Logaritmo discreto: perché è difficile attaccarlo?

E perché è ancora più difficile su una curva ellittica?

Ottavio Giulio Rizzo
Ottavio.Rizzo@UniMI.it

Dipartimento di matematica «Federigo Enriques»
Università degli Studi di Milano

La De Cifris incontra Milano
11 settembre 2018

Il problema del logaritmo discreto

Esempio (Scambio di chiavi di Diffie-Hellman)

- Fissiamo un numero primo p.
- Alice e Bob scelgono ciascuno un intero a caso n_A e n_B
- Alice e Bob si scambiano $2^{n_A} \bmod p$ e $2^{n_B} \bmod p$
- Alice e Bob hanno condiviso il segreto $2^{n_A n_B}$

Problema

- *Eva intercetta i messaggi e conosce* $2^{n_A} \bmod p$, $2^{n_B} \bmod p$
- *Eva è in grado di calcolare la chiave segreta* $2^{n_A n_B}$ *?*

Soluzione

Se Eva è in grado di calcolare n_A *dato* 2^{n_A}*, allora ha risolto il Problema del logaritmo discreto*

Il logaritmo

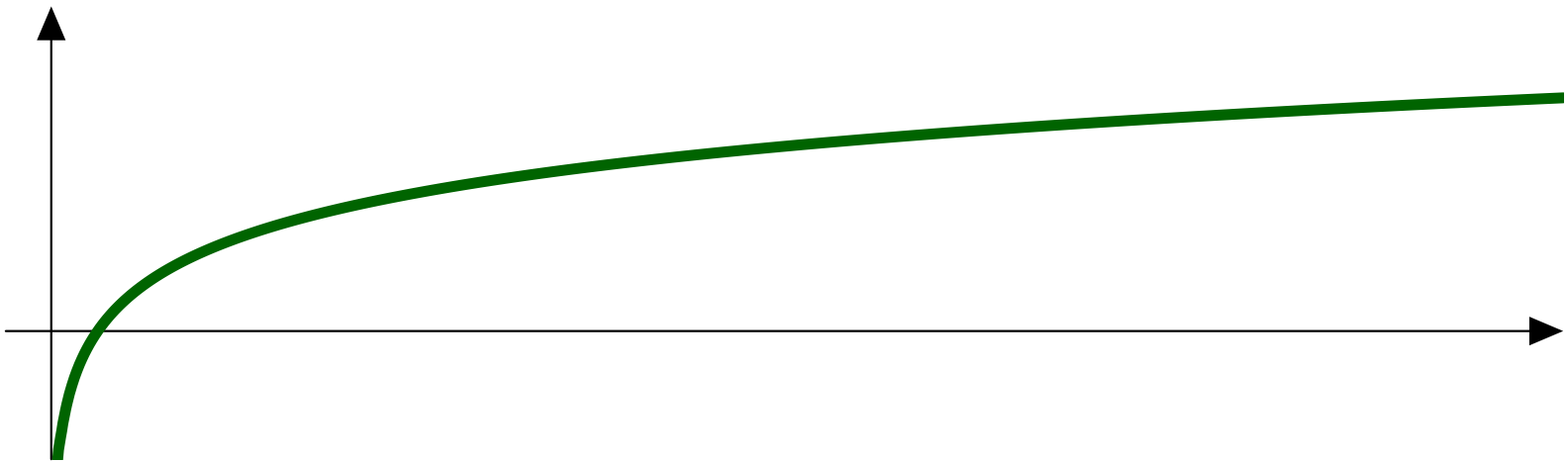
Definizione

Il logaritmo di a in base b è

$$c = \log_b(a) \text{ tale che } a = b^c$$

Proprietà

- $\log(x \cdot y) = \log(x) + \log(y)$
- ecc. ecc.



Calcolo

Fatto

È facile calcolare il logaritmo

Dimostrazione.

- Contare le cifre
- Interpolazione lineare
- *Bit shuffling*

□

Logaritmo discreto

Definizione (logaritmo modulare)

c è il logaritmo di a in base b modulo n se

$$a \equiv b^c \bmod n$$

Definizione (logaritmo generico)

Sia G un gruppo (moltiplicativo) generato da b: c è il logaritmo di a in base b se

$$a = b^c$$

Dove a e b sono elementi di G

Dove vive c?

