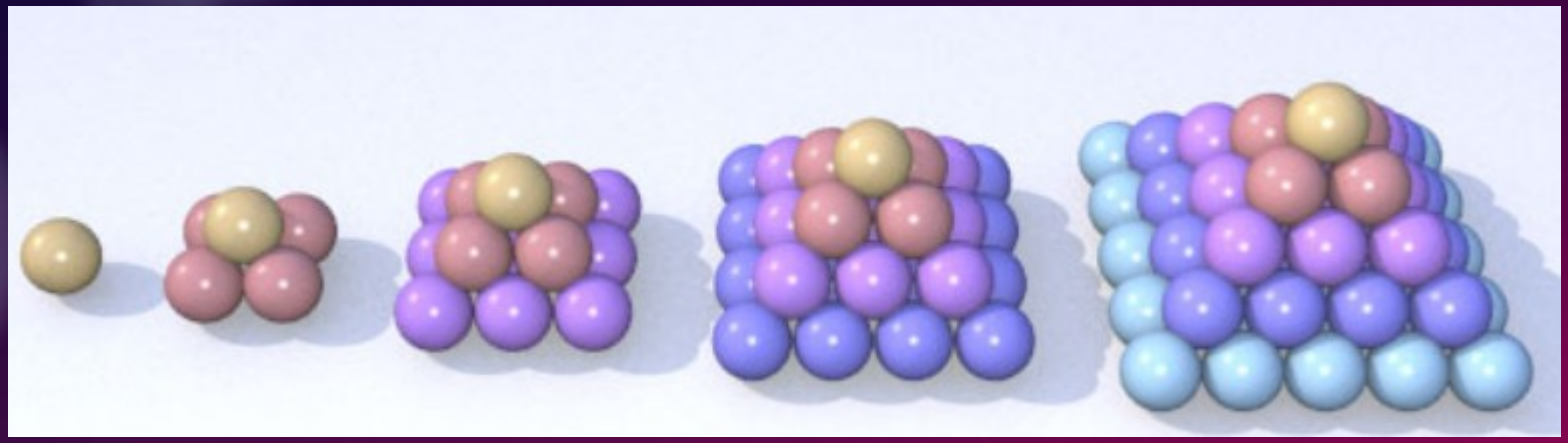
CURVE ELLITTICHE
&
CRITTOGRAFIA

Angela Zottarel
Mathesis
Padova, 28/01/2022

Piramidi

Immaginiamo una piramide di biglie, in cui ogni livello è un quadrato.



Se la piramide crollasse, riusciremmo a costruire un quadrato?

Per n=1 certo!

Per n=2 ci sono 1+4=5 biglie: no!

Per n=3 ci sono 1+4+9=14 biglie: no!

In generale, se la piramide ha altezza x, le biglie saranno: $1^2+2^2+3^2+\ldots+x^2=\frac{x(x+1)(2x+1)}{6}$

Se vogliamo ottenere una quadrato, dovremo risolvere l'equazione:

$$y^2=\frac{x(x+1)(2x+1)}{6}$$

Equazioni Diofantee – III sec

Risolvere il nostro problema significa cercare le soluzioni intere di $y^2=\frac{x(x+1)(2x+1)}{6}$

ovvero risolvere un’equazione diofantea!

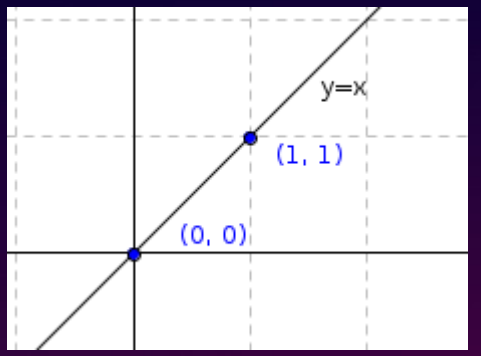
Il metodo usato da Diofanto ci permette di trovare nuove soluzioni partendo da soluzioni note.

Scriveremo la retta passante per i punti noti e andremo ad intersecare la curva data dall’equazione, sperando di ottenere una nuova soluzione

$$y^2=\frac{x(x+1)(2x+1)}{6}$$

Due soluzioni note sono (0,0) e (1,1).

La retta passante per questi punti è y=x



$$\begin{cases} y^2=\frac{x(x+1)(2x+1)}{6} \\ y=x \end{cases} \rightarrow x^2=\frac{x(x+1)(2x+1)}{6} \rightarrow \frac{1}{3}x^3-\frac{1}{2}x^2+\frac{1}{6}x=0$$

Ovvero otteniamo l'equazione $x^3-\frac{3}{2}x^2+\frac{1}{2}x=0$

Di cui conosciamo già due soluzioni.

Potremmo scomporre il polinomio...ma c'è un modo migliore!

Osserviamo che $(x-a)(x-b)(x-c)=x^3-(a+b+c)x^2+(ab+bc+ac)x-abc$

Troviamo quindi l'ultima soluzione x di $x^3-\frac{3}{2}x^2+\frac{1}{2}x=0$

come $0+1+x=\frac{3}{2}$ ovvero $x=\frac{1}{2}$

Con un po' di fatica abbiamo trovato un'altra soluzione razionale: (½, ½)!

E, vista la simmetria di $y^2=\frac{x(x+1)(2x+1)}{6}$, anche (½, -½) è una soluzione.

Se dovessimo ripetere questo metodo con i punti (1,1) e (½,-½) andremmo a trovare una soluzione ulteriore: (24,70)!

