AGRA IV, 2021
T.A. SESSION: DIOPHANTINE EQUATIONS WITH FEW SOLUTIONS

Teaching Assistant: Jerson Leonardo Caro Reyes
Departamento de Matemáticas, PUC, Chile
Email address, J. Caro: jocaro@mat.uc.cl

LECTURE 1. ELLIPTIC CURVES

(1) Let E be the elliptic curve given by the equation $y^2 = x^3 + 17$. Check that $P = (-1, 4)$ and $Q = (2, 5)$ are in E, and compute $P + Q$, $2P$ and $2Q$.

(2) Let $y^2 = f(x) = x^3 + Ax^2 + Bx + C$. Prove that the 2-torsion subgroup $E(\mathbb{Q})[2]$, i.e. $P \in E(\mathbb{Q})$ such that $2P = 0$, is given as follows

$$E(\mathbb{Q})[2] = \begin{cases} \{0\} & \text{if } f \text{ has no integral solutions} \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } f \text{ has exactly one integral solutions} \\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{otherwise.} \end{cases}$$

(3) (a) Show that $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ are Euclidean domains. In particular, they are UFD's.
(b) Find the integral solutions to the Diophantine equation $y^2 = x^3 - 2$.
(c) Taking into account the previous item, show that the elliptic curve $E : y^2 = x^3 - 2$ has positive rank.

(4) (a) Consider the elliptic curve

$$E\colon y^2 = x^3 - x^2 + x.$$

Use Lutz-Nagell Theorem to compute $\#\operatorname{Tor}(E(\mathbb{Q}))$. Can we know which is this group?.
(b) Now, consider an elliptic curve $E : y^2 = x^3 + Ax^2 + Bx + C$ such that $\operatorname{Disc}(x^3 + Ax^2 + Bx + C)$ is a squarefree integer. Give an upper bound for $\#\operatorname{Tor}(E(\mathbb{Q}))$.

(5) Consider the elliptic curve $E\colon y^2 = x^3 + x^2 + x + 1$.
(i) Prove that $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \leq 1$. (**Hint:** Do $z = x + 1$ and apply Theorem 1.7).
(ii) Find some $x \in E$ with infinite order, in particular, $\operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 1$

(6) Find all the cubic triangular numbers (A cubic triangular number is a positive integer that is simultaneously cubic and triangular).

(7) Show that each of the following elliptic curves defined over $\mathbb{Q}$ has the stated torsion group:
- $y^2 = x^3 - 2$; $\{O\}$
- $y^2 = x^3 + 8$; $\mathbb{Z}/2\mathbb{Z}$
- $y^2 = x^3 + 4$; $\mathbb{Z}/3\mathbb{Z}$
- $y^2 = x^3 + 4x$; $\mathbb{Z}/4\mathbb{Z}$
- $y^2 = x^3 - 432x + 8208$; $\mathbb{Z}/5\mathbb{Z}$
- $y^2 = x^3 + 1$; $\mathbb{Z}/6\mathbb{Z}$

Elliptic curves over finite fields

(8) Consider the elliptic curve $E\colon y^2 = x^3 + x + 3$ over the field $F = \mathbb{F}_7$.
(a) For which values of $x \in \mathbb{F}_7$ is $x^3 + x + 3$ equal to a perfect square in $\mathbb{F}_7$?
(b) List $E(\mathbb{F}_7)$.
(c) Find the line through the two points $(4, 1)$ and $(6, 1)$. Find the third point of E which this line passes through. Find $(4, 1) + (6, 1)$.
(d) Show that $E(F)$ is cyclic and find a generator.

(9) Let $E_1\colon y^2 = x^3 + 2$ over the field $F = \mathbb{F}_7$. Let $E_2\colon y^2 = x^3 + 3x + 2$ over F. Find the number of points in $E_1(F)$ and in $E_2(F)$. Is $E_1(F)$ a cyclic group? Is $E_2(F)$ a cyclic group? Useful Magma commands:

```
F := GF(7);
E := EllipticCurve([F!3,2]);
P := E![F!3,2];
```

LECTURE 2. RATIONAL APPROXIMATIONS AND INTEGRAL POINTS

(1) **Dirichlet's Approximation Theorem.** Show that for any irrational $\alpha \in \mathbb{R}$, there are infinitely many rational numbers $q = a/b$, $b > 0$ such that

$$|\alpha - q| < \frac{1}{b^2}.$$

Can you improve the bound to $1/b(b+1)$?

(2) Prove Corollary 2.4.

(3) **Liouville's Theorem** Let $\alpha \in \mathbb{R}$ be an irrational algebraic number of degree d. There is a constant $c(\alpha) > 0$ depending only on α such that for every rational number $q = a/b$ with a, b coprime integers and $b > 0$ we have

$$|\alpha - q| > \frac{c(\alpha)}{b^d}.$$

Step 1: Let $P(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α scaled so that its coefficients are integers having $\gcd$ equal to 1 and the leading coefficient is positive. We let $A_\alpha \in \mathbb{Z}$ be this leading coefficient. We note that $d = \deg(P) \geq 2$. Prove that $P(q) \neq 0$, whenever $q \in \mathbb{Q}$.