Fatti

- c non è un elemento di G
- Se G ha k elementi, allora $c \in \mathbf{Z}/k\mathbf{Z}$
- In particolare, il logaritmo modulo n è definito modulo $\phi(n)$

Quindi

Il logaritmo è una funzione da un insieme in uno totalmente diverso!

Cos'è veramente il logaritmo?

Ricordiamo

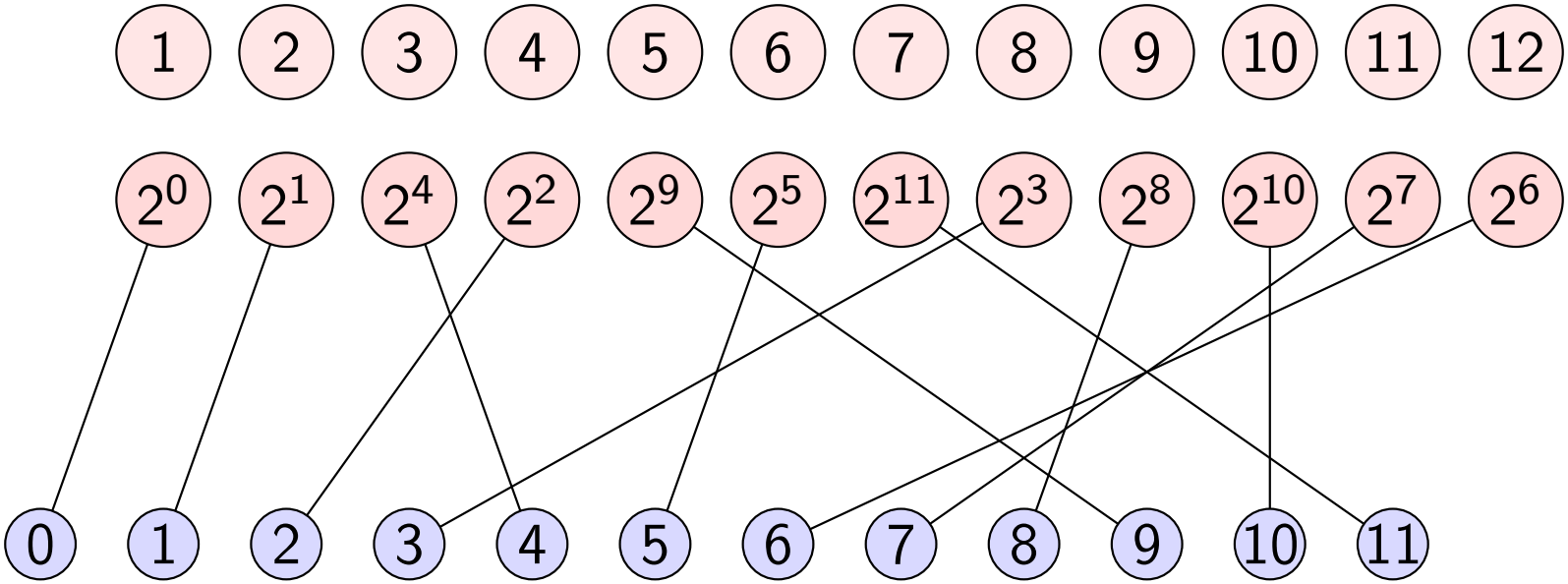
- Non esiste $\log(0)$
- $\log(a \cdot b) = \log(a) + \log(b)$

Quindi

- Il logaritmo è una mappa fra un gruppo (moltiplicativo) e un gruppo (addittivo).
- O meglio: è un isomorfismo fra due gruppi, la cui mappa inversa è l'elevamento a potenza.
- L'isomorfismo dipende dalla scelta della base.

