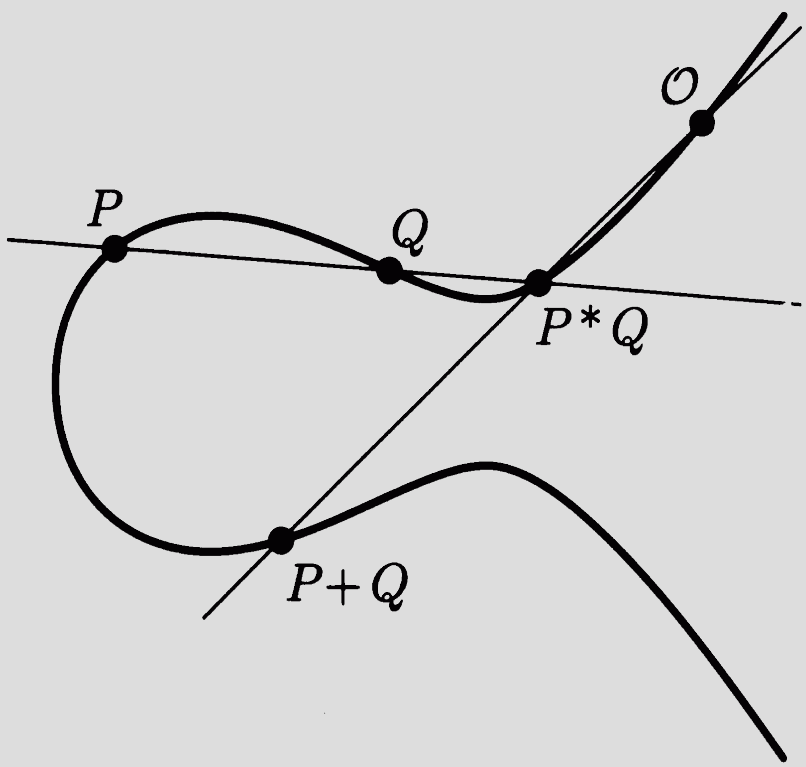
Eliptické křivky

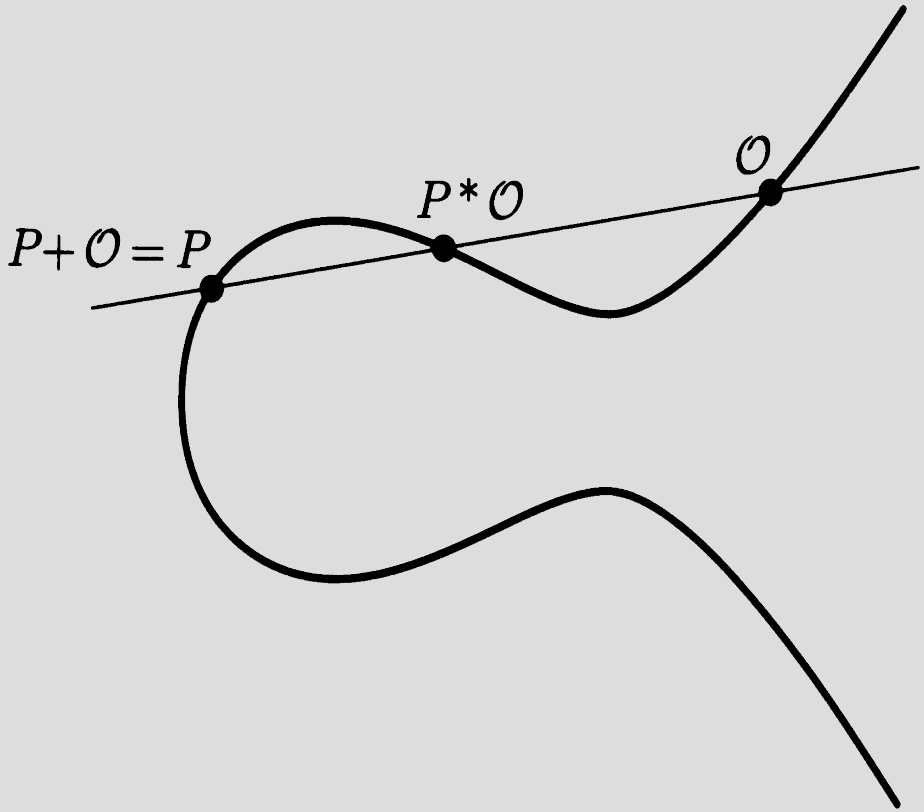
- Využití v šifrování
- Rozklady na prvočísla
- Alternativa k RSA
- Objevena N. Koblitzem roku 1985

Algebraická křivka

- Uvažme množinu bodů v rovině splňující rovnost $y^2=ax^3+bx^2+cx+d$ a na této křivce uvažme bod *O*. Nyní budeme definovat sčítání bodů na této křivce.

