Michel Waldschmidt update : 23/08/2022

Exercises on elliptic curves.

August 15 - 26 , 2022.
African Institute for Mathematical Sciences (AIMS), M'Bour, Senegal
https://aims-senegal.org/
CIMPA Research School
https://www.cimpa.info/fr/node/6755
Cryptography, theoretical and computational aspects of number theory.
https://indico.math.cnrs.fr/event/5731/

1. **Eisenstein series**

   Recall, for a lattice Λ in $\mathbb{C}$ and $k \geq 3$,

   $$G_k(\Lambda) = \sum_{\lambda \in \Lambda \neq \{0\}} \frac{1}{\lambda^k} \cdot$$

   Check
   • for k odd, $G_k(\Lambda) = 0$.
   • for $\lambda \in \mathbb{C} \setminus \{0\}$, and $\Lambda = \mathbb{Z}\lambda + \mathbb{Z}\mathrm{i}\lambda$, $G_6(\Lambda) = 0$.
   • for $\lambda \in \mathbb{C} \setminus \{0\}$, and $\Lambda = \mathbb{Z}\lambda + \mathbb{Z}\varrho\lambda$ with $\varrho = \mathrm{e}^{2\pi\mathrm{i}/3}$, $G_4(\Lambda) = 0$.

2. **Isogenies**

   Let a_1 and a_2 be positive integers, Λ a lattice in $\mathbb{C}$, λ_1, λ_2 a basis of Λ and Λ' the sublattice $a_1\lambda_1\mathbb{Z} + a_2\lambda_2\mathbb{Z}$ of Λ :

   $$\Lambda' = a_1\lambda_1\mathbb{Z} + a_2\lambda_2\mathbb{Z} \subset \Lambda = \lambda_1\mathbb{Z} + \lambda_2\mathbb{Z}.$$

   The two canonical surjections $\mathbb{C} \to \mathbb{C}/\Lambda'$ and $\mathbb{C} \to \mathbb{C}/\Lambda$ give rise to a homomorphism $\psi : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ which is an isogeny :

   $$\begin{tikzcd} \mathbb{C} \arrow[r] \arrow[d] & \mathbb{C}/\Lambda \\ \mathbb{C}/\Lambda' \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

   Compute the degree n of the isogeny ψ, write the dual isogeny $\hat{\psi} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ and check that

   $$\psi \circ \hat{\psi} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \quad \text{and} \quad \hat{\psi} \circ \psi : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda'$$

   are the multiplications by n.

3. **Modular invariant**
Write $g_i(\tau)$ for $g_i(\mathbb{Z}+\mathbb{Z}\tau)$ and $i \in \{2,3\}$.
For $\mathrm{Im}(\tau) \to \infty$ check

$$g_2(\tau) \to 120 \sum_{m \geq 1} \frac{1}{m^4} = \frac{4\pi^3}{3} \quad \text{and} \quad g_3(\tau) \to 280 \sum_{m \geq 1} \frac{1}{m^6} = \frac{8\pi^6}{27}.$$

Deduce $\Delta(\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2 \to 0$ and $j(\tau) \to \infty$.

4. **Complex multiplication**
Let $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ be a lattice with $\mathrm{Im}(\tau) \in \mathfrak{H}$ and let $\alpha \in \mathbb{C}^\times \setminus \mathbb{Z}$ satisfy $\alpha\Lambda \subset \Lambda$.
(a) Check that $(1,\tau) \in \mathbb{C}^2$ is an eigenvector of a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

with eigenvalue α.
(b) Deduce that τ and α are quadratic numbers with $\mathbb{Q}(\alpha) = \mathbb{Q}(\tau)$ and that α is an algebraic integer (the irreducible polynomial of α over $\mathbb{Q}$ is monic).
(c) Let $AX^2 + BX + C$ be the minimal polynomial of τ over $\mathbb{Z}$ with $A > 0$, $\gcd(A,B,C) = 1$. Check that

$$\alpha \in \mathbb{Z} + \mathbb{Z}A\tau.$$

(d) Let $\overline{\alpha}$ be the complex conjugate of α. Check that α and $\overline{\alpha}$ define two dual isogenies of degree $\alpha\overline{\alpha}$ (the norm of α) of the torus $\mathbb{C}/\Lambda$.