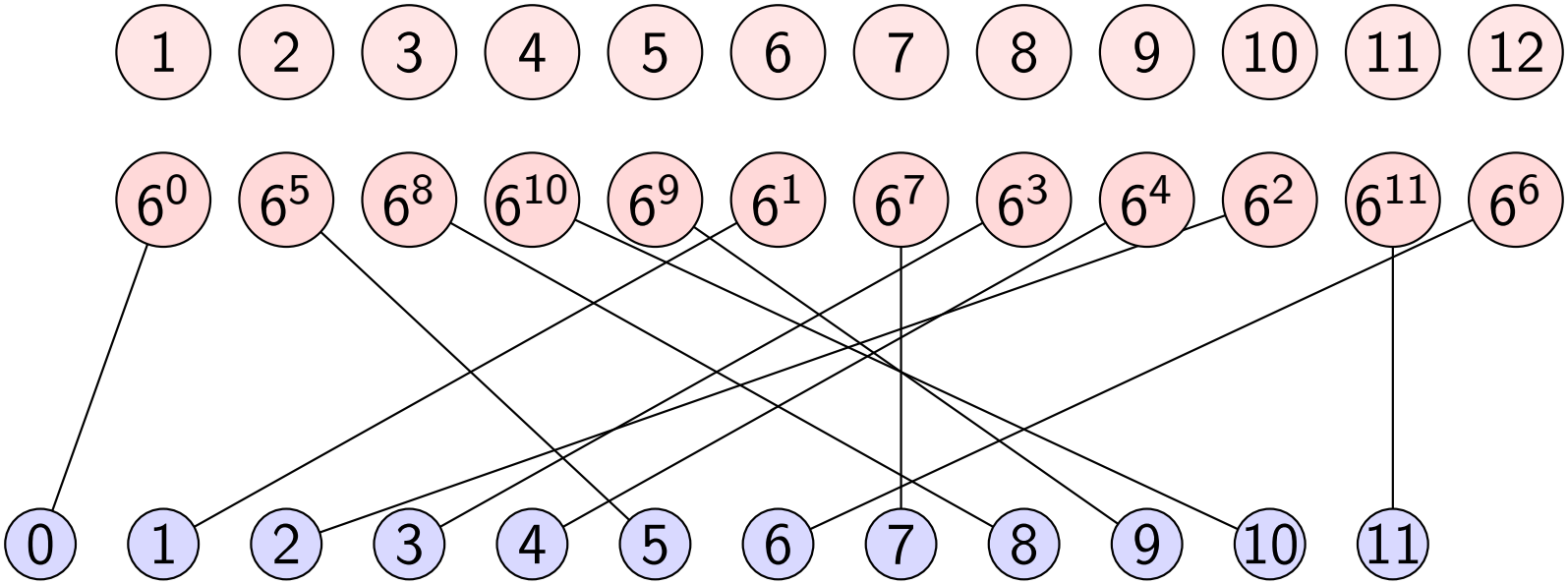
Logaritmo modulo 13

Il numero $p = 13$ ha esattamente quattro generatori: 2, 6, 7, 11.