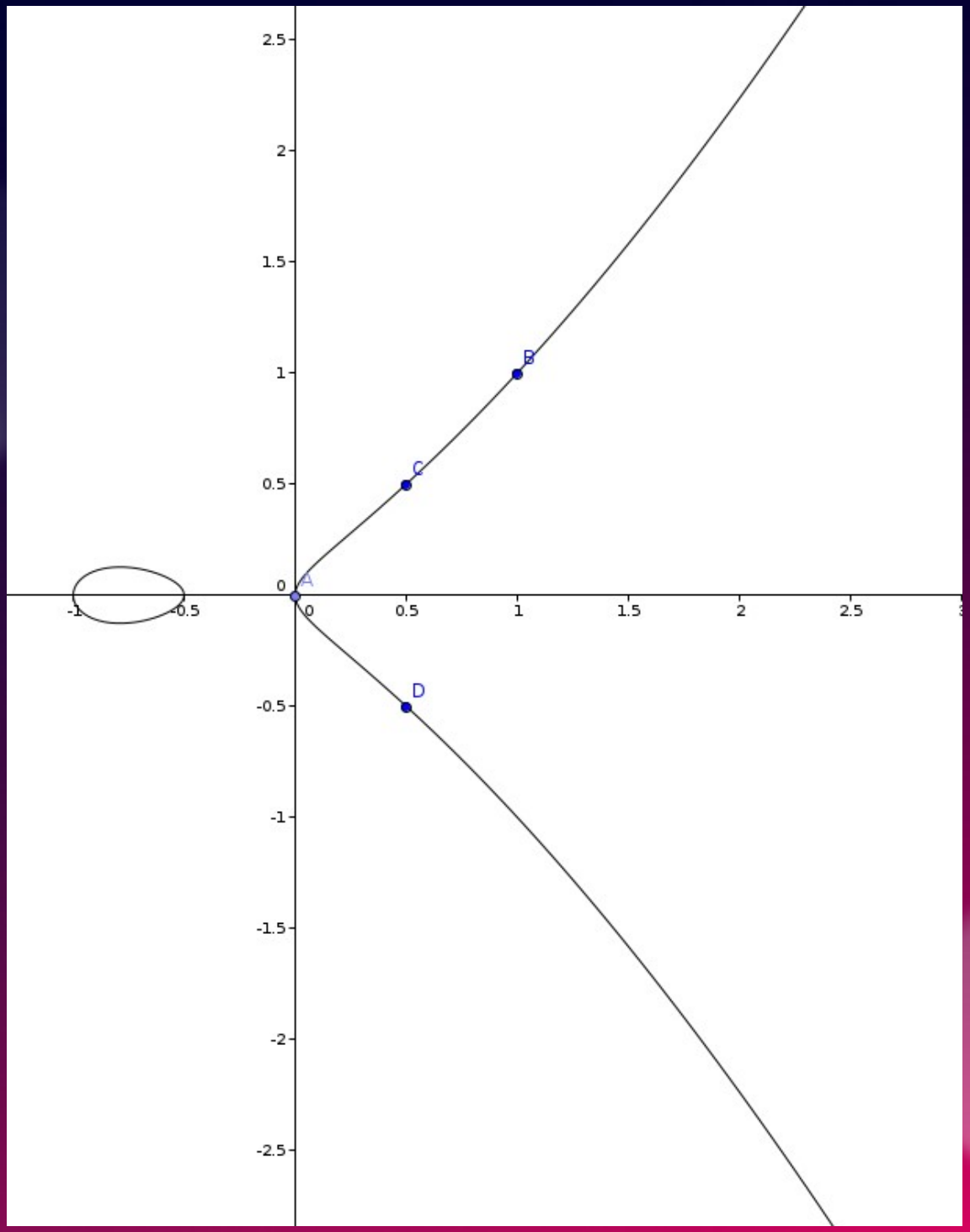
Una piramide con 24 piani può trasformarsi in un quadrato 70x70

Questa, assieme alla soluzione banale x=1, è l'unica soluzione intera positiva al nostro problema.

Biglie e curve

Ma cosa hanno a che fare queste piramidi e le curve ellittiche?

L’equazione $y^2=\frac{x(x+1)(2x+1)}{6}$ descrive una curva ellittica


2.5
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
-2.5
-1
-0.5
0
0.5
1
1.5
2
2.5
A
B
C
D

