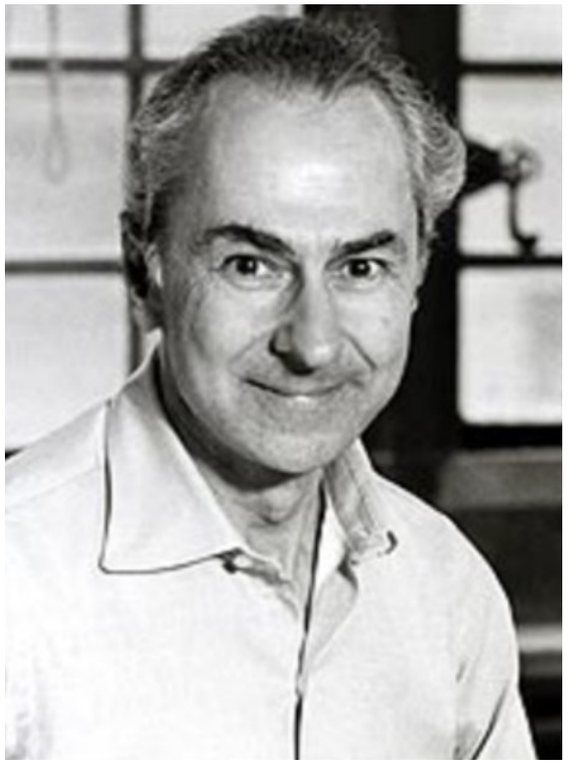
From Diophantus to Bitcoin...


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
M. SIRIACO SEBVSIANO, V. C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Why are elliptic curves everywhere?

Álvaro Lozano-Robledo
University of Connecticut

UCONN
UNIVERSITY OF CONNECTICUT



"It is possible to write endlessly
on elliptic curves.
(This is not a threat.)"

- Serge Lang
Diophantine Analysis.

PlayStation 3 hack – how it happened and what it means

(2010)

A group of coders claims the PS3 has been hacked, opening the doors to software piracy. We look into the implications

The PS3 has been hacked. But how – and why? Photograph: Kevork Djansezian/AP

In December, a group of coders operating under the name Fail0verflow stood up at the Chaos Communications hackers conference in Berlin and proclaimed that the Sony PS3 security system was an epic fail. Through the use of what they termed "simple algebra" they had managed to exploit a weakness in the PlayStation 3's encryption system, thereby gaining the public key required to run any software on the machine.

(2013)

BIZ & IT —

Google confirms critical Android crypto flaw used in $5,700 Bitcoin heist

Java Crypto weakness could affect security in hundreds of thousands of apps.

DAN GOODIN - 8/14/2013, 9:15 PM

$$e^{\pi\sqrt{163}} = 262537412640768743.\underbrace{999999999999}_{\text{twelve 9's !}}250072\ldots$$

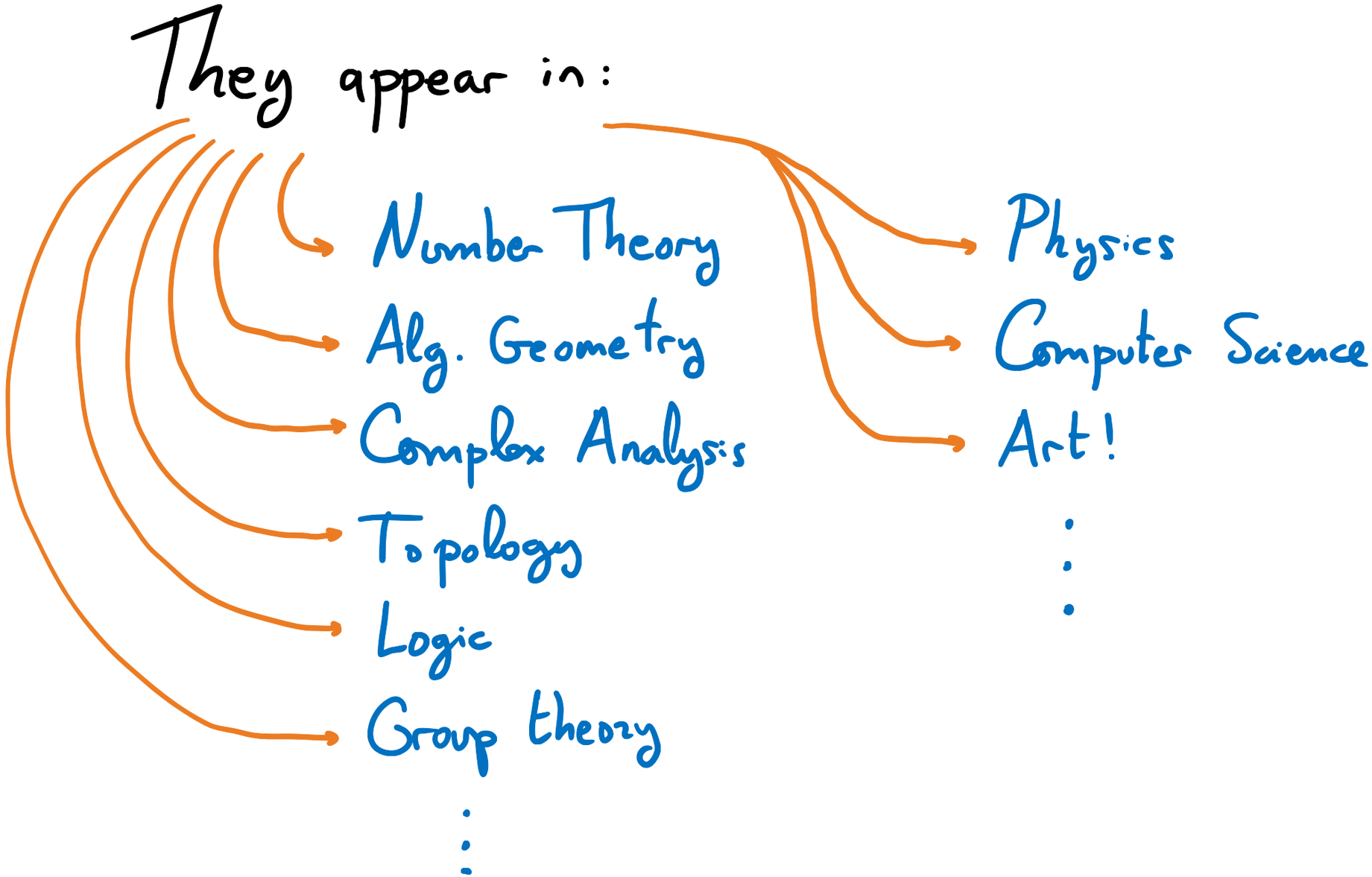
Transcendental by Gelfond-Schneider's Theorem!

$$p(n) = n^2 + n + 41$$

takes prime values for $n = 0, 1, \ldots, 39$

$41, 43, 47, 53, \ldots, 1601$, $1681 = 41^2$, $1763 = 41 \cdot 43$

$n=0$ $n=1$ $n=2$ $\ldots$ $n=39$ $n=40$ $n=41$


They appear in:
Number Theory
Alg. Geometry
Complex Analysis
Topology
Logic
Group theory
Physics
Computer Science
Art!

But ... Why?

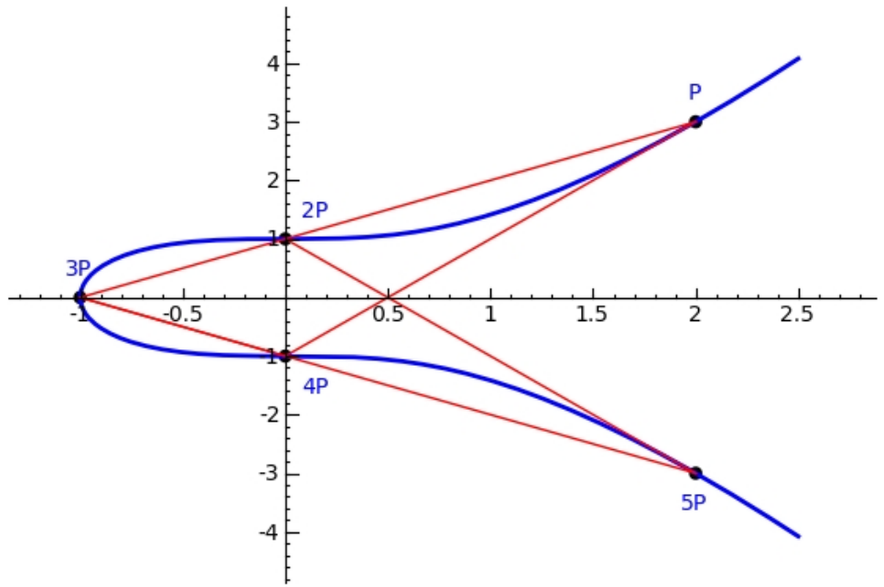
Because they are in the

"Sweet Spot"

of arithmetic, geometry, complex analysis, complexity, and "cognition".

The Arithmetic "Sweet Spot"

"What is an elliptic curve?"



What is a Diophantine Equation?

- $x^5 - x = 0$
- $3x + 5y = 1$
- $x^2 - 61y^2 = 1$
- $y^2 = x^3 - 157^2 x$
- $x^3 + y^3 + z^3 = 42$


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

What is a Diophantine Equation?

More generally:

$$f(x_1, \ldots, x_n) = 0$$

where $f \in \mathbb{Z}[x_1, \ldots, x_n]$.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
M. ZIRIACO SEBVSIANO, V. C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diophantus of Alexandria (born ~ 200 C.E.)

"The Father of Algebra"

- Known for the books

  "Arithmetica,"

  the first systematic study of

  Diophantine equations.

Diophantus of Alexandria (born ~ 200 C.E.)

"The Father of Algebra"

Diophantus' epitaph:

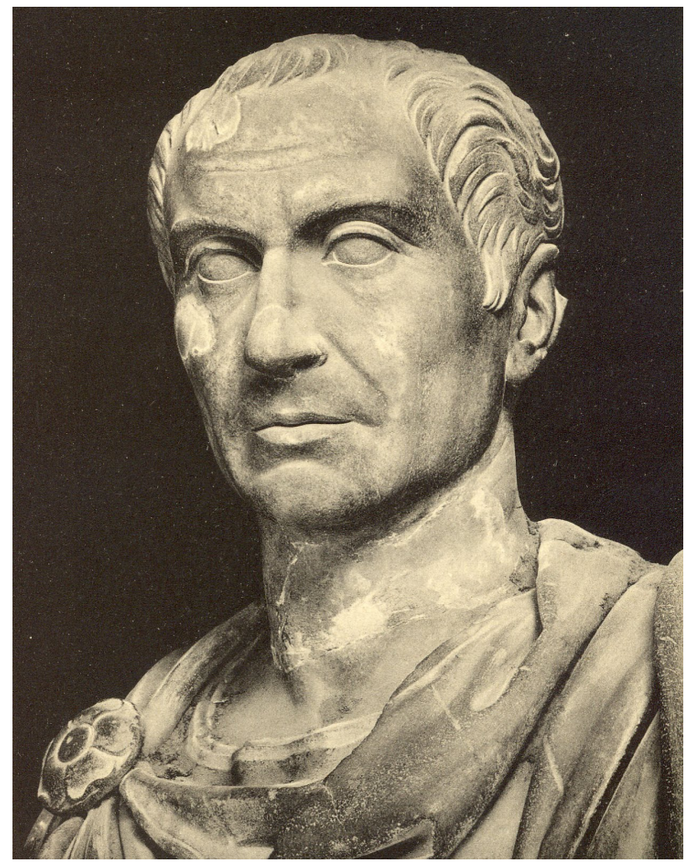
'Here lies Diophantus,' the wonder behold.
Through art algebraic, the stone tells how old:

'God gave him his boyhood one-sixth of his life,
One twelfth more as youth while whiskers grew rife;
And then yet one-seventh ere marriage begun;
In five years there came a bouncing new son.
Alas, the dear child of master and sage
After attaining half the measure of his father's life chill fate took him.
After consoling his fate by the science of numbers for four years,
he ended his life.'

