# Preliminari e nozioni di base della teoria dei gruppi.

Denotiamo con $\mathbb{Z}$ l'insieme degli interi.

Per $a, b \in \mathbb{Z}$, $a$ divide $b$, scritto $a \mid b$ se

$\exists$ un intero $c$ tale che $ac = b$.

Se $a$ non divide $b$, scriveremo $a \nmid b$

Anche se le nozioni hanno senso in ogni caso,

considereremo essenzialmente $a$, $b$ e $c$ tutti positivi.

Se $a \mid b$ e $a \mid c$, allora $a \mid (Xb + Yc)$

per ogni $X, Y \in \mathbb{Z}$

Se $a \mid b$ e $a > 0$, $a$ è un divisore di $b$

Inoltre, se $a \notin \{1, b\}$, $a$ è un divisore non banale,

o fattore, di $b$.

Un intero positivo $p > 1$ è primo se non ha fattori.

Un intero positivo $n > 1$ non primo è composto.

Per convenzione 1 non è né primo né composto

Ogni intero maggiore di 1 può essere espresso unicamente come un prodotto di primi. Precisamente

$$N > 1 \implies N = \prod_i p_i^{e_i} \qquad e_i \geq 1 \text{ per ogni } i$$

($p_i$: primi distinti $p_i$)

Proposizione 8.1. Sia $a$ un intero e sia $b$ un intero positivo. Allora esistono e sono unici gli interi $r$ e $q$ tali che

$$a = qb + r, \qquad 0 \leq r < b$$

($q$: quoziente; $r$: resto)

Gli interi $q$ ed $r$ possono essere calcolati in tempo polinomiale (funzione della lunghezza degli input, espressi in binario).

Intero $N$ $\implies$ tempo espresso in termini di: $\|N\| = \lfloor \log N \rfloor + 1$ lunghezza della rappresentazione binaria di $N$

Il massimo comune divisore (greatest common divisor) di due interi $a$ e $b$, $\gcd(a,b)$, è il più grande intero $c$ tale che $c \mid a$ e $c \mid b$.

$\gcd(a,b)$ ha senso anche quando $a$ o $b$ oppure entrambi sono negativi, ma tipicamente abbiamo $a, b \geq 1$.

In ogni caso, $\gcd(a,b) = \gcd(|a|, |b|)$

Nota: $\gcd(b,0) = \gcd(0,b) = b$

$\gcd(a,p) \in \{1, p\}$ e se risulta, per due interi $a$ e $b$,

$p$ primo

$\gcd(a,b) = 1$, $a$ e $b$ sono relativamente primi

Proposizione 8.2 Siano $a$ e $b$ interi positivi. Allora

$\exists\ X, Y$ (interi) tali che $Xa + Yb = \gcd(a,b)$.

Inoltre, $\gcd(a,b)$ è il più piccolo intero positivo che può essere rappresentato in questo modo.

Pertanto concludiamo che $d$ è il più grande intero che divide sia $a$ che $b$, e quindi $d = \gcd(a, b)$. ∎

L'algoritmo di Euclide calcola $\gcd(a, b)$ in tempo polinomiale.

L'algoritmo di Euclide Esteso calcola gli interi $X$ e $Y$ tali che $d = Xa + Yb$ in tempo polinomiale.

Proposizione 8.3. Se $c \mid ab$ e $\gcd(a, c) = 1$, allora $c \mid b$. Quindi, se $p$ è primo e $p \mid ab$ allora o $p \mid a$ oppure $p \mid b$.

Dim. Poiché $c \mid ab$, esiste $y$ : $ab = yc$

Se $\gcd(a, c) = 1$, allora esistono $X, Y$ tali che $1 = Xa + Yc$. Moltiplicando entrambi i membri dell'uguaglianza per $b$:

$$b = \underbrace{Xab} + Ycb = Xyc + Ycb = c\underbrace{(Xy + Yb)}_{\text{intero}}$$

$$\Rightarrow \quad c \mid b.$$

Pertanto, se $p$ è primo e $p \nmid a$, allora

$\gcd(a, p) = 1 \Rightarrow p \mid b$ (per la precedente). ∎

---

Es. $3 \mid 30 = 5 \cdot 6$ $\quad \gcd(3, 5) = 1$, allora $3 \mid 6$

$c \quad ab \quad a \cdot b$

---

**Proposizione 8.4** Se $a \mid N$, $b \mid N$ e $\gcd(a, b) = 1$,

allora $a \cdot b \mid N$

Dim. $a \mid N \Rightarrow N = c \cdot a$

$b \mid N \Rightarrow N = d \cdot b$

$\gcd(a, b) = 1 \Rightarrow 1 = Xa + Yb$

↓

Moltiplicando entrambi i membri per $N$, si ha:

$$N = NXa + NYb = (d\bar{b})X\bar{a} + (c\bar{a})Y\bar{b} = ab(Xd + Yc)$$

($N$ = $N$ = intero)

$\Longleftrightarrow \quad ab \mid N$

---

Es. $a = 2 \quad b = 3 \quad N = 30 \quad a \mid N \Leftrightarrow 2 \mid 30 \quad b \mid N \Leftrightarrow 3 \mid 30$

$\gcd(2, 3) = 1 \Rightarrow 2 \cdot 3 = 6 \mid 30$

# Aritmetica modulare

Siano $a, b$ ed $N \in \mathbb{Z}$, con $N > 1$

Sia $[a \bmod N]$ il resto della divisione per $N$

( $\exists\ q, r$ tali che $a = qN + r, \quad 0 \leq r < N$ )

$\downarrow$

$[a \bmod N]$

Il processo che associa $[a \bmod N]$ ad $a$ è chiamato riduzione modulo $N$.

Diciamo che $a$ e $b$ sono congrui modulo $N$, scrivendo $a = b \bmod N$, se $[a \bmod N] = [b \bmod N]$

Nota che $a = b \bmod N$ se e solo se $N \mid (a - b)$.

In termini di notazione

$$a = b = c = \dots = z \bmod N$$

ogni segno uguale fa riferimento ad una congruenza mod $N$.

Nota ancora che:

$$a = [b \bmod N] \implies a = b \bmod N$$

$$a = b \bmod N \not\implies a = [b \bmod N]$$

e.g. $36 = 21 \bmod 15$ ma $36 \neq [21 \bmod 15] = 6$

La congruenza modulo $N$ è una relazione di equivalenza

- riflessiva $\quad a = a \bmod N \quad \forall a$
- simmetrica $\quad a = b \bmod N \Rightarrow b = a \bmod N$
- transitiva $\quad a = b \bmod N,\ b = c \bmod N \Rightarrow a = c \bmod N$

La congruenza modulo $N$ rispetta anche le regole standard dell'aritmetica rispetto all'addizione, la sottrazione e la moltiplicazione

$$a = a' \bmod N,\ b = b' \bmod N \Rightarrow (a+b) = (a'+b') \bmod N,\ a \cdot b = a' \cdot b' \bmod N$$

Conseguenza importante: possiamo "ridurre e poi addizionare/moltiplicare" invece di "addizionare/moltiplicare e poi ridurre"

$\Longrightarrow$ semplifica i calcoli

Esempio 8.5 $\quad 1093028 \cdot 190301 \bmod 100$

$\downarrow \qquad \downarrow$

$28 \bmod 100 \qquad 1 \bmod 100$

$\Rightarrow \quad 28 \cdot 1 \bmod 100 = 28 \bmod 100.$

La congruenza in generale NON rispetta la divisione

$a = a' \bmod N$ e $b = b' \bmod N$ non implica necessariamente $a/b = a'/b' \bmod N$

↓ non sempre definito ↓

Parimenti, $ab = cb \bmod N \not\Rightarrow a = c \bmod N$

Es. 8.6

$N = 24$ $\quad 6 = 3 \cdot 2 = 15 \cdot 2 \bmod 24 \not\Rightarrow 3 = 15 \bmod 24$

Infatti $3 \neq 15 \bmod 24$

In certi casi, però possiamo definire una nozione di divisione significativa.

Se per $b$ (intero) esiste $c$ (intero) tale che $bc = 1 \bmod N$

diciamo che $b$ è invertibile modulo $N$ e $c$ è l'inverso moltiplicativo di $b$ modulo $N$.