5. **Congruent numbers**
Let n be a positive integer. Check that the following conditions are equivalent.
(i) The number n is congruent : there is a rectangle triangle with rational side lengths of area n :

$$n = \frac{ab}{2}, \quad a^2 + b^2 = c^2.$$

(ii) There is an arithmetic progression of rational squares with 3 terms and common difference n :

$$e^2 - g^2 = n, \quad g^2 - f^2 = n.$$

(iii) The elliptic curve $y^2 = x^3 - n^2 x$ has a rational point with $y \neq 0$.
`Hint.` Set

$$(e,f,g) = ((a+b)/2, (a-b)/2, c/2), \quad (a,b,c) = (e+f, e-f, 2g),$$

$$(x,y) = (nb/(c-a), 2n^2/(c-a)), \quad (a,b,c) = ((x^2-n^2)/y, 2nx/y, (x^2+n^2)/y).$$

Subsidiary question.
Check the following dictionary due to Claude Levesque :

$n = \frac{1}{2}ab \in \mathbb{Z}_{>0}$	a	$= e + f$	$= \frac{C+F}{B}$	$= \frac{Y}{X}$	$= \frac{\alpha^2 - \beta^2}{\delta}$	$= \frac{nV}{U}$
$a^2 + b^2 = c^2$	b	$= e - f$	$= \frac{C-F}{B}$	$= \frac{2nX}{Y}$	$= \frac{2\alpha\beta}{\delta}$	$= \frac{2U}{V}$
$a, b, c \in \mathbb{Q}_{>0}$ $b < a$	c	$= 2g$	$= \frac{2A}{B}$	$= \frac{X^2 + n^2}{Y}$	$= \frac{\alpha^2 + \beta^2}{\delta}$	$= \frac{U^2 + 1}{V}$
$n = e^2 - g^2$	e	$= \frac{a+b}{2}$	$= \frac{C}{B}$	$= \frac{X^2 + 2nX - n^2}{2Y}$	$= \frac{\alpha^2 + 2\alpha\beta - \beta^2}{2\delta}$	$= \frac{nV^2 + 2U^2}{2UV}$
$n = g^2 - f^2$	f	$= \frac{a-b}{2}$	$= \frac{F}{B}$	$= \frac{X^2 - 2nX - n^2}{2Y}$	$= \frac{\alpha^2 - 2\alpha\beta - \beta^2}{2\delta}$	$= \frac{nV^2 - 2U^2}{2UV}$
$e, f, g \in \mathbb{Q}_{>0}$	g	$= \frac{c}{2}$	$= \frac{A}{B}$	$= \frac{X^2 + n^2}{2Y}$	$= \frac{\alpha^2 + \beta^2}{2\delta}$	$= \frac{U^2 + 1}{2V}$
$A^2 + nB^2 = C^2$	$\frac{A}{B}$	$= \frac{c}{2}$	$= g$	$= \frac{X^2 + n^2}{2Y}$	$= \frac{\alpha^2 + \beta^2}{2\delta}$	$= \frac{U^2 + 1}{2V}$
$A^2 - nB^2 = F^2$	$\frac{C}{B}$	$= \frac{a+b}{2}$	$= e$	$= \frac{X^2 + 2nX - n^2}{2Y}$	$= \frac{\alpha^2 + 2\alpha\beta - \beta^2}{2\delta}$	$= \frac{nV^2 + 2U^2}{2UV}$
$A, B, C, F \in \mathbb{Z}_{>0}$	$\frac{F}{B}$	$= \frac{a-b}{2}$	$= f$	$= \frac{X^2 - 2nX - n^2}{2Y}$	$= \frac{\alpha^2 - 2\alpha\beta - \beta^2}{2\delta}$	$= \frac{nV^2 - 2U^2}{2UV}$
$Y^2 = X^3 - n^2X$	$\lvert X \rvert$	$= \frac{c^2}{4}$	$= g^2$	$= \frac{A^2}{B^2}$	$= \frac{n\alpha}{\beta}$	$= nU$
$X, Y \in \mathbb{Q}^{\times}$	$\lvert Y \rvert$	$= \frac{c(a^2 - b^2)}{8}$	$= efg$	$= \frac{ACF}{B^3}$	$= \frac{n^2\delta}{\beta^2}$	$= n^2V$
$n\delta^2 = \alpha^3\beta - \alpha\beta^3$	$\frac{\alpha}{\beta}$	$= \frac{c^2}{4n}$	$= \frac{g^2}{n}$	$= \frac{A^2}{nB^2}$	$= \frac{X}{n}$	$= U$
$\alpha, \beta, \delta \in \mathbb{Q}_{>0}$	$\frac{\delta}{\beta^2}$	$= \frac{c(a^2 - b^2)}{8n^2}$	$= \frac{efg}{n^2}$	$= \frac{ACF}{n^2B^3}$	$= \frac{Y}{n^2}$	$= V$
$nV^2 = U^3 - U$	U	$= \frac{c^2}{4n}$	$= \frac{g^2}{n}$	$= \frac{A^2}{nB^2}$	$= \frac{X}{n}$	$= \frac{\alpha}{\beta}$
$U, V \in \mathbb{Q}_{>0}$	V	$= \frac{c(a^2 - b^2)}{8n^2}$	$= \frac{efg}{n^2}$	$= \frac{ACF}{n^2B^3}$	$= \frac{Y}{n^2}$	$= \frac{\delta}{\beta^2}$