(Metrodorus, ~ 500 CE)

Diophantus of Alexandria (born ~ 200 C.E.)

"The Father of Algebra"



Book IV, Problem 24:

To divide a given number into two numbers such that their product is a cube minus its side.

Diophantus of Alexandria (born ~ 200 C.E.)

"The Father of Algebra"

Book IV, Problem 24:

To divide a given number into two numbers such that their product is a cube minus its side.

$$a = y + (a-y)$$

such that

$$y \cdot (a-y) = x^3 - x$$

↖ an elliptic curve!

Diophantus of Alexandria (born ~ 200 C.E.)

"The Father of Algebra"

Book IV, Problem 24:

To divide a given number into two numbers such that their product is a cube minus its side.

$$a = y + (a-y)$$

such that

$$y \cdot (a-y) = x^3 - x$$

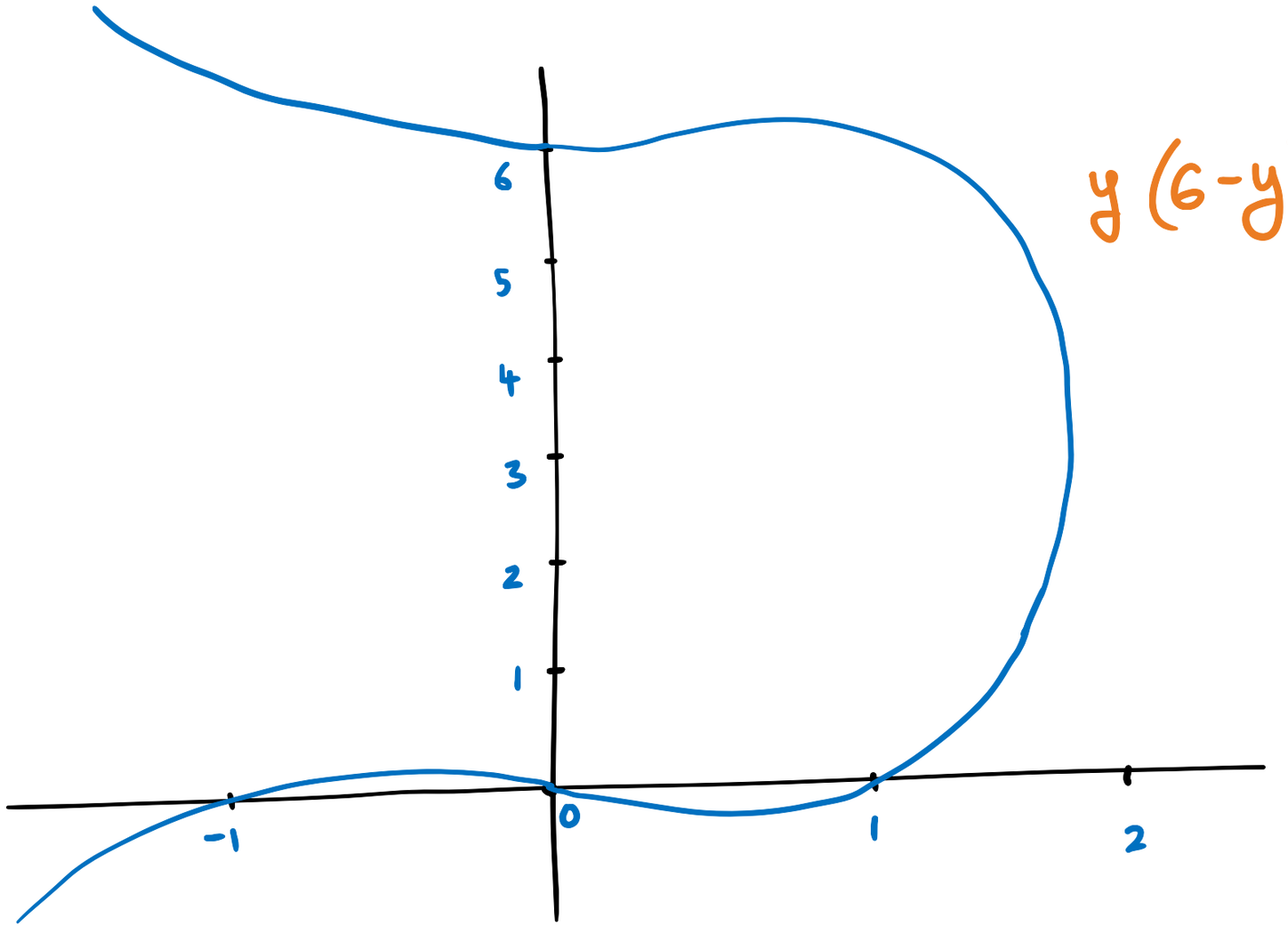
Example

For $a = 6$

Diophantus finds:

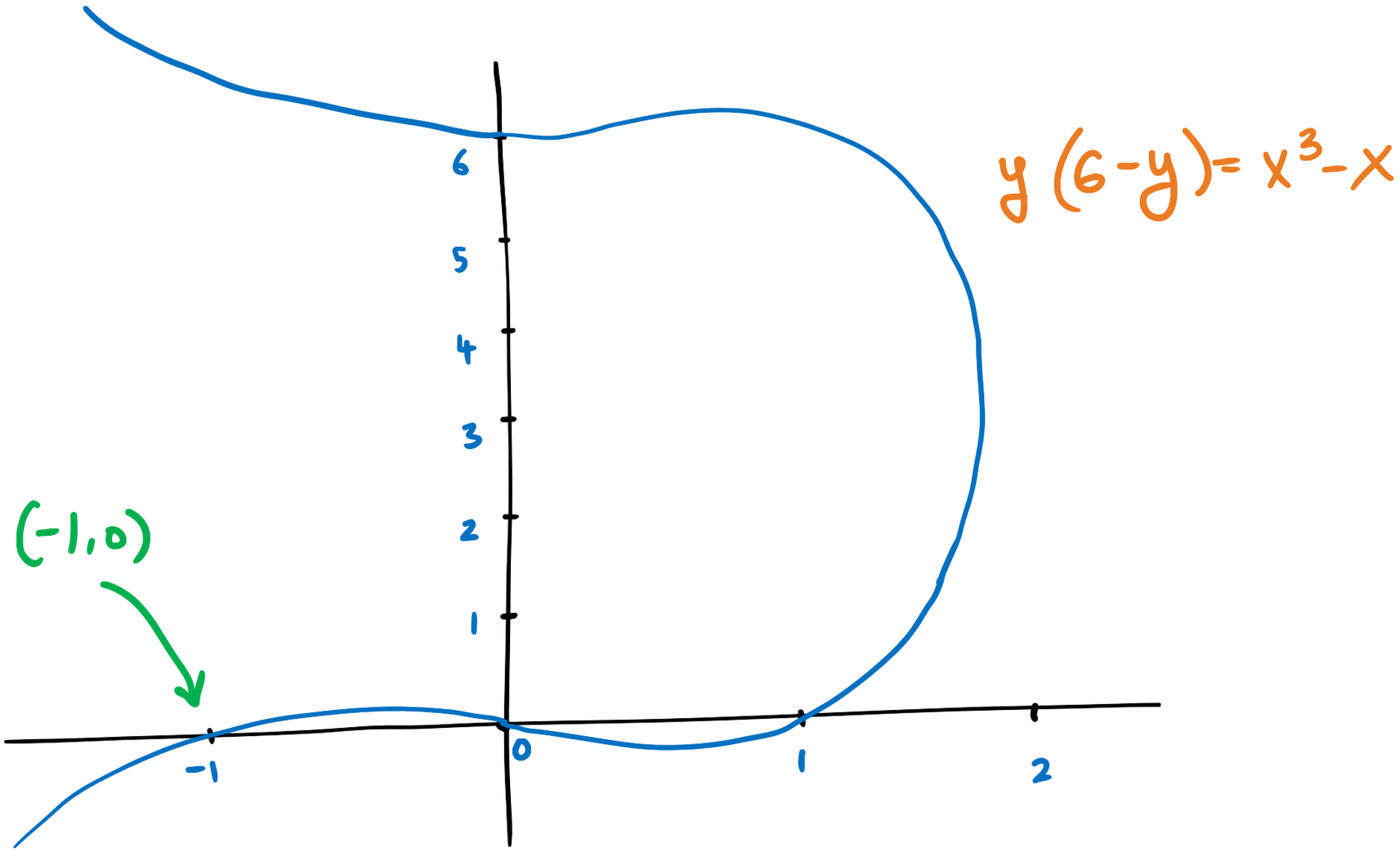
$$y = \frac{26}{27}$$

How? [Given a, find y s.t. $y(a-y) = x^3 - x$]



