Il gruppo ciclico $\mathbf{Z}_p^*$, radici primitive modulo p, logaritmo discreto in $\mathbf{Z}_p^*$, il gruppo $\mathbf{Z}_{p^k}^*$.

Lo scopo principale di questa nota è dimostrare che il gruppo moltiplicativo $\mathbf{Z}_p^*$ delle classi resto modulo un primo p è un gruppo ciclico: dimostreremo l'esistenza di un generatore del gruppo $\mathbf{Z}_p^*$, detto anche *radice primitiva*.

Il piccolo Teorema di Fermat dice che $\overline{y}^{p-1} = \overline{1}$, per ogni $\overline{y}$ in $\mathbf{Z}_p^*$. Questo implica che l'ordine di un elemento $\overline{y}$ di $\mathbf{Z}_p^*$ è al massimo $p-1$. Poiché $\#\mathbf{Z}_p^* = p-1$, se esiste $\bar{x} \in \mathbf{Z}_p^*$ di ordine esattamente $p-1$, allora $\mathbf{Z}_p^*$ coincide con l'insieme delle potenze $\overline{x}, \overline{x}^2, \ldots, \overline{x}^{p-1} = \overline{1}$. In altre parole un elemento $\bar{x}$ di ordine $p-1$ è automaticamente un generatore di $\mathbf{Z}_p^*$.

Lemma 1 (Formula di Gauss). *Sia n un numero naturale. Allora*

$$\sum_{d|n} \varphi(d) \;=\; n,$$

dove d varia fra i divisori positivi di n.

Dim. Scriviamo

$$\mathbf{Z}_n = \bigcup_{d|n} \{\bar{x} \in \mathbf{Z}_n \mid gcd(x,n) = d\}$$

e calcoliamo la cardinalità dell'insieme $\{\bar{x} \in \mathbf{Z}_n \mid gcd(x,n) = d\}$. Sia $0 < x < n$. Abbiamo che

$$gcd(x,n) = d \;\Leftrightarrow\; gcd(\frac{x}{d}, \frac{n}{d}) = 1 \;\Leftrightarrow\; \frac{\bar{x}}{d} \in \mathbf{Z}_{\frac{n}{d}}^*.$$

Dunque la cardinalità cercata è $\varphi(\frac{n}{d})$, da cui segue che

$$n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d).$$

Lemma 2. *Sia n un numero naturale e sia $x \in \mathbf{Z}$ con* $\mathrm{mcd}(x,n) = 1$. *Sia $a = \mathrm{ord}_n(x)$ l'ordine di $\bar{x}$ in $\mathbf{Z}_n^*$. Allora*

(a) Per ogni $k \in \mathbf{Z}$ il numero $\mathrm{ord}_n(x^k)$ *divide $a = \mathrm{ord}_n(x)$.*

(b) Si ha che $\mathrm{ord}_n(x^k)$ *è uguale ad $a = \mathrm{ord}_n(x)$ se e solo se* $\mathrm{mcd}(k,a) = 1$.

Dim. La dimostrazione della parte (a) è facile. Dimostriamo (b). Se d divide $\mathrm{mcd}(k,a)$, allora $(x^k)^{a/d} \equiv (x^a)^{k/d} \equiv 1 \pmod{n}$. Se quindi $\mathrm{mcd}(k,a) \neq 1$, allora l'ordine di $\overline{x}^k$ non è uguale a a. Viceversa, supponiamo che $\mathrm{mcd}(k,a) = 1$. Per la parte (a) sappiamo già che $b = \mathrm{ord}_n(x^k)$ divide $a = \mathrm{ord}_n(x)$. Per stabilire che a divide b, basta dimostrare che $x^b \equiv 1 \pmod{n}$.
Per il Teorema di Bézout esistono $\lambda, \mu \in \mathbf{Z}$ tali che $\lambda k + \mu a = 1$. Adesso abbiamo che

$$x^b = x^{b(\lambda k + \mu a)} = (x^k)^{b\lambda} \cdot (x^a)^{b\mu}.$$

Siccome l'ordine di x^k è b e siccome $x^a \equiv 1 \pmod{n}$, vediamo che l'espressione a destra è congrua a $1 \pmod{n}$. Quindi $x^b \equiv 1 \pmod{n}$ e concludiamo che a divide b come richiesto.