L'intero 0 non è mai invertibile

È possibile dimostrare che:

se $c$ è un inverso moltiplicativo di $b \bmod N$, allora anche $[c \bmod N]$ lo è

se $c'$ è un altro inverso moltiplicativo di $b \bmod N$, allora $[c' \bmod N] = [c \bmod N]$

$\Rightarrow$ quando $b$ è invertibile, possiamo semplicemente denotare con $b^{-1}$ l'UNICO inverso moltiplicativo che si trova nel range $\{1, \dots, N-1\}$

Quando $b$ è invertibile modulo $N$, definiamo la divisione per $b$ modulo $N$ come la moltiplicazione per $b^{-1}$, i.e.

$$[a / b \bmod N] \stackrel{def}{=} [a \cdot b^{-1} \bmod N]$$

Nota che:

$$ab = cb \bmod N \quad \text{e } b \text{ invertibile} \Rightarrow a = c \bmod N$$

$$(a \cdot b) \cdot b^{-1} \bmod N = (cb) \cdot b^{-1} \bmod N \Rightarrow a = c \bmod N$$

Gli interi invertibili modulo $N$ sono "ottimi per lavorarci".

Quali interi sono invertibili modulo $N$?

Proposizione 8.7. Siano $b, N$ interi, $b \geq 1$, $N > 1$.
L'intero $b$ è invertibile modulo $N$ se e solo se

$$\gcd(b, N) = 1.$$

Dim. Supponiamo $b$ invertibile modulo $N$.
Sia $c$ il suo inverso.

Poiché $b \cdot c = 1 \bmod N$ risulta

$$bc - 1 = 0 \bmod N \iff bc - 1 = yN, \quad y \in \mathbb{Z}$$

Allora $bc - yN = 1$ → più piccolo intero positivo che può essere espresso in questo modo

($bc$: intero, $yN$: intero; $(bX + NY)$)

$$1 = \gcd(b, N) \Leftarrow$$

Viceversa, se $\gcd(b, N) = 1$, allora $\exists X, Y$ interi tali che $Xb + YN = 1$

$\Rightarrow$ riducendo entrambi i lati modulo $N$

risulta $Xb = 1 \bmod N$

↳ è l'inverso di $b$!

Esempio 8.8

Siano $b = 11$ e $N = 17$. Allora risulta

$$(-3) \cdot 11 + 2 \cdot 17 = 1$$

$\Rightarrow$ $14 = [-3 \bmod 17]$ è l'inverso di 11.

Infatti $11 \cdot 14 = 1 \bmod 17$.

Nota: $-x \bmod N \iff N - x \bmod N$

In conclusione: addizione, sottrazione, moltiplicazione e calcolo dell'inverso (quando esiste) possono essere effettuati in tempo polinomiale.

Anche l'esponenziazione, i.e., calcolare $[a^b \bmod N]$, per $b > 0$, può essere calcolata in tempo polinomiale.

# Gruppi

$G$ insieme. Un'operazione binaria $\circ$ su $G$ è una funzione $\circ(\cdot,\cdot)$ che prende due elementi di $G$. Useremo la notazione

$$g \circ h \quad \text{invece di} \quad \circ(g,h).$$

**Definizione 8.9** Un gruppo $(G, \circ)$ soddisfa

- Chiusura: per tutti i $g, h \in G$, $g \circ h \in G$
- Esistenza di una identità: $\exists\ e \in G$ tale che, per ogni $g \in G$ risulta
$$e \circ g = g \circ e = g$$
- Esistenza degli inversi: per ogni $g \in G$, $\exists$ un elemento $h \in G$ tale che $g \circ h = h \circ g = e$
$h$ viene detto "inverso di $g$"
- Associatività: per tutti i $g_1, g_2, g_3 \in G$ risulta
$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

Quando $G$ ha un numero finito di elementi, diciamo che $G$ è finito. Il valore $|G|$ è l'ordine del gruppo.

Un gruppo $G$ è abeliano se

- Commutatività: per tutti gli $g, h \in G$, risulta

$$g \circ h = h \circ g$$

Osservazione: l'elemento identità in un gruppo $G$ è unico ed ogni elemento $g$ del gruppo ha un unico inverso.

Un insieme $H \subseteq G$ è un sottogruppo di $G$ se $H$ (gruppo) stesso forma un gruppo (rispetto alla stessa operazione)

Ogni gruppo ha due sottogruppi banali: $G$, $\{\}$ e $\{\}$

Solitamente non usiamo $\circ$ per denotare l'operazione definita su $G$. Piuttosto usiamo due notazioni:

| Notazione additiva | Notazione moltiplicativa |
|---|---|
| $g, h$ | $g, h$ |
| $g + h$ | $g \cdot h$ |
| $0$, identità | $1$, identità |
| $-g$, inverso | $g^{-1}$, inverso |
| $h - g \to (h + (-g))$ | $h/g \to h \cdot g^{-1}$ |

Nota: NON corrispondono all'addizione e alla moltiplicazione tra interi!

Esempio 8.10

$\mathbb{Z}$ (insieme degli interi)

$(\mathbb{Z}, +)$ → gruppo abeliano

$(\mathbb{Z}, \cdot)$ → NON è un gruppo, e.g., 2 non possiede un inverso moltiplicativo nell'insieme degli interi.

Esempio 8.11

$\mathbb{R}$ (insieme dei reali)

$(\mathbb{R}, \cdot)$ → NON è un gruppo, 0 non ha inverso

$(\mathbb{R} \setminus \{0\}, \cdot)$ → gruppo abeliano

Esempio 8.12

Sia $N > 1$ un intero. L'insieme $\{0, 1, \dots, N-1\}$ con l'operazione di somma modulare, i.e., $a+b \stackrel{\text{def}}{=} [a+b \bmod N]$ è un gruppo abeliano di ordine $N$. Infatti

- chiusura $\longrightarrow$ ovvia
- associatività/commutatività $\longrightarrow$ ereditata dagli interi
- identità $\longrightarrow$ $0$
- inverso $\longrightarrow$ poiché $a + (N-a) = 0 \bmod N$

  $\Rightarrow [(N-a) \bmod N]$ è l'inverso di $a$, per ogni $a$.

Lemma 8.13 (Legge di cancellazione)

Sia $G$ un gruppo ed $a, b, c \in G$.

Se $ac = bc$, allora $a = b$. In particolare

se $ac = c$, allora $a$ è l'identità di $G$.

Dim. Poiché $ac = bc$, moltiplicando per $c^{-1}$ entrambi i lati

$$ac = bc \iff \underbrace{(a \cdot c) \cdot c^{-1}}_{a \cdot 1} = \underbrace{(b \cdot c) \cdot c^{-1}}_{b \cdot 1} \Rightarrow a = b$$

Osservazione: gli elementi invertibili modulo $N$ formano un gruppo rispetto alla moltiplicazione modulo $N$.

È spesso utile esprimere l'operazione del gruppo applicata $m$ volte ($m$ intero positivo) ad un elemento fissato $g$.

Con la notazione additiva useremo

intero positivo ↓

$$m \cdot g \overset{\text{def}}{=} \underbrace{g + g + \dots + g}_{m \text{ volte}}$$

↑ elemento del gruppo

mentre, con la notazione moltiplicativa useremo

intero positivo ↓

$$g^m \overset{\text{def}}{=} \underbrace{g \cdot g \cdot \dots \cdot g}_{m \text{ volte}}$$

↓ elemento del gruppo

Nota che valgono le seguenti:

$g \in G$, $m, m'$ interi $\Rightarrow$ $(mg) + (m'g) = (m+m')g$

$m(m'g) = (m \cdot m') \cdot g$

$g, h \in G$ (↓ abeliano), $m$ intero $\Rightarrow$ $(mg) + (mh) = m(g+h)$

($g+h$: elemento gruppo)

E, similmente:

$g \in G$, $m, m'$ interi $\Rightarrow$ $g^m \cdot g^{m'} = g^{(m+m')}$

$(g^m)^{m'} = g^{m \cdot m'}$

$g, h \in G$ (abeliano), $m$ intero $\Rightarrow$ $g^m \cdot h^m = (g \cdot h)^m$

La notazione si estende al caso in cui $m$ è $0$ o è negativo.