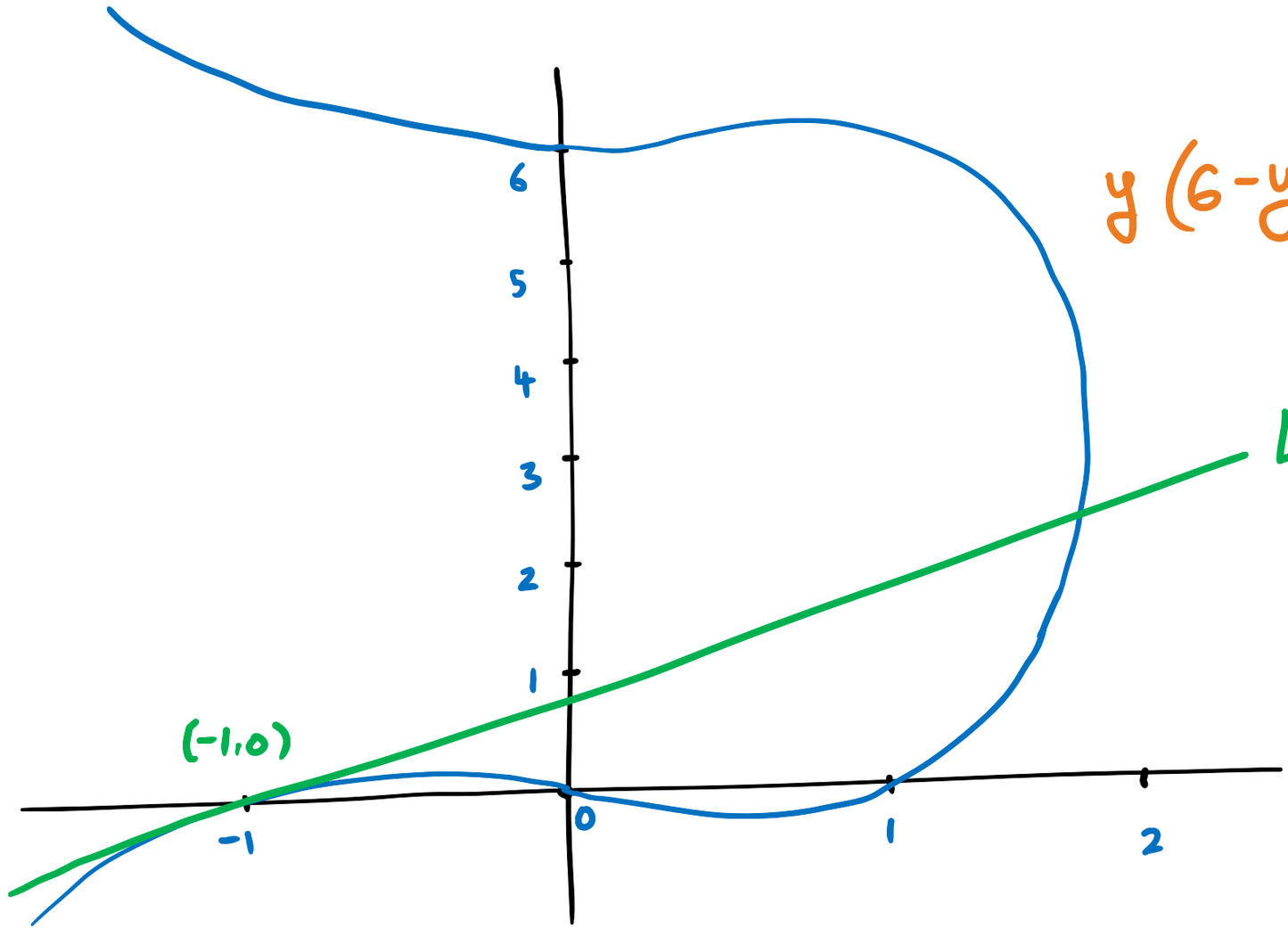
$y(6-y) = x^3 - x$

How? [Given a, find y s.t. $y(a-y) = x^3 - x$]



$y(6-y) = x^3 - x$

How? [Given a, find y s.t. $y(a-y) = x^3 - x$]

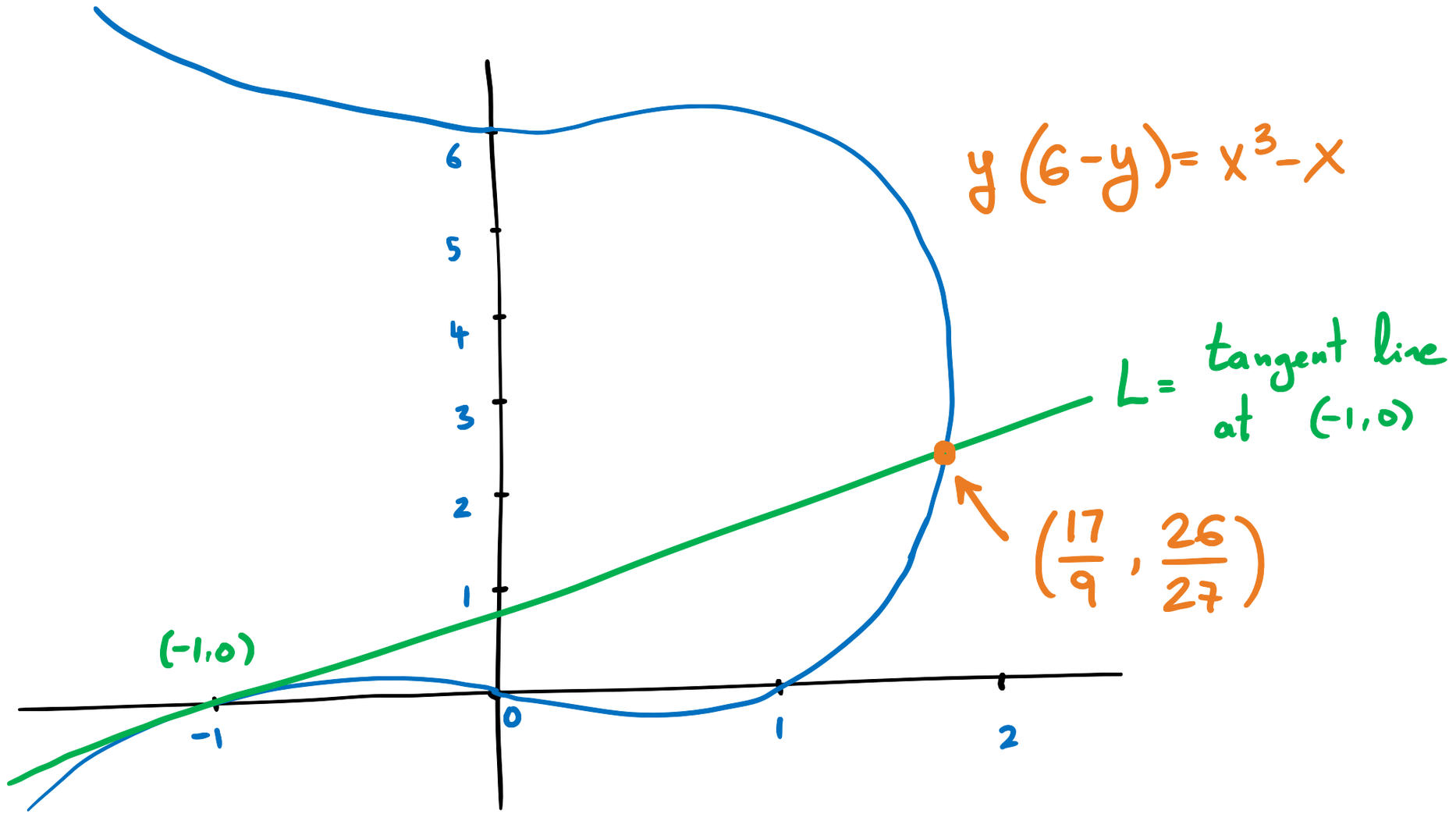


$y(6-y) = x^3 - x$

L = tangent line at $(-1,0)$

How?

Given a, find y s.t. $y(a-y) = x^3 - x$



$y(6-y) = x^3 - x$ is an example of an elliptic curve.

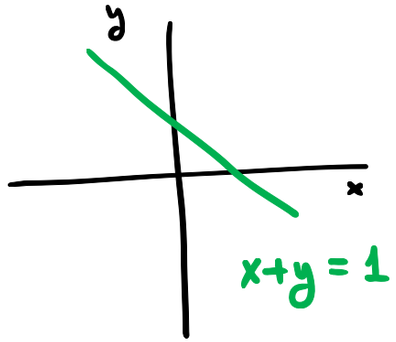
Diophantine Equations : $f(x_1, \dots, x_n) = 0$

($\deg f$, number of variables)

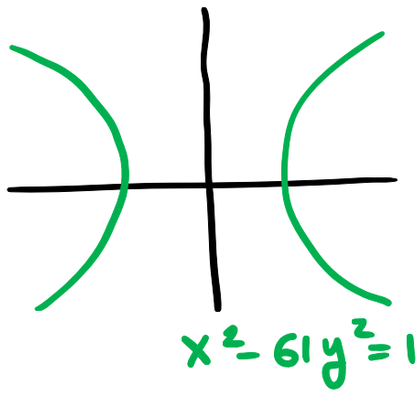
- One variable : $f(x) = 0$ (a polynomial with $\mathbb{Z}$-coefficients)
  ($n = 1$, arbitrary $\deg f$)
- Two variables : $f(x, y) = 0$
  - ($\deg f = 1$) Lines.
  - ($\deg f = 2$) Conics and "products" of lines.
  - ($\deg f = 3$) Smooth cubics and "products" of lines and conics.
  - ⋮

- Two variables: $f(x,y)=0$. Can we find $\mathbb{Z}$ or $\mathbb{Q}$ solutions?

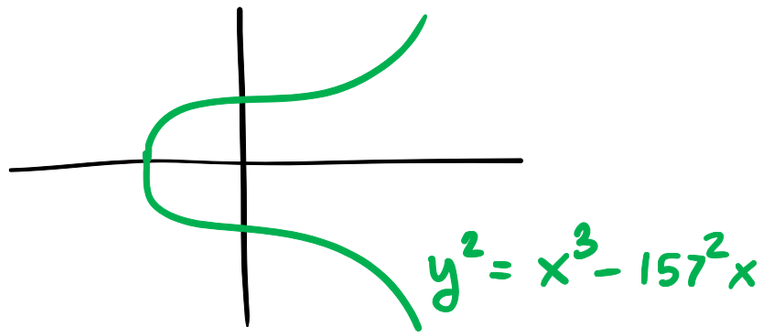
  - ($\deg f = 1$) Lines.
    - YES! Using divisibility and GCD's.



  - ($\deg f = 2$) Conics and "products" of lines.
    - YES! Hasse-Minkowski, Continued Fractions



  - ($\deg f = 3$) Smooth cubics and "products" of lines and conics.
    - ???



  - ⋮

Elliptic Curves

An elliptic curve over a field F is a smooth, projective curve of genus 1 with at least one point defined over F.

$$\begin{cases} y^2 = x^2(x-1) & \text{✗} \\ y^2 = x^3 & \text{✗} \\ y = x^3 & \text{✗ at } \infty \end{cases}$$

NOT SMOOTH!

FACT: Every elliptic curve can be given by a Weierstrass model:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad , \quad a_i \in F.$$

If $\operatorname{char} F \neq 2,3$, then

$$y^2 = x^3 + Ax + B \quad , \quad A, B \in F$$
$$4A^3 + 27B^2 \neq 0.$$

Integer Solutions of Diophantine Equations

... can be very intricate!