Step 2: Let $q \in \mathbb{Q}$ and write $q = a/b$ as in the statement. Prove that $|P(q)| \geq 1/b^d$.

Step 3: Let $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be the roots of P, say $\alpha = \alpha_1$. Let

$$D_\alpha = \max |\alpha - \alpha_j| : j = 2, \ldots, d.$$

Prove that for every $q \in \mathbb{Q}$ satisfying $|\alpha - q| \leq 1$, we have the following inequality

$$|P(q)| \leq A_\alpha \cdot (D_\alpha + 1)^{d-1} |\alpha - q|.$$

Step 4: Let $c_\alpha = A_\alpha^{-1}(D_\alpha + 1)^{1-d}$. Prove the inequality in the statement.

(4) Find all integer solutions to $x^3 + y^3 = 7$

(5) State and prove a p-adic analogue of Liouville's theorem.

(6) State and prove an analogue of Thue's theorem, where F is only required to be square-free (and not irreducible).

(7) Formally the field of the p-adic rationals $\mathbb{Q}_p$ are the elements ξ which can be represented as follows

$$\xi = p^m(a_0 + a_1 p + \cdots + a_n p^n + \ldots),$$

with $m = \nu_p(\xi) \in \mathbb{Z}$ (the p-adic valuation), $1 \leq a_0 \leq p-1$, $0 \leq a_n \leq p-1$ for $(n = 1, 2, \cdots)$.

(a) Prove that a sequence $\{x_n\}$ converges in $\mathbb{Q}_p$ if and only if

$$\lim_{n \to \infty} \nu_p(x_{n+1} - x_n) = \infty.$$

(b) Let $x_n := 1 + p + \cdots + p^{n-1}$. Prove that in $\mathbb{Q}_p$ the sequence $\{x_n\}$ converges to $1/(1-p)$.

(c) Prove that for every $n \in \mathbb{N}$, the polynomial $x^n - p \in \mathbb{Q}_p[x]$ is irreducible in $\mathbb{Q}_p[x]$, in particular $\mathbb{Q}_p$ has at least one finite extension of an arbitrary degree.

LECTURE 3. CHABAUTY'S p-ADIC APPROXIMATION

(1) Exercise 1: Consider $(\mathbb{Q}_p, |\cdot|_p)$ a non-Archimedean normed field, and let $\{x_n\}_{n\geq 0}$ be a sequence of elements in $\mathbb{Q}_p$.
   (a) Prove that $\{x_n\}_{n\geq 0}$ is a Cauchy sequence if and only if $|x_{n+1} - x_n| \to 0$ as $n \to \infty$.
   (b) Prove that the series $\sum_{n\geq 0} x_n$ is convergent if and only if $x_n \to 0$ as $n \to \infty$.

(2) Let p be a prime and $\mathbb{Z}_p$ be the ring of integers of the field $\mathbb{Q}_p$ of p-adic numbers. Recall that

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

   (a) Show that $\mathfrak{m} := \{x \in \mathbb{Q}_p : |x|_p < 1\}$ is a maximal ideal in $\mathbb{Z}_p$, and that $\mathfrak{m} = p\mathbb{Z}_p$.
   (b) Show that the only ideals in $\mathbb{Z}_p$ are the ideals $\mathfrak{m}^k = p^k\mathbb{Z}$, for integers $k \geq 0$. In particular, $\mathfrak{m} = (p)$ is the unique maximal ideal in $\mathbb{Z}_p$.
   (c) Show that the group of invertible elements is $\mathbb{Z}_p^\times = u \in \mathbb{Z}_p : |u|_p = 1$, and prove that every element $x \in \mathbb{Z}_p$ can be written as $x = up^k$ for some $u \in \mathbb{Z}_p^\times$ and some $k \geq 0$.
   (d) Prove that $\mathbb{Z}_p/\mathfrak{m}$ is a finite field isomorphic to the finite field $\mathbb{F}_p$ of p elements. It is the residue field of $\mathbb{Z}_p$.
   (e) The group of units $U_0 := \mathbb{Z}_p^\times$ admits a natural decreasing filtration $(U_n)_{n\geq 0}$, where for each $n \geq 1$

$$U_n := 1 + m^n = \{x \in \mathbb{Z}_p : x - 1 \in \mathfrak{m}^n\}.$$

   The group U_1 is usually referred to as the group of principal units, and in general U_n is called the n-th higher unit group or the group of n-th principal units. Prove that

$$U_0/U_n \cong (\mathbb{Z}_p/\mathfrak{m}^n)^\times \text{ and } U_n/U_{n+1} \cong \mathbb{Z}_p/\mathfrak{m} \cong \mathbb{F}_p.$$