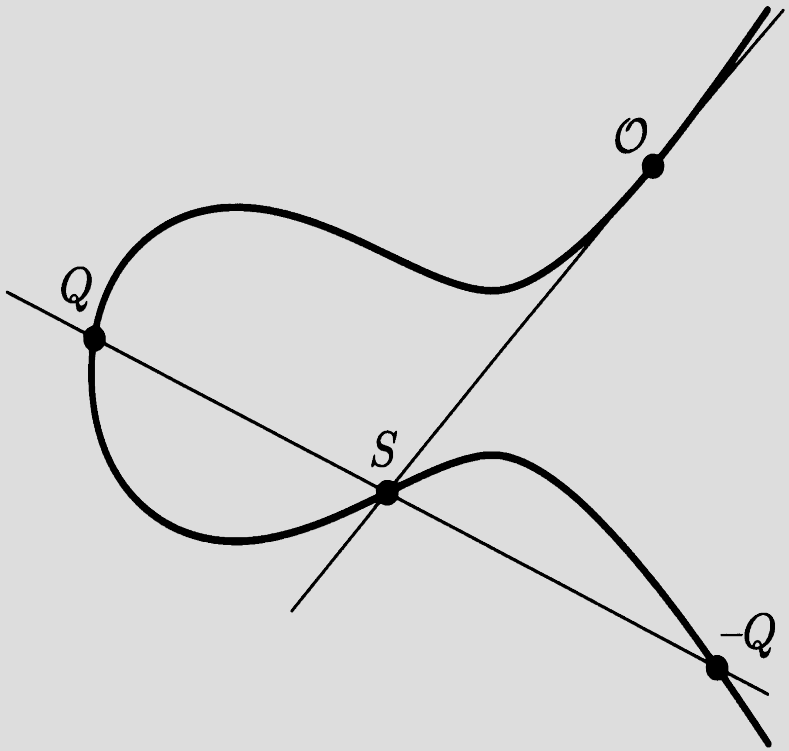
Sčítání bodů na křivce

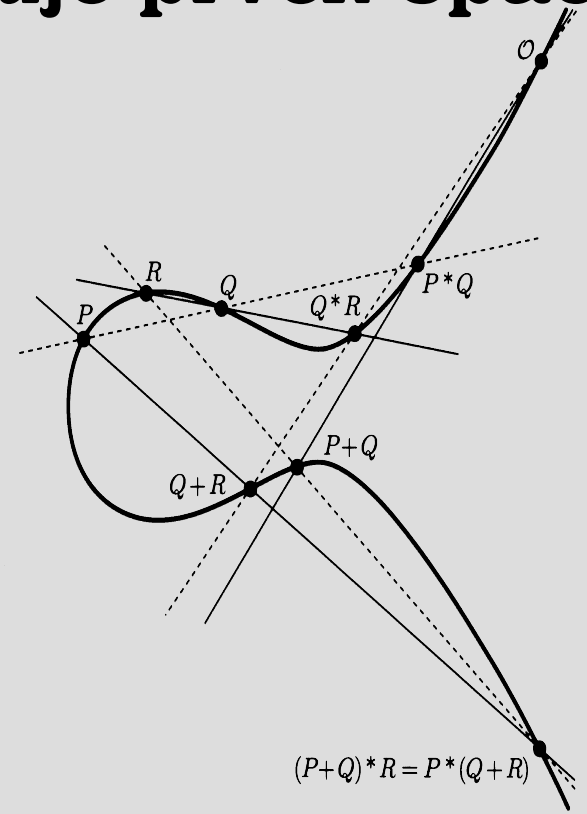




Sčítání bodů na křivce

- **Operace sčítání je komutativní, asociativní s neutrálním prvkem O a ke každému prvku existuje prvek opačný.**





Co je eliptická křivka

- **Definice: Eliptickou křivkou budeme rozumět již zmíněnou množinu bodů spolu s bodem O a operací +.**
- **Každou eliptickou křivku můžeme převést na tvar $y^2=x^3+ax+b$ (Weierstrassova forma), kde bodem O bude nevlastní bod přímky $x=0$**