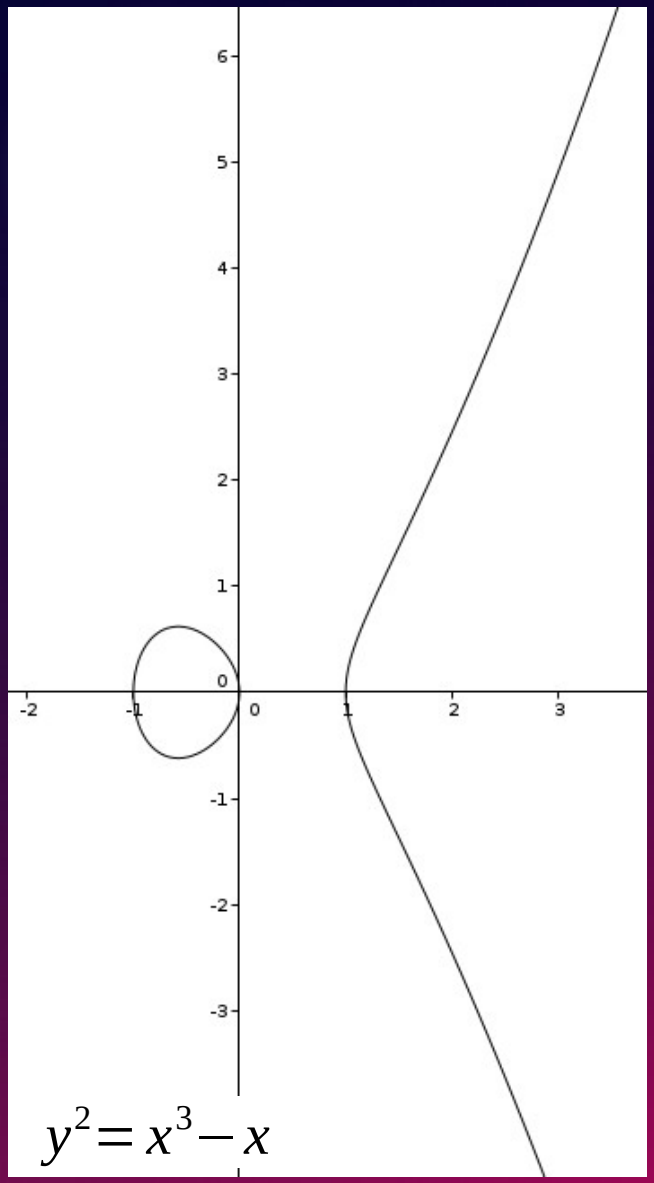
Equazioni di Weierstrass

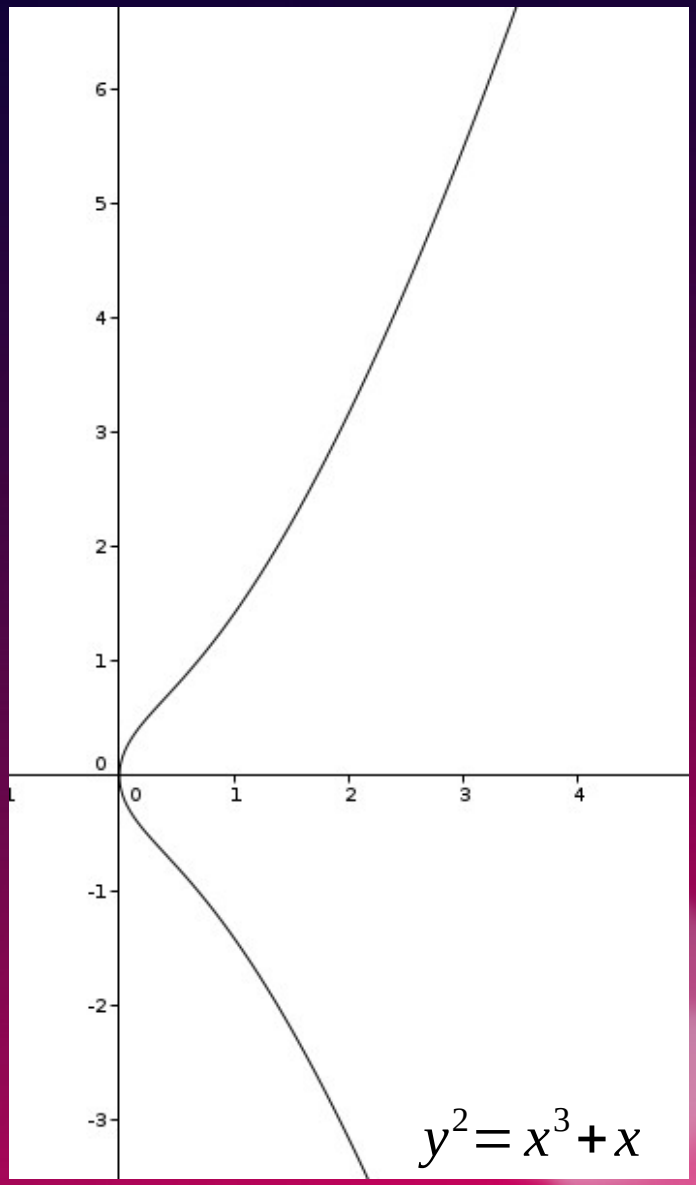
Una curva ellittica E è il grafico di una equazione del tipo: $y^2 = x^3 + Ax + B$

Non è la forma più generale, ma è nota come forma di Weierstrass di una curva ellittica.

Le costanti A e B, le variabili x e y possono essere definite su campi diversi...per semplicità pensiamo a R.

Curve ellittiche su R





Puntualizzazione

Nei due casi mostrati, le curve ellittiche hanno 3 zeri distinti o un solo zero reale.

Per evitare che ci siano zeri doppi si impone:

$$4A^3 + 27B^2 \neq 0$$

La curva ellittica è così non singolare.

- Ci sono forme più generali dell'equazione di Weierstrass...
- Si può mostrare che $cy^2 = dx^3 + ax + b$ può essere portata in forma di Weierstrass con un cambio di variabile.

Altre curve ellittiche

Soluzioni intere di $a^4+b^4=c^4 \rightarrow$ caso particolare dell'ultimo teorema di Fermat.

$$y^2=x^3-4x$$

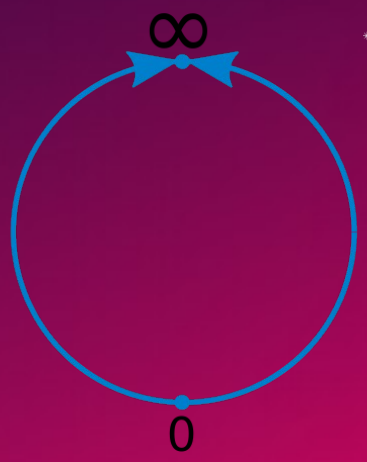
Anche $a^3+b^3=c^3$ può essere trasformata in una curva ellittica