(3) Consider the hyperelliptic curve $C\colon y^2 = x(x-1)(x-2)(x-5)(x-6)$.
   - Find $C_7(\mathbb{F}_7)$, where C_7 is the reduction of C modulo 7.
   - Shows that $\#C(\mathbb{Q}) \geq 10$, taking into account that $(10, 120) \in C$.
   - We can use Magma in order to compute $\mathrm{rank}_{\mathbb{Z}}(J(\mathbb{Q}))$.

```
> _<x> := PolynomialRing(Rationals());
> C := HyperellipticCurve(x*(x-1)*(x-2)*(x-5)*(x-6));
> ptsC := Points(C : Bound:= 1000);
ptsC;
{@ (1 : 0 : 0), (0 : 0 : 1), (1 : 0 : 1), (2 : 0 : 1),
(3 : -6 : 1), (3 : 6 :1), (5 : 0 : 1), (6 : 0 : 1),
(10 : -120 : 1), (10 : 120 : 1) @}
> J := Jacobian(C);
> PJ := J! [ ptsC[5], ptsC[1]];
> Order(PJ);
0
```

   The previous code shows that there exists an element of $J(\mathbb{Q})$ (in this case $[(3 : 6 : 1) - (0 : 0 : 1)]$) which has infinite order. Furthermore, Magma can give us an upper bound for $\mathrm{rank}_{\mathbb{Z}}(J(\mathbb{Q}))$.

```
> RankBound(J);
1
```

   As a consequence, $\mathrm{rank}_{\mathbb{Z}}(J(\mathbb{Q})) = 1$.
   - Apply the method of Chabauty-Coleman to prove that $\#C(\mathbb{Q}) = 10$.

LECTURE 4. THE THEOREMS OF FALTINGS

(1) (i) Prove that the product of hyperbolic manifolds are hyperbolic too.
   (ii) Let $X = C_1 \times C_2$ be a surface, where C_i is a smooth curve with genus g_i. Prove that X is hyperbolic if and only if $g_1, g_2 \geq 2$.
(2) *(Symmetric square of a curve)* The symmetric square $Sym^2(C)$ of an algebraic curve C is the quotient space of the cartesian product $C \times C$ or C^2 by the relation $(a, b) \sim (b, a)$.
   (i) Let C be a curve defined over $\mathbb{Q}$. Characterize $Sym^2(C)(\mathbb{Q})$ in terms of C. (**Recall that if X is a variety defined over $\mathbb{Q}$, then $x \in X(\mathbb{Q})$ if and only if $\sigma(x) = x$ for all** $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$).
   (ii) Prove that if C is a hyperelliptic curve, then $Sym^2(C)(\mathbb{Q})$ is an infinite set.
(3) Let E_1, E_2, E_3 three elliptic curves which are no isogenous, every of them has coordinates x_i, y_i. Consider the hyperplane X in $A := E_1 \times E_2 \times E_3$ given by the equation $x_1 + x_2 + x_3 = 0$.
   (i) Prove that if $E \subset A$ is an elliptic curve, then it is isogenous to E_i for some $i \in \{1, 2, 3\}$.
   (ii) Prove that if $B \subset A$ is an abelian surface, then it is isogenous to $E_i \times E_j$ for $i, j \in \{1, 2, 3\}$, with $i \neq j$.
   (iii) Use Theorem 4.6 to prove that $X(\mathbb{Q})$ is finite

LECTURE 5. CONJECTURES OF BOMBIERI AND LANG

(1) Prove Lemma 5.2.
(2) Let $F_n \subset \mathbb{P}^3_{\mathbb{C}}$ be the variety defined by $x_0^n + x_1^n + x_2^n + x_3^n = 0$.
   (i) Prove that F_n is a smooth irreducible surface for every $n \geq 1$. (These are called Fermat surfaces.)
   (ii) For each $n \geq 1$, compute the Kodaira dimension of F_n . (Hint. A possible way to approach this is by applying Exercise II.8.4(e) from R. Hartshorne *Algebraic Geometry*.)
   (iii) For which values of n is the surface F_n of general type?
   (iv) Is there some integer $n \geq 1$ such that F_n is hyperbolic?
(3) Let X be a smooth projective surface defined over $\mathbb{Q}$ such that $X(\mathbb{C})$ is hyperbolic. Prove that if Bombieri's Question 5.3 has a positive answer, then $X(\mathbb{Q})$ is finite.
(4) Let C be smooth projective geometrically irreducible curve over $\mathbb{Q}$ of genus $g \geq 2$ and let $X = C \times \mathbb{P}^1_{\mathbb{Q}}$. Prove that for every number field L we have that $X(L)$ is algebraically degenerate. Prove, however, that there is no proper Zariski closed subset $Z \subset X$ such that for all L the set $(X - Z)(L)$ is finite. Does this contradict the Bombieri-Lang conjecture?