Sčítání bodů na křivce

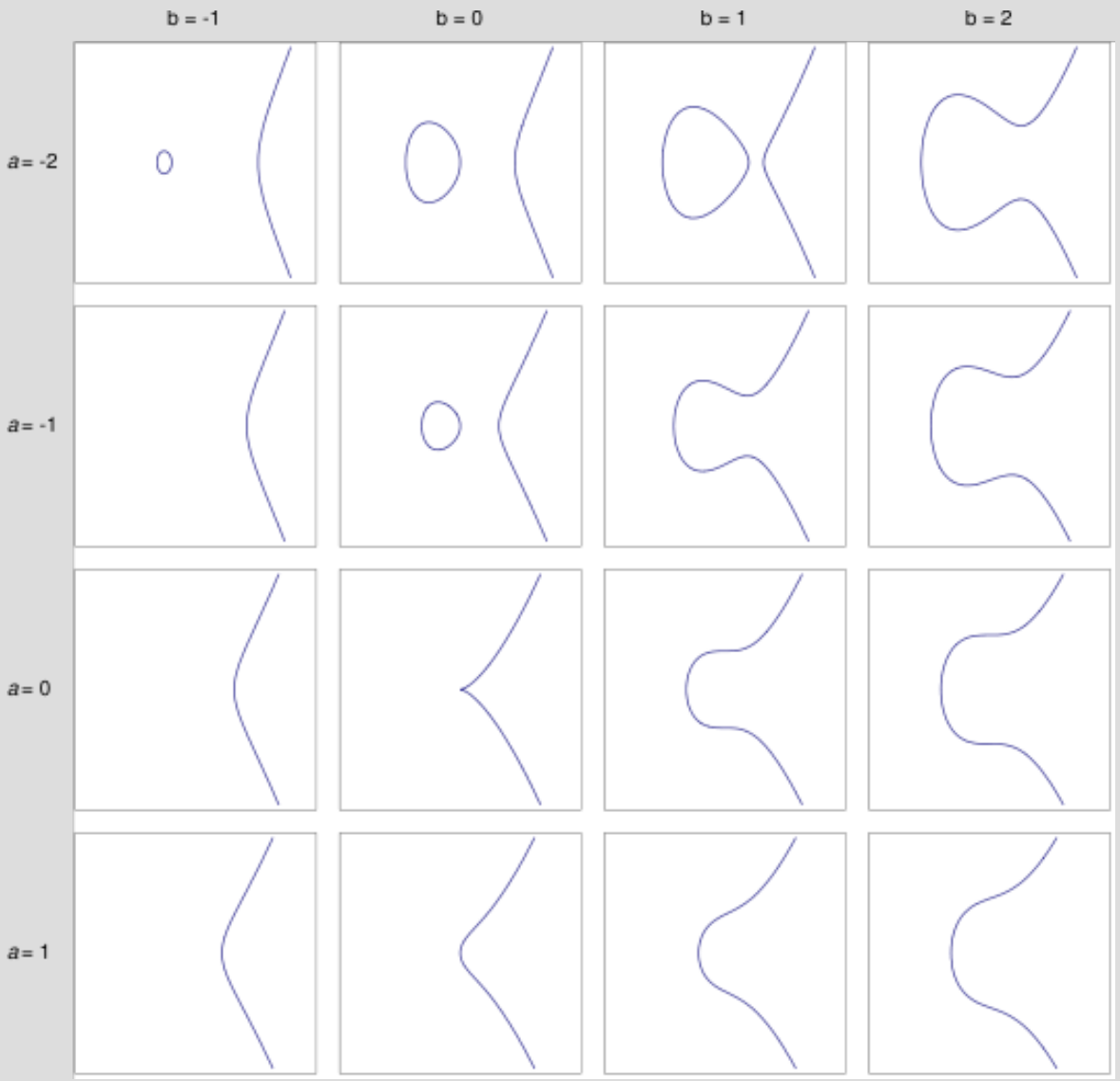
- Máme-li body $A[p,q]$, $B[r,s]$, potom bod

