Elliptic curve

From Wikipedia, the free encyclopedia

Not to be confused with Ellipse.

In mathematics, an **elliptic curve** is a plane algebraic curve defined by an equation of the form

$$y^2 = x^3 + ax + b$$

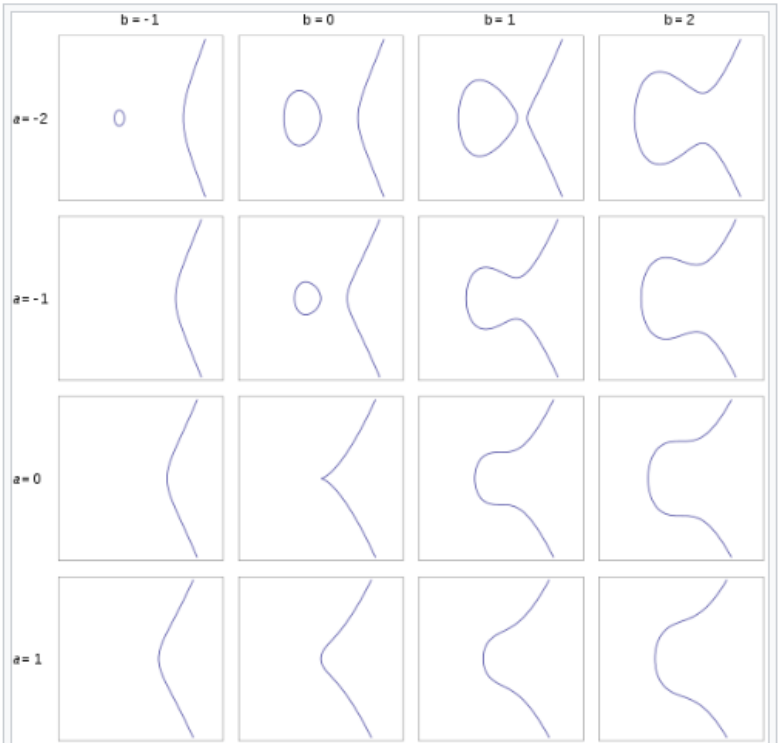
which is non-singular; that is, the curve has no cusps or self-intersections. (When the coefficient field has characteristic 2 or 3, the above equation is not quite general enough to comprise all non-singular cubic curves; see § Elliptic curves over a general field below.)

Formally, an elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O. An elliptic curve is an abelian variety – that is, it has a multiplication defined algebraically, with respect to which it is an abelian group – and O serves as the identity element. Often the curve itself, without O specified, is called an elliptic curve; the point O is often taken to be the curve's "point at infinity" in the projective plane.

If $y^2 = P(x)$, where P is any polynomial of degree three in x with no repeated roots, the solution set is a nonsingular plane curve of genus one, an elliptic curve. If P has degree four and is square-free this equation again describes a plane curve of genus one; however, it has no natural choice of identity element. More generally, any algebraic curve of genus one, for example from the intersection of two quadric surfaces embedded in three-dimensional projective space, is called an elliptic curve, provided that it has at least one rational point to act as the identity.