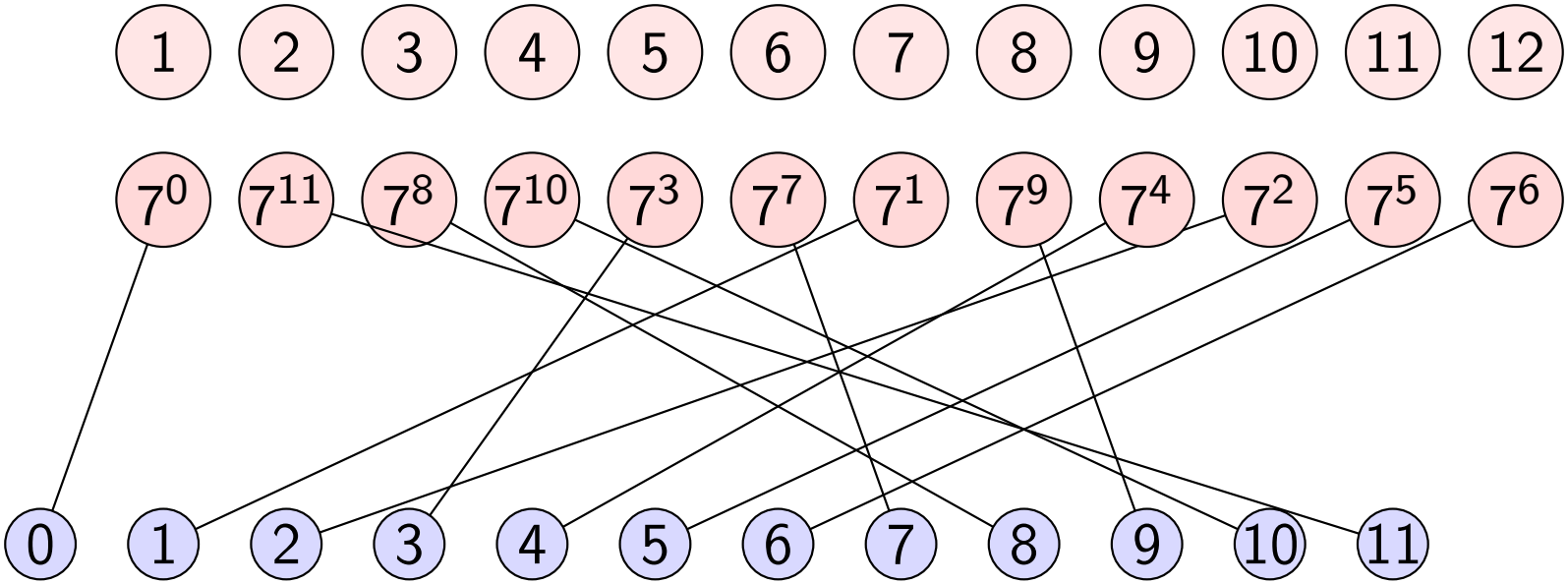
Logaritmo modulo 13

Il numero $p = 13$ ha esattamente quattro generatori: 2, 6, 7, 11.