$$A+B=[E^2-p-r,\ E(p-r)-q],$$

kde $E=s-q/r-p$ ..... pokud $A \neq B$

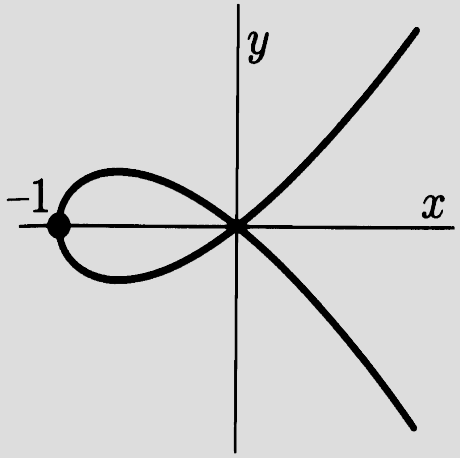
$E=3p^2-a/2q$ ... pokud $A=B$

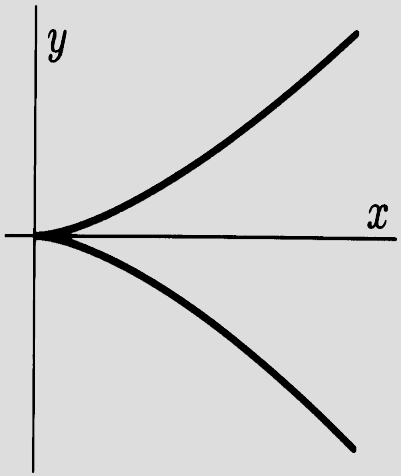
Eliptické křivky

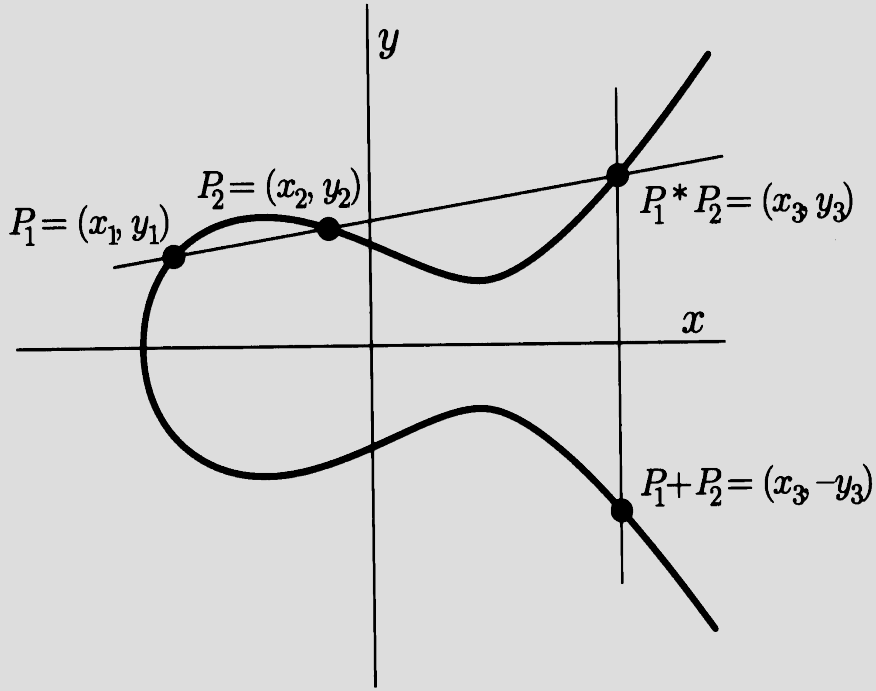


Eliptické křivky

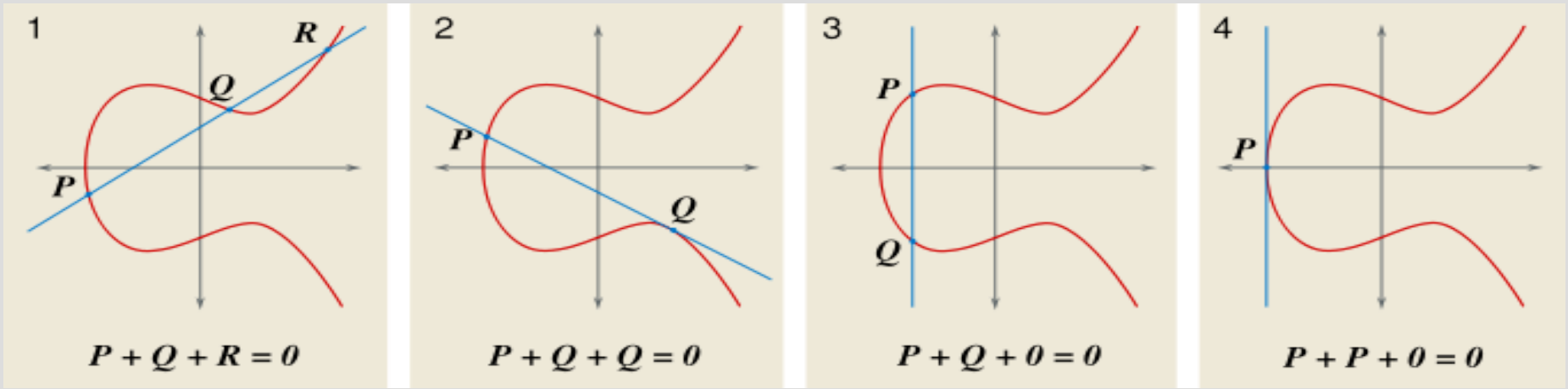
- Řekneme, že Eliptická křivka je nesingulární, jestliže $4a^3+27b^2 \neq 0$