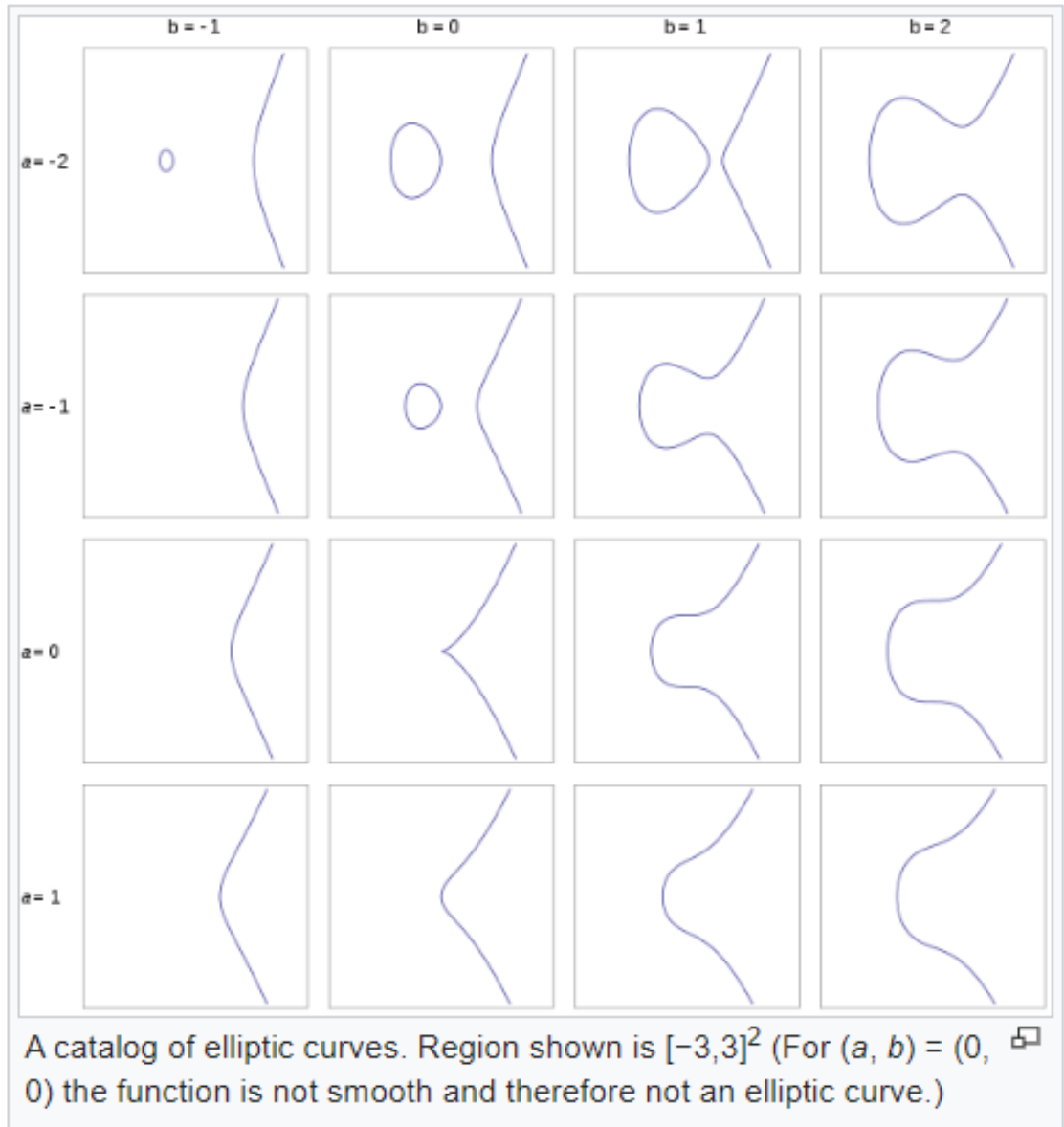
Using the theory of elliptic functions, it can be shown that elliptic curves defined over the complex numbers correspond to embeddings of the torus into the complex projective plane. The torus is also an abelian group, and in fact this correspondence is also a group isomorphism.

Elliptic curves are especially important in number theory, and constitute a major area of current research; for example, they were used in the proof, by Andrew Wiles, of Fermat's Last Theorem. They also find applications in elliptic curve cryptography (ECC) and integer factorization.