$0 \cdot g \overset{def}{=} 0$

$0$: intero; $0$: elemento identità del gruppo

$(-m) \cdot g \overset{def}{=} m(-g)$, $m$ intero positivo

$m$: intero positivo; $-g$: elemento del gruppo inverso di $g$

$g^0 \overset{def}{=} 1$

$1$: identità del gruppo

$g^{-m} \overset{def}{=} (g^{-1})^m$

$g^{-1}$: inverso di $g$

Osservazione: sia $g \in G$, $b \geq 0$ intero

l'esponenziazione $g^b$ può essere calcolata in tempo polinomiale se l'operazione del gruppo può essere calcolata in tempo polinomiale.

Teorema 8.14 Sia $G$ un gruppo finito, $|G| = m$.

Allora, per ogni elemento $g \in G$, $g^m = \underline{1}$

Dim. (Supponiamo $G$ abeliano ma il risultato vale in genere)

Allora, fissiamo $g \in G$, e siano $g_1, g_2, \dots g_m$ gli elementi di $G$.

↓ arbitrario

Risulta:

$$g_1 \cdot g_2 \cdots g_m = (g \cdot g_1) \cdot (g \cdot g_2) \cdots (g \cdot g_m)$$

Infatti, nota che $g \cdot g_i = g \cdot g_j \Rightarrow g_i = g_j$ per la legge di cancellazione. Pertanto,

$(g g_1), (g \cdot g_2), \dots (g \cdot g_m)$ sono tutti distinti

e sono una permutazione di $g_1 \dots g_m$.

Poiché $G$ è abeliano

$$\underline{g_1 \cdot g_2 \cdots \cdot g_m} = (g \cdot g_1) \cdots (g \cdot g_m) = g^m \underline{(g_1 \cdot g_2 \cdots \cdot g_m)}$$

$$\Downarrow$$

$$1 = g^m$$

(applicando la legge di cancellazione)

Un corollario importante del risultato precedente è che possiamo lavorare nell'esponente "modulo l'ordine del gruppo".

**Corollario 8.15** $G$ gruppo finito, $|G| = m > 1$

Allora, per ogni $g \in G$ ed ogni intero $x$, risulta:

$$g^x = g^{[x \bmod m]}$$

**Dim.** Sia $x = q \cdot m + r$, $q, r$ interi, $r = [x \bmod m]$.

Si ha che:

$$g^x = g^{qm+r} = g^{qm} \cdot g^r = \underbrace{(g^m)}_{1}{}^q \cdot g^r$$

$$= g^r = g^{[x \bmod m]}$$

**Esempio 8.16** Sailto adolitivamente il corollario dice che

se $g$ è un elemento di $G$ di ordine $m$,

allora $x \cdot g = [x \bmod m] \cdot g$

$\mathbb{Z}_{15}$, $m = 15$, prendiamo $g = 11$

$$\underbrace{152}_{x} \cdot \underbrace{11}_{g} = [152 \bmod 15] \cdot 11 = 2 \cdot 11 = 11 + 11 = 22 = 7 \bmod 15.$$

$\Longrightarrow$ "riduci e moltiplica".

Corollario 8.17. $G$ finito, $|G| = m > 1$

Sia $e > 0$ un intero, sia

$f_e : G \to G$ definita da $f_e(g) = g^e$.

Se $\gcd(e, m) = 1$ ($e$ è invertibile)

allora $f_e$ è una permutazione. Inoltre,

se $d = e^{-1} \bmod m$, allora $f_d$ è

l'inversa di $f_e$.

Dim. $G$ finito $\Rightarrow$ la seconda parte

dell'enunciato implica la prima.

Mostriamo allora che $f_d$ è l'inversa di $f_e$

$$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{ed}$$

$$= g^{[ed \bmod m]} = g^1 = g$$

per ogni $g \in G$.

# Il gruppo $\mathbb{Z}_N^*$

$\mathbb{Z}_N = \{0, 1, \dots N-1\}$, gruppo rispetto alla somma mod $N$.

Possiamo definire un gruppo rispetto alla moltiplicazione?

↓

Dobbiamo rimuovere da $\mathbb{Z}_N$ tutti gli elementi non invertibili

Per ogni $N > 1$, sia

$$\mathbb{Z}_N^* = \{ b \in \{1, \dots, N-1\} \mid \gcd(b, N) = 1 \}$$

interi relativamente primi ad $N$

operazione del gruppo $a \cdot b \stackrel{def}{=} [a \cdot b \bmod N]$

$\mathbb{Z}_N^*$ è un gruppo abeliano

- contiene un elemento identità: 1
- ciascun elemento ha un inverso $\cdot \bmod N$
- commutatività ed associatività $\Rightarrow$ dagli interi
- chiusura: $a, b \in \mathbb{Z}_N^*$

$[a \cdot b \bmod N]$ ha inverso $[b^{-1} \cdot a^{-1} \bmod N]$

$\Rightarrow \gcd(a \cdot b, N) = 1 \Rightarrow a \cdot b \in \mathbb{Z}_N^*$

Sia $\varphi(N) \stackrel{def}{=} |\mathbb{Z}_N^*|$ l'ordine del gruppo $\mathbb{Z}_N^*$

Qual è il valore di $\varphi(N)$ ?

$N = p$, primo $\Rightarrow$ tutti gli elementi in $\{1, \dots, p-1\}$ sono relativamente primi a $p$

$\Rightarrow \varphi(p) = p - 1 = |\mathbb{Z}_p^*|$

$N = p \cdot q$ ($p$ primo, $q$ primo) $\Rightarrow$ se $a \in \{1, \dots, N-1\}$ non è relativamente primo con $N$, allora $p \mid a$ o $q \mid a$

$(p \cdot q = N > a \Rightarrow N \nmid a)$

Osservazione: gli elementi divisibili da $p$ sono: $p, 2p, 3p, \dots (q-1)\cdot p$

gli elementi divisibili da $q$ sono: $q, 2q, 3q, \dots (p-1)q$

$\Downarrow$

Gli elementi restanti in tutto sono

$$N - 1 - (q-1) - (p-1) = p \cdot q - (q-1) - (p-1) - 1$$

$$= p \cdot q - q - p + 1$$

$$= q(p-1) - (p-1) = (p-1) \cdot (q-1)$$

$$\Rightarrow \varphi(N) = \varphi(p \cdot q) = (p-1)(q-1) = |\mathbb{Z}_N^*|$$

In generale, vale il seguente:

**Teorema 8.19** $N = \prod_{i=1}^{n} p_i^{e_i}$, $\{p_i\}_i$ primi distinti e $\{e_i\}_i$ con $e_i \geq 0$. Allora risulta

$$\varphi(N) = \prod_{i=1}^{n} p_i^{e_i - 1}(p_i - 1)$$

---

**Esempio 8.20**

$N = 15 = 5 \cdot 3$

(primo, primo)

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$|\mathbb{Z}_{15}^*| = 8 = 4 \cdot 2$

$(5-1) \cdot (3-1)$

L'inverso di 8 in $\mathbb{Z}_{15}^*$ è 2, poiché $8 \cdot 2 = 16 = 1 \bmod 15$

---

**Corollario 8.21** $N > 1$, $a \in \mathbb{Z}_N^*$

Risulta: $a^{\varphi(N)} = 1 \bmod N$

Nel caso specifico $N = p$ (primo), $a \in \{1, \dots, p-1\}$

risulta: $a^{p-1} = 1 \bmod N$

(Piccolo teorema di Fermat)

Corollario 8.22. Fissiamo $N > 1$. Per ogni intero $e > 0$ definiamo $f_e : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ come

$$f_e(x) = [x^e \bmod N]$$

Se $e$ è relativamente primo a $\varphi(N)$, allora $f_e$ è una permutazione. Inoltre, se $d = e^{-1} \bmod \varphi(N)$, allora $f_d$ è l'inversa di $f_e$.