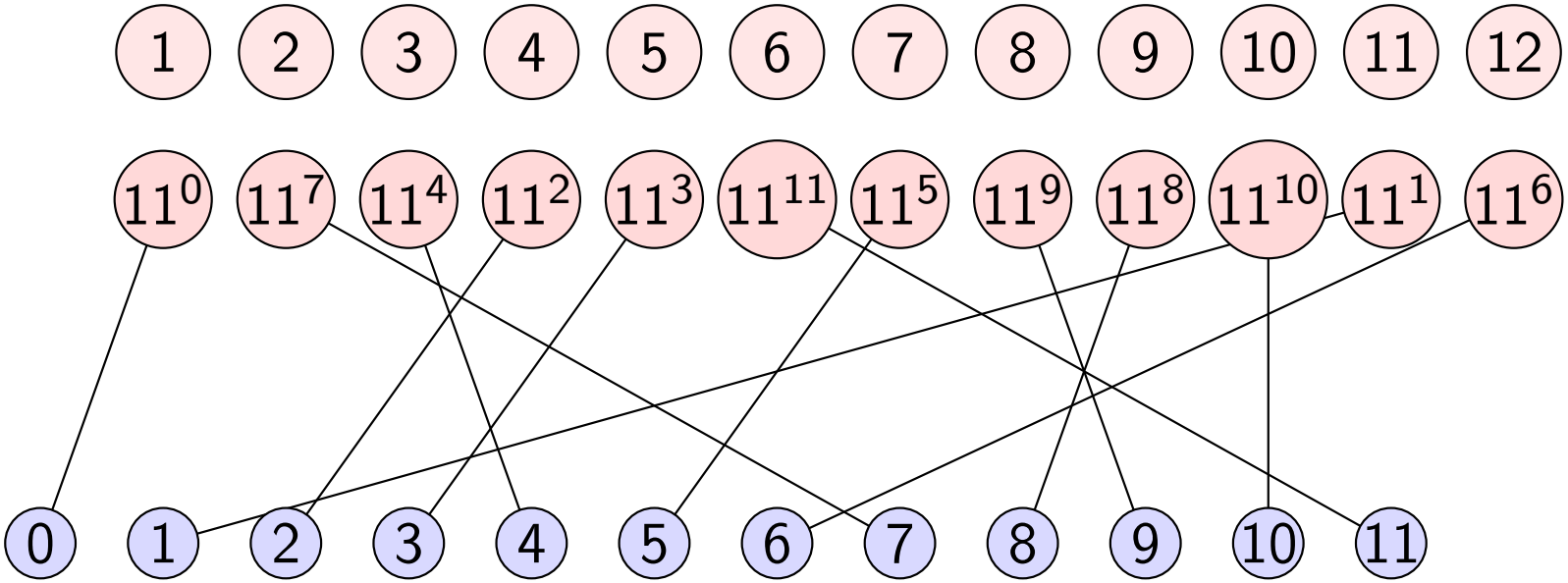
Logaritmo modulo 13

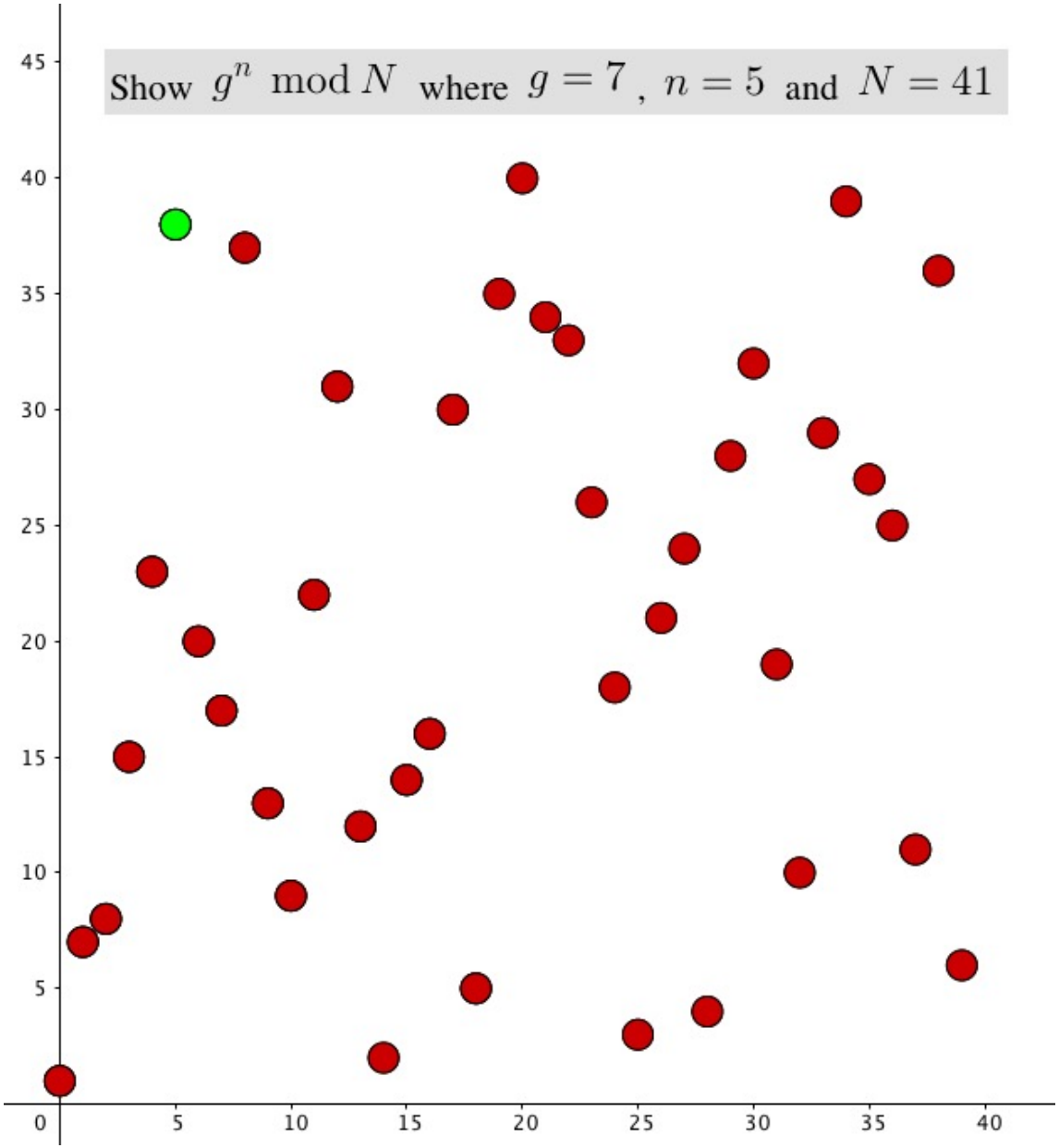
Il numero $p = 13$ ha esattamente quattro generatori: 2, 6, 7, 11.