- $x^2 - 61 \cdot y^2 = 1$

$1^2 - 61 \cdot 0^2 = 1$

$1766319049^2 - 61 \cdot 226153980^2 = 1$

The solution:

$$1766319049^2 - 61 \cdot 226153980^2 = 1$$

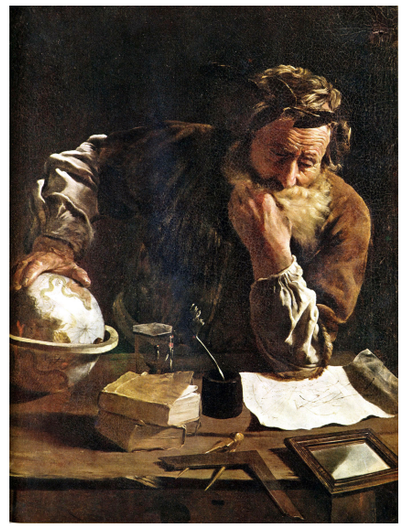
comes from the continued fraction of $\sqrt{61}$:

$$\sqrt{61} = [7; \overline{1,4,3,1,2,2,1,3,4,1,14}]$$

$$= 7 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \ddots}}}}}}}$$

Integer Solutions of Diophantine Equations

... can be very intricate!



- Archimedes' cattle problem:
  (287 – 212 BCE)

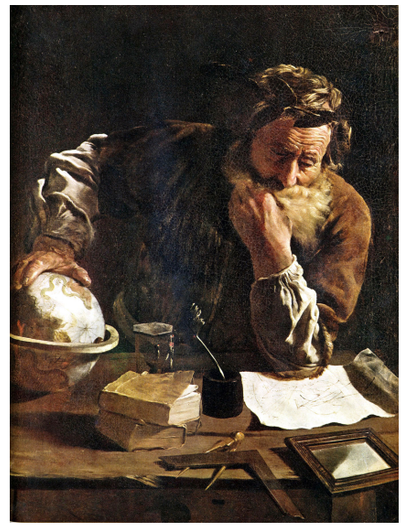
$$\begin{cases} 5B = 6(W-Y) \\ 9D = 20(B-Y) \\ 13W = 42(D-Y) \\ 12W = 7(B+b) \\ 20b = 9(D+d) \\ 30d = 11(Y+y) \\ 42y = 13(W+w) \end{cases}$$

and

$$\begin{cases} W+B = m^2 \\ 2(Y+D) = n(n+1) \end{cases}$$

Integer Solutions of Diophantine Equations

... can be very intricate!



- Archimedes' (287 - 212 BCE) cattle problem:

leads to a Pell's equation

$$u^2 - 4729494 \cdot v^2 = 1$$

leads to a sol'n

$$7.76 \cdot 10^{206544} \text{ cattle.}$$

Integer Solutions of Diophantine Equations

... can be very intricate!

- Is 42 a sum of three cubes?

$$X^3 + Y^3 + Z^3 = 42$$

The answer to Life, the Universe, and Everything! (Douglas Adams)

X = -80538738812075974

Y = 80435758145817515

Z = 12602123297335631

(Booker and Sutherland, 2019)

Elliptic Curves in the Cognitive "Sweet Spot"

- Find all perfect squares that are one more than a cube.

$$y^2 = x^3 + 1$$ (an elliptic curve!)

Theory of elliptic curves

$$y^2 = 0,\ 1,\ \text{or}\ 9.$$

Elliptic Curves in the Cognitive "Sweet Spot"

- Find all consecutive non-zero integers whose product is a perfect square:

$$y^2 = x(x+1)(x+2)$$

elliptic curves

OR

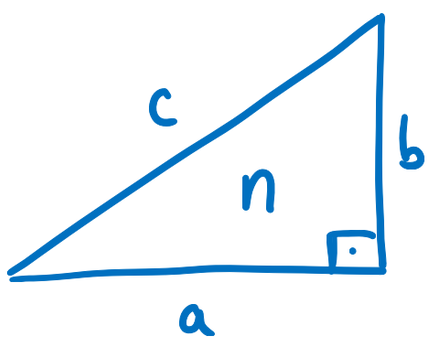
$$y^2 = (x-1)x(x+1) = x^3 - x$$

Theory of ell. curves

A: None.

Elliptic Curves in the Cognitive "Sweet Spot"

- Is there a right triangle with sides of rational length and...
  - area = 6 ? Yes! $(a,b,c) = (3,4,5)$
  - area = 5 ? Yes! $(a,b,c) = \left(\frac{20}{3}, \frac{3}{2}, \frac{41}{6}\right)$ Fibonacci 1200's
  - area = 1 ? No! Fermat 1600's
  - area = 157 ? Yes... Zagier 1900's



Elliptic Curves in the Cognitive "Sweet Spot"

- Is there a right triangle with sides of rational length and... area = n?

  ↘ if and only if

  $$y^2 = x^3 - n^2 x$$ (an elliptic curve!)

  has a $\mathbb{Q}$-solution with $y \neq 0$.

Elliptic Curves in the Cognitive "Sweet Spot"

- Is there a right triangle with sides of rational length and... area = 157?

$$y^2 = x^3 - 157^2 x$$

leads to (a,b,c) with:

$$a = \frac{411340519227716149383203}{21666555693714761309610}, \quad b = \frac{6803298487826435051217540}{411340519227716149383203},$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

(due to D. Zagier)

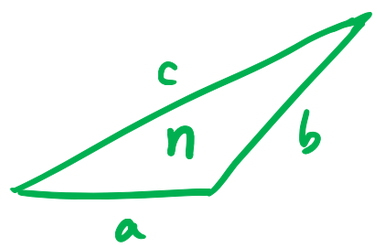
Elliptic Curves in the Cognitive "Sweet Spot"

- Is there a ~~right~~ triangle with sides of rational length and... area = n?

Heron triangles (rational sides and area)

EXAMPLE: $n = 1$ is the area of

$$\left(\frac{3}{2}, \frac{5}{3}, \frac{17}{6}\right)$$



Elliptic Curves in the Cognitive "Sweet Spot"

- Is there a ~~right~~ triangle with sides of rational length and... area = n?

Heron triangles (rational sides and area)

THEOREM (Goins, Maddox, 2006)

A number n is the area of a Heron triangle iff there is a rational number t s.t. $y^2 = x(x-nt)(x+nt^{-1})$ has a rational point with $y \neq 0$.

↖ an elliptic curve!

+ every n is the area of a Heron triangle.

Elliptic Curves in the Historical "Sweet Spot"

- **Fermat's Last Theorem:** $\begin{cases} x^n + y^n = z^n \\ xyz \neq 0 \end{cases}$ has no $\mathbb{Z}$-solutions for $n > 2$.

$x^3 + y^3 = z^3$ in $\mathbb{Z}$ $\longleftrightarrow$ $x^3 + y^3 = 1$ in $\mathbb{Q}$ (an elliptic curve)

Hellegouarch, Frey: if $a^p + b^p = c^p$, study $E: y^2 = x(x - a^p)(x + b^p)$ — (an elliptic curve??)

Serre, Ribet: E is semi-stable but not modular

Wiles, Taylor-Wiles: Every ell. curve is modular! ✓

$\Rightarrow$ E cannot exist!

Integer Solutions of Diophantine Equations

... can be very intricate! Algorithm?

Hilbert's Tenth Problem (1900)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients:

To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

Integer Solutions of Diophantine Equations

... can be very intricate! Algorithm?

Hilbert's Tenth Problem

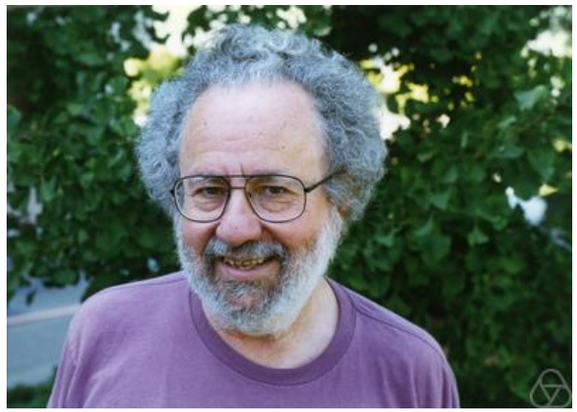
Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients:

To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

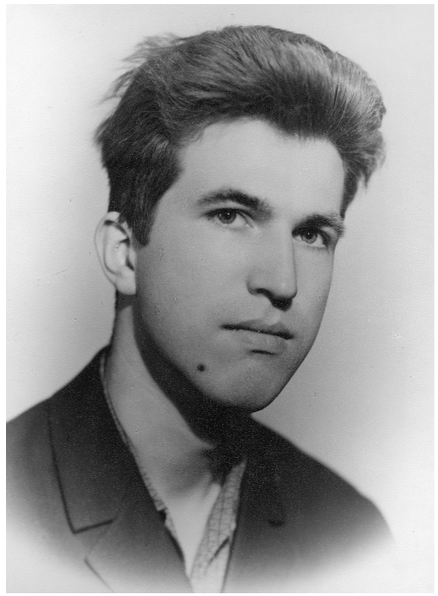
- Lines ✓
- Conics ✓
- Elliptic curves ???

XXTH CENTURY SURPRISE

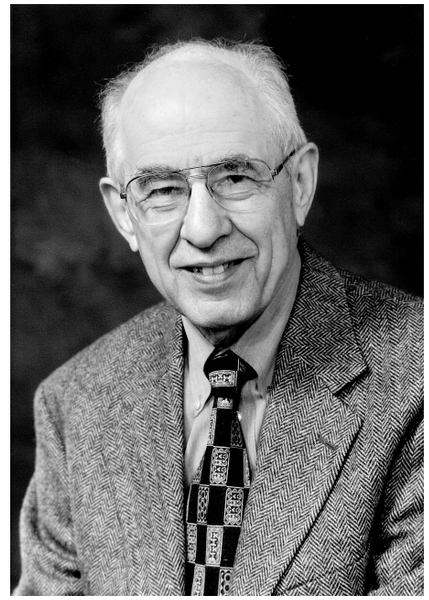
LOGIC!



