

# Random Diophantine Equations

Felipe Voloch

NTDU

September, 2023



## Abstract

Diophantine equations are polynomial equations in several variables and integer coefficients where the solutions are sought among integer or rational values. It is notoriously difficult to decide whether such equations have solutions. In this talk we will discuss an old conjecture of B. Poonen and the speaker about what happens for a random such equation and recent progress made on this conjecture.

## Poonen and V



## Diophantine Equations

$$2x + 3y = 1$$

$$x^2 + y^2 = z^2$$

$$x^3 + y^3 = z^3$$

$$x^2 - 4729494y^2 = 1$$

$$x^3 + y^3 + z^3 = 33, \quad x, y, z = 8866128975287528, -8778405442862239, -27361111468807040$$

$$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z - 32x^2z^2 -$$

$$40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$$

# Hilbert's 10th problem

## Theorem 1

*(Davis, Putnam, Robinson and Matiyasevich, aka Hilbert's 10th problem) There is no algorithm that, given a diophantine equation as input, decides whether it has a solution in integers.*

If we suspect it has a solution, it can be found by search.

How do we show an equation has no solutions?

## Local obstructions

If equation has no solution in  $\mathbb{R}$  then it has no solution in  $\mathbb{Q}$ .

The equation  $x^2 + y^2 = 3$  has no solutions in  $\mathbb{Q}$ . Otherwise, we have  $a, b, c \in \mathbb{Z}$  coprime with  $a^2 + b^2 = 3c^2$ . If 3 does not divide  $a$  then 3 does not divide  $b$  either, but then  $a^2 + b^2 \equiv 2 \pmod{3}$  so is not a multiple of 3.

## Local obstructions II

The equation  $x^3 + 2y^3 + 4z^3 = 0$  has no solutions in  $\mathbb{Q}$  other than  $(0, 0, 0)$ . Again assume variables are coprime integers. Then 2 divides  $x$ , so  $4(x/2)^3 + y^3 + 2z^3 = 0$ , so 2 divides  $y$ , etc.

Local obstructions use fields like  $\mathbb{R}, \mathbb{Q}_p$ . But  $3x^3 + 4y^3 + 5z^3 = 0$  has no solutions but no local obstruction (Selmer).

# Random Diophantine Equation

$$\begin{aligned} &7752x^4 + (7416y + (5821z + (3663w + 5919)))x^3 + (700y^2 + (9053z + (8810w + 2311)))y \\ &+ (3298z^2 - (2485w + 4288)z + (8914w^2 + 4480w + 3041))x^2 \\ &+ (2389y^3 + (2196z + (8543w + 5093)))y^2 + \\ &+ (2152z^2 - (6546w + 5751)z + (8904w^2 + 5302w + 7708))y \\ &+ (3273z^3 + (9062w + 2185)z^2 + (6224w^2 + 6121w + 2919)z \\ &+ (7710w^3 + 866w^2 - 8083w + 9028))x - (7284y^4 + (2077z + (2667w + 5581)))y^3 \\ &+ (2748z^2 + (5407w - 4034)z + (8846w^2 + 8317w + 4951))y^2 \\ &+ (7937z^3 + (1604w - 6516)z^2 + (6788w^2 + 2658w + 1589)z + (4119w^3 - 2414w^2 + 9946w + 9922))y \\ &+ (8084z^4 - (2184w + 5953)z^3 - (9551w^2 + 1493w + 8749)z^2 + (2176w^3 - 3687w^2 - 9490w + 490)z \\ &+ (6389w^4 + 4243w^3 + 5214w^2 + 4960w + 3582)) \end{aligned}$$



## Random Diophantine Equations

If  $f(x_0, \dots, x_n) \in \mathbb{Z}[x_0, \dots, x_n]$  of degree  $d$  with coprime coefficients, the height of  $f$ ,  $h(f)$  is the maximum of the absolute value of the coefficients of  $f$

$$N_{\text{tot}}(H) = \#\{f : h(f) \leq H\},$$

$$N_{\text{loc}}(H) = \#\{f : h(f) \leq H, \forall v, \exists x \in \mathbb{Q}_v^{n+1} \setminus \{0\}, f(x) = 0\}.$$

$$N(H) = \#\{f : h(f) \leq H, \exists x \in \mathbb{Z}^{n+1} \setminus \{0\}, f(x) = 0\},$$

where  $f$  ranges in  $\mathbb{Z}[x_0, \dots, x_n]$ ,  $\deg f = d$ , homogeneous.

## Conjecture

The limit of  $N(H)/N_{\text{tot}}(H)$  as  $H \rightarrow \infty$  if it exists, is the proportion of solvable equations.

### Conjecture 1

*(Poonen and V. 2002) For  $d > n + 1$ ,  $N(H)/N_{\text{tot}}(H) \rightarrow 0$  and for  $d < n + 1$ ,  $(d, n) \neq (2, 2)$ ,  $N(H)/N_{\text{tot}}(H) \rightarrow c > 0$ . Moreover,  $c = \prod c_v$ , where  $c_v$  is the proportion of hypersurfaces solvable in  $\mathbb{Q}_v$  and  $v$  runs through all places of  $\mathbb{Q}$ .*

# Conjecture

The limit of  $N(H)/N_{\text{tot}}(H)$  as  $H \rightarrow \infty$  if it exists, is the proportion of solvable equations.

