Arithmetics under the influence of geometry

Emmanuel Peyre

Université de Grenoble

IF-IMP Conference

History (18th century bc.)

The old babylonian clay tablet called “Plimpton 322”

History (18th century bc.)

According to J. Conway and R. Guy, the first lines on this tablet should be read as

119	169
3367	4825*
4601	6649
12709	18541
65	97
319	481

What are these numbers?

History (18th century bc.)

They verify the following relations

$$169^2 - 119^2 = 120^2$$
$$4825^2 - 3367^2 = 3456^2$$
$$6649^2 - 4601^2 = 4800^2$$
$$18541^2 - 12709^2 = 13500^2$$
$$97^2 - 65^2 = 72^2$$
$$481^2 - 319^2 = 360^2$$

History (17th century ad.)

Theorem (Fermat's last theorem, Wiles)

If $p > 2$, any integral solution of the equation

$$x^p + y^p = z^p$$

satisfies $xyz = 0$.

History (17th century ad.)

Theorem (Fermat's last theorem, Wiles)

If $p > 2$, any integral solution of the equation

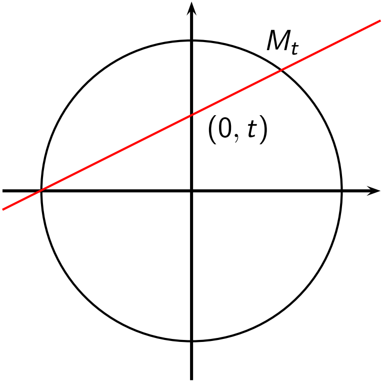
$$x^p + y^p = z^p$$

satisfies $xyz = 0$.

Question

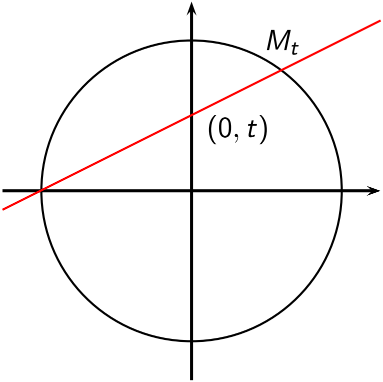
Why are the situations for $p = 2$ and $p > 2$ so different?

Rational points on the circle



$$\begin{cases} x^2 + y^2 = 1, \\ y = t(x+1). \end{cases}$$

Rational points on the circle



$$\begin{cases} x^2 + y^2 = 1, \\ y = t(x+1). \end{cases} \qquad \begin{cases} x = \frac{1-t^2}{1+t^2}, \\ y = \frac{2t}{1+t^2}. \end{cases}$$

Primitive solutions of $X^2 + Y^2 = Z^2$.

The rational solutions of $x^2 + y^2 = 1$ are of the form

$$\begin{cases} x = \frac{1-t^2}{1+t^2}, \\ y = \frac{2t}{1+t^2}. \end{cases}$$

for some $t \in \mathbf{Q}$. One may show that, up to permutation, and multiplication by an integer, any integral solution of the equation $x^2 + y^2 = z^2$ is of the form

$$(u^2 - v^2, 2uv, u^2 + v^2)$$

for some $(u, v) \in \mathbf{Z}^2$.

Plimpton 322

u	v	x	z
5	12	119	169
27	64	3367	4825
32	75	4601	6649
54	125	12709	18541
4	9	65	97
9	20	319	481

More precisely the cardinal $N(B)$ of the set

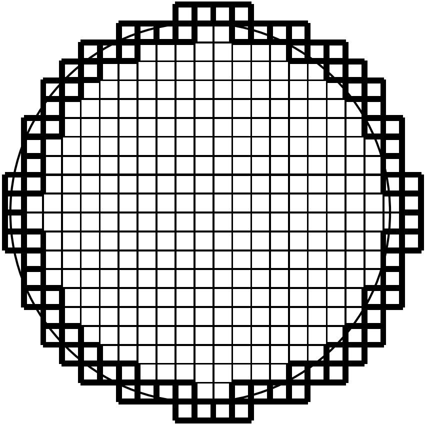
$$\left\{ (x,y,z) \in \mathbf{Z}^3 \;\middle|\; \begin{cases} x^2+y^2=z^2, \\ \max(|x|,|y|,|z|) \leqslant B, \\ \gcd(x,y,z)=1 \end{cases} \right\}$$

is up to some constant, equivalent to the cardinal

$$\sharp\{ (u,v) \in \mathbf{Z}^2 \mid u^2+v^2 \leqslant B \}$$

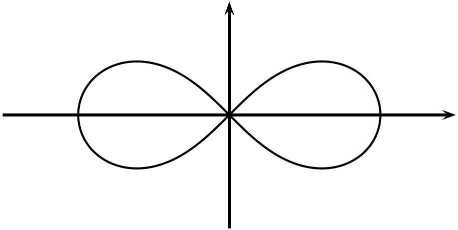
Points in a disk

$$\left|\sharp\{\,(u,v)\in\mathbf{Z}^2 \mid 0<u^2+v^2\leqslant B\,\}-\pi(\sqrt{B})^2\right|\leqslant C\sqrt{B}.$$