$$y^2=x^3-432$$

Uno strano punto

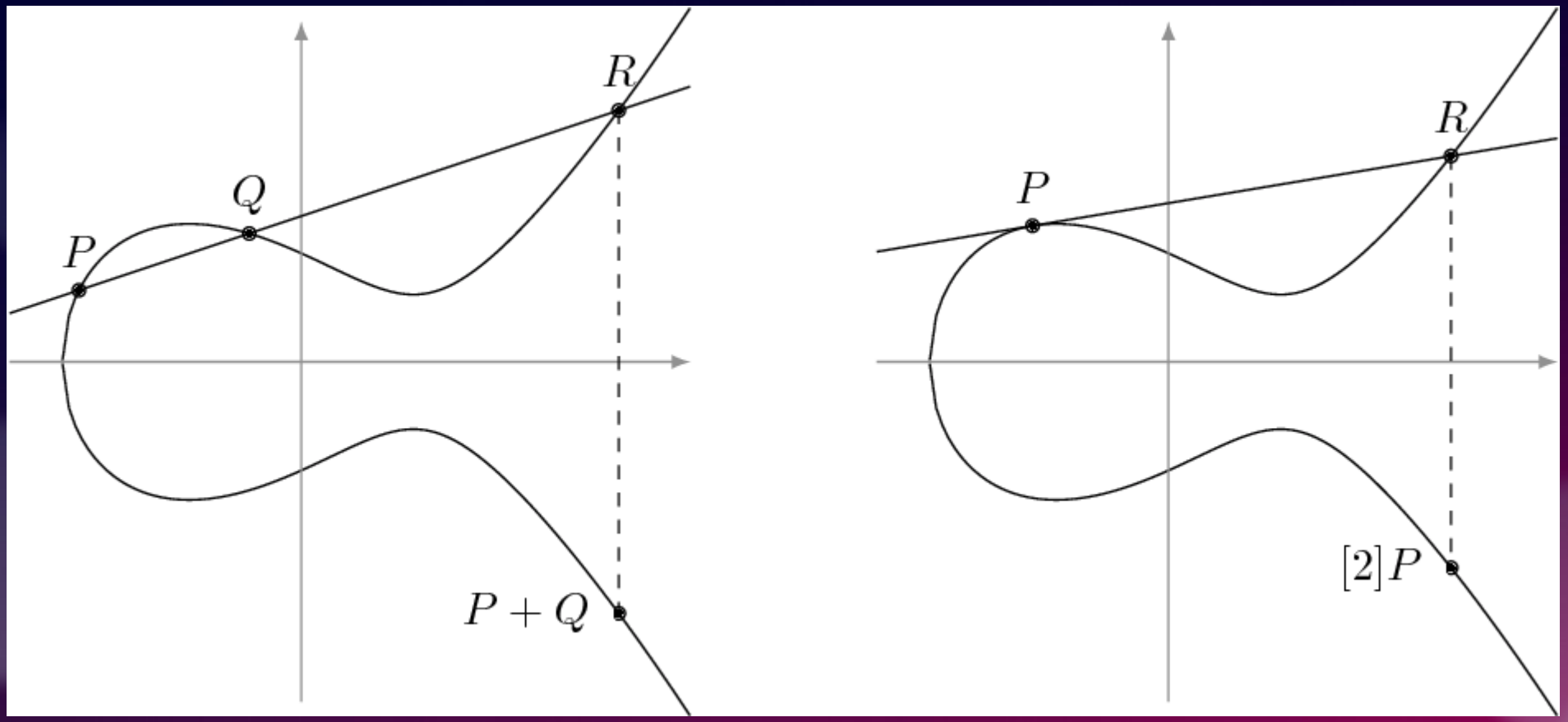
Ci sarà utile aggiungere un punto alle curve: ∞.

- Il punto (∞,∞) si trova in cima all'asse y.
- Tutte le rette verticali (x=k) passano per ∞.
- Tutte le rette verticali si intersecano in ∞.
- ∞ si trova anche sotto all'asse y: le due estremità di una retta verticale si incontrano in ∞.



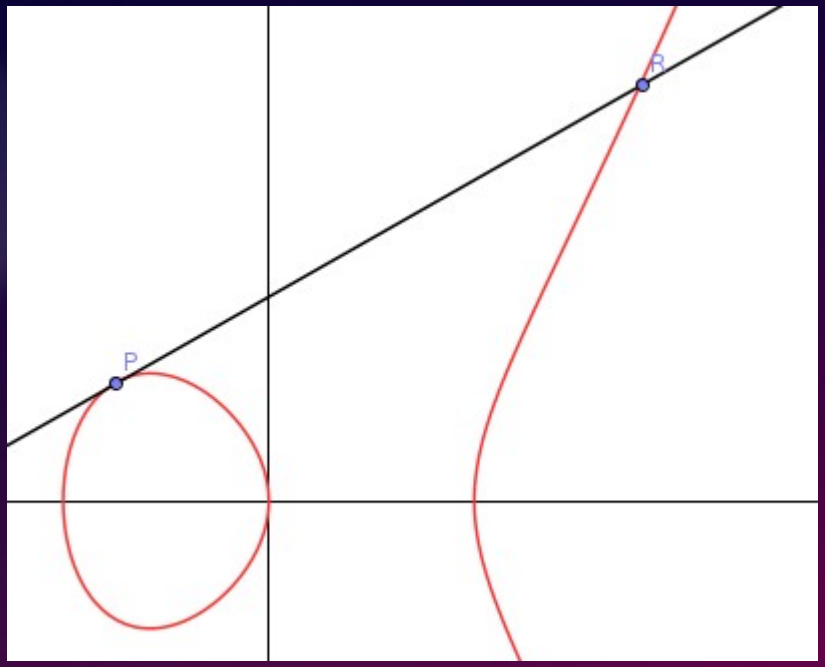
Sommare i punti di E

- Simile alla procedura vista inizialmente
- Dati due punti P e Q su E, traccio la retta passante per i due punti e chiamo R l’ulteriore intersezione tra la retta ed E.
- Rifletto R rispetto all’asse x ottendo R' (stessa ascissa, ma ordinata opposta rispetto a R)
- Definisco P+Q=R'



Nella seconda immagine vediamo come calcolare P+P=2P: si considera la tangente!