Eliptické křivky



Eliptické křivky nad jiným tělesem

- Doposud jsme se bavili o eliptických křivkách, kde koeficienty byly reálná čísla. Co ale zvolit jako koeficienty zbytkové třídy modulo nějaké prvočíslo.

Zbytkové třídy

- Nechť m je libovolné přirozené číslo. Uvažme rozklad množiny celých čísel takový, že v jedné třídě rozkladu budou ležet všechna celá čísla, která dávají stejný zbytek po dělení přirozeným číslem m. Tedy dvě čísla leží ve stejné třídě, jestliže jsou spolu kongruentní modulo m.
- Třídě rozkladu říkáme zbytková třída modulo m. S těmito zbytkovými třídami můžeme počítat jako s celými čísly.

Opět eliptické křivky

- Počítá se stejně jako s eliptickými křivkami nad reálnými čísly, pouze modulo prvočíslo p.
- Příklad: Určete body na eliptické křivce $y^2=x^3+x+1$, $y^2=x^3+3x+1$ nad tělesem zbytkových tříd modulo 5.

Řád prvku

- Řekneme, že bod P eliptické křivky je řádu r, jestliže $rP=O$.
- Například bod C je řádu 2, bod O je řádu 1
- Řád libovolného prvku dělí počet prvků eliptické křivky
- Pokud každý prvek eliptické křivky můžeme napsat jako nějaký násobek prvku P, potom bod P nazýváme generátor.

Šifrování pomocí EK

- Máme-li bod P na nějaké eliptické křivce. Zvolíme libovolné (velké) přirozené číslo r a spočítáme rP, což je nějaký bod Q eliptické křivky. Nyní pokud bychom chtěli z bodů P a Q určit číslo r, je to velmi obtížné. Tomuto úkolu se říká Problém diskrétního logaritmu

Šifrování pomocí EK

- **Obě strany komunikace si dohodnou bod P na eliptické křivce. Každá strana si zvolí přirozené číslo k (privátní klíč) a vypočítají Q=kP, což bude veřejný klíč. Pokud tedy Ondra má privátní klíč a, veřejný klíč A=aP, Zdenda má privátní klíč b, veřejný klíč B=bP. Potom tedy pokud dostanu od Zdendy veřejný klíč B a spočítám Z=aB=abP, dostanu stejný bod, který spočítá Zdenda, když od Ondry dostane bod A, tedy bA=baP=Z.**

Elektronický podpis

- **Vytvoření veřejného klíče:**
  - **Vybereme eliptickou křivku E nad Z_p , počet prvků eliptické křivky by měl být dělitelný velkým prvočíslem n**
  - **Zvolíme bod P na E řádu n**
  - **Zvolíme privátní klíč d z intervalu (1,n-1)**
  - **Vypočítáme bod Q=dP**
  - **Veřejný klíč tvoří čtveřice (E,P,n,Q)**

Vytvoření podpisu

- Mějme zprávu m
- Vybereme k z intervalu (1,n-1)
- Vypočítáme bod kP, r bude jeho první souřadnice modulo n
- Je-li r=0, zvolíme jiné k
- Vypočítáme k^{-1} mod n
- Vypočítáme s= k^{-1} (h(m)+dr)
- Je-li s=0, zvolíme jiné k
- Podpis potom tvoří čtveřice (r,s)

Ověření podpisu

- Mějme zprávu m a její podpis (r,s) a veřejný klíč (E,P,n,Q)
- Ověříme, že r,s jsou z intervalu (1,n-1)
- Vypočteme $w=s^{-1} \bmod n$, dále vypočteme h(m)
- Vypočteme $u_1=h(m)w \bmod n$, $u_2=rw \bmod n$
- Vypočteme první souřadnici v bodu na eliptické křivce u_1P+u_2Q
- Podpis je platný, pokud v=r