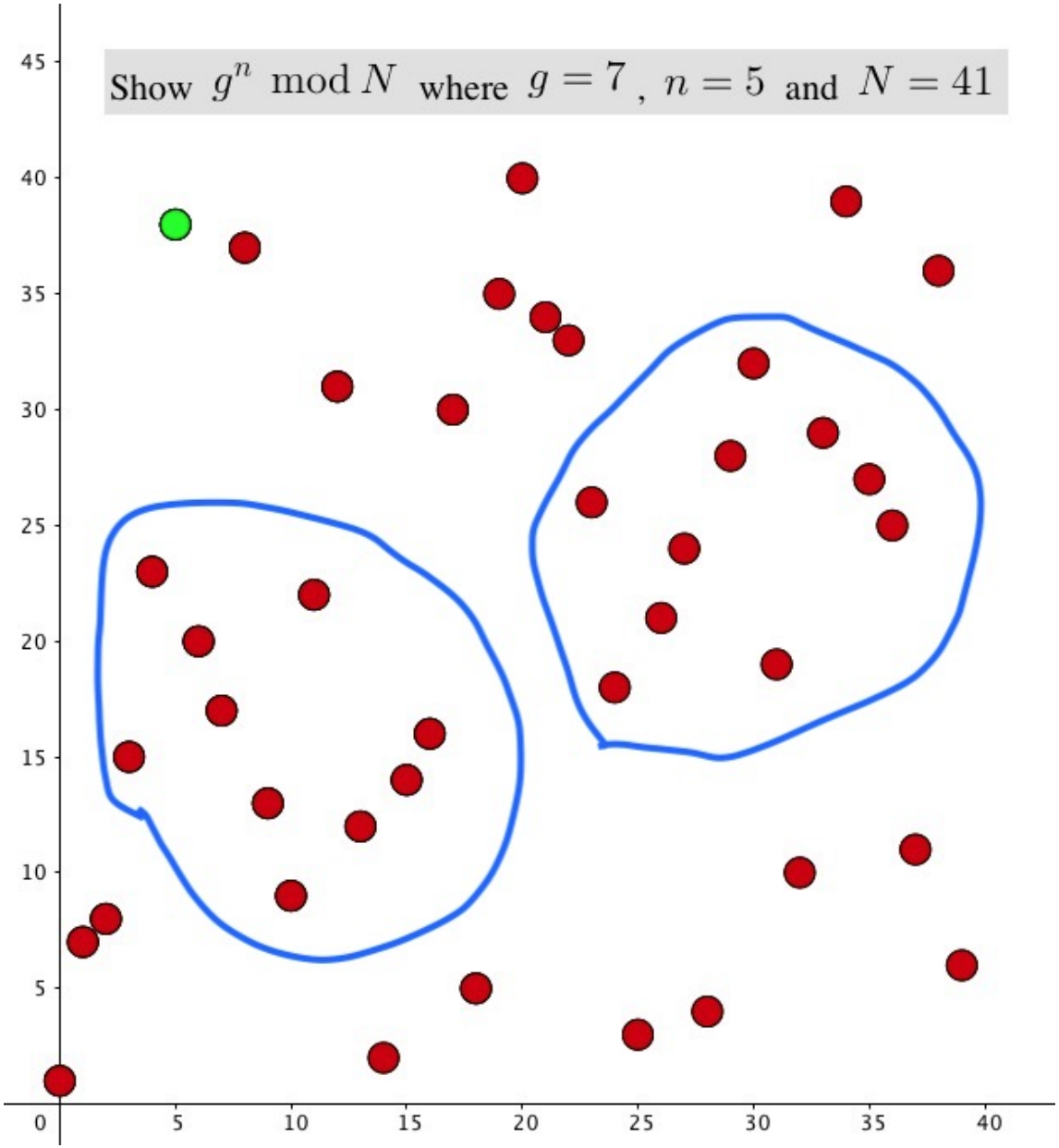


Logaritmo modulo 13

Il numero $p = 13$ ha esattamente quattro generatori: 2, 6, 7, 11.