---

## Isomorfismi e teorema cinese del resto

Due gruppi sono isomorfi se hanno la stessa struttura

Un isomorfismo → modo alternativo di vedere $G$

Da un punto di vista computazionale → modo differente di rappresentare gli elementi

↓

operazioni più efficienti

In maniera più formale, vale la seguente definizione:

**Definizione 8.23.** Siano $G$ e $H$ gruppi con operazioni $\circ_G$ e $\circ_H$. Una funzione $f: G \to H$ è un isomorfismo da $G$ ad $H$ se

1. $f$ è bigettiva
2. per ogni $g_1, g_2 \in G$, risulta

$$f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$$

Se esiste un isomorfismo da $G$ ad $H$, i gruppi sono isomorfi e scriviamo $G \approx H$.

Isomorfismo = "rinominazione degli elementi di $G$" come elementi di $H$

Nota: $G$ finito, $G \approx H \Rightarrow H$ finito e $|H| = |G|$

Se $\exists\, f: G \to H \Rightarrow f^{-1}$ è un isomorfismo da $H$ a $G$

può accadere che:

- $f$: efficientemente calcolabile
- $f^{-1}$: non è efficientemente calcolabile

# Assunzioni Grittografiche in Gruppi Ciclici

$G$ gruppo finito di ordine $m$. Per $g \in G$ arbitrario

$$\langle g \rangle \overset{def}{=} \{ g^0, g^1, g^2, \dots \}$$

Risulta $g^m = 1$. Sia $i \leq m$ il più piccolo intero positivo per cui $g^i = 1$. La sequenza $g^0, g^1, \dots$ si ripete dopo $i$ termini, i.e., $g^i = g^0$, $g^{i+1} = g^1$, ...

quindi

$$\langle g \rangle = \{ g^0, g^1, \dots, g^{i-1} \}$$

$\downarrow$

contiene esattamente $i$ elementi

(se fosse $g^j = g^k$, per $0 \leq j < k < i$, allora $g^{k-j} = 1$ con $0 < k-j < i$ $\Rightarrow$ contraddizione con l'assunzione che $i$ è "il più piccolo")

$\langle g \rangle$ è un SOTTOGRUPPO di $G$ per ogni $g \in G$

$\downarrow$

sottogruppo generato da $g$ di ordine $i$

$i$ viene anche detto "ordine di $g$".

**Definizione 8.51** Sia $G$ un gruppo finito e $g \in G$. L'ordine di $g$ è il più piccolo intero positivo $i$ tale che $g^i = 1$.

**Proposizione 8.52** $G$ gruppo finito, $g$ di ordine $i$. Allora, per ogni intero $x$, risulta:

$$g^x = g^{[x \bmod i]}$$

**Proposizione 8.53** $G$ gruppo finito, $g$ di ordine $i$. Allora, $g^x = g^y$ se e solo se $x = y \bmod i$

Dim. Se $x = y \bmod i \Rightarrow [x \bmod i] = [y \bmod i]$

$$\Rightarrow g^x = g^{x \bmod i} = g^{y \bmod i} = g^y$$

(8.52)

Sia $g^x = g^y$. Allora $1 = g^{x-y} = g^{[(x-y) \bmod i]}$.

Poiché $[(x-y) \bmod i] < i$ ma $i$ è il più piccolo intero positivo per cui $g^i = 1$

$$\Rightarrow [(x-y) \bmod i] = 0 \Rightarrow x = y \bmod i$$

∎

Nota: l'elemento identità di ogni gruppo $G$ è il solo elemento di ordine 1, i.e., $\langle 1 \rangle = \{1\}$

Se esiste un elemento $g$ di ordine $m$, allora

$\langle g \rangle = G$ → si dice gruppo ciclico

↓ è un generatore del gruppo $G$

→ ci possono essere molti generatori

$g$ generatore di $G$ $\Rightarrow$ ogni $h \in G$ è uguale a $g^x$ per qualche $x \in \{0, 1, \dots, m-1\}$

Proposizione 8.54 $G$ gruppo finito di ordine $m$, $g$ di ordine $i$. Allora, risulta $i \mid m$.

Dim. $g^m = 1 = g^0 \Rightarrow m = 0 \bmod i \iff i \mid m$.

8.53

Corollario 8.55. $G$ gruppo di ordine primo $p$. Allora $G$ è ciclico. Inoltre, tutti gli elementi $g \in G$ (eccetto l'identità) sono generatori di $G$.

Dim. 8.54 $\Rightarrow$ i possibili "i" sono divisori di p

Ma p primo $\Rightarrow$ 1, p

l'elemento 1 è l'unico con ordine 1.

Tutti gli altri hanno ordine p. Pertanto sono generatori.

I gruppi di ordine primo formano una classe di gruppi ciclici.

$(\mathbb{Z}_N, +)$ per $N > 1$ è un altro esempio di gruppo ciclico

l'elemento 1 è un generatore del gruppo.

Teorema 8.56. Se p è primo allora $\mathbb{Z}_p^*$ è un gruppo ciclico di ordine $p-1$.

Dim. Complessa ... credeteci! :)

(... o consultate un manuale di algebra astratta)

Esempio 8.57

$(\mathbb{Z}_{15}, +_{15})$ ciclico, 1 è un generatore, $15 \cdot 1 = 0 \bmod 15$

e per $0 < i < 15$, $i \cdot 1 = i \neq 0 \bmod 15$

$\mathbb{Z}_{15}$ ha altri generatori

$$\langle 2 \rangle = \{0, 2, 4, \dots 14, 1, 3, \dots 13\}$$

Non tutti gli elementi di $\mathbb{Z}_{15}$ sono generatori

$$\langle 3 \rangle = \langle 0, 3, 6, 9, 12 \rangle \qquad \underbrace{5 \cdot 3 = 0 \bmod 15}_{\downarrow}$$

Nota che $5 \mid 15$ $\longleftarrow$ ordine 5

l'elemento 10 ha ordine 3 poiché $3 \cdot 10 = 0 \bmod 15$

$$\langle 10 \rangle = \{0, 5, 10\}$$

Esempio 8.58

$(\mathbb{Z}_{15}^*, *_{15})$, $\mathbb{Z}_{15}^*$ ha ordine $(p-1)(q-1) = (5-1)(3-1) = 8$

$$\langle 2 \rangle = \{1, 2, 4, 8\} \Rightarrow \text{ordine di } 2 \text{ è } 4,\ 4 \mid 8$$

$$\begin{array}{cccc} | & | & | & | \\ 2^0 & 2^1 & 2^2 & 2^3 \\ | & | & | & | \\ 2^4 & 2^5 & 2^6 & 2^8 \end{array}$$

Esempio 8.59

$(\mathbb{Z}_p, +_p)$ ha ordine primo $p$. È ciclico. Inoltre sappiamo che tutti gli elementi (eccetto 0) sono generatori.

Infatti, per ogni $h \in \{1, \dots, p-1\}$ ed intero $i > 0$,

$$i \cdot h = 0 \bmod p \quad \text{se e solo se} \quad p \mid ih$$

Ma per la Prop. 8.3,

$$\underbrace{p \mid i}_{\text{il più piccolo intero positivo per cui può accadere è } i = p} \quad \text{oppure} \quad \underbrace{p \mid h}_{\text{impossibile perché } h < p}$$

$$\Downarrow$$

$h$ ha ordine $p$ (quindi genera $\mathbb{Z}_p$)

Esempio 8.60

$(\mathbb{Z}_7^*, *_7)$, ciclico perché 7 è primo (Teorema 8.56)

$\langle 2 \rangle = \{1, 2, 4\} \Rightarrow$ 2 NON è un generatore

$$\langle 3 \rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_p^*$$

$$3^0 \quad 3^1 \quad 3^2 \quad 3^3 \quad 3^4 \quad 3^5 \quad \bmod 7$$

3 è generatore di $\mathbb{Z}_7^*$

Esempio 8.61

$G$ un gruppo ciclico di ordine $n$, con $g$ generatore di $G$.

La funzione $f : \mathbb{Z}_n \to G$ data da $f(a) = g^a$

è un isomorfismo tra $\mathbb{Z}_n$ e $G$.