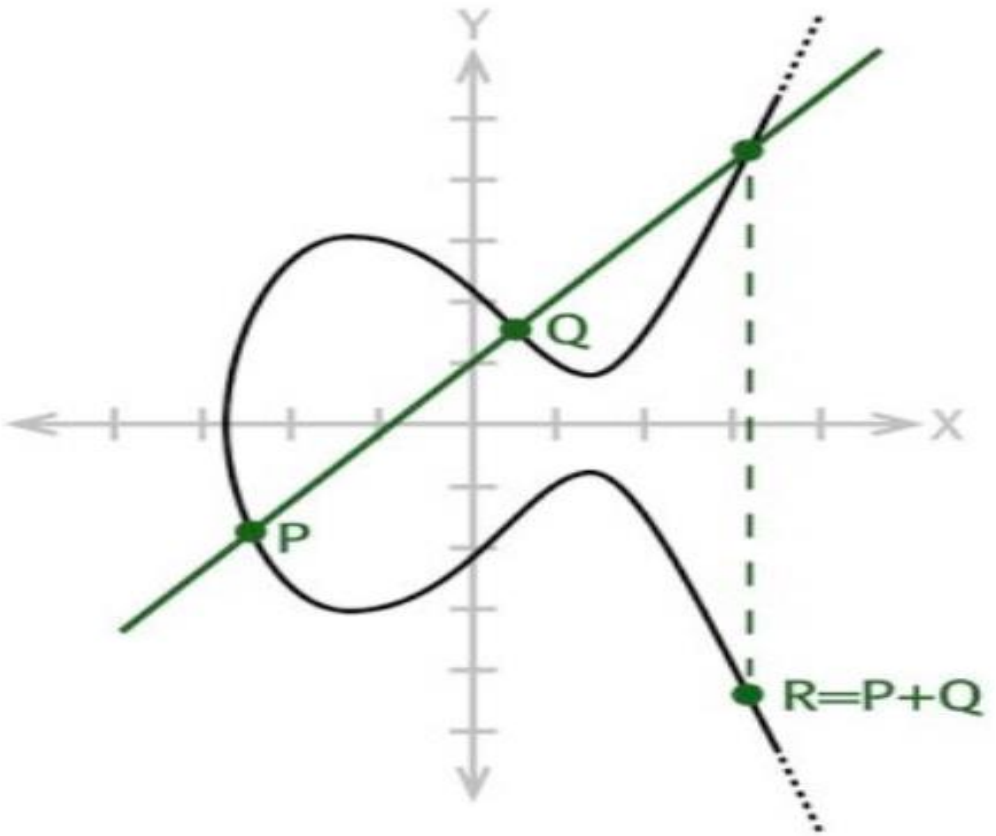
A catalog of elliptic curves. Region shown is $[-3,3]^2$ (For $(a, b) = (0, 0)$ the function is not smooth and therefore not an elliptic curve.)