Show $g^n \bmod N$ where $g = 7$, $n = 5$ and $N = 41$
45
40
35
30
25
20
15
10
5
0
5
10
15
20
25
30
35
40


Show $g^n \bmod N$ where $g = 7$, $n = 5$ and $N = 41$
45
40
35
30
25
20
15
10
5
0
5
10
15
20
25
30
35
40

Attacchi brutali

Attacchi?

Sia G un gruppo di n elementi

Forza bruta	n potenze
Teorema cinese del resto	Se n è prodotto di primi piccoli, attacco ciascun primo separatamente
Baby step–giant step	$\sqrt{n}$ potenze

Attacchi migliori?

Solo usando struttura dello specifico gruppo

Calcolo dell'indice

Obiettivo

Vogliamo calcolare $\log_7(26 \bmod 41)$.

Idea

- Ricordiamo che $\log_7$ è una funzione a valori $\bmod 40$
- Troviamo potenze di 7 che si fattorizzano in primi piccoli
- Calcoliamo $\log_7$ per tutti i primi piccoli, usando l'algebra lineare $\bmod 40$
- Cerchiamo α tale che $7^\alpha \cdot 26$ si fattorizza in primi piccoli
- Ricaviamo $\log_7(26)$

$7^2 \equiv 49 \equiv 8 = 2^3 \bmod 41$, perciò $2 = 3\log_7(2)$

quindi $\log_7(2) \equiv 2/3 \equiv 14 \bmod 40$

$7^{32} \equiv 10 \equiv 2 \cdot 5 \bmod 41$, perciò $32 = \log_7(2) + \log_7(5)$

quindi $\log_7(5) \equiv 32 - \log_7(2) \equiv 18 \bmod 40$

$7^{21} \equiv 34 \equiv 2 \cdot 17 \bmod 41$, primo grande

$7^{13} \equiv 12 \equiv 2^2 \cdot 3 \bmod 41$, perciò $13 = 2\log_7(2) + \log_7(3)$

quindi $\log_7(3) \equiv 13 - 2\log_7(2) \equiv 25 \bmod 40$

Abbiamo

$\log_7(2) \equiv 14 \bmod 40, \quad \log_7(3) \equiv 25 \bmod 40, \quad \log_7(5) \equiv 18 \bmod 40$

Vogliamo

α tale che $7^\alpha \cdot 26$ abbia fattori primi $2, 3, 5$

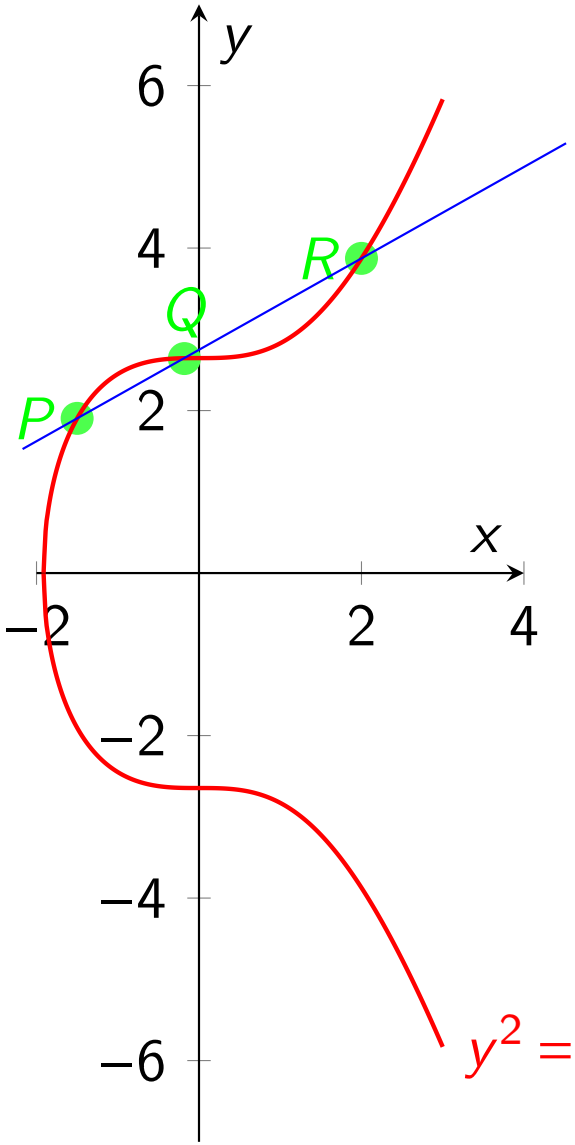
$7^{18} \cdot 26 \equiv 7$
$7^{21} \cdot 26 \equiv 23$
$7^{12} \cdot 26 \equiv 27 \equiv 3^3$, quindi