Infatti, per ogni $a, a' \in \mathbb{Z}_n$

$$f(a+a') = g^{[(a+a') \bmod n]} = g^{a+a'}$$

$$= g^a \cdot g^{a'} = f(a) \cdot f(a')$$

La biiettività di $f$ può essere provata usando il fatto che $n$ è l'ordine di $g$.

Tutti i gruppi ciclici dello stesso ordine sono isomorfi.

⇓

Sono della stessa forma da un punto di vista algebrico.

NON è vero che "sono la stessa cosa" in senso COMPUTAZIONALE.

In particolare, un isomorfismo $f^{-1} : G \to \mathbb{Z}_n$

(che deve esistere) NON È DETTO che sia

efficientemente calcolabile (di seguito capirete perché...)

Assunzioni: Logaritmo Discreto e Diffie-Hellman

Problemi computazionali definiti per qualsiasi classe di gruppi ciclici.

Sia $\mathcal{G}$ un generico algoritmo di generazione di gruppi PPT

Input: $1^n$

Output: descrizione di $G$, il suo ordine $q$ (con $\|q\| = n$)
ed un generatore $g \in G$.

descrizione: "come gli elementi sono rappresentati attraverso stringhe di bit".

Richiediamo:

- algoritmi efficienti per calcolare l'operazione del gruppo $G$
- algoritmi efficienti per verificare l'appartenenza a $G$

Le precedenti implicano:

- esponenziazione efficiente
- campionamento efficiente di elementi uniformi.

Tutti i gruppi ciclici di un dato ordine sono isomorfi ma ... la RAPPRESENTAZIONE determina la complessità computazionale delle operazioni matematica del gruppo.

Sia $G$ un gruppo ciclico di ordine $q$, con generatore $g$

$\Rightarrow \{g^0, g^1, \dots g^{q-1}\}$ è l'intero $G$.

Per ogni $h \in G$, $\exists$ un UNICO $x \in \mathbb{Z}_q$ : $g^x = h$.

$x$ è il logaritmo discreto di $h$ rispetto a $g$.

↓

perché prende valore in un insieme finito

Scriviamo $x = \log_g h$.

Se $g^{x'} = h$ per un $x'$ arbitrario, allora $[x' \bmod q] = \log_g h$.

Nota che i logaritmi discreti obbediscono alle regole standard dei logaritmi. Per esempio:

$$\log_g 1 = 0 \quad (1 \text{ è l'identità di } G)$$

$\forall$ intero $z$, $\log_g h^z = [z \cdot \log_g h \bmod q]$

$\forall h_1, h_2$ $\log_g (h_1 \cdot h_2) = [(\log_g h_1 + \log_g h_2) \bmod q]$

Il problema del logaritmo discreto in un gruppo ciclico $G$ con generatore $g$ consiste nel calcolare $\log_g h$ per un elemento $h \in G$ uniforme.

$\mathrm{DLog}_{A,\mathcal{G}}(n)$

ordine $q$: $\|q\| = n$

gruppo ciclico ↓ , ↓ generatore

1. Esegui $\mathcal{G}(1^n)$ per ottenere $(G, q, g)$.
2. Scegli uniformemente $h \in G$.
3. $A$ riceve $(G, q, g)$ ed $h$ e dà in output $x \in \mathbb{Z}_q$
4. L'output è 1 se $g^x = h$; 0, altrimenti.

Definizione 8.62. Il problema del logaritmo discreto è difficile relativamente a $\mathcal{G}$ se, $\forall$ (PPT) algoritmo $A$, $\exists$ una funzione trascurabile $\mathrm{negl}$, tale che

$$P_n\left[\mathrm{DLog}_{A,\mathcal{G}}(n) = 1\right] \leq \mathrm{negl}(n).$$

L'assunzione del logaritmo discreto

$\Rightarrow$ $\exists$ un $\mathcal{G}$ per cui il problema del logaritmo discreto (DL) è difficile.

# Problemi Diffie-Hellman

Due varianti

**CDH**
Computational Diffie-Hellman
↓
Problema computazionale

**DDH**
Decisional Diffie-Hellman
↓
Problema decisionale

Si fissi un gruppo ciclico $G$ ed un generatore $g \in G$.

Dati $h_1, h_2 \in G$, $DH_g(h_1, h_2) \stackrel{def}{=} g^{\log_g h_1 \cdot \log_g h_2}$.

Cioè, se $h_1 = g^{x_1}$ e $h_2 = g^{x_2}$

$$DH_g(h_1, h_2) = g^{x_1 x_2} = h_1^{x_2} = h_2^{x_1}$$

Il problema CDH consiste nel calcolare $DH_g(h_1, h_2)$ per $h_1, h_2 \in G$ uniformi.

Nota: Se il problema DL è facile $\Rightarrow$ CDH è anche facile.

dati $h_1, h_2$, calcola $x_1 = \log_g h_1$ e dà in output $h_2^{x_1}$. Non sappiamo se:

DL difficile $\stackrel{?}{\Rightarrow}$ CDH difficile

Il problema DDH consiste nel distinguere $DH_g(h_1, h_2)$ da un elemento uniforme del gruppo, quando $h_1$ ed $h_2$ sono uniformi.

Dati $h_1, h_2$ e $h'$ il problema consiste nel decidere se

$h'$ è $DH_g(h_1, h_2)$

$h'$ è scelto uniformemente in $G$

Definizione 8.63. Il problema DDH è difficile relativamente a $\mathcal{G}$, se $\forall$ algoritmo $A$ PPT, esiste una funzione trascurabile negl tale che:

$$\left| P_2[A(G, q, g, g^x, g^y, g^z) = 1] - P_2[A(G, q, g, g^x, g^y, g^{xy}) = 1] \right| \leq \text{negl}(n)$$

$\downarrow$ $\mathcal{G}(1^n)$

$x, y, z$ uniformi in $\mathbb{Z}_q$

$\downarrow$ $\mathcal{G}(1^n)$

$x, y$ uniformi in $\mathbb{Z}_q$

Nota: se CDH è facile $\Rightarrow$ DDH anche è facile

L'inverso non sembra essere vero: ci sono esempi in cui DDH è facile, mentre DL e CDH sembrano difficili.

# Uso di gruppi di ordine primo.

Ci sono varie classi di gruppi ciclici in cui i problemi DL ed i problemi Diffie-Hellman sono ritenuti difficili.

Una classe preferita: GRUPPI CICLICI DI ORDINE PRIMO

Ragioni:

- il problema DL è più difficile (rispetto agli algoritmi noti per calcolare il DL)
- il problema DDH è facile se l'ordine del gruppo q ha fattori primi piccoli
- trovare un generatore del gruppo è banale (ogni elemento, eccetto l'identità, è un generatore)
- ragione tecnica: le prove di sicurezza di alcune costruzioni richiedono il calcolo degli inversi moltiplicativi di certi esponenti. In tali gruppi ogni esponente non nullo è invertibile.

- quando si usa il problema DDH, fissato $G$ ed un generatore $g$, alla fin fine occorre distinguere

$$(h_1, h_2, DH_g(h_1, h_2)) \quad \text{da} \quad (h_1, h_2, Y)$$

uniformi uniformi

Pertanto, una condizione necessaria è che $DH_g(h_1, h_2)$ dovrebbe essere indistinguibile da un elemento uniforme.

Se l'ordine del gruppo è primo, si può dimostrare che

$DH_g(h_1, h_2)$ è "quasi" uniforme.

# Lavorare in $\mathbb{Z}_p^*$

Gruppi della forma $\mathbb{Z}_p^*$, con p primo, danno una classe di gruppi ciclici in cui il DL è ritenuto difficile.

$\mathcal{G}(1^n)$ $\Rightarrow$ sceglie un primo di n bit p e dà in output $p$, $q = p-1$ ed un generatore $g$ (ci sono metodi efficienti per calcolarlo)

Rappresentazione: gli elementi del gruppo sono interi $\in \{1, 2, \ldots, p-1\}$

Assunzione: DL è difficile relativamente a $\mathcal{G}$.

Sfortunatamente, per $p > 3$ primo, il gruppo ciclico $\mathbb{Z}_p^*$ NON ha ordine primo ($q = (p-1)$ è pari)

Inoltre, il problema DDH è in generale NON è difficile in questi gruppi.