$$y^2 = x^3 + ax + b$$

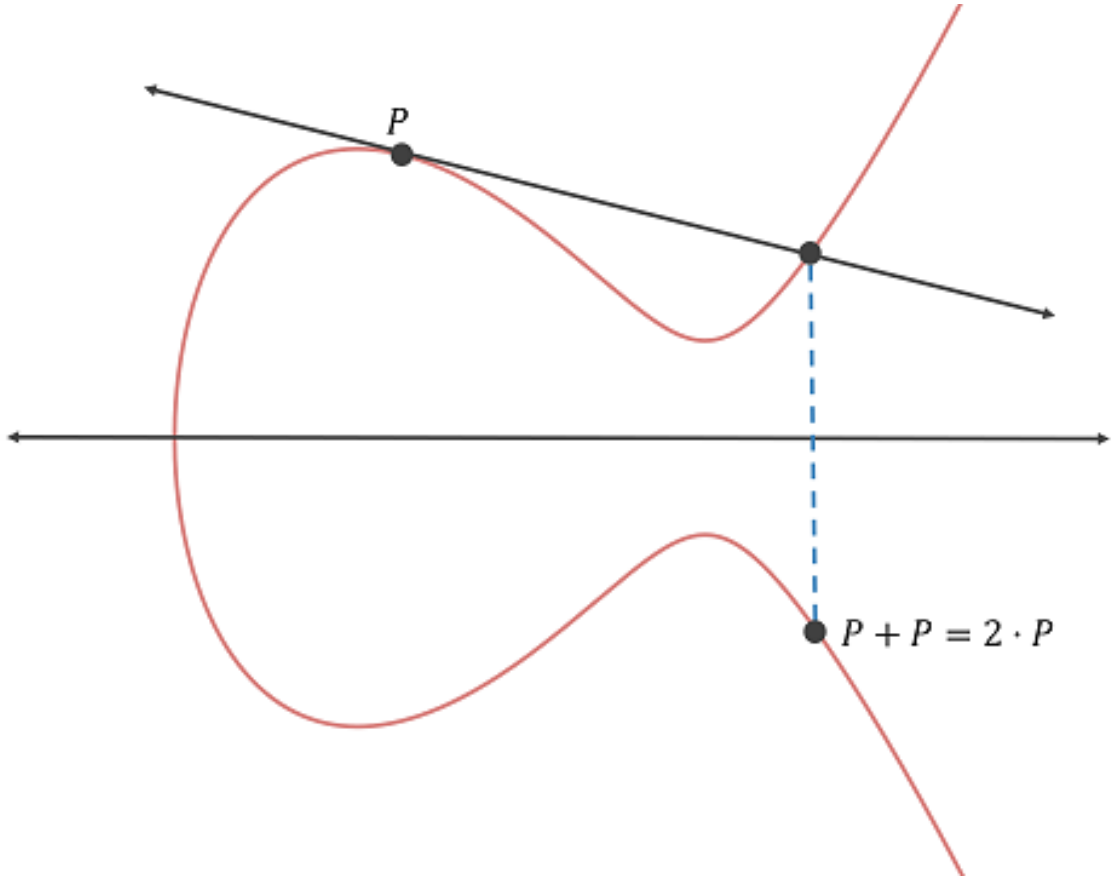


A catalog of elliptic curves. Region shown is $[-3,3]^2$ (For $(a, b) = (0, 0)$ the function is not smooth and therefore not an elliptic curve.)