DAVIS



MATIYASEVICH



PUTNAM

ROBINSON

HILBERT'S 10TH (OVER $\mathbb{Z}$): NO! THERE IS NO SUCH ALGORITHM. (1970)

The Geometric "Sweet Spot"

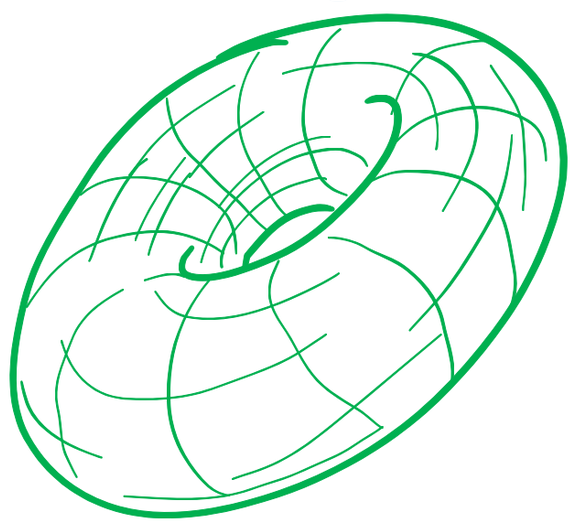
- Complex algebraic curves are classified by their genus:

$$C : f(x,y) = 0 \qquad f \in \mathbb{Z}[x,y].$$

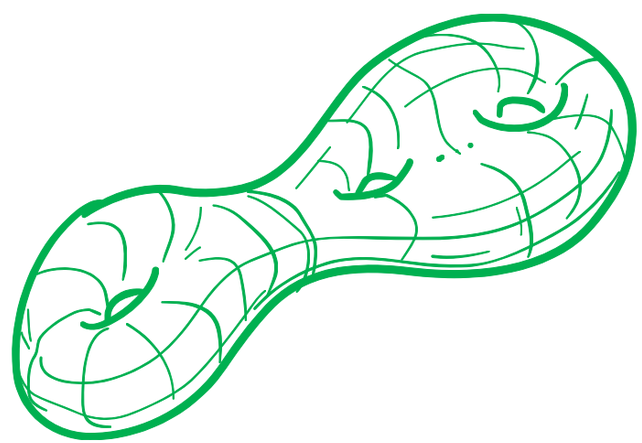
genus: dim. of space of regular diff. 1-forms on C.

over $\mathbb{C}$ classified according to their genus

$g = 0$



$g = 1$



$g \geq 2$

The Geometric "Sweet Spot"

- Complex algebraic curves are classified by their genus:

$$C : f(x,y) = 0 \qquad f \in \mathbb{Z}[x,y].$$

genus = dim. of space of regular diff. 1-forms on C.

over $\mathbb{C}$ classified according to their genus

Curves	deg f	genus	# rational points over $\mathbb{Q}$
Lines, Conics	1, 2	0	$\emptyset$ or ∞'ly many
Cubics$^+$	3, 4	1	$\emptyset$, or finitely many, or ∞'ly many
Higher genus	≥ 4	≥ 2	$\emptyset$ or finitely many. (Faltings')

The Geometric "Sweet Spot"

EXAMPLES

$g=0$
- $x^2+y^2=-1$ — no $\mathbb{Q}$-points
- $x^2+y^2=1$ — ∞'ly many: $\left\{\left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right) : t\in\mathbb{Q}\right\}\cup\{(1,0)\}$

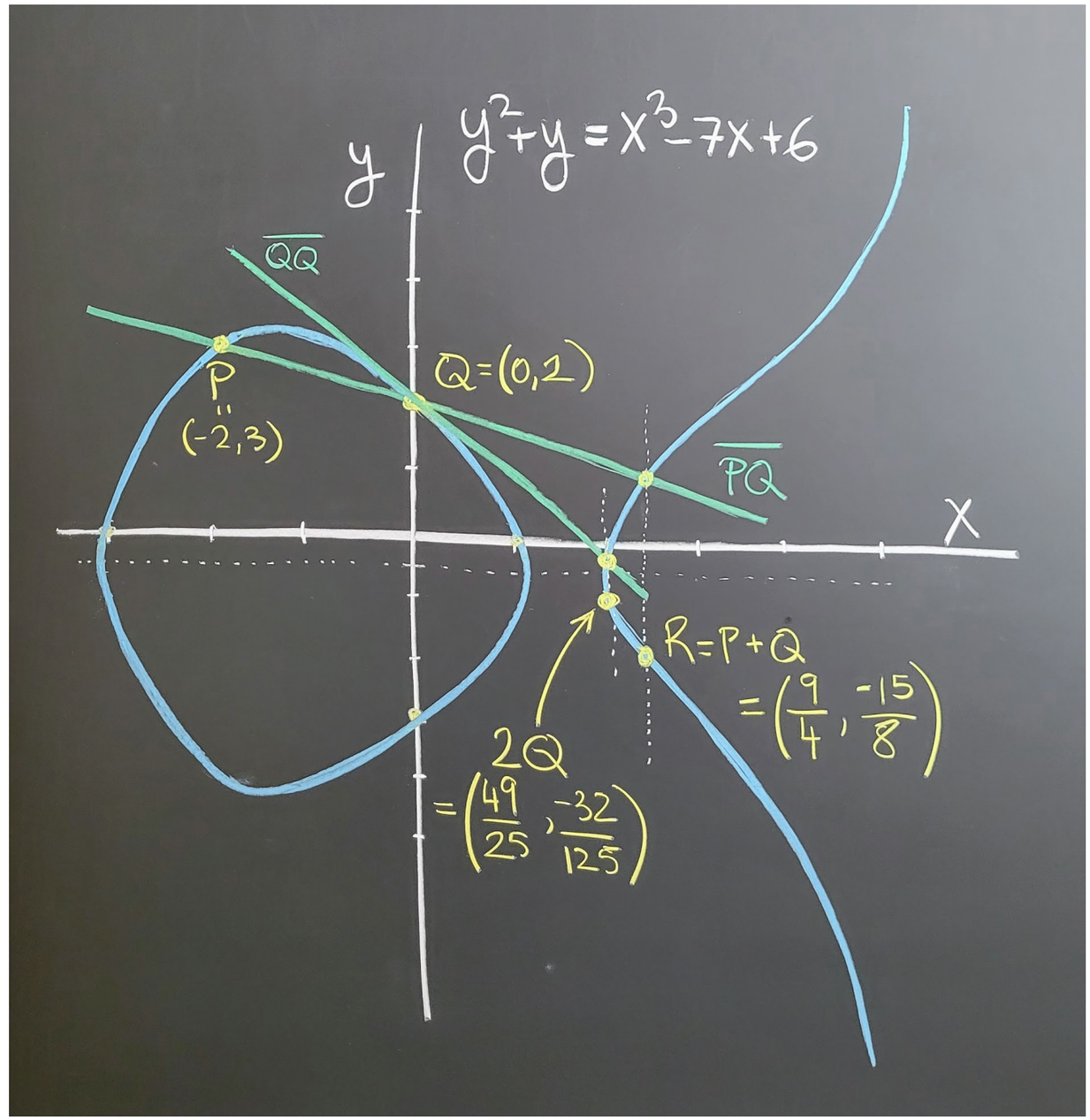
$g=1$
- $3x^3+4y^3+5=0$ — no $\mathbb{Q}$-points (one pt. at ∞: $[0,1,0]$)
- $x^3+y^3=1$ — 2 $\mathbb{Q}$-points (plus one pt at ∞)
- $y^2=x^3-2$ — ∞'ly many $\mathbb{Q}$-points

$y^2-9y=x^3-27$

$g\geq 2$
- $x^4+y^4=-1$ — no $\mathbb{Q}$-points
- $y^2=x-x^5$ — 3 $\mathbb{Q}$-points (plus one at ∞)

Moreover!

$g = 1$ + one pt. $\Rightarrow$ Geometric Group Structure!



Mordell (- Weil), 1922

Let $E/\mathbb{Q}$ be an elliptic curve. Then, the set of rational points on E, denoted by $E(\mathbb{Q})$, is a finitely generated abelian group.

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_{E/\mathbb{Q}}}$$

Mazur: 15 possibilities

Elkies: $\sup\{R_{E/\mathbb{Q}}\} \geq 28$.

RANKS

Logic "Sweet Spot"

- Hilbert's 10^{TH} Problem ...

  ... over other rings?

EXAMPLE: Replace $\mathbb{Z}$ by $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}, i^2 = -1\}$

- Is there an algorithm to determine (in a finite number of steps) if a diophantine equation over $\mathbb{Z}[i]$ has a solution over $\mathbb{Z}[i]$?

Logic "Sweet Spot"

- Hilbert's 10^{TH} Problem ...

... over other rings?

Example

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

$R_{E/\mathbb{Q}(i)} = R_{E/\mathbb{Q}} = 1$

$\Rightarrow$ $H10/_{\mathbb{Z}[i]}$ no algorithm exists!

Denef, Pheidas, Shlapentokh, Poonen:

Theorem Let F be a number field. If there is an elliptic curve $E/\mathbb{Q}$ s.t.

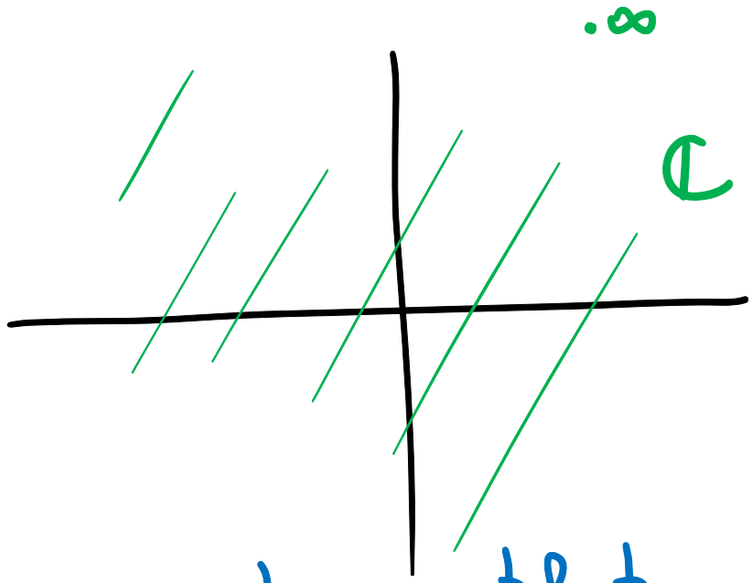
$$R_{E/F} = R_{E/\mathbb{Q}} = 1$$

then H10 is false over $\mathcal{O}_F$, the ring of integers of F.

Complex Analysis "Sweet Spot"

A central object of study is a Riemann Surface:
a connected one-dimensional complex manifold.

FACT: {compact R.S.} $\longleftrightarrow$ {complex smooth proj. alg. curves/$\mathbb{C}$}



one pt. compactification

$\longleftrightarrow$

Riemann Sphere

$\cong \mathbb{P}^1(\mathbb{C})$

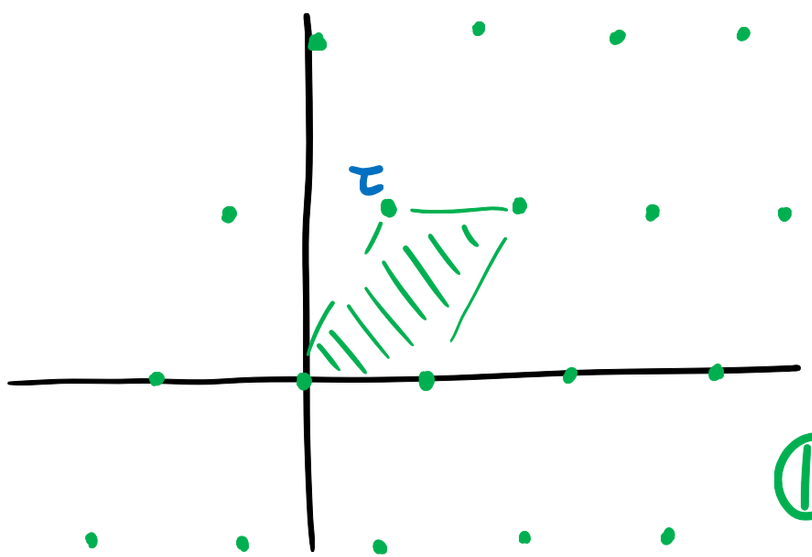
$g=0$

(positive curvature.)