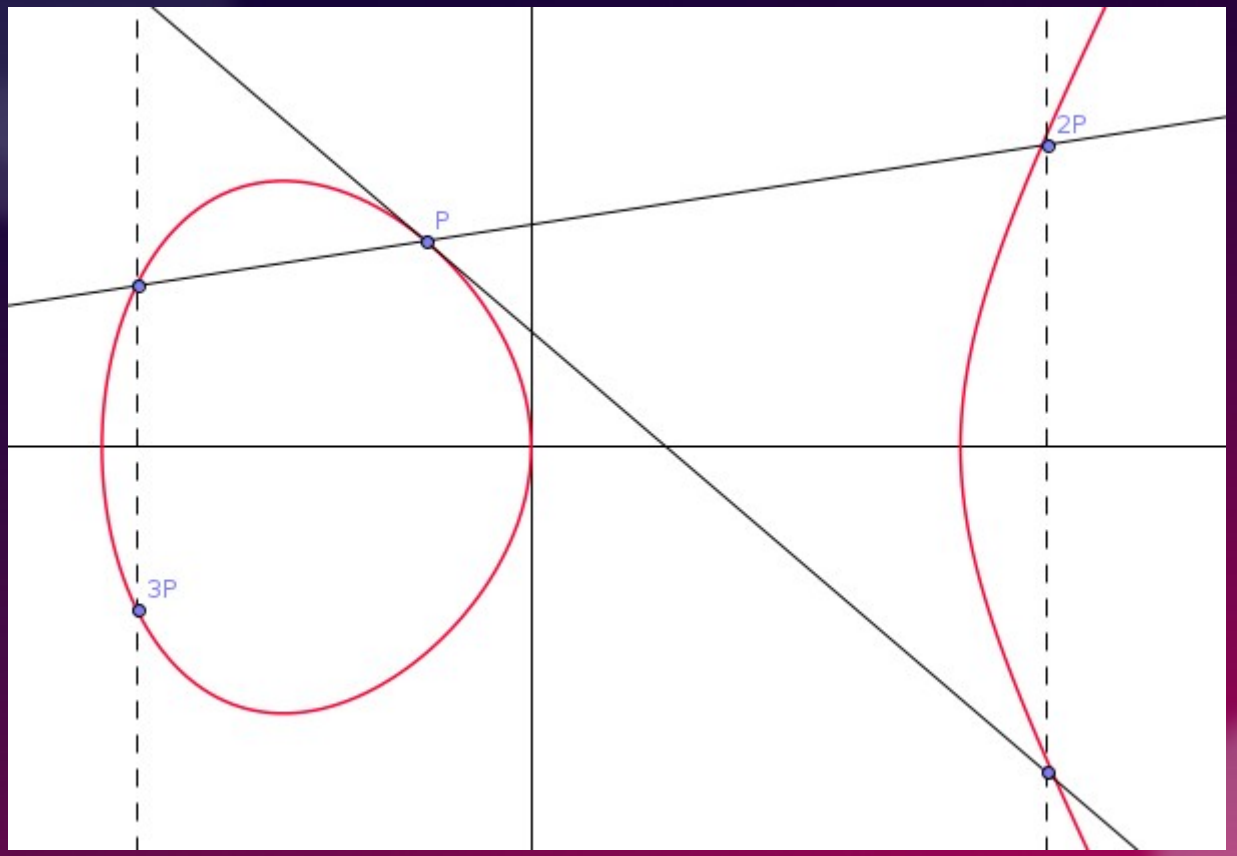
Perchè dobbiamo riflettere?



Se R=P+P=2P avremo che 3P=P+R=P

Come vedremo in seguito è importante che nP generi punti diversi. La riflessione permette di ottenere proprio questo.

Esempio: P, 2P, 3P,...



Che bello sommare punti...

Questa addizione non è fine a sè stessa…

E con questa operazione assume la struttura di gruppo!

Gruppi

Un gruppo (G, *) è un insieme dotato di una operazione binaria *, tale che:

1)* ha un elemento neutro e: e*a=a*e=a per ogni a in G.

2)* è invertibile: per ogni a in G esiste a’ tale che

$$a*a'=a'*a=e$$

3)* è associativa: (a*b)*c=a*(b*c).

Esempio: Z

$(Z,+)$

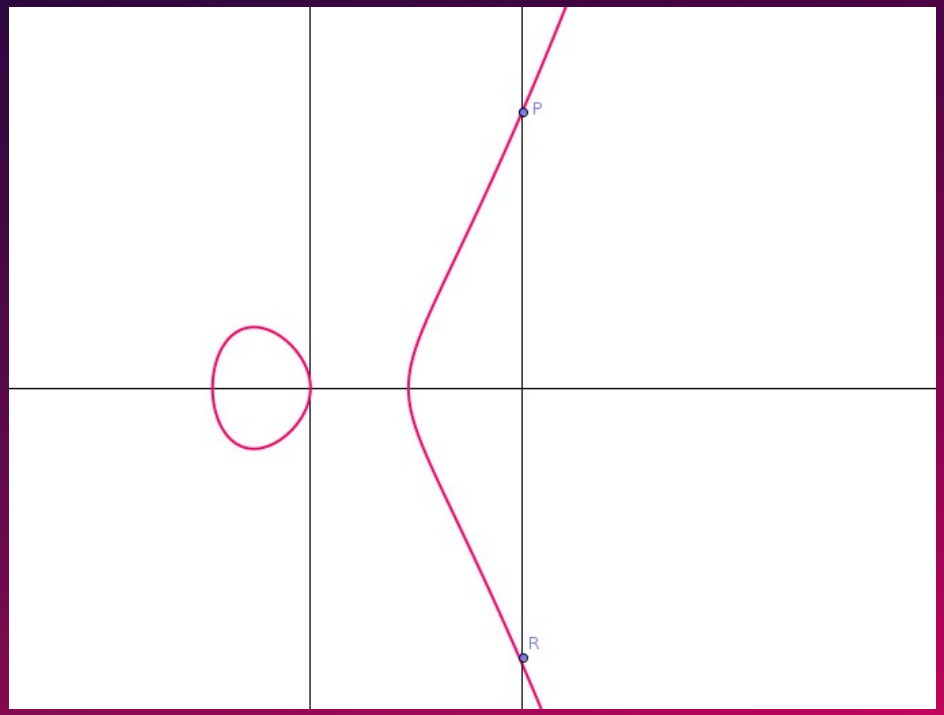
- L’addizione è associativa
- 0 è l’elemento neutro
- Dato n, -n è il suo inverso: 3+(-3)=0

$(Z,\cdot)$

- Non è un gruppo: 1 è elemento neutro...
- Ad esempio, 2 non è invertibile.