$$12 \log_7(7) + \log_7(26) \equiv 3 \log_3(3) \bmod 40$$
$$\log_7(26) \equiv 12 - 3 \cdot 25 \equiv 23 \bmod 40$$

Costo

Il calcolo dell'indice modulo p ha costo $L_p[1/2, \sqrt{2}]$

Curve ellittiche



- Una curva ellittica E è data da

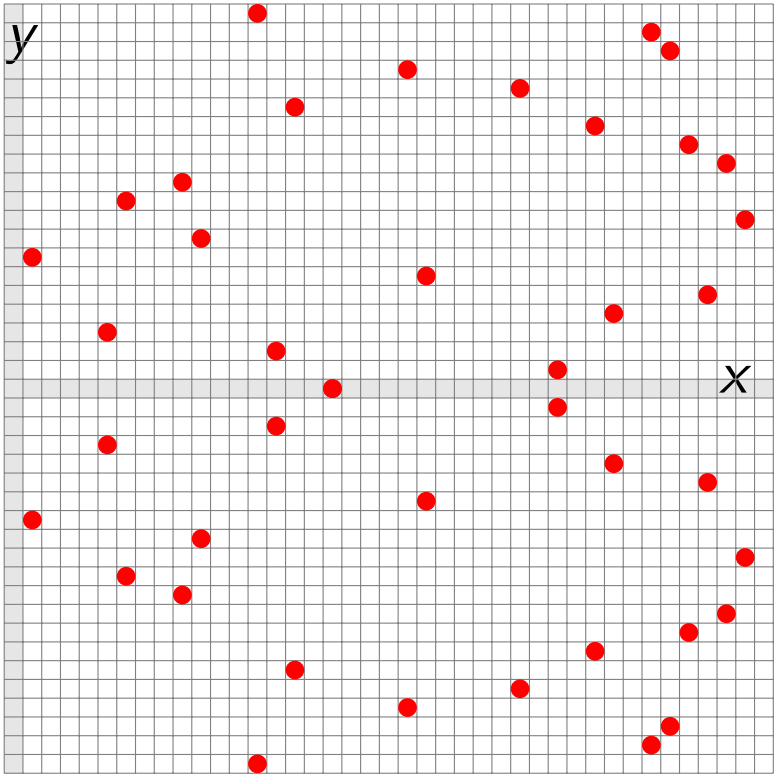
$$y^2 = x^3 + Ax + B$$

- Tre punti P, Q, R della curva soddisfano

$$P + Q + R = O$$

se e solo se sono allineati

- Dati P e Q multiplo di P è banale trovare l'intero n tale che $Q = nP$, se. . .



$y^2 = x^3 + 7 \bmod 7$

- Una curva ellittica $\bmod p$ è data da
$$y^2 = x^3 + Ax + B$$
- Un punto (α, β) appartiene alla curva se
$$\beta^2 \equiv \alpha^3 + A\alpha + B \bmod p$$
- Non c'è nessun analogo di fattorizzazione in primi piccoli, quindi il calcolo dell'indice non funziona
- DLP su curve ellittiche è molto più duro che su classi di resto, purché...