Cosa possiamo fare?

La questione può essere affrontata usando un SOTTOGRUPPO di ordine primo di $\mathbb{Z}_p^*$.

Sia $p = 2q + 1$. Proviamo che $\mathbb{Z}_p^*$ ha un sottogruppo $G$ di ordine $q$
(p primo, q primo)

Teorema 8.66. Sia $p = 2q + 1$, con $p$ e $q$ primi. Allora

$$G \stackrel{def}{=} \{ [h^2 \bmod p] \mid h \in \mathbb{Z}_p^* \}$$

è un sottogruppo di $\mathbb{Z}_p^*$ di ordine $q$.

Nota: per $2 = 2$, $G$ è l'insieme dei "quadrati" modulo $p$ di $\mathbb{Z}_p^*$

Dim. Per mostrare che $G$ è un sottogruppo di $\mathbb{Z}_p^*$ occorre far vedere che tutte e quattro le proprietà sono soddisfatte.

È facile. Provatelo per esercizio!

Proviamo invece che $G$ ha ordine $q$.

La funzione $f_2 : \mathbb{Z}_p^* \to G$ definita da $f_2(g) = g^2 \bmod p$ è una funzione 2-a-1. Poiché $|\mathbb{Z}_p^*| = p-1$, ciò mostra che $|G| = \frac{p-1}{2} = q$. Per vedere la precedente,

sia $g$ un generatore di $\mathbb{Z}_p^*$

$g^0, g^1, \ldots, g^{p-2}$ sono tutti gli elementi di $\mathbb{Z}_p^*$

La proposizione 8.53 implica

$$(g^i)^2 = (g^j)^2 \text{ se e solo se } i \cdot 2 = j \cdot 2 \bmod (p-1)$$

$$\iff (p-1) \mid (i-j)2$$

Poiché $p-1 = 2q$, possiamo scrivere

$$q \mid (i-j) \qquad (\text{i.e. } (i-j) = kq \iff i = j + kq)$$

Per ogni fissato $j \in \{0, 1, \ldots, p-2\}$, ciò significa che l'insieme di valori $i \in \{0, 1, \ldots, p-2\}$ per cui $(g^i)^2 = (g^j)^2$ è esattamente l'insieme di 2 valori distinti

$$\{j, j+q, j+2q, \ldots, j+(2-1)q\}$$

tutti ridotti modulo $p$. (Nota: $j + 2q = j \bmod (p-1)$)

Pertanto, $f_2$ è $2 - a - 1$. ∎

Il Teorema 8.64 fornisce anche un metodo per generare un elemento uniforme di $G$ e verificare se un elemento di $\mathbb{Z}_p^*$ appartiene a $G$.

① (generazione): scegli uniformemente $h \in \mathbb{Z}_p^*$ e calcola $h^2 \bmod p$ (ogni elemento di $G$ è un generatore)

② (verifica per $h \in \mathbb{Z}_p^*$ dell'appartenenza a $G$): controlla se $h^q \stackrel{?}{=} 1 \bmod p$

$\Downarrow$

funziona perché...

sia $h = g^i$ ($g$ generatore di $\mathbb{Z}_p^*$, $i \in \{0, 1, \dots, p-2\}$)

$$h^q = 1 \bmod p \iff (g^i)^q = 1 \bmod p$$

$$\iff iq = 0 \bmod (p-1) \iff 2q \mid iq \iff 2 \mid i.$$

Pertanto, $h = g^i = g^{c \cdot 2} = (g^c)^2$ per qualche $c$

$$\Longrightarrow \quad h \in G$$

∎

Algoritmo 8.65

Input : $1^n$, $\ell = \ell(n)$

Output : Gruppo ciclico $G$, ordine primo $q$, generatore $g$.

Genera un primo $q$ di $n$ bit uniforme

Genera un primo $p$ di $\ell$ bit tale che $q \mid p-1$

Scegli uniformemente $h \in \mathbb{Z}_p^*$, con $h \neq 1$

Poni $g = [h^{(p-1)/q} \bmod p]$

Return $p, q, g$ // $G$ è un sottogruppo di $\mathbb{Z}_p^*$ di ordine $q$

La scelta di $\ell = \ell(n)$ dipende dagli algoritmi ad oggi noti per calcolare il DL in sottogruppi di ordine $q$ di $\mathbb{Z}_p^*$

NIST raccomanda valori per $p, q$ e $g$.

Esempio 8.66

$(\mathbb{Z}_{11}^*, \cdot_{11})$ 11 primo, ordine $p-1 = 11-1 = 10$

Potenze di 2 :

| $2^0$ | $2^1$ | $2^2$ | $2^3$ | $2^4$ | $2^5$ | $2^6$ | $2^7$ | $2^8$ | $2^9$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 |

$\Rightarrow$ 2 è un generatore del gruppo.

Potenze di 3 :

| $3^0$ | $3^1$ | $3^2$ | $3^3$ | $3^4$ | $3^5$ | $3^6$ | $3^7$ | $3^8$ | $3^9$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 9 | 5 | 4 | 1 | 3 | 9 | 5 | 4 |

$\Rightarrow$ 3 NON è un generatore del gruppo.

Esso genera il sottogruppo $G = \{1, 3, 9, 5, 4\}$ di ordine 5.

Potenze di 10 :

| $10^0$ | $10^1$ | $10^2$ | $10^3$ | $10^4$ | $10^5$ | $10^6$ | $10^7$ | $10^8$ | $10^9$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 |

$\Rightarrow$ 10 genera il sottogruppo $G = \{1, 10\}$ (ordine 2)

Nota che $11 = 2 \cdot 5 + 1$

| | | |
|---|---|---|
| p | q | r |

Il teorema 8.64 $\Rightarrow$ i quadrati di tutti gli elementi di $\mathbb{Z}_{11}^*$ dovrebbero dare un sottogruppo di ordine 5.

Controlliamo!

| Elementi : | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| | \| | \| | \| | \| | \| | \| | \| | \| | \| | \| |
| Quadrati : | 1 | 4 | 9 | 5 | 3 | 1 | 4 | 9 | 5 | 3 |

Abbiamo mostrato in precedenza che 3 è un generatore di questo sottogruppo. Ma, in realtà, poiché 9 è primo, TUTTI gli elementi del sottogruppo (eccetto 1) sono generatori.

D'altra parte nota che $11 = 5 \cdot 2 + 1$

$p \quad 2 \quad q$

Il Teorema 8.64 $\Rightarrow$ le potenze quinte di tutti gli elementi di $\mathbb{Z}_{11}^*$ dovrebbero dare un sottogruppo di ordine 2.

Controlliamo!

| Elementi : | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| | \| | \| | \| | \| | \| | \| | \| | \| | \| | \| |
| Potenze quinte : | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 |

In precedenza abbiamo visto che 10 è un generatore di questo sottogruppo.

# Curve Ellittiche

Gruppi visti fino ad ora $\Longrightarrow$ basati sull'aritmetica modulare

Un'altra classe di gruppi importante per la crittografia $\Longrightarrow$ gruppi di punti su curve ellittiche

$\Downarrow$

Allo stato attuale delle conoscenze NON si conoscono algoritmi quasi-esponenziali per risolvere il problema DL in gruppi di punti di una curva ellittica opportunamente scelta.

$\Downarrow$

Implementazioni basate su gruppi di punti di curve ellittiche sono pertanto più efficienti di quelle basate su sottogruppi di ordine primo di $\mathbb{Z}_p^*$ PER OGNI LIVELLO DI SICUREZZA FISSATO.

Breve introduzione a questi gruppi

Sia $p \geq 5$ primo. Si consideri l'equazione $E$ in $x$ e $y$

$$y^2 = x^3 + Ax + B \bmod p$$

dove $A, B \in \mathbb{Z}_p$ sono costanti tali che $4A^3 + 27B^2 \neq 0 \bmod p$.