Complex Analysis "Sweet Spot"

A central object of study is a Riemann Surface:
a connected one-dimensional complex manifold.

FACT: {compact R.S.} $\longleftrightarrow$ {complex smooth proj. alg. curves/$\mathbb{C}$}



uniformization theorem

$\cong E(\mathbb{C})$
ell. curves/$\mathbb{C}$
$g=1$
(zero curvature)

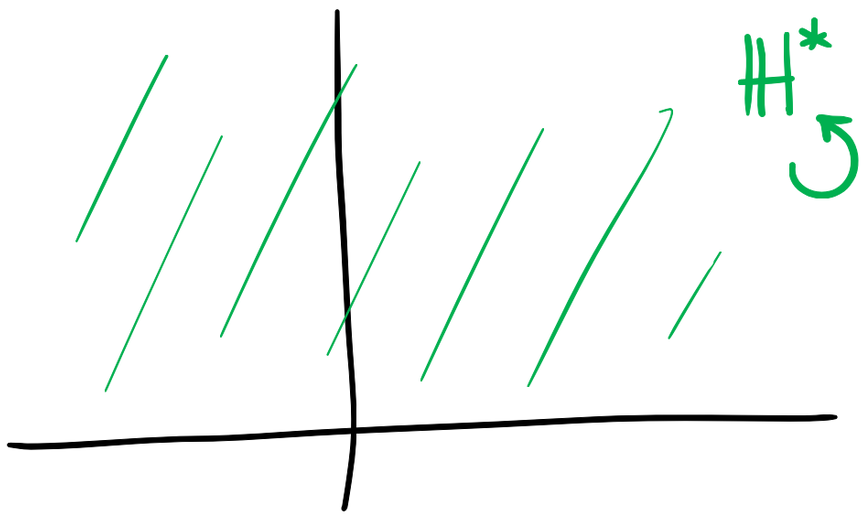
$\mathbb{C}/\Lambda = \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$

$\therefore$ natural gp structure! $\therefore$

Complex Analysis "Sweet Spot"

A central object of study is a Riemann Surface:
a connected one-dimensional complex manifold.

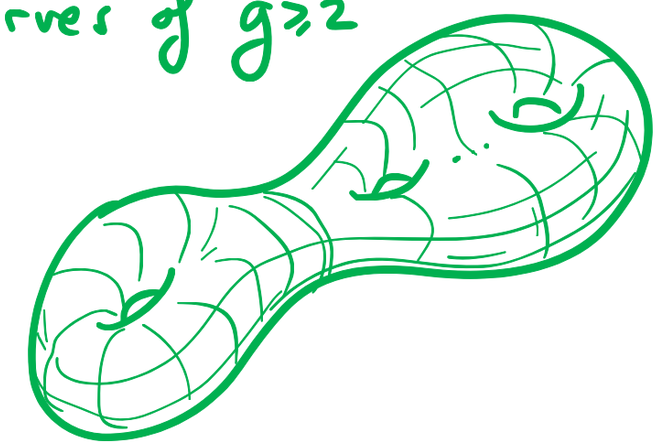
FACT: {compact R.S.} $\longleftrightarrow$ {complex smooth proj. alg. curves/$\mathbb{C}$}



$\mathbb{H}^*$ $\curvearrowright \Gamma$

$\mathbb{H}^*/\Gamma$ $\longleftrightarrow$ Curves of $g \geq 2$

(neg. curvature)

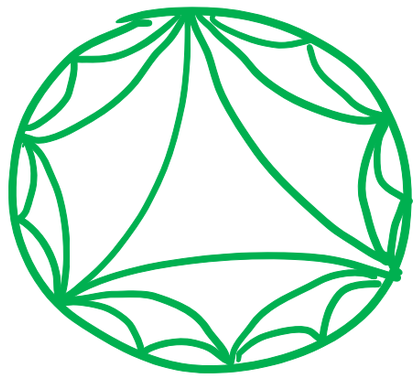


Holomorphic Diff. Forms ⇝ Modular Forms ⟷ * Elliptic Curves !

Algebraic Topology ⇝ Hopkins - Mahowald - Miller Topological Modular Forms

$\mathbb{H}^*/\Gamma$

hyperbolic Poincare plane



Art!

Escher Tilings.

Complex Analysis "Sweet Spot"

$$\left\{\mathbb{C}/\Lambda_\tau\right\}_{/iso} \longleftrightarrow \left\{E/\mathbb{C}\right\}_{/iso} \longleftrightarrow \mathbb{C}$$

$$\mathbb{C}/\Lambda_\tau \longleftrightarrow y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \longleftrightarrow j(\tau)$$

$$z \bmod \Lambda_\tau \longleftrightarrow (\wp(z,\Lambda), \wp'(z,\Lambda)) \qquad \frac{12^3 \cdot g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}$$

where

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \quad \text{w/ } q = e^{2\pi i \tau}$$

is the modular j-invariant function.

Group Theory ??

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \quad \text{w/ } q = e^{2\pi i \tau}$$

$r_1 = 1$

$r_1 + r_2$

$r_1 + r_2 + r_3$

(John McKay in 1978)

Group Theory ??

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \quad \text{w/ } q = e^{2\pi i \tau}$$

$r_1 = 1$ $\qquad$ $r_1 + r_2$ $\qquad$ $r_1 + r_2 + r_3$

where r_i = dim. of irreducible representations of M, the **MONSTER GROUP!**

(John McKay in 1978)

↓

Conway-Norton

↓

Borcherds, 1992 ✓

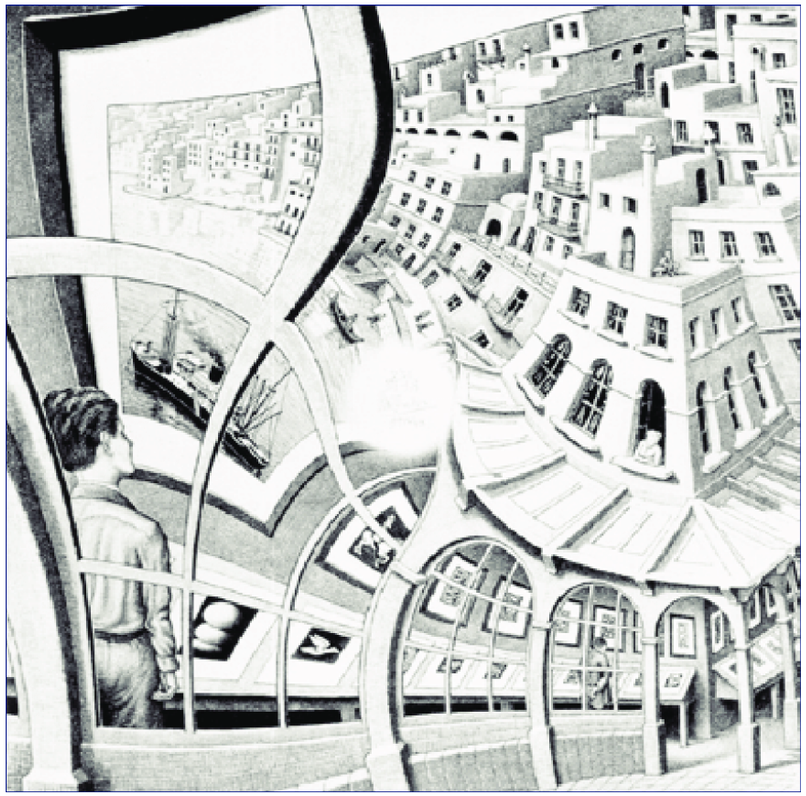
$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \quad \text{w/ } q = e^{2\pi i \tau}$$

$$E: y^2 + y = x^3 - 2174420x + 1234136692$$

$$\tau = \frac{1+\sqrt{-163}}{2} + \text{CM} \Rightarrow j(\tau) \text{ is an integer}$$

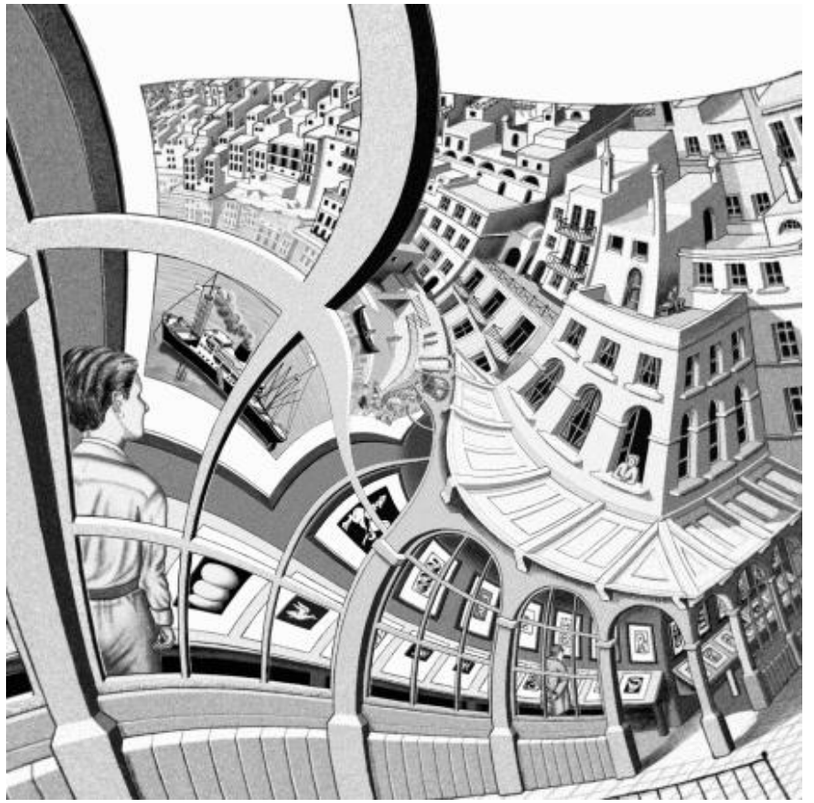
$$-\frac{1}{q} = e^{\pi\sqrt{163}} \text{ is very close to an integer}$$

$\mathbb{C}/\Lambda$ and Art!