(E,+) è un gruppo commutativo

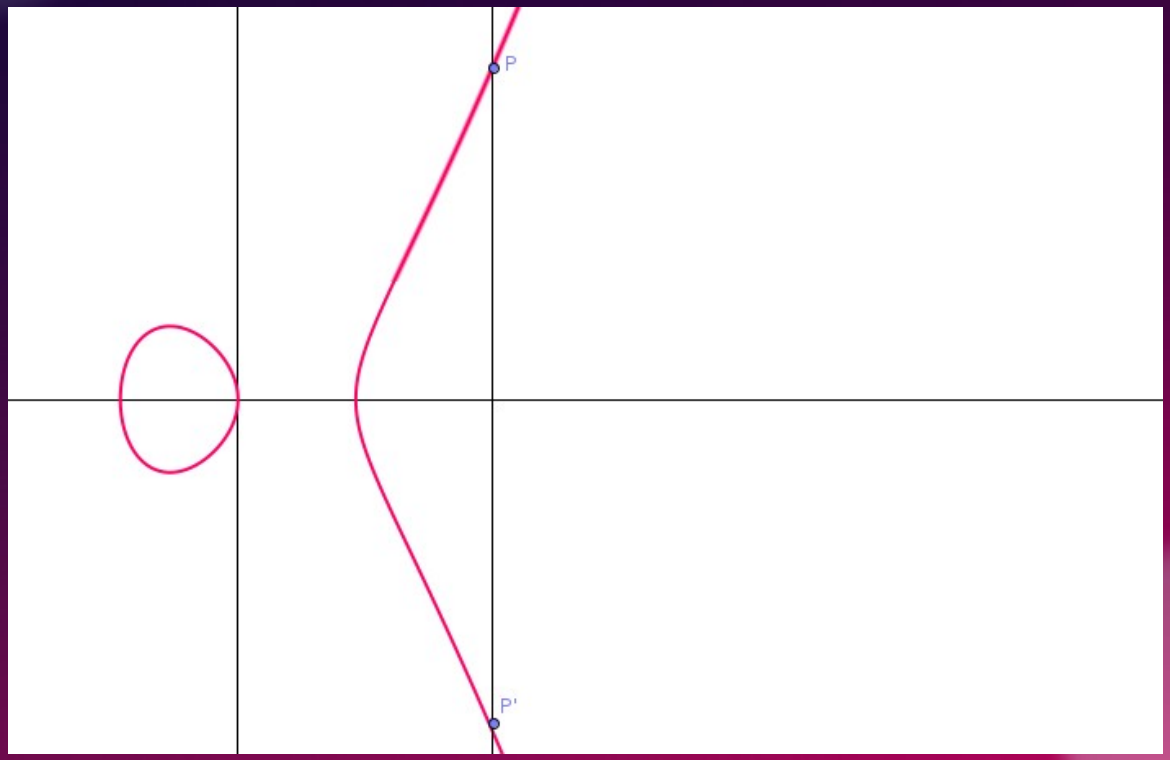
- Commutativo P+Q=Q+P perchè la retta passante per i due punti è la stessa.
- Elemento neutro ∞: P+∞=P



- Inverso: simmetrico rispetto asse x

  -P è il punto per cui P+(-P)=∞

  (∞ è l'elemento neutro!)