## Conjecture 1

*(Poonen and V. 2002) For  $d > n + 1$ ,  $N(H)/N_{\text{tot}}(H) \rightarrow 0$  and for  $d < n + 1$ ,  $(d, n) \neq (2, 2)$ ,  $N(H)/N_{\text{tot}}(H) \rightarrow c > 0$ . Moreover,  $c = \prod c_v$ , where  $c_v$  is the proportion of hypersurfaces solvable in  $\mathbb{Q}_v$  and  $v$  runs through all places of  $\mathbb{Q}$ .*

In the case  $d = n + 1$ , we don't know what to expect. As a special case, if you write down a plane cubic, how likely is it to have a rational point?

## Motivation I

Consider the set of  $f$  of height at most  $H$  having a given solution  $a \in \mathbb{Z}^{n+1} \setminus \{0\}$  with coprime coordinates. The equation  $f(a) = 0$  is a hyperplane in the parameter space so has  $cH^{m-1}/\phi(a) + O(H^{m-2})$  integral points of height at most  $H$ , where  $m$  is the dimension of the parameter space,  $c$  is an universal constant and  $\phi(a)$  is the norm of the vector formed by the monomials of degree  $d$  in the coordinates of  $a$ . If we ignore the error term, then we get that  $N(H) \leq cH^{m-1} \sum 1/\phi(a)$  and is an exercise to show that  $\sum 1/\phi(a)$  converges if and only if  $d > n + 1$ . As  $N_{\text{tot}}(H) \sim H^m$ , this leads to the first part of the conjecture.

## Motivation II

If, for most  $f$  in our parameter space, the Hasse principle holds then we would get that  $N(H)/N_{\text{tot}}(H) \sim N_{\text{loc}}(H)/N_{\text{tot}}(H)$ .

### Theorem 2

*(Poonen and V., 2002)  $N_{\text{loc}}(H)/N_{\text{tot}}(H) \rightarrow c > 0$  if  $n, d \geq 2$  and  $(n, d) \neq (2, 2)$ . Moreover,  $c = \prod c_v$ , where  $c_v$  is the proportion of hypersurfaces solvable in  $\mathbb{Q}_v$  and  $v$  runs through all places of  $\mathbb{Q}$ .*

# Bhargava

Selmer (1951):  $3X^3 + 4Y^3 + 5Z^3$  has a  $\mathbb{Q}_p$ -pt.  $\forall p$  but no  $\mathbb{Q}$ -pt.

Q How frequent are such failures of the Hasse principle among plane cubics?

More precisely, for an integral t.c.f.  $f$ , let  $h(f) := \max\{\text{abs values of the coeffs of } f\}$

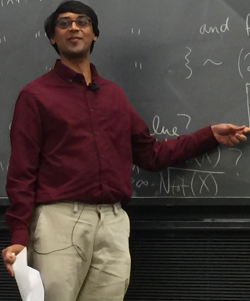
and let  $N_{\text{fail}}(X) = \{\text{int. t.c.f.'s } f : h(f) < X \text{ and } f \text{ fails Hasse}\}$

$N_{\text{sol}}(X) = \{\text{" " " " and } f \text{ has a } \mathbb{Q}\text{-pt}\}$

$N_{\text{tot}}(X) = \{\text{" " " " } \sim (2X+1)^0$

Does  $\lim_{X \rightarrow \infty} \frac{N_{\text{fail}}(X)}{N_{\text{tot}}(X)}$  exist, and if so, what is it?

Poonen-Voloch MathOve



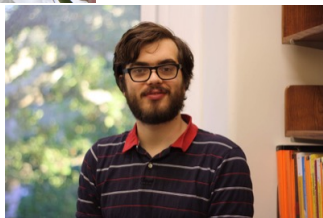
## Cubic curves

### Theorem 3

(Bhargava 2014) If  $(d, n) = (3, 2)$ , then  $N(H)/N_{\text{tot}}(H) \rightarrow c$  with  $0 < c < \prod c_v$ .

Conjecturally,  $c = \frac{\prod c_v}{3}$ .

## le Boudec, Browning, Sawin





## Fano hypersurfaces

### Theorem 4

(*le Boudec, Browning, Sawin, Annals of Math, 2023*) If  $d < n + 1$ ,  $(d, n) \neq (3, 3)$  then conjecture 1 is true. Moreover, in this case, 100% of the everywhere locally solvable equations have a solution  $x \in \mathbb{Z}^{n+1}$ ,  $x \neq 0$  with

$$\max\{|x_i|\} \leq h(f)^{\frac{1}{n+1-d} + \epsilon}.$$

The proof uses the circle method and geometry of numbers as in the motivation for the case  $d > n + 1$ !

THANK YOU