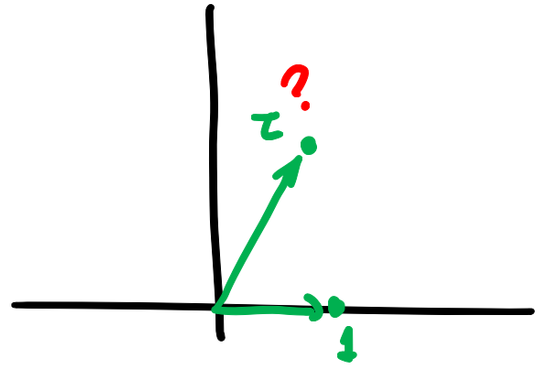
Escher's incomplete
"Prentententoonstelling"

de Smit
+
Lenstra

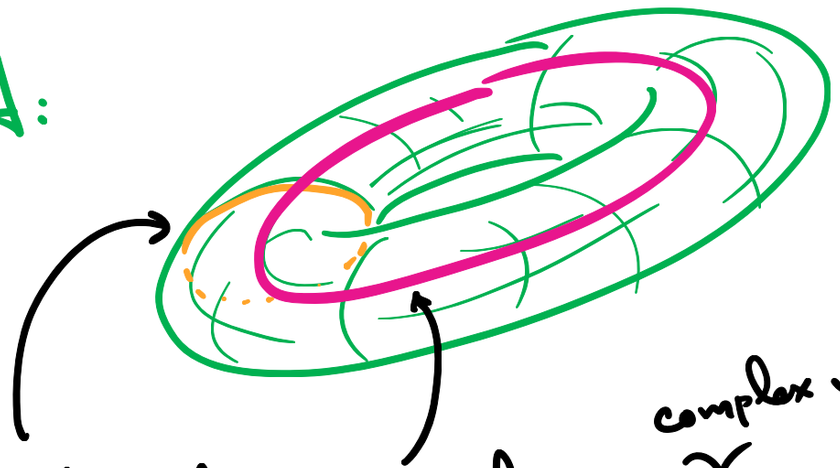


Escher's complete
"Prentententoonstelling"

Q Given $E/\mathbb{C}$ what is Λ_τ?



A:

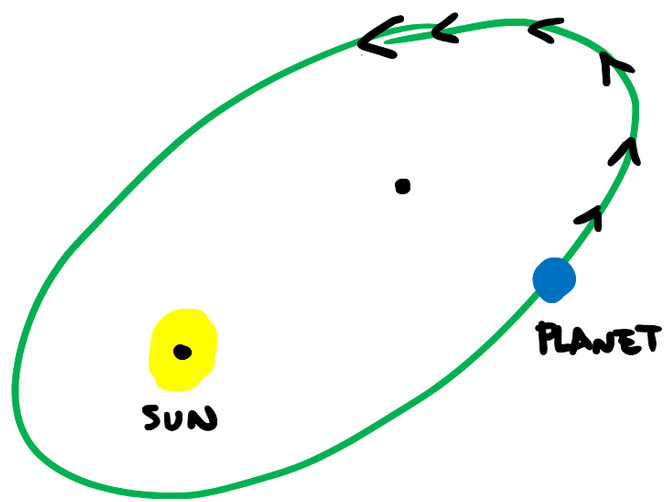


two line integrals give complex values ω_1, ω_2 s.t. $\Lambda = \langle \omega_1, \omega_2 \rangle$

Why "elliptic" curves?

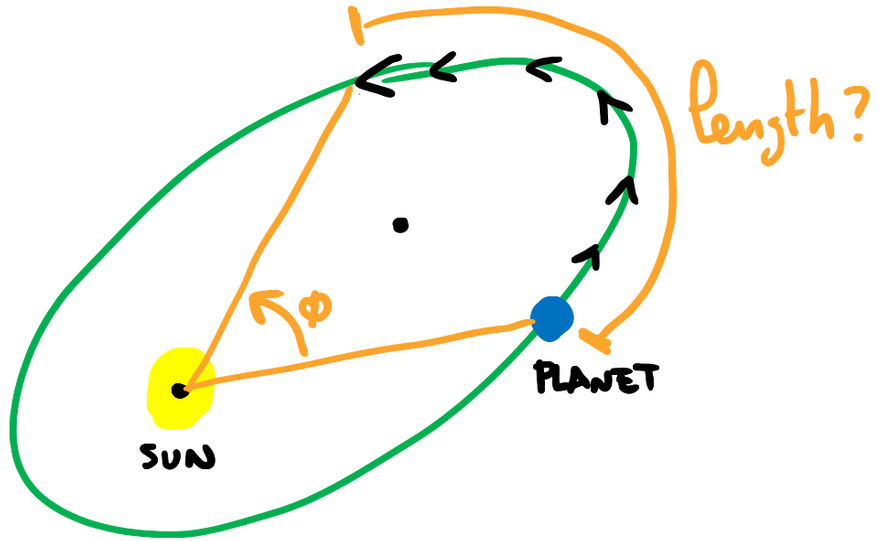
Elliptic curves in the Physics "Sweet Spot" ... in the 1600's!

Kepler's Laws (1609-1619):
Planets move in elliptical orbits around the Sun.



Kepler's Laws (1609 - 1619):

Planets move in elliptical orbits around the Sun.



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

Q Arc length on an ellipse?

Soln as an inf. series: Newton, Euler, ...

As an integral?

Circumf.: $4\int_0^{\pi/2} \sqrt{a^2\cos^2 t + b^2 \sin^2 t}\, dt = 2\int_{b^2/a^2}^{1} \frac{t\,dt}{\sqrt{t(t-1)(t-b^2/a^2)}}$

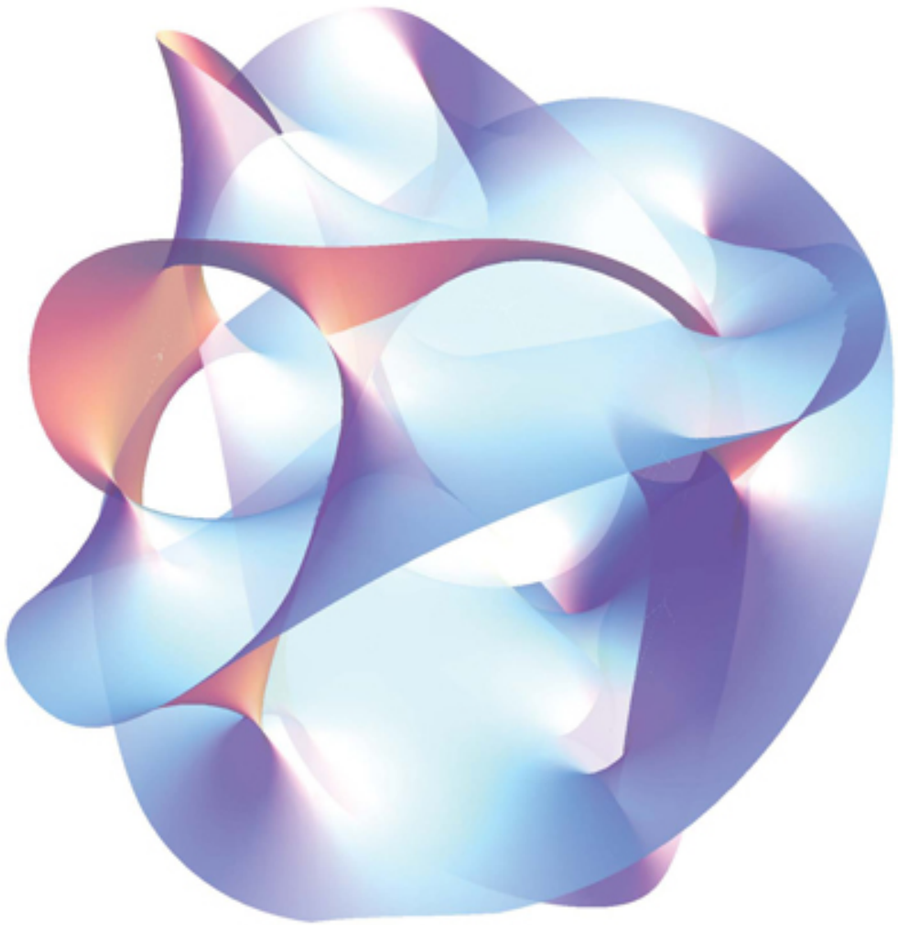
Arc length: $u = F(\phi) \longleftrightarrow \phi = F^{-1}(u)$

Jacobi
Abel

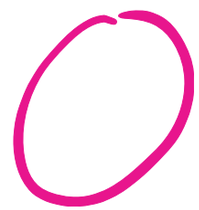
ELLIPTIC FUNCTIONS
$\wp(z)$

$y^2 = x(x-1)(x-b^2/a^2)$

Physics in the 1900's : String Theory



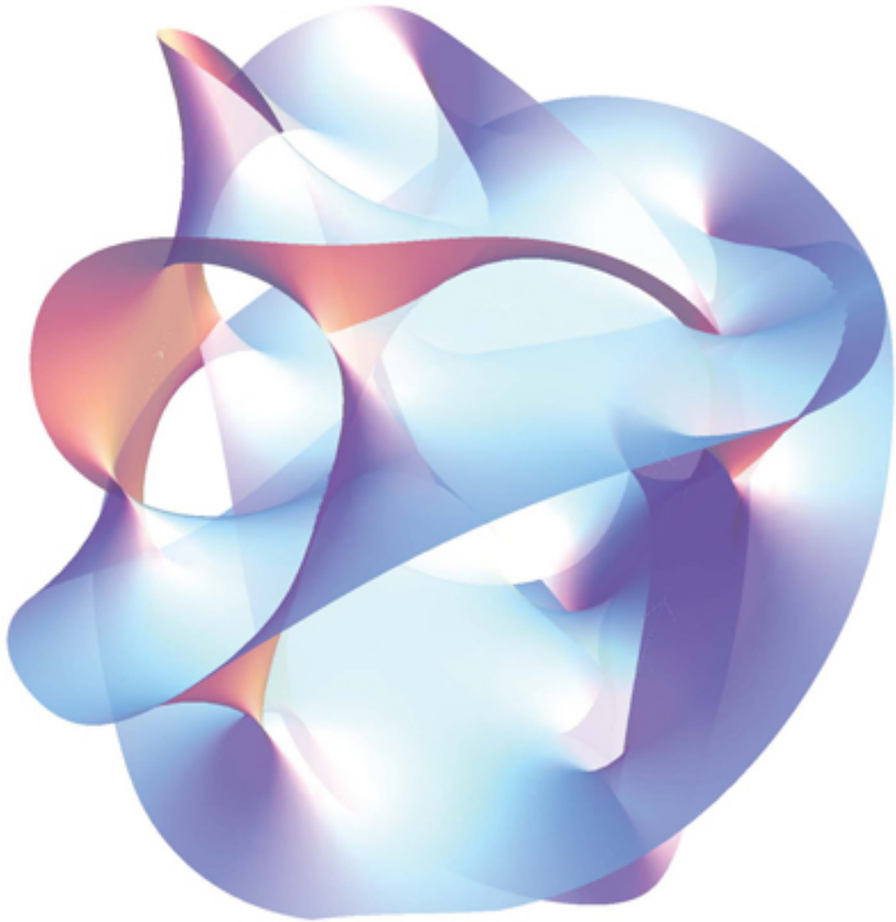
Space time in 6- or 23-dimensional Calabi-Yau manifold