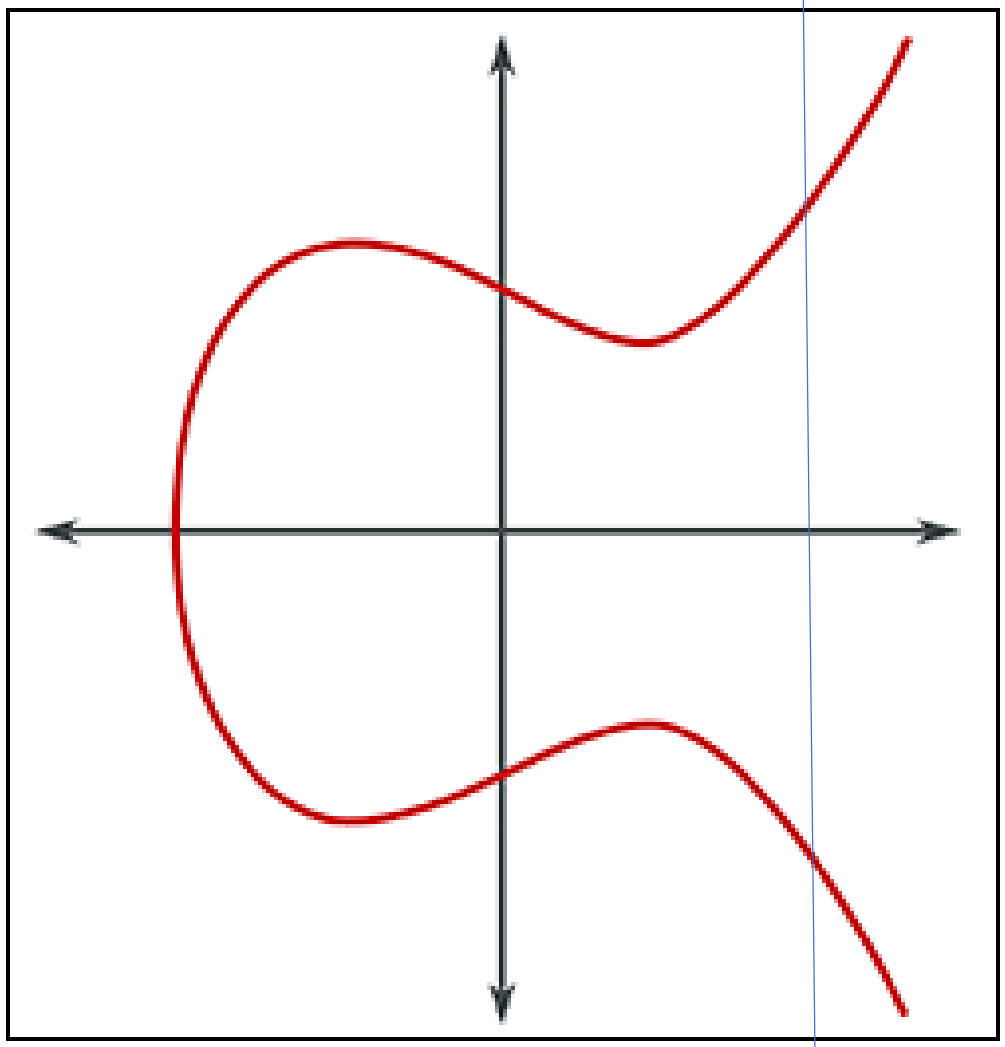
Grupová operace na eliptické křivce



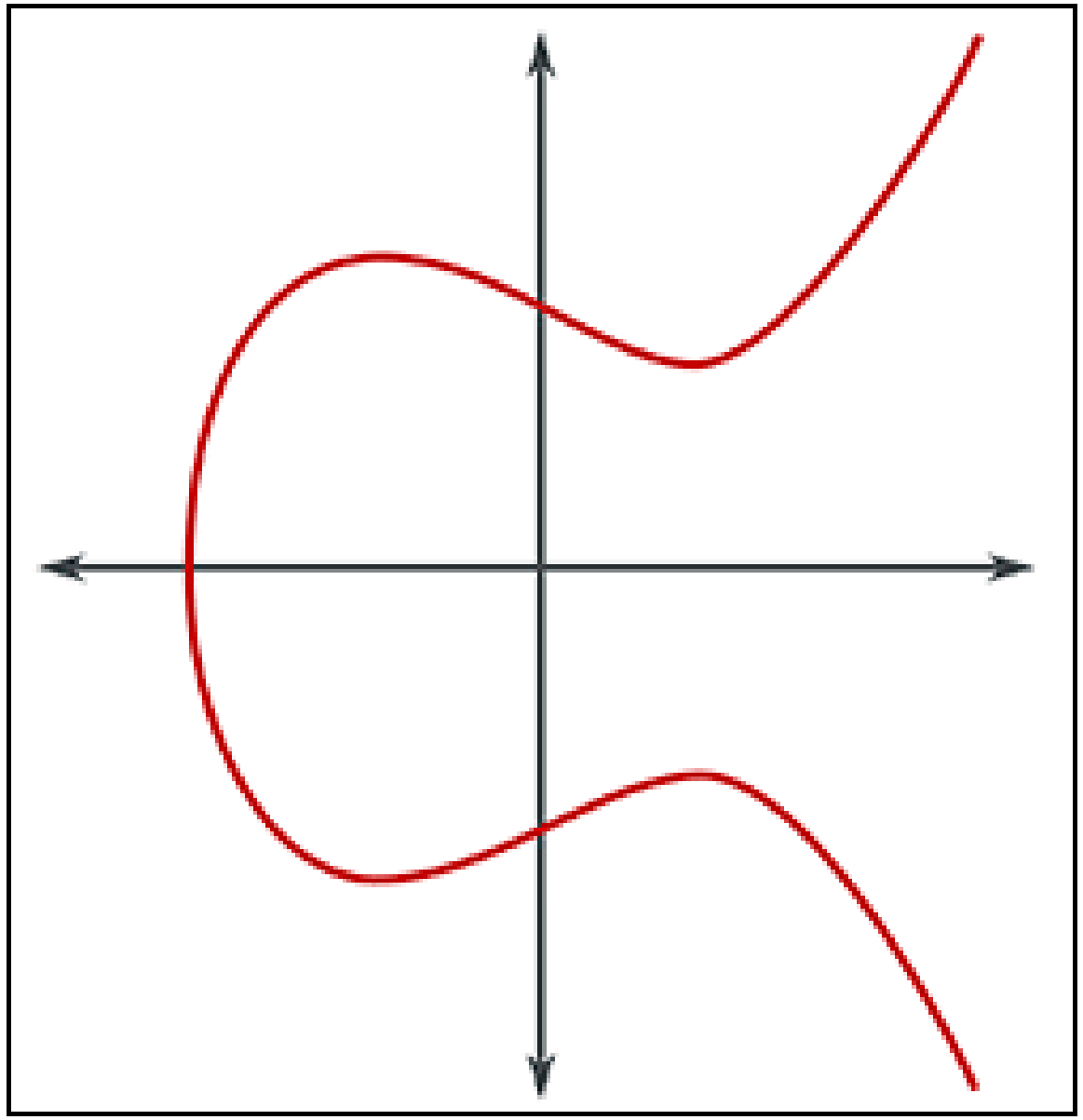
Grupová operace na eliptické křivce



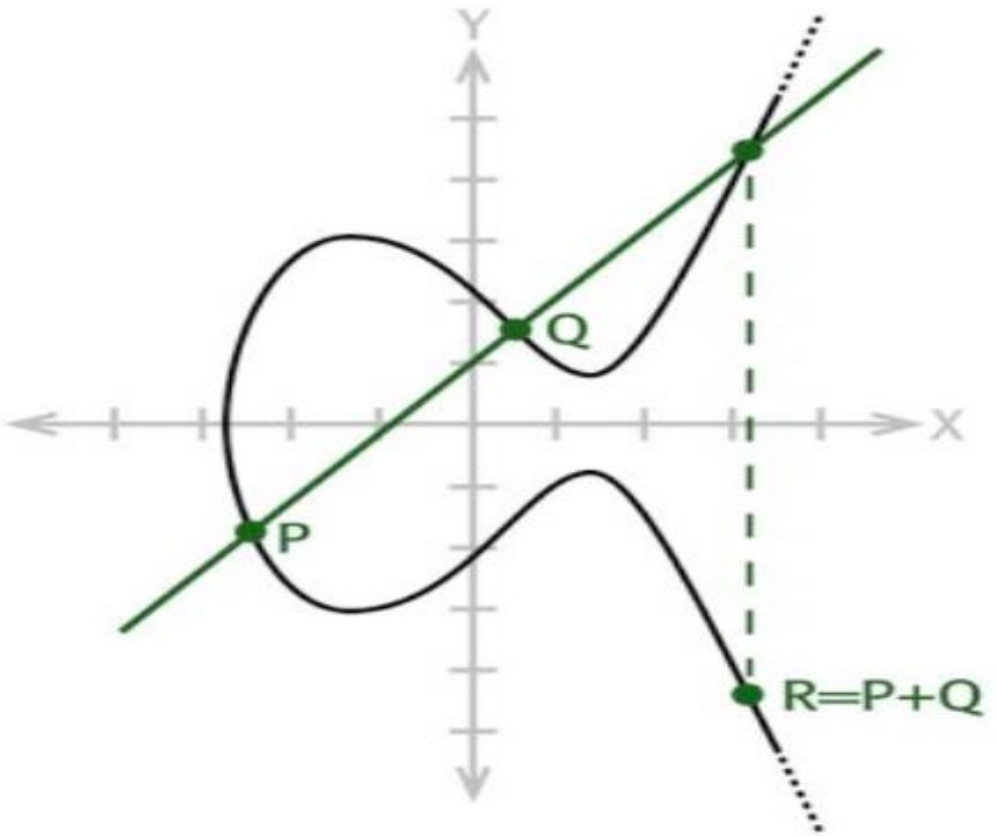
Jednotka a inverz



Asociativita



Podgrupa $E_T(f)$ pro číselné těleso T



Eliptické křivky a teorie čísel

Křivky nad tělesem **Q** = diofantické rovnice

Grupa $\mathbf{E}_{\mathbf{Q}}$ umožňuje konstruovat nová řešení:

A $\longrightarrow$ 2A=A+A, 3A, -6A, …

A, B $\longrightarrow$ A+B, 7A-13B, …

Podobný trik se použije pro Pellovu rovnici: $(x + \sqrt{s}y)^n$

Mordell-Weilova věta: $E_T(f)$ je konečně generovaná

(pro libovolné $\mathbb{Q} \leq T$ konečného stupně)

$$\Rightarrow \quad E_T(f) \simeq \mathbb{Z}^r \times \left(\mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_n^{k_n}} \right)$$

$\mathbb{Z}^r$: prvky nekonč. řádu; $\mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_n^{k_n}}$: konečná