Lemma 3. *Sia p un numero primo e sia $f \in \mathbf{Z}_p[X]$ un polinomio di grado d. Allora f ammette al più di d zeri in $\mathbf{Z}_p$.*

Dim. Sia $f(X) = b_d X^d + b_{d-1}X^{d-1} + \ldots + b_1 X + b_0$ un polinomio di grado d, con coefficienti $b_i \in \mathbf{Z}_p^*$ e $b_d \neq 0$. Dividendo tutti i coefficienti per b_d (questo è possibile perché $\mathbf{Z}_p^*$ è un campo) possiamo ridurci al caso di un polinomio monico, ossia con coefficiente di grado massimo uguale ad 1, cioè

$$f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0.$$

Adesso procediamo per induzione sul grado di f.

Se f ha grado 0, allora è costante e non ha zeri.
Per ipotesi induttiva, supponiamo che un polinomio monico di grado $d-1$ abbia al più $d-1$ zeri.
Sia ora f un polinomio monico di grado d. Se f non ammette zeri in $\mathbf{Z}_p$, non c'è niente da dimostrare. Supponiamo che $f(\overline{a}) = \overline{0}$ per un certo $\overline{a} \in \mathbf{Z}_p$. Dividendo il polinomio $f(X)$ per $X - \overline{a}$, otteniamo un quoziente $g(X)$ e un resto di grado zero $\overline{r} \in \mathbf{Z}_p$:

$$f(X) = g(X)(X - \overline{a}) + \overline{r}.$$

Sostituendo $X = \overline{a}$ in questa relazione, troviamo che $\overline{r} = \overline{0}$. Sia ora $\overline{b}$ uno zero di $f(X)$; allora abbiamo che

$$\overline{0} = f(\overline{b}) = g(\overline{b})(\overline{b} - \overline{a}), \quad \text{in } \mathbf{Z}_p.$$

Poiché p *è primo*, si ha che p divide $b-a$ oppure p divide $g(b)$. Nel primo caso $\overline{b} = \overline{a}$ e nel secondo $g(\overline{b}) = \overline{0}$. Osserviamo che il polinomio $g(X)$ ha grado $d-1$ e per ipotesi induttiva ammette al più di $d-1$ zeri. Ci sono quindi al più $(d-1)+1 = d$ possibilità per $\overline{b}$.
Questo conclude la dimostrazione del Lemma.

Teorema 4. *Sia p un numero primo. Allora esiste $\overline{x} \in \mathbf{Z}_p^*$ di ordine $p-1$.*

Dim. Per ogni numero naturale d definiamo

$$g(d) = \#\{\overline{y} \in \mathbf{Z}_p^* : \mathrm{ord}_p(y) = d\}.$$

Affermiamo che vale $g(d) = 0$ oppure $g(d) = \varphi(d)$.
Supponiamo che $g(d) \neq 0$, ossia che esista $\overline{x} \in \mathbf{Z}_p^*$ di ordine d. Siano $\{\overline{x}, \overline{x}^2, \ldots, \overline{x}^d = \overline{1}\}$ le d potenze distinte di $\bar{x}$. Si verifica facilmente che

$$\{\overline{x}, \overline{x}^2, \ldots, \overline{x}^d\} \quad \subset \quad \{\overline{y} \in \mathbf{Z}_p^* : \overline{y}^d = \overline{1}\}.$$

Infatti $(\bar{x}^k)^d = (\bar{x}^d)^k = \bar{1}$, per ogni $1 \leq k \leq d$. L'insieme a destra, che consiste negli elementi di $\mathbf{Z}_p^*$ il cui ordine divide d, coincide con l'insieme degli zeri del polinomio $X^d - 1$. Per il Lemma 3, tali zeri sono al più d. Ne segue che

$$\{\overline{x}, \overline{x}^2, \ldots, \overline{x}^d\} \quad = \quad \{\overline{y} \in \mathbf{Z}_p^* : \overline{y}^d = \overline{1}\}. \qquad (*)$$

L'insieme W degli elementi di $\overline{y} \in \mathbf{Z}_p^*$ che hanno ordine *uguale* a d, è contenuto nell'insieme (*). In particolare esso consiste in potenze di $\overline{x}$, e per il Lemma 2, precisamente nelle potenze $\overline{x}^i$ con $\mathrm{mcd}(i,d) = 1$. Quindi la cardinalità di W è $\varphi(d)$. D'altra parte, per definizione della funzione g, la cardinalità di W è anche uguale a $g(d)$, ossia $g(d) = \varphi(d)$ come affermato.

