LMS SUMMER SCHOOL 2023—SOME TOPICS IN COMPUTATIONAL NUMBER THEORY PROBLEMS

LEWIS COMBES

1. Lecture 1 - Irrational and transcendental numbers

Problem 1.1. Let $a, b \in \mathbb{Z}$. Write down quadratic integer polynomials $P_1(x)$, $P_2(x)$ such that

$$P_1(\sqrt{a}) = 0, \quad P_2(\sqrt{b}) = 0.$$

By squaring $\sqrt{a} + \sqrt{b}$ and rearranging, find a third integral polynomial $P_3(x)$ such that

$$P_3(\sqrt{a} + \sqrt{b}) = 0.$$

What do you notice about the degrees of P_1, P_2 and P_3? If you repeated the process for the algebraic numbers $\sqrt{a}$, $\sqrt[3]{b}$, what would you expect the degree of P_3 to be?

Problem 1.2. Recall the Lindemann-Weierstrass theorem: if θ is an algebraic number, then e^θ is transcendental. Use Lindemann-Weirstrass to prove the transcendence of

(i) e^2
(ii) $\log(2)$
(iii) $\cos(1)$ (hint: consider the polynomial $x^2 - 2\cos(1)x + 1$ evaluated at e^{i})

2. Lecture 2 - The Riemann Hypothesis

Problem 2.1. Using the product expansion

$$\frac{\sin(x)}{x} = \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right)$$

evaluated at x and $\mathrm{i}x$, prove (in the manner of Euler[1]) that

$$\zeta(4) = \frac{\pi^4}{90}.$$

[1] Which is to say, without worrying about technical details like convergence.

Using the same trick as above, with canny choices of cx for constants $c \in \mathbb{C}$, it is possible to write down all even values of the zeta function. What is $\zeta(8)$?

Problem 2.2. In this question, we prove the Euler product expansion of the zeta function. Recall that

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

First, compute

$$\left(1 - \frac{1}{2^s}\right) \zeta(s)$$

as a series in s^{th} powers of integers. What do you notice about these integers? Now compute

$$\left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{2^s}\right) \zeta(s).$$

Again, what do you notice? How can one continue this process to prove the Euler product formula? Where does the product converge?

Problem 2.3. Recall the zeta functional equation:

$$\zeta(s) = 2^s \pi^{s-1} \sin(\tfrac{\pi s}{2}) \Gamma(1-s) \zeta(1-s).$$

Using this, and the fact that $\Gamma(s) \neq 0$ for all $s \in \mathbb{C}$, prove the following: if ρ is a zero of ζ in the critical strip (so $0 < \mathrm{Re}(\rho) < 1$) but **not** on the critical line (so $\mathrm{Re}(\rho) \neq \frac{1}{2}$), then ζ has another zero ρ^*, which is the reflection of ρ in the critical line.

3. Lecture 3 - Dirichlet's theorem on primes in arithmetic progressions

Problem 3.1. Let $\chi : \mathbb{Z} \to \mathbb{C}$ be a **totally multiplicative function**. This means that

$$\chi(ab) = \chi(a)\chi(b)$$

for all $a, b \in \mathbb{Z}$. Define the **L-series of χ** as

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Assuming $L(\chi, s)$ converges for $\mathrm{Re}(s) > d$ for some $d \in \mathbb{R}^+$, prove that

$$L(\chi, s) = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

for $\mathrm{Re}(s) > d$.

(Hint: write $\frac{1}{1-\frac{\chi(p)}{p^s}}$ as a geometric series, then use the unique factorisation of integers.)

Problem 3.2. Fix some integer m. Let G be the set of homomorphisms $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$. Prove G is an abelian group under pointwise multiplication, i.e.

$$(f \cdot g)(a) := f(a)g(a).$$

What is the identity element of G? Why is $\cdot$ commutative? Why is it associative? What is the inverse of $f \in G$?

This group G is the **group of Dirichlet characters mod** m.

Show that the image of any $f \in G$ lies on the unit circle in $\mathbb{C}$. Show that $|G| = \phi(m)$, where ϕ is Euler's totient function, the number of elements of $\mathbb{Z}/m\mathbb{Z}$ coprime to m.

Finally, prove the following:

Lemma 3.3. Let $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then

$$\sum_\chi \chi(a) = \begin{cases} \phi(m) & \text{if } a = 1 \\ 0 & \text{else} \end{cases}$$

where the sum runs over all χ in the character group mod m.

And hence, that

Lemma 3.4. Suppose a, n are coprime to m. Then

$$\sum_\chi \chi(a)^{-1}\chi(n) = \begin{cases} \phi(m) & \text{if } n \equiv a \pmod{m} \\ 0 & \text{else} \end{cases}$$

4. Lecture 4 - Elliptic curves

Problem 4.1. Recall Diophantus' elliptic curve $6Y - Y^2 = X^3 - X$. Find a substitution $x = aX + b$, $Y = cX + d$ that puts it into *short Weierstrass form*, i.e. of the form

$$y^2 = x^3 + sx + t$$

for some $s, t \in \mathbb{Q}$.

Problem 4.2. This problem concerns the group law on an elliptic curve. Let E be the elliptic curve $y^2 = x^3 - x + 9$, and let $P = (1, 3)$. Show that P lies on E. Compute $2P$ in the following way:

(1) Compute the tangent line ℓ to E at P by implicitly differentiating the equation for E.
(2) Find the point R of E where ℓ intersects E for a third time.
(3) Find the point $2P$ by reflecting R in the x-axis.

Writing the coordinates of $2P$ as (x, y), compute the point $(x, y + 3)$.