CTNT 2020 **Computations in Number Theory Research** Álvaro Lozano-Robledo

Suggested Exercises

Mathematics is not about numbers, equations, computations, or algorithms: it is about understanding. – William Paul Thurston

LMFDB - Day 1

Exercise 1. A number field K is a finite degree field extension of $\mathbb{Q}$. The discriminant Δ_K of K over $\mathbb{Q}$ (which is, more precisely, the discriminant $\Delta(\mathcal{O}_K)$ of the ring of integers $\mathcal{O}_K$ of K) serves as a measure, in a sense, of the arithmetic complexity of the field K (in that it keeps track of the primes of $\mathbb{Z}$ that ramify in $\mathcal{O}_K$). For example, $K = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ is a finite extension of $\mathbb{Q}$ of degree 2 (we say $K/\mathbb{Q}$ is a quadratic extension), and the discriminant of K over $\mathbb{Q}$ is -4. There is one quadratic extension of $\mathbb{Q}$ of discriminant -3, and this is the smallest discriminant (in absolute value) among all of the quadratic extensions of $\mathbb{Q}$.

Your task: Use the LMFDB to build a table with the number fields of smallest discriminant for each degree $d = 2, \ldots, 10$.

Exercise 2. Let G be a finite group. The inverse Galois problem is the following open problem: for each finite group G, is there a finite Galois extension K of $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$? For example, the extension $\mathbb{Q}(i)/\mathbb{Q}$ has Galois group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Your task: Use the LMFDB to build a table with all the finite groups G (up to isomorphism) up to order 10, and then find Galois extensions $K/\mathbb{Q}$ of the smallest possible discriminant such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. (Hint: you can also use groupnames.org to find the list of groups you need.)

Exercise 3. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. The Mordell–Weil theorem says that $E(\mathbb{Q})$, the set of rational points on E (points on E with rational coefficients), has the structure of a finitely generated abelian group, and therefore $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$, where $E(\mathbb{Q})_{\mathrm{tors}}$ is a finite abelian group formed by the points of finite order, and $R_{E/\mathbb{Q}} \geq 0$ is an integer called the rank and it represents the number of generators of the group of infinite order. A theorem of Mazur (which proves a conjecture of Levi and Ogg) shows that $E(\mathbb{Q})_{\mathrm{tors}}$ is one of 15 groups (up to isomorphism). The conductor of an elliptic curve measures, in a sense, the arithmetic complexity of an elliptic curve. For example, the curve $E : y^2 + xy + y = x^3 - 2731x - 55146$ has conductor 14 with $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ and $R_{E/\mathbb{Q}} = 0$.

Your task: Use the LMFDB to build a table of elliptic curves with each of possible 15 torsion groups (up to isomorphism) with the smallest possible conductor.

Your more challenging task: Use the LMFDB to build a table of elliptic curves with each of possible 15 torsion groups (up to isomorphism) with the smallest possible *discriminant* in the tables.

Another task: Find elliptic curves with each possible torsion group and rank, that appear in the LMFDB, with the smallest possible conductor.

Exercise 4. The primes that divide the conductor of an elliptic curve are called the *bad primes* of $E/\mathbb{Q}$ (that is, primes of bad reduction). If the conductor E is a prime number, then E has bad reduction exactly at one prime.

Your task: Use the LMFDB to build a table of elliptic curves with prime conductor (and smallest possible discriminant among curves in the tables with said conductor).

SAGEMATH - Day 2

Exercise 5. Let a, N be positive integers that are relatively prime. By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes $p \equiv a \bmod N$.

1. Write a function $\pi_{a,N}(X)$ in SageMath that counts how many primes $p \equiv a \bmod N$ there are up to X (so your function is analogous to `prime_pi` but only counting primes in a congruence class). You can find how to build functions here.

2. Plot your prime counting function $\pi_{1,5}(X)$ for $(a, N) = (1, 5)$ and up to $X = 10000$.

3. Plot the quotient of $\pi_{1,5}(X)$ and $x/\log(x)$. The limit is known. Can you estimate the limit?

Exercise 6. Let $\pi'(X) = \sum_{n=2}^{\lfloor X \rfloor} \frac{1}{\log(n)}$. Write a Sage function that gives the values of $\pi'(X)$ and plot it together with the prime-counting function $\pi(X)$ and $x/\log(x)$ (in different colors!). Draw a separate plot of the quotients $\pi(X)/(x/\log x)$ and $\pi(X)/\pi'(X)$.

Exercise 7. Let $\mathrm{Li}(X) = \int_2^{\lfloor X \rfloor} \frac{1}{\log t} dt$. Write a Sage function that gives the values of $\mathrm{Li}(X)$ and plot it together with the prime-counting function $\pi(X)$, our $\pi'(X)$ from the previous problem, and $x/\log(x)$ (all in different colors!). What function seems to be the best approximation of $\pi(X)$? Draw a separate plot of the quotients $\pi(X)/(x/\log x)$ and $\pi(X)/\pi'(X)$ and $\pi(X)/\mathrm{Li}(X)$.

Exercise 8. Can you find elliptic curves E and E' over a finite field $\mathbb{F}_p$ (resp. $\mathbb{F}_q$) such that

1. $E(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$,

2. $E'(\mathbb{F}_q)[5] \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Here $E(\mathbb{F}_p)[n]$ is the n-torsion subgroup of $E(\mathbb{F}_p)$, so it is the subgroup of all points in $E(\mathbb{F}_p)$ of order dividing n.

