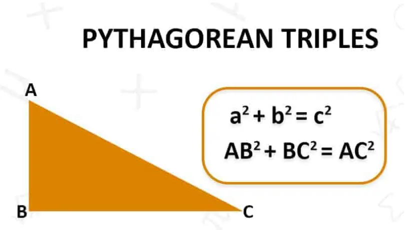
What is...the Birch–Swinnerton-Dyer conjecture?

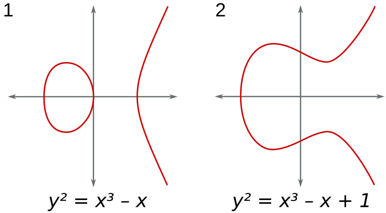
Or: Counting, of course

Rational solutions

general Diophantine:

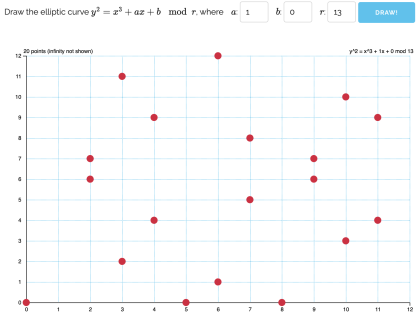


elliptic curves:



- **Task** Find integer/rational solutions to Diophantine equations
- **Elliptic curves** "=" something of the form $y^2 = x^3 + ax + b$
- **Easier** than general equations but still **nontrivial**

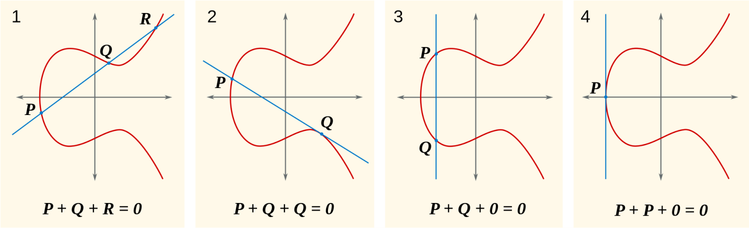
Counting mod p

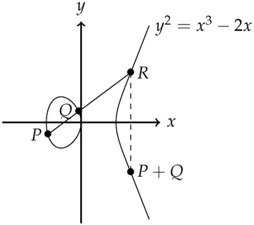



```
> K<w> := FiniteField(2, 160); // finite field of size 2^160
> f<x> := MinimalPolynomial(w); f;
x^160 + x^5 + x^3 + x^2 + 1
> E := EllipticCurve([K| 1, 0, 0, 0, w]);
> time #E;
1461501637330902918203686141511652467686942715904
Time: 0.050
```

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, \ldots, p-1\}$ = integers modulo the prime p
- Finding points in $\mathbb{F}_p$ of elliptic curves is easy
- Dream Use the solutions mod p to say something about the rational solutions

Elliptic groups





- The above defines an abelian group structure on the rational points $E(\mathbb{Q})$ of an elliptic curve
- Fact $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \bigoplus_k \mathbb{Z}/m_k\mathbb{Z}$ and surprisingly little is known about r
- Question Can one determine the rank r?

Enter, the theorem

For an elliptic curve E of rank r setup the following:

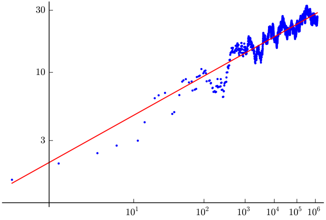
(i) Let N_p=number of points on E modulo p Easy to get

(ii) Set $f:\mathbb{N}\to\mathbb{Q}, x\mapsto\prod_{p\leq x}N_p/p$ Easy to get

(iii) Conjecture We have asymptotically $f\sim\mathrm{const.}\log(x)^r$

(iv) The conjecture is true if $r=0$

- Here is an example for $y^2=x^3-5$ (red=expected value, blue=actual value):



- There is a more general version which is the actual conjecture

Analytic method

```
> n := 101000;
> S := [ p : p in [1..n] | IsPrime(p) ];
> X := 1;
> for p in S do
>     ok, E := IsEllipticCurve([GF(p) | 0, 1, 0, 0, 1 ]);
>     if ok
>     then X := X*#E/p;
>         if p ge 100000 then
>         print RealField(10)!X/Log(p);
>         end if;
>     end if;
> end for;
```

Cancel Submit

```
1.972420629
1.972243705
1.967074969
1.968638530
1.978595716
1.982372770
```

- The conjecture was born in the 1950s by computer help (and was one of the first conjectures coming from computer aid)
- Note that we can compute r from the asymptotic if the conjecture is true
- The conjecture addresses an algebraic question analytically

Thank you for your attention!

I hope that was of some help.