Denoti $E(\mathbb{Z}_p)$ l'insieme di coppie $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ che soddisfano l'equazione più un valore speciale $\mathcal{O}$, i.e.,

$$E(\mathbb{Z}_p) = \{(x,y) \mid x, y \in \mathbb{Z}_p \text{ e } y^2 = x^3 + Ax + B \bmod p\} \cup \{\mathcal{O}\}$$

$\downarrow$ punti sulla curva ellittica $E$ — $\downarrow$ punto all'infinito

Esempio 8.67

$y \in \mathbb{Z}_p^*$ è un (quadratico residuo) modulo $p$ se $\exists\ x \in \mathbb{Z}_p^*$ tale che $x^2 = y \bmod p$. Diciamo che $x$ è una radice quadrata di $y$. Per $p > 2$ primo, si può mostrare che:

- metà degli elementi in $\mathbb{Z}_p^*$ sono residui quadratici
- ogni residuo quadratico ha esattamente due radici quadrate

$f(x) \stackrel{def}{=} x^3 + 3x + 3$ , $E : y^2 = f(x) \bmod 7$

($E$: curva)

Ciascun valore di $x$ per cui $f(x)$ è un residuo quadratico dà due punti sulla curva.

I valori di $x$ per cui $f(x)$ non è un residuo quadratico non danno punti.

I valori di $x$ per cui $f(x) = 0$, danno un punto.

$f(0) = 3 \bmod 7$, non è un residuo quadratico mod 7

$f(1) = 0 \bmod 7$, punto $(1, 0) \in E(\mathbb{Z}_7)$

$f(2) = 3 \bmod 7$, non è un residuo quadratico mod 7

$f(3) = 4 \bmod 7$, residuo quadratico - radici quadrate 2 e 5
punti $(3, 2), (3, 5) \in E(\mathbb{Z}_7)$

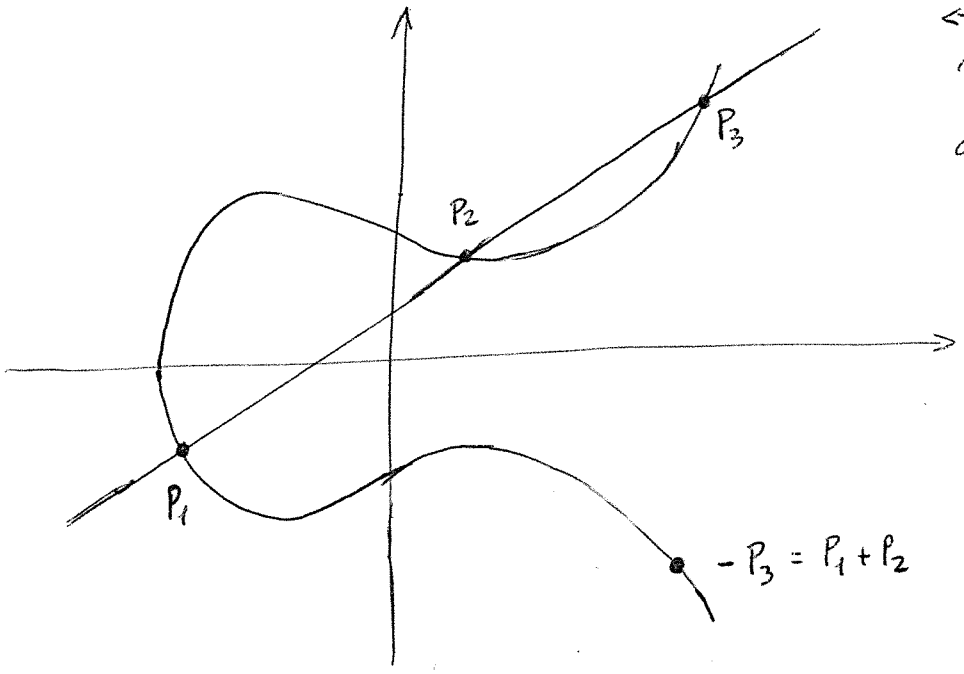
$f(4) = 2 \bmod 7$, residuo quadratico, radici quadrate 3 e 4
punti $(4, 3), (4, 4) \in E(\mathbb{Z}_7)$

$f(5) = 3 \bmod 7$, non è un residuo quadratico

$f(6) = 6 \bmod 7$, non è un residuo quadratico

$E(\mathbb{Z}_7) = \{(1,0), (3,2), (3,5), (4,3), (4,4)\} \cup \{\mathcal{O}\}$

Un modo utile di pensare alla curva $E(\mathbb{Z}_p)$ è guardare il grafico dell'equazione sui numeri reali. Ha figura NON corrisponde ad $E(\mathbb{Z}_p)$ ma... dà un'intuizione utile.




← Immagina O "sulla sommità dell'asse delle y e posizionato su OGNI linea verticale"

Si può dimostrare che OGNI linea intersecante $E(\mathbb{Z}_p)$ interseca la curva in 3 punti, dove

1) un punto P viene contato due volte se la linea è tangente alla curva in P

2) il punto all'infinito $\mathcal{O}$ viene contato se la linea è verticale

Questo fatto viene usato per definire un'operazione binaria, chiamata "addizione" e denotata con + sui punti di $E(\mathbb{Z}_p)$

- Il punto $\mathcal{O}$ viene definito come l'identità additiva, i.e., per ogni $P \in E(\mathbb{Z}_p)$, $\quad P + \mathcal{O} = \mathcal{O} + P = P$

- Per due punti $P_1, P_2 \neq \mathcal{O}$ su $E$, valutiamo $P_1 + P_2$ disegnando la linea da $P_1$ a $P_2$ (se $P_1 = P_2$ allora disegniamo la linea tangente alla curva in $P_1$) e trovando il terzo punto di intersezione (può essere $\mathcal{O}$ se la linea è verticale)

  Se $P_3 = (x, y) \neq \mathcal{O}$, allora definiamo

  $$P_1 + P_2 \stackrel{def}{=} (x, -y)$$

  Se $P_3 = \mathcal{O}$, allora $\quad P_1 + P_2 = \mathcal{O}$

Si noti che, se $P = (x, y) \neq \mathcal{O}$ è un punto di $E(\mathbb{Z}_p)$,
allora $-P = (x, -y)$ (punto di $E(\mathbb{Z}_p)$) è l'inverso di $P$
$\Rightarrow$ la linea
che passa per $(x, y)$ e $(x, -y)$ è verticale $\Rightarrow P + (-P) = \mathcal{O}$

Algebricamente, la legge dell'addizione può essere derivata come segue:

Siano $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2) \in E(\mathbb{Z}_p)$, $P_1, P_2 \neq \mathcal{O}$

Supponiamo $x_1 \neq x_2$ (il caso $x_1 = x_2$ è simile ma tedioso)

Il coefficiente angolare della linea passante per questi punti è:

$$m \overset{def}{=} \left[ \frac{y_2 - y_1}{x_2 - x_1} \bmod p \right]$$

$x_1 \neq x_2 \implies (x_2 - x_1)^{-1} \bmod p$ esiste.

La linea passante per $P_1$ e $P_2$ ha equazione

$$y = m(x - x_1) + y_1 \bmod p \qquad (8.2)$$

Per trovare il terzo punto di intersezione di questa linea con $E(\mathbb{Z}_p)$ sostituiamo la precedente nell'equazione di $E$, ottenendo

$$\left(m(x - x_1) + y_1\right)^2 = x^3 + Ax + B \bmod p$$

I valori di $x$ che soddisfano questa equazione sono $x_1$, $x_2$ e $x_3 \overset{def}{=} [m^2 - x_1 - x_2 \bmod p]$

dove $x_3$ è la coordinata $x$ di $P_3$.

Usando la (8.2), otteniamo $y_3 = [m(x_3 - x_1) + y_1 \bmod p]$

Per ottenere $P_1 + P_2$, cambiamo il segno di $y_3$

$$\Rightarrow (x_1, y_1) + (x_2, y_2) = \left( [m^2 - x_1 - x_2 \bmod p], [m(x_1 - x_3) - y_1 \bmod p] \right).$$

Utilizzando tecniche simili, arriviamo alla seguente

Proposizione 8.68. Sia $p \geq 5$ primo e sia $E$ una curva ellittica data da $y^2 = x^3 + Ax + B \bmod p$, dove $4A^3 + 27B^2 \neq 0 \bmod p$. Siano $P_1, P_2 \neq \mathcal{O}$ punti di $E$, $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$.