Exercise 9. Let $\phi_n(x)$ be the *polynomial*

$$(x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \cdots + x + 1.$$

When $n = p$ is prime, the polynomial $\phi_p(x)$ is irreducible over $\mathbb{Q}$ (can you prove this?). Let $p = 7$, let $q \neq 7$ be another prime, and let $\mathbb{Q}_q$ be the field of q-adic numbers, and let $\mathbb{Q}_q[x]$ be the polynomial ring in one variable with coefficients in $\mathbb{Q}_q$. Depending on q, the polynomial $\phi_7(x)$ factors in different ways in $\mathbb{Q}_q[x]$ (irreducible, product of two cubics, etc).

Your taks: use Sage to find primes such that $\phi_7(x)$ factors in different ways over $\mathbb{Q}_q[x]$. Can you characterize the primes that make $\phi_7(x)$ factor in each possible way over $\mathbb{Q}_q[x]$?

Exercise 10. Let $F = \mathbb{Q}(\zeta_{32})$ be the 32-th cyclotomic field. Use the Galois group functionality in Sage to describe all the quadratic extensions K of $\mathbb{Q}$ that are contained in F. That is, find all $K/\mathbb{Q}$ quadratic with $K \subseteq F$. How many are there? Then, find all the cyclic quartic extensions $L/\mathbb{Q}$ contained in F, that is, find all $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ such that $L \subseteq F$.

MAGMA - Day 3

Note: your institution may be able to provide a Magma student license for you, thanks to the Simons Foundation Magma agreement (click here). Otherwise, you can use the Magma online calculator (click here).

Exercise 11. Let $n \geq 1$ be an integer. We will say that an n-tuples of (odd) primes $T = (p_1, \ldots, p_n)$ is a Legendre n-tuple if $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_i}\right) = 1$ for all $1 \leq i < j \leq n$, where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre quadratic residue symbol.

1. Show that, for any fixed $n \geq 2$, there are infinitely many Legendre n-tuples.
2. Use Magma to find 10 Legendre n-tuples, for each of $n = 2, 3, 4, 5$.
3. Let n be fixed, and let $T = (p_1, \ldots, p_n)$ be a Legendre n-tuple. We define the height of T by $\text{ht}(T) = |p_1 \cdot p_2 \cdots p_n|$. What is the Legendre 6-tuple of primes with the smallest height?

Note: these n-tuples are related to a research paper on elliptic curves.

Exercise 12. Let n be an integer with $1 \leq n \leq 15$. Use the LMFDB to find a number field K_n such that the class group of K is n, with smallest possible discrimiant (in the database). Then, use Magma to describe the ring of integers $\mathcal{O}_K$ of K, and find prime ideals (in terms of a basis of $\mathcal{O}_K$) that generate the class group $\text{Cl}(K)$. (For those n where there is more than one abelian group isomorphism class, e.g., $n = 4$, include a number field for each class.)

Exercise 13. Use Magma to find concrete examples (polynomial equations) of projective curves defined over $\mathbb{Q}$ of genus $0, 1, 2, 3, 4, 5$. (Hint: LMFDB can also be helpful here.) Can you find models that are the "smallest" in some sense? Describe your notion of "small model".

Exercise 14. If you have read Chapters 1-3 of Silverman's "The Arithmetic of Elliptic Curves", use Magma to replicate the proof of Theorem 3.1.(a) for the concrete case of $C : x^3 + y^2 = 2$ and $\mathcal{O} = (1, 1)$. That is, find a Weierstrass equation for C by computing bases of the appropriate Riemann–Roch spaces $\mathcal{L}(n \cdot \mathcal{O})$ to find a linear relation from which you can deduce the coefficients of a Weierstrass form.

MAGMA - Day 4

Exercise 15. Let $\mathbb{Q}(\mu_{3^\infty})$ be the 3-th cyclotomic tower, that is, the compositum of all cyclotomic fields $\mathbb{Q}(\zeta_{3^n})$ for $n \geq 1$, where ζ_{3^n} is a primitive 3^n-th root of unity. Let $K_{3,\infty}$ be the unique $\mathbb{Z}_3$-extension inside $\mathbb{Q}(\mu_{3^\infty})$, so that $\mathrm{Gal}(K_{3,\infty}/\mathbb{Q}) \cong \mathbb{Z}_3$, the 3-adic integers, which is a compositum of number fields K_n over $\mathbb{Q}$ such that $K_n \subseteq K_{n+1} \subseteq K_{3,\infty} \subseteq \mathbb{Q}(\zeta_{3^\infty})$ and $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}/3^n\mathbb{Z}$. Use Magma to find equations that define K_1, K_2, and K_3. (Try also to do the same for $p = 5$ instead of $p = 3$.)

Exercise 16. Let C be the hyperelliptic curve $y^2 = x^5 + x^4 + 1$ defined over $\mathbb{F}_5$. Use Magma to compute the zeta function $\zeta_C(z)$ of C, and verify the Riemann Hypothesis (in the sense of the Weil conjectures) for this zeta function.

Exercise 17. Find an elliptic curve $E/\mathbb{Q}$ of rank 0 (over $\mathbb{Q}$) and an integer d, such that the quadratic twist E^d of E has rank ≥ 3. (Note: if $E : y^2 = x^3 + Ax + B$ then E^d is given by $y^2 = x^3 + d^2Ax + d^3B$.)

Exercise 18. Find an elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/5\mathbb{Z}$ and rank ≥ 2. Then, use Magma to verify the Birch and Swinnerton-Dyer conjecture numerically for $E/\mathbb{Q}$.

Exercise 19. Find an elliptic curve $E/\mathbb{Q}$ with rank ≥ 5. Then, use Magma to verify the Birch and Swinnerton-Dyer conjecture numerically for $E/\mathbb{Q}$.