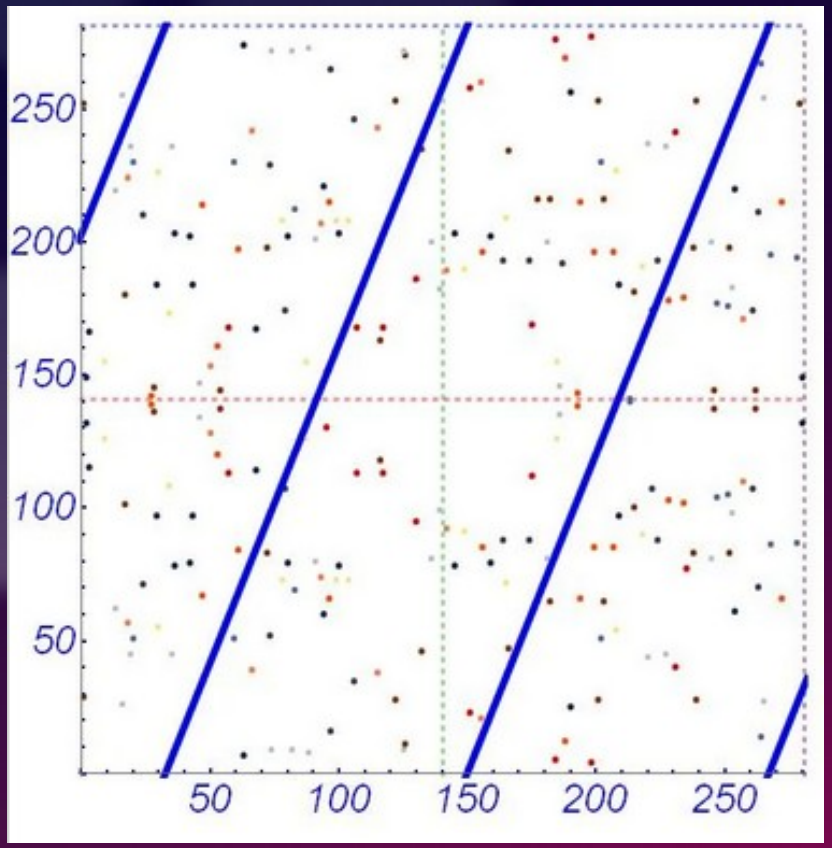


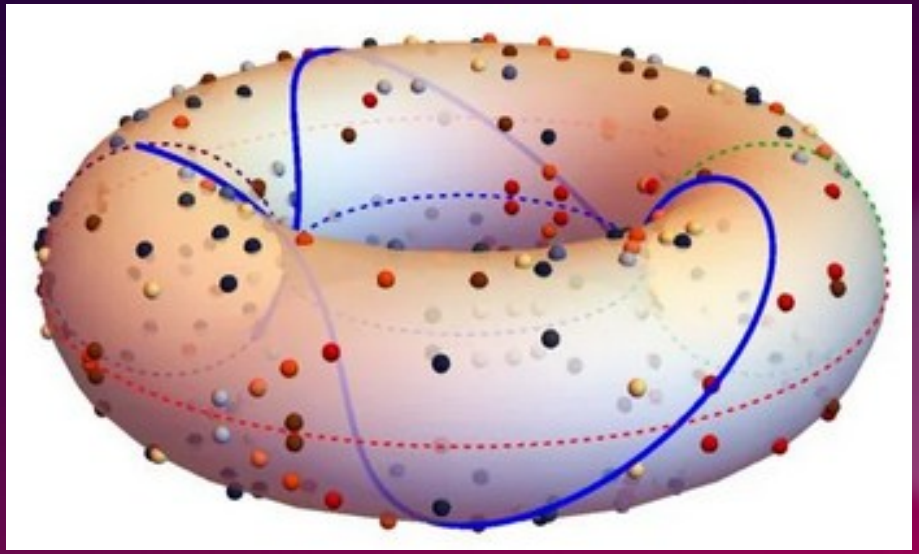
- Associatività più laboriosa...usando un po’ di geometria analitica si possono ricavare le formule algebriche che esprimono le coordinate della somma!

...quanti punti...

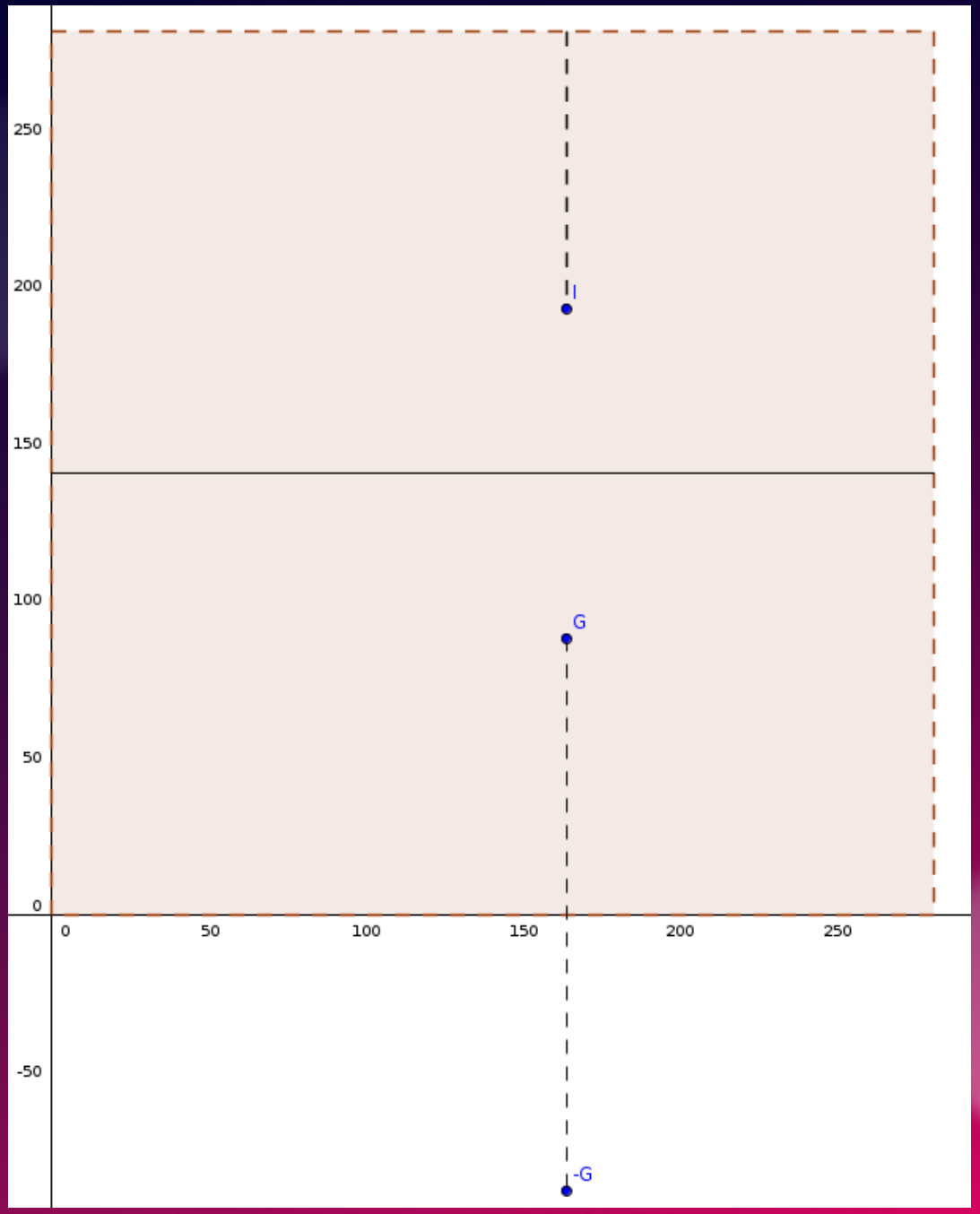
- In crittografia non si lavora in R
- Avere numeri eccessivamente grandi non è utile e può essere dispendioso…
- Modulo: si fissa un numero primo p (grande) e si lavora con $p+1 \rightarrow 1$
- Consideriamo solo i punti con coordinate intere

$$E: y^2 - x^3 + 3x = 0 \pmod{281}$$





Simmetria G(164,88) e I(164,193)



Crittografia finalmente!

- Il fatto che (E,+) sia un gruppo, ci permette di sfruttare le curve ellittiche per costruire varie primitive crittografiche...essenzialmente tutte quelle che si basano su gruppi (finiti)
- Ma cos’è e cosa fa la crittografia?