1. Se $x_1 \neq x_2$, allora $P_1 + P_2 = (x_3, y_3)$ con

$$x_3 = [m^2 - x_1 - x_2 \bmod p] \quad \text{e} \quad y_3 = [m(x_1 - x_3) - y_1 \bmod p]$$

dove $$m = \left[ \frac{y_2 - y_1}{x_2 - x_1} \bmod p \right]$$

2. Se $x_1 = x_2$ ma $y_1 \neq y_2$, allora $P_1 = -P_2$

pertanto $P_1 + P_2 = \mathcal{O}$

3. Se $P_1 = P_2$ e $y_1 = 0$, allora

$$P_1 + P_2 = 2P_1 = \mathcal{O}$$

4. Se $P_1 = P_2$ e $y_1 \neq 0$, allora

$P_1 + P_2 = 2P_1 = (x_3, y_3)$ con

$x_3 = [m^2 - 2x_1 \bmod p]$ e $y_3 = [m(x_1 - x_3) - y_1 \bmod p]$

dove $m = \left[\frac{3x_1^2 + A}{2y_1} \bmod p\right]$

L'insieme di punti $E(\mathbb{Z}_p)$ munito

dell'operazione di addizione appena definita

forma un GRUPPO ABELIANO chiamato

"il gruppo della curva ellittica $E$"

$\mathcal{O}$ agisce come l'identità

la commutatività deriva dalla definizione

dell'operazione di somma +

chiusura ed esistenza dell'inverso altrettanto

l'associatività è più complicata da dimostrare

ma ... vale!

⇓

Per convincersi consideriamo un esempio.

Esempio 8.69 Mostriamo l'associatività per 3 punti dell'esempio precedente

$P_1 = (1, 0)$ , $P_2 = Q_2 = (4, 3)$

$P_1 + P_2 \Rightarrow m = [(3-0)(4-1)^{-1} \bmod 7] = 1$ , $x_3 = [1^2 - 1 - 4 \bmod 7] = 3$

Quindi $P_3 \overset{def}{=} P_1 + P_2 = (3, [1(1-3) - 0 \bmod 7]) = (3, 5)$

↳ punto di $E(\mathbb{Z}_7)$

Se calcoliamo $P_3 + Q_2$, otteniamo

$m = [(3-5)(4-3)^{-1} \bmod 7] = 5$ e $x_3 = [5^2 - 3 - 4 \bmod 7] = 4$

Quindi $(P_1+P_2) + Q_2 = P_3 + Q_2 = (4, [5(3-4) - 5 \bmod 7]) = \underline{(4, 4)}$.

D'altra parte, $P_2 + Q_2 = 2P_2$ dà

$m = [(3 \cdot 4^2 + 3)(2 \cdot 3)^{-1} \bmod 7] = 5$ e $x_3 = [5^2 - 2 \cdot 4 \bmod 7] = 3$

Quindi $P_3' \overset{def}{=} P_2 + Q_2 = (3, [5(4-3) - 3 \bmod 7]) = (3, 2)$

Se poi calcoliamo $P_1 + P_3'$, troviamo che

$m = [2(3-1)^{-1} \bmod 7] = 1$ e $x_3 = [1^2 - 1 - 3 \bmod 7] = 4$

Pertanto, $P_1 + (P_2 + Q_2) = P_1 + P_3' = (4, [1(1-4) - 0 \bmod 7]) = \underline{(4, 4)}$

$\Rightarrow P_1 + (P_2 + Q_2) = (P_1 + P_2) + Q_2$

( il caso generale è più complicato ... )

# Notazioni per i gruppi

Additiva → esponenziazione = addizioni ripetute

Moltiplicativa

Se fissiamo un punto $P$ in un gruppo di una curva ellittica il problema DL diviene (informalmente) il problema di calcolare l'intero $x$ a partire dal punto $xP$. E la versione decisionale del problema DH, diventa distinguere

$$(aP, bP, abP) \quad \text{da} \quad (aP, bP, cP)$$

Questi problemi sono ritenuti difficili in gruppi di punti di curve ellittiche (o sottogruppi di punti) <u>di ordine primo</u> grande.

Domanda: ma quanto sono grandi i gruppi delle curve ellittiche?

Valutazione euristica: metà degli elementi di $\mathbb{Z}_p^*$ sono residui quadratici, ciascun residuo quadratico dà due punti (+ il punto $\mathcal{O}$)

$$\Rightarrow \quad 2\,\frac{(p-1)}{2} + 1 = p \text{ punti}$$

Teorema 8.70 (Hasse bound)

Sia $p$ un primo, e sia $E$ una curva ellittica su $\mathbb{Z}_p$.

Allora:

$$p+1-2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p+1+2\sqrt{p}$$

Il bound implica: è facile trovare un punto su $E(\mathbb{Z}_p)$

- scegli uniformemente $x \in \mathbb{Z}_p$, verifica se $f(x)$ è $0$ o un (quadratico residuo) e, in tal caso, sia $y$ una radice quadrata di $f(x)$.

[ - decidere la residuosità quadratica e trovare radici mod $p$ verrà discusso nel seguito... ]

Nota che esistono algoritmi efficienti per calcolare il numero ESATTO di punti di una curva ellittica.

Un approccio per la generazione dei parametri di una curva ellittica è suggerito dall'algoritmo che segue:

Algoritmo 8.71

Algoritmo $\mathcal{G}$ per la generazione di un gruppo su una curva ellittica

Input: parametro di sicurezza $1^m$

Output: gruppo ciclico $G$, il suo ordine (primo) $q$ ed un generatore $g$.

Genera un primo $p$ di $m$ bit uniforme

Fino a quando $q$ non diventa un primo di $m$ bit, ripeti:

scegli $A, B \leftarrow \mathbb{Z}_p$ con $4A^3 + 27B^2 \neq 0 \bmod p$

che definiscono una curva ellittica $E$

sia $q$ il numero di punti su $E(\mathbb{Z}_p)$

Scegli $g \in E(\mathbb{Z}_p) \setminus \{\mathcal{O}\}$

Return $(A, B, p)$, $q$, $g$

- $(A, B, p)$ → Parametri che definiscono la curva $E$
- $q$ → ordine del gruppo (# di punti della curva)
- $g$ → generatore

Nota: certe classi di curve ellittiche sono deboli e non dovrebbero essere usate. Per esempio:

- curve anomale (ordine uguale a p)
- curve supersingolari (ordine uguale a $p+1$)
- curve il cui ordine divide $p^K - 1$ per $K$ "piccolo"

Ad ogni modo, il NIST suggerisce curve standard che possono essere usate.

## Considerazioni sull'efficienza

Compressione dei punti. Il numero di bit necessario per rappresentare un punto su una curva ellittica può essere ridotto della metà.

Per ogni punto $(x, y)$ su $E: y^2 = f(x) \bmod p$ ci sono al più due punti su $E$ con coordinata $x$:

$$(x, y) \quad \text{ed} \quad (x, -y)$$

Pertanto $P = (x, y)$ può essere specificato da $(x, \underline{b})$ — $\underline{b}$ bit: 0 se $y < p/2$, 1 se $y \geq p/2$

Per "recuperare" $P$ allora basta:

calcolare le due radici quadrate $\underline{y_1}$ ed $\underline{y_2}$ e decidere in accordo a $\underline{b}$.

Coordinate proiettive.

$P = (x, y)$ → coordinate affini

Coordinate proiettive → modo alternativo per rappresentare i punti della curva

↳ Uno strumento utile per accelerare le computazioni

NON devono essere usate per memorizzare e trasmettere i punti!

In coordinate proiettive un punto è rappresentato da:

→ tre elementi di $\mathbb{Z}_p$

$P = (x, y) \quad (\neq \mathcal{O})$

$(x, y) \iff (X, Y, Z) \in \mathbb{Z}_p^3$

↑ coordinate proiettive

coordinate affini

$x = \frac{X}{Z} \bmod p, \quad y = \frac{Y}{Z} \bmod p, \quad Z \neq 0$