Attenzione: a questo punto dobbiamo ancora dimostrare che $g(p-1) \neq 0$ e che quindi $g(p-1) = \varphi(p-1) \neq 0$.
Scriviamo $\mathbf{Z}_p^*$ come unione disgiunta dei sottoinsiemi di elementi che hanno lo stesso ordine d. Abbiamo che

$$\sum_{d|p-1} g(d) = p - 1.$$

Per il Lemma 1 sappiamo che vale anche $\sum_{d|p-1} \varphi(d) = p-1$. Siccome $0 \leq g(d) \leq \varphi(d)$ per ogni d, abbiamo quindi uguaglianza per ogni d. In particolare, troviamo che

$$\#\{\overline{x} \in \mathbf{Z}_p^* : \mathrm{ord}_p(x) = p-1\} = \varphi(p-1).$$

Siccome questo numero è almeno 1, abbiamo dimostrato il teorema.

Criterio della radice primitiva. *Sia $\bar{x} \in \mathbf{Z}_p^*$, con p primo. Allora $\bar{x}$ è una radice primitiva in $\mathbf{Z}_p^*$ se e solo se $\bar{x}^{\frac{p-1}{d}} \not\equiv \bar{1} \mod p$, per ogni d divisore primo di $p-1$.*

Dim. Ricordiamo che per definizione l'ordine di un elemento $\bar{y} \in \mathbf{Z}_p^*$ è il *più piccolo* intero k per cui $\bar{y}^k \equiv \bar{1}$. Se l'ordine di $\bar{x}$ è $p-1$, allora certamente $\bar{x}^{\frac{p-1}{d}} \not\equiv \bar{1} \mod p$, per ogni divisore primo d di $p-1$.
Viceversa, se $\bar{x}^{\frac{p-1}{d}} \not\equiv \bar{1} \mod p$, per ogni divisore primo d di $p-1$, allora l'ordine di $\bar{x}$ è $p-1$. Infatti, se l'ordine di $\bar{x}$ fosse minore di $p-1$, sarebbe della forma $\frac{p-1}{m}$, per un intero m divisore di $p-1$ (l'ordine di un elemento $\bar{y} \in \mathbf{Z}_p^*$ divide l'ordine del gruppo $\mathbf{Z}_p^*$ che è appunto $p-1$). In particolare esiterebbe un divisore primo d di $p-1$ per cui $\bar{x}^{\frac{p-1}{d}} \equiv \bar{1} \mod p$:
se m fosse un divisore primo di $p-1$, avremmo già una contraddizione. Altrimenti, se fosse ad esempio $m = d_1 d_2$, con d_1, d_2 divisori primi di m, allora scrivendo $\frac{p-1}{d_1} = \frac{p-1}{d_1 d_2} d_2$, avremmo

$$\bar{x}^{\frac{p-1}{d_1}} = \bar{x}^{\frac{p-1}{d_1 d_2} d_2} = (\bar{x}^{\frac{p-1}{d_1 d_2}})^{d_2} = \bar{1}.$$

Assurdo.

Osservazione sulla Formula di Gauss. Nel corso della dimostrazione del teorema precedente abbiamo visto che se d è un divisore positivo di $p-1$, ci sono esattamente $\varphi(d)$ elementi di ordine d in $\mathbf{Z}_p^*$. Ad esempio ci sono $\varphi(1) = 1$ elementi di ordine uno e $\varphi(2) = 1$ elementi di ordine due, dati rispettivamente da $\bar{1}$ e $\overline{-1}$. In particolare in $\mathbf{Z}_p^*$ ci sono $\varphi(p-1)$ radici primitive, ossia elementi di ordine $p-1$. D'altra parte il teorema non ci dà alcun metodo per determinarne una. Per determinare una radice primitiva di $\mathbf{Z}_p^*$, si prende una classe a caso e si applica il criterio precedente (una volta fattorizzato $p-1$.....).