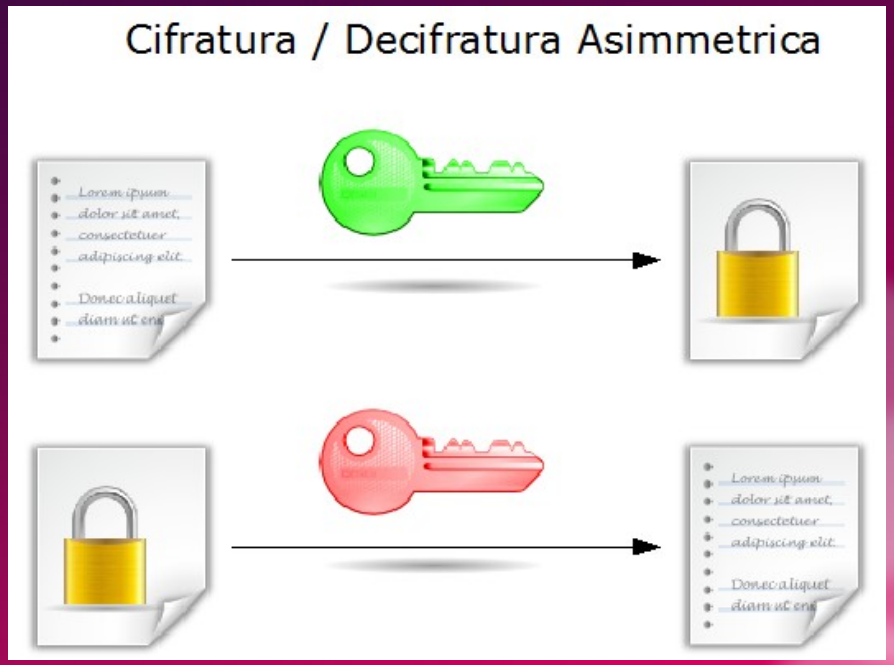
Scopi della crittografia

Scopi molto ampi

- Confidenzialità → schemi di crittazione
- Integrità, autenticazione → firme digitali
- Secure MP computation...

Schema di crittazione asimmetrica

- Il destinatario genera due chiavi diverse (privata e pubblica) e distribuisce la chiave pubblica.
- Il mittente usa la chiave pubblica per ottenere un testo cifrato.
- Il destinatario decritta il testo cifrato con la chiave privata.



Premessa: sicurezza in crittografia

- La crittografia moderna si basa sull'ipotesi che alcuni problemi siano *difficili da risolvere*
- Non esistono (...non si conoscono…) metodi efficienti per risolvere tale problema.
- Non efficienti → quasi come fare tutti i tentativi
- Esempio: fattorizzare un numero. Posso provare tutti i primi uno dopo l'altro...

Logaritmo discreto

- Consideriamo (E,+) e P un punto generico di E
- Possiamo calcolare P+P=2P, P+P+P=3P, P+P+P+P=4P e così via…
- 2P,3P,…,nP sono punti distinti
- Dati P e Q trovare n per cui Q=nP è detto calcolo del logaritmo discreto.

Perchè logaritmo discreto???

- (E,+) è un gruppo additivo
- Consideriamo la notazione moltiplicativa:
- $P*P=P^2$, $P*P*P=P^3$ e così via
- Logaritmo discreto: dati P e Q calcolare n tale che Q=P^n
- Ovvero n=log_P(Q)!

Un problema difficile e utile

- Calcolare il logaritmo discreto in alcuni gruppi è ritenuto un problema difficile da risolvere
- Ovvero: non sono noti procedimenti per calcolare DL in un tempo breve
- Molte primitive crittografiche si basano sul DL

Schema ElGamal su EC

- Chiavi: il destinatario sceglie una curva ellittica E su un campo finito e un punto P di E. Sceglie anche un numero s e calcola sP=Q.

  Il destinatario tiene sk=s e pubblica pk=(E,P,Q)
- Crittazione: il mittente sceglie k e calcola C=kP e C'=M+kQ. (C,C') sarà il testo cifrato.
- Decrittazione: il destinatario calcola sC e ricava attraverso M=C'-sC

Funziona?

- Chiave pubblica è P e Q=sP
- C=kP e C'=M+kQ
- Il destinatario non conosce k ma calcolando sC ottiene sC=s(kP)=k(sP)=kQ
- Quindi C'-sC=C'-kQ=M
- Il destinatario riesce quindi a ricavare correttamente il testo in chiaro.

E’ sicuro?

- La sicurezza del sistema discende dalla difficoltà di calcolare il logaritmo discreto nelle curve ellittiche
- pk=(P,Q)=(P,sP). s è il logaritmo discreto
- Il parametro di sicurezza dipende da quanto grande è il gruppo usato, ovvero dal modulo usato
- 160 bit $\sim$ 48 cifre del numero primo per cui si calcola mod p

Parametri dello schema

E è specificata da i valori di A e B in $y^2=x^3+Ax+B$

e dal numero primo p (modulo)

La chiave è costituita da G, punto sulla curva

G definisce due altri numeri n e h

n → lunghezza della sequenza G, 2G, 3G,…

hn → totale dei punti della curva

Verifica dei Parametri

I parametri scelti vanno verificati!

Spesso si sceglie una curva già preparata per non rischiare di fare una cattiva scelta.

NIST → prepara delle scelte standard e pubblica i parametri da usare

Curve225519 curva ellittica modulo 2^255-19

Parametri a confronto

www.keylength.com riporta varie indicazioni sui parametri da usare per una sicurezza accettabile

Protection	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve
Legacy standard level *Should not be used in new systems*	80	1024	160	1024	160
Near term protection *Security for at least ten years (2022-2028)*	128	3072	256	3072	256
Long-term protection *Security for thirty to fifty years (2022-2068)*	256	15360	512	15360	512

Considerazioni finali

- Crittografia simmetrica: molto conveniente. Ma rimane il problema della distribuzione delle chiavi
- ECC necessita di chiavi molto più piccole rispetto all'RSA:

  160 bits ~ 48 cifre vs 1024 bits ~ 309 cifre
- Minor dispendio di spazio e miglior efficienza nei calcoli

From Bits and Mips to Pools, Lakes and Beyond [Lenstra, Kleinjung, Thomé]

- Livello odierno di sicurezza (80bit) richiede di fare bollire 2^15 piscine olimpiche al giorno (media pioggia giornaliera in Olanda)
- Un livello di sicurezza a 128 bit sarebbe equivalente a far bollire la tutta l’acqua della terra

Grazie per l'attenzione!