Birch & Swinnerton-Dyerova domněnka (za \$1M)

- $\prod_{p \leq x} \frac{N_p}{p} \approx c \cdot (\log x)^r$ kde $N_p = \#$ bodů na křivce f v $\mathbb{Z}_p$

Eliptické křivky a kryptografie

Křivky nad konečnými tělesy – všechno funguje jako nad **C**

Fakt: Grupa $E_{Fq}(f)$ má často prvek velkého řádu (řádově jako q)

➔ Uvažuj grupu G generovanou tímto prvkem

- Snadno se počítají mocniny
- Nezná se algoritmus na výpočet diskrétního logaritmu

➔ Diffie-Hellmanův protokol, El Gamalův protokol, atd.

Apple HomeKit and Curve25519. We give one last application of elliptic curves which is causing something of a controversy. Apple Computers has software which developers are slow to use because the software uses elliptic curves. Apple has created *HomeKit*, a platform for connecting your smartphones with WiFi and Bluetooth enabled accessories such as lights, cameras, and thermostats. Apple wishes to have strong security in this platform, so it has decided to employ 3072-bit encryption—much, much stronger than the 256-bit key Advanced Encryption Standard (AES).

To this end, Apple has asked developers to use elliptic curve cryptography for digital signatures and encrypted keys; the most secure seems to be an elliptic curve called `Curve25519`. Rather concretely, this is the curve $E : y^2 = x^3 + 486662\,x^2 + x$ defined over the field $k = \mathbb{F}_q$, where $q = (2^{255} - 19)^2$ is the square of a prime number. Daniel J. Bernstein et al. [3] showed that the abelian group $E(\mathbb{F}_q)$ has a subgroup $(\mathbb{Z}/n\,\mathbb{Z})$ of order

$$n = 2^{252} + 27742317777372353535851937790883648493$$

as generated by a K-rational point $P = (x_1 : y_1 : 1)$ having coordinate $x_1 = 9$. It is thought that elliptic curve cryptography is to blame for the slow rollout of *HomeKit*-ready devices for the market: developers are finding the mathematics behind this implementation to be. . . unusual.