Arithmetic Geometry: Some common objects and well-known problems

Elliptic Curves

Motivating Question: Are there three consecutive numbers whose product is a square?

$y^2 = x(x+1)(x+2)$ $(x,y \in \mathbb{Z})$? Ans: No

$(x,y \in \mathbb{Q})$? Ans: No

Similar Question: $y^2 = x(x+5)(x+10)$ $(x,y \in \mathbb{Z})$?

Yes!!

Ex: $x = -9$, $y = 6$

Ex: $x = \frac{-50}{9}$, $y = \frac{100}{27}$ | $x = \frac{5}{4}$, $y = \dots$ | $x = \frac{961}{144}$, $y = \dots$ etc.

Question: Which numbers n can be written as areas of rt. triangles w/ ~~integer~~ rational edges?

$a,b,c \in \mathbb{Q}$, $n = \frac{ab}{2}$

Prop: n can be written as above iff $y^2 = x^3 - n^2x$ has a point (x,y) w/ $x,y \in \mathbb{Q}$.

Pf:

a,b,c ⟷ x,y

$(a,b,c) \longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right)$

$\left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right) \longmapsto (x,y)$

∎

→ **Note:** Question #2 can be written

$y^2 = (x-5)x(x+5)$

$y^2 = x^3 - 25x$

Ans to Q2 ⟹ $n = 5$ has ∞ many triangles

Results: (1975) **Stephen:** If $n \equiv 5, 6, 7 \pmod 8$ then n is area of Δ w/ $\mathbb{Q}$ sides. (assuming Birch, Swinnerton-Dyer conjecture)

Zagier: Example for $n = 157$ w/

$$c = \frac{224\ldots41}{891\ldots31}$$ ← 49 digits / ← 45 digits

Tunnel:

- If n odd, square-free, pos. integer then

$$\left(n = \text{area of } \Delta \text{ w/ } \mathbb{Q} \text{ sides}\right) \Rightarrow \left(\#\{(x,y,z) \in \mathbb{Z}^3 \mid n = 2x^2+y^2+32z^2\} = \tfrac{1}{2}\#\{(x,y,z) \mid n = 2x^2+y^2+8z^2\}\right)$$

- If n even, ~~square free~~, pos. integer then

$$\left(n = \text{area of } \Delta \text{ w/ } \mathbb{Q} \text{ sides}\right) \Rightarrow \left(\#\{(x,y,z) \mid n/2 = 4x^2+y^2+32z^2\} = \tfrac{1}{2}\#\{(x,y,z) \mid n/2 = 4x^2+y^2+8z^2\}\right)$$

- Furthermore w/ B.S.D. we have $\Leftarrow$ above

Note: These can be checked by computer, b/c possible x, y are bounded and these are integers.

Common Setup: $y^2 = x^3 + ax^2 + bx + c$ has how many solns?

Modular Forms (for $SL_2(\mathbb{Z})$) is $f : \mathbb{H} \to \mathbb{C}$ (upper half-plane)

w/ $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$

(Equivalent to: $f(-\frac{1}{z}) = z^k f(z)$ $\quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in SL_2(\mathbb{Z})$

$f(1+z) = f(z)$ $\quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$)

& • f holomorphic at $i\infty$

Motivating Question: Can you write $n = a_1^2 + a_2^2 + \cdots + a_k^2$?

In how many different ways ?

$S_k(n) = \#$ of $\{a_1, \ldots, a_k\}$ s.t. $n = a_1^2 + \cdots + a_k^2$

Ex: $S_2(n) = 2\left(1 + \left(\frac{-1}{n}\right)\right) \sum_{d \mid n} \left(\frac{-1}{d}\right)$

Jacobi symbol $\left(\frac{a}{p}\right)$ (p prime) $= \begin{cases} 0 & \gcd(a,p) \neq 1 \\ 1 & \text{if } x^2 \equiv a \bmod p \text{ sol} \\ -1 & x^2 \equiv a \bmod p \text{ no sol} \end{cases}$

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then

$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$

Generating Function:

$\Theta(q) = \sum_{j=-\infty}^{\infty} q^{j^2} \longrightarrow \Theta^k(q) = \left(\sum_{a_1=-\infty}^{\infty} q^{a_1^2}\right)\left(\sum_{-\infty}^{\infty} q^{a_2^2}\right) \cdots \left(\sum_{-\infty}^{\infty} q^{a_k^2}\right)$

$= \sum_{n=0}^{\infty} c_n q^n \qquad c_n = S_k(n)$

($q = e^{2\pi i z}$ Fourier series)

Θ^k is a modular form of weight $k/2$ for

$\Gamma_1(4) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 4 \right\}$

$M_{k/2}(\Gamma_1(4))$ is 2-dim'l v.s. over $\Gamma_1(4)$

Modular forms of wt $= k/2$ over $\Gamma_1(4)$

w/ known basis $f = 1 + 2q^2 + \cdots$, $g = q + q^3 + \cdots$ if $k=4$

$\Theta^4(q) = 1 + 8q + 24q^2 + \cdots$

$= f + 8g$

these coefficients are the values of $S_4(n)$

Next: L-functions !!