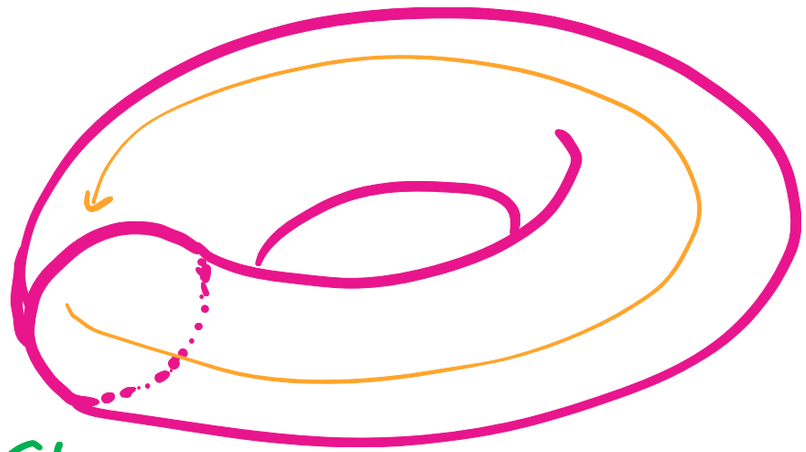


String

Physics in the 1900's : String Theory

Space time is 6- a 23-dimensional Calabi-Yau manifold



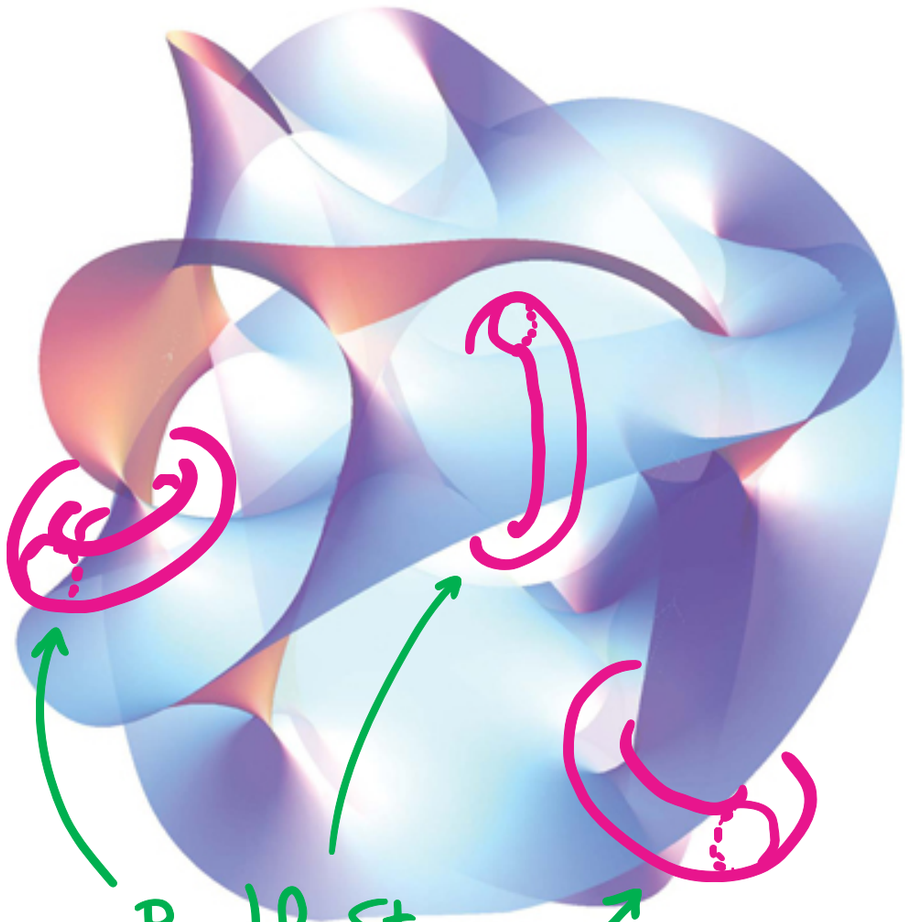


String
Closed Path

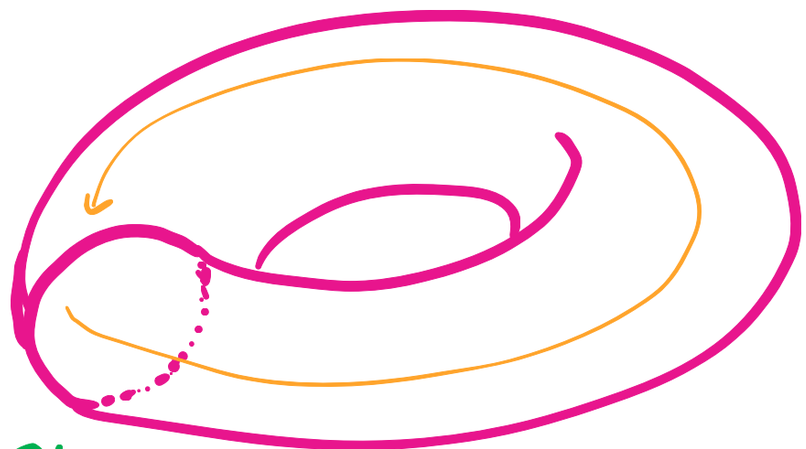
Physics in the 1900's : String Theory

Space time is 6- or 23-dimensional

Calabi-Yau manifold



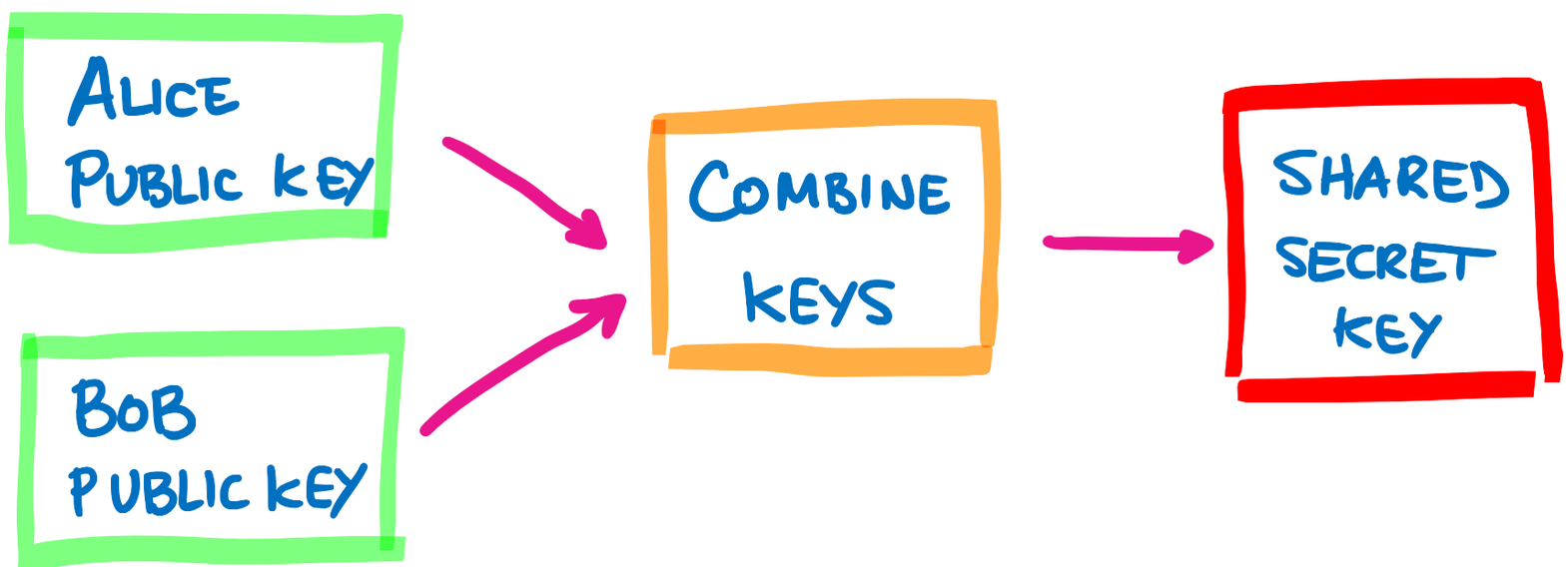
Possible Strings
"Vibrations"



String
Closed Path

Complexity "Sweet Spot"

Public Key Cryptography: Public Key Exchange



Diffie - Hellman (on $\mathbb{Z}/p\mathbb{Z}$)

1) Agree on a (public) prime p and base g

2) Alice :
   - chooses secret exponent a
   - public key: $A \equiv g^a \bmod p$

3) Bob :
   - chooses secret exponent b
   - public key : $B \equiv g^b \bmod p$

4) Alice and Bob compute secret key:

$$S \equiv B^a \equiv A^b \equiv g^{ab} \bmod p$$

STRENGTH:

DISCRETE LOG PROBLEM

Now replace $\mathbb{Z}/p\mathbb{Z}$ by another group that offers:

- efficiency (key storage/transmission economy)
- greater security

Abstract Group ⇝ *ALGEBRAIC* GROUP ⇝ ABELIAN VARIETIES ($\dim \geq 1$) ⇝ **ELLIPTIC CURVES** ($\dim = 1$)

Elliptic Curve Diffie-Hellman

1) Agree on p, ell. curve $E/\mathbb{F}_p$, and $G \in E(\mathbb{F}_p)$

2) Alice: · choose a
· publish $A = [a](G) \in E(\mathbb{F}_p)$

3) Bob: · choose b
· publish $B = [b](G) \in E(\mathbb{F}_p)$

4) Alice and Bob compute secret key:

$$S = [a](B) = [b](A) = [ab](G)$$

Example: WhatsApp

Use RSA directly to encrypt?

STRENGTH:

FACTORIZATION OF INTEGERS

ELLIPTIC CURVE FACTORIZATION ALGORITHM!

Lenstra:
- Pick $E/\mathbb{Q}$, P of infinite order, compute $P' \equiv P \bmod n$
- Compute $[k](P')$ for k with many small prime divisors p
  - ↳ if it works, new E, P, k
  - ↳ if it doesn't, $\exists\, p \mid k$ s.t. $p \mid n$.

ECDSA : Elliptic Curve Digital Signature

EXAMPLES PS3, Bitcoin.

2010 : Reused k

2013 : alg. for k caused "collisions"

1) Pick E, $G \in E$ of large prime order p

2) Alice:
- Private key d_A, Public key : $[d_A](G) = A$
- Message to be signed : z (integer or l-most bits of message)
- Select "SAFE" $k \in \{1, \dots, n-1\}$
- Compute $[k](G) = (x_1, y_1)$ → SIGNATURE : $(x_1, k^{-1}(z + r \cdot d_A)) \bmod p$ ~ (r, s)

3) Bob : Verify signature:
- $A \in E$ ✓
- $(u_1, u_2) = (zs^{-1}, rs^{-1}) \bmod p$ ✓
- $(x_1, y_1) = [u_1](G) + [u_2](A)$

  if $x_1 \equiv r \bmod p$ ✓

Sweet Spot ?? Maybe just...

LAW OF SMALL NUMBERS

- Dioph. eqn's w/ small degree → Conics, ell. curves
- Riemann surfaces of low genus
- Abelian varieties of low dimension
- "Weak" computing power

Thank You!

alvaro@uconn.edu