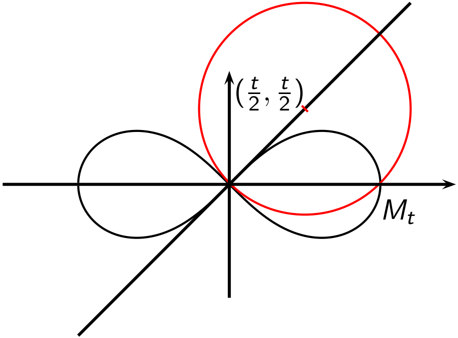


Bernoulli's lemniscate

$$(X^2 + Y^2)^2 - X^2 + Y^2 = 0$$



Bernoulli's lemniscate (parametrisation)



$$\begin{cases} x = \frac{t(1-t^2)}{1+t^4}, \\ y = \frac{t(1+t^2)}{1+t^4}. \end{cases}$$

Let $F \in \mathbf{Z}[X, Y, Z]$ be a homogeneous polynomial and let

$$C = \{\, (x : y : z) \in \mathbf{P}^2(\mathbf{C}) \mid F(x, y, z) = 0 \,\}$$

The set C is a Riemann surface (a complex curve). We denote by g the genus of C. We also denote by $N_F(B)$ the cardinal of the set

$$\left\{ (x, y, z) \in \mathbf{Z}^3 \;\middle|\; \begin{cases} F(x, y, z) = 0, \\ \gcd(x, y, z) = 1, \\ \max(|x|, |y|, |z|) \leqslant B. \end{cases} \right\}$$

Conclusion for curves

Conclusion

1. If $g = 0$, the number $N_F(B)$ is either 0 or equivalent to CB^a for some $a > 0$;
2. if $g = 1$, the number of primitive integral solutions is finite or $N_F(B)$ is equivalent to $C\log(B)^{a/2}$ for some strictly positive integer a;
3. if $g \geqslant 2$, the number of primitive integral solutions is finite (theorem of Faltings).

Higher dimension

Let $F(X_0, \ldots, X_N) \in \mathbf{Z}[X_0, \ldots, X_N]$ be some homogeneous polynomial of degree d. We are interested in $N_F(B)$, the cardinal of

$$\left\{ (x_0, \ldots, x_N) \in \mathbf{Z}^3 \;\middle|\; \begin{cases} F(x_0, \ldots, x_N) = 0, \\ \gcd(x_0, \ldots, x_N) = 1, \\ \max(|x_0|, \ldots, |x_N|) \leqslant B. \end{cases} \right\}$$

Birch's theorem

If A is a ring, a solution $(x_0, \ldots, x_N) \in A^{N+1}$ of $F(x_0, \ldots, x_N) = 0$ is said to be primitive if A is generated, as an ideal, by $x_0, \ldots, x_N$. We also define

$$V = \{ (x_0 : \cdots : x_N) \in \mathbf{P}^N(\mathbf{C}) \mid F(x_0, \ldots, x_N) = 0 \}$$

Theorem (Littlewood, Davenport, Birch)

Assume that $N > 2^{d-1}(d+1)$, that V is smooth and that there exists a primitive solution in $\mathbf{R}^{N+1}$ and $(\mathbf{Z}/m\mathbf{Z})^{N+1}$ for any integer $m \geqslant 2$. Then there exists a real constant $C > 0$

$$N(B) \sim CB^{N+1-d}.$$

Quartic surface

Noam Elkies found the following remarkable relations, thus disproving a long standing conjecture of Euler:

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

and

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

The end of history?

Theorem (Davis, Putnam, Robinson, Matijacevič, et al.)

There exists a polynomial $f \in \mathbf{Z}[T, X_1, \dots, X_{11}]$ *such that the application*

$$\begin{array}{rcl} \mathbf{Z} & \longrightarrow & \{0,1\} \\ n & \longmapsto & \begin{cases} 1 \text{ if } \{\, (x_1, \dots, x_{11}) \in \mathbf{Z}^{11} \mid f(n, x_1, \dots, x_{11}) = 0 \,\} \neq \emptyset \\ 0 \text{ otherwise} \end{cases} \end{array}$$

can not be computed with an algorithm.

The end of history?

Theorem (Davis, Putnam, Robinson, Matijacevič, et al.)

There exists a polynomial $f \in \mathbf{Z}[T, X_1, \dots, X_{11}]$ such that the application

$$\begin{array}{rcl} \mathbf{Z} & \longrightarrow & \{0,1\} \\ n & \longmapsto & \begin{cases} 1 \text{ if } \{\,(x_1,\dots,x_{11}) \in \mathbf{Z}^{11} \mid f(n,x_1,\dots,x_{11}) = 0\,\} \neq \emptyset \\ 0 \text{ otherwise} \end{cases} \end{array}$$

can not be computed with an algorithm.

Remark

The problem of the existence of an algorithm for homogeneous polynomials is still open.

Rational points on Iskovskih surfaces

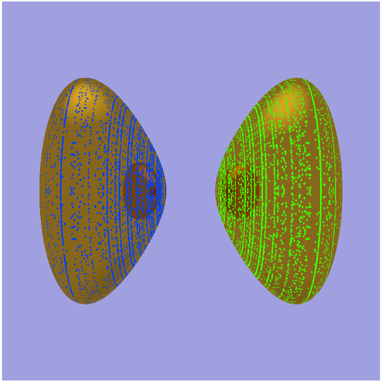


Image of the points of bounded size on the Iskovskih surface

$$Y^2 + Z^2 = X(X-1)(X+1)$$

using the projection mapping (X, Y, Z) to (x, y) where

$$\begin{aligned} x &= \frac{(1+\sqrt{2})X - 1}{X + (1+\sqrt{2})}, \\ y &= \frac{Y}{(X + (1+\sqrt{2}))^2} \end{aligned}$$