n)$ the integer defined by $\mu(n) = 0$ if n is divisible by the square of a prime number, else $\mu(n) = (-1)^r$ if n admits r (non-repeated) prime factors[3]. Prove that for all $n \neq 1$, we have the identity

$$\sum_{d|n} \mu(d) = 0.$$

2. Let H be a nonzero function from $\mathbb{N}$ to $\mathbb{C}$ such that for all $m, n \in \mathbb{N}$, $H(mn) = H(m)H(n)$. Determine $H(1)$. Suppose also that F and G are functions from $[1, +\infty)$ to $\mathbb{C}$ such that

$$\forall x \in [1, +\infty),\ G(x) = \sum_{1 \leqslant k \leqslant x} F(x/k)H(k).$$

Prove the formula[4]

$$\forall x \in [1, +\infty),\ F(x) = \sum_{1 \leqslant k \leqslant x} \mu(k)G(x/k)H(k).$$

3. Let Λ be the function[5] from $[1, +\infty)$ to $\mathbb{R}$ which maps p^n to $\log p$ and which vanishes at all the real numbers which are not integers of the form p^n. Prove the formula

$$\Lambda(m) = \sum_{d|m} \mu(d) \log(m/d).$$

V

Let χ be a nontrivial character which may or may not be real-valued.

1. Let $G(x) = \sum_{1 \leqslant n \leqslant x} \frac{x}{n}\chi(n)$. Prove that $G(x) - xL(\chi)$ is bounded.

   Suppose $L(\chi) \neq 0$. By using part IV, deduce that $\sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n}$ is bounded.

2. Suppose that $L(\chi) = 0$. Define $G_1(x) = \sum_{1 \leqslant n \leqslant x} \frac{x}{n} \log\left(\frac{x}{n}\right)\chi(n)$. Prove that $G_1(x) = -xL_1(\chi) + O(\log x)$. As in the previous question, deduce that the function

$$L_1(\chi) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} + \log x$$

is bounded.

---

[3]Translator's note: μ is called the *Möbius* function.

[4]Translator's note: This is known as the *Möbius inversion formula.*

[5]Translator's note: Λ is called the *von Mangoldt function.*

3. By using part IV, prove that

$$L_1(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}=\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}+O(1).$$

4. Deduce from the above that

$$\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=\begin{cases}O(1)\text{ if }L(\chi)\neq 0,\\ -\log x+O(1)\text{ if }L(\chi)=0.\end{cases}$$

5. Let T be the number of nontrivial characters such that $L(\chi)=0$. By considering the expression

$$\sum_{\chi\in\widehat{G(N)}}\sum_{p\leqslant x}\frac{\chi(p)\log p}{p},$$

prove the estimate

$$|G(N)|\sum_{\substack{p\leqslant x\\ p\equiv 1 \bmod N}}\frac{\log p}{p}=(1-T)\log x+O(1).$$

6. Prove that $T=0$ (make the distinction between the real-valued case and the complex-valued case).

   Let ℓ be an integer which is coprime to N. By considering the sum

$$\sum_{\chi\in\widehat{G(N)}}\sum_{p\leqslant x}\overline{\chi}(\ell)\frac{\chi(p)\log p}{p},$$

   prove that[6] there exists infinitely many primes p such that $p\equiv\ell \bmod N$.

VI

Let P be a nonzero polynomial with integer coefficients. We denote by $c(P)$ the gcd of the coefficients of P.

1. Prove that if P and Q are nonzero polynomials with integer coefficients, then

$$c(PQ)=c(P)c(Q).$$

   Hint: Reduce to the case $c(P)=c(Q)=1$, and consider a prime divisor of $c(PQ)$.

2. Let ζ be an n-th root of 1. Let P_ζ be the monic polynomial[7] with coefficients in $\mathbb{Q}$ and of minimal degree that vanishes at ζ. Prove that the coefficients of P_ζ are actually integers.

   We denote by $\mathbb{Z}[\zeta]$ (respectively, $\mathbb{Q}[\zeta]$) the subring of $\mathbb{C}$ spanned by $\mathbb{Z}$ and ζ (respectively, by $\mathbb{Q}$ and ζ). Let d be the degree of P_ζ.

[6] Translator's note: This is known as *Dirichlet's theorem on primes in arithmetic progressions.*

[7] Translator's note: Such a polynomial is called a *cyclotomic polynomial.*

3. Prove that $\mathcal{B} = (1, \zeta, \zeta^2, \cdots, \zeta^d - 1)$ is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[\zeta]$.

4. Let P be a polynomial with integer coefficients. Prove that for any prime number p, there eixts a polynomial G_p with integer coefficients such that

$$P(X^p) = P(X)^p + pG_p(X).$$

Whenever $x \in \mathbb{Q}[\zeta]$, let $M(x)$ be the matrix with respect to $\mathcal{B}$ of the $\mathbb{Q}$-linear map

$$\begin{array}{ccc} \mathbb{Q}[\zeta] & \longrightarrow & \mathbb{Q}[\zeta] \\ y & \longmapsto & xy. \end{array}$$

5. By using V.7., and by considering matrices $M(x)$ for suitable $x \in \mathbb{Q}[\zeta]$, prove that if ℓ is an integer which is coprime to n, then

$$P_\zeta(\zeta^\ell) = 0.$$

6. Prove that the union of the sets

$$E_d = \left\{ \frac{k}{d} \mid 1 \leqslant k \leqslant d \text{ and } \gcd(k, d) = 1 \right\}$$

for $d \geqslant 1$ dividing n agrees with

$$\left\{ \frac{k}{n} \mid 1 \leqslant k \leqslant n \right\},$$

ad that the sets E_d for $d \geqslant 1$ dividing n are pairwise disjoint. Define

$$\Phi_n(x) = \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,n)=1}} \left(X - e^{2\pi i k/n} \right).$$

Prove the identity

$$\prod_{d|n} \Phi_d(X) = X^n - 1.$$

Deduce that $\Phi_n(x)$ has integer coefficients for all n.

7. Which conclusions can you draw about P_ζ?

END