Definizione (Logaritmo discreto). Sia p un numero primo e sia $\bar{g}$ una radice primitiva in $\mathbf{Z}_p^*$. Sia $\bar{y} \in \mathbf{Z}_p^*$. Il *logaritmo discreto di $\bar{y}$ in base $\bar{g}$* è un intero m per cui vale

$$\bar{g}^m = \bar{y}.$$

Si indica con $m = \log_{\bar{g}} \bar{y}$ (o semplicemente con $m = \log \bar{y}$ se la base $\bar{g}$ è chiara dal contesto). Il logaritmo discreto $m = \log_{\bar{g}} \bar{y}$ è unico modulo $(p-1)$ (vedi Esercizio 4.a).

Esercizi.

1. Calcolare gli zeri del polinomio $x^2 - 1$ in $\mathbf{Z}_7$.
2. Calcolare gli zeri del polinomio $x^2 - 3$ in $\mathbf{Z}_7$.
3. Calcolare gli zeri del polinomio $x^2 - 1$ in $\mathbf{Z}_{pq}$, con p e q primi distinti. Ad esempio, calcolare gli zeri del polinomio $x^2 - 1$ in $\mathbf{Z}_{15}$.
4. Sia p un numero primo e sia $\bar{g}$ una radice primitiva in $\mathbf{Z}_p^*$.
   (a) Verificare che il logaritmo discreto in base $\bar{g}$ è ben definito modulo $p-1$, ossia $\bar{g}^i = \bar{g}^j$ se e solo se $i \equiv j \mod p-1$.
   (b) Verificare che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori (modulo $p-1$).
   (c) Verificare che $\log \overline{-1} = \frac{p-1}{2}$.

5. Sia p un numero primo e siano $\bar{g}$ e $\bar{g}'$ due radici primitive in $\mathbf{Z}_p^*$. Siano $\log_g$ il logaritmo in base g e $\log_{g'}$ il logaritmo in base g'. Verificare che esiste $c \in \mathbf{Z}$ tale che $\log_g \bar{a} = c \log_{g'} \bar{a}$, per ogni $\bar{a} \in \mathbf{Z}_p^*$.

Abbiamo visto che per ogni numero primo p il gruppo $\mathbf{Z}_p^*$ è ciclico. Cosa possiamo dire per $\mathbf{Z}_{p^k}^*$, con $k \geq 2$?

(1) Per $p > 2$ vale un analogo del teorema della radice primitiva.

Teorema 5. *Sia $p > 2$ un numero primo. Allora $\mathbf{Z}_{p^k}^*$ è ciclico per ogni $k \geq 1$.*

Dim.: Consideriamo l'omomorfismo di gruppi $\phi\colon \mathbf{Z}_{p^k}^* \to \mathbf{Z}_p^*$. Chiaramente ϕ è suriettivo ed il suo nucleo è dato dal sottogruppo $\{\bar{x} \in \mathbf{Z}_{p^k}^* \mid \bar{x} \equiv \bar{1} \bmod p\}$ di ordine p^{k-1}. Poiché $\gcd(p-1, p^{k-1}) = 1$, se mostriamo che quest'ultimo è un gruppo ciclico, ne segue che

$$\mathbf{Z}_{p^k}^* \cong \mathbf{Z}_p^* \times \{\bar{x} \in \mathbf{Z}_{p^k}^* \mid \bar{x} \equiv \bar{1} \bmod p\}$$

è un gruppo ciclico di ordine $(p-1)p^{k-1} = p^k - p^{k-1}$.

Concludiamo la dimostrazione del teorema, dimostrando che

• *Claim.* L'elemento $\overline{1+p}$ di $\{\bar{x} \in \mathbf{Z}_{p^k}^* \mid \bar{x} \equiv \bar{1} \bmod p\}$ ha ordine p^{k-1}.

Dim.: Definiamo $v_p(x-1) := a$ se a è il più piccolo intero positivo per cui $p^a \mid x-1$. In altre parole $x \equiv 1 \bmod p^a$ ed a è il più piccolo intero con questa prorietà. Mostriamo che

$$v_p(x-1) = a,\ a \geq 1 \quad \Rightarrow \quad v_p(x^p - 1) = a + 1. \tag{$*$}$$

Scriviamo $x = 1 + bp^a$, con $p \not| b$ e sviluppiamo

$$x^p - 1 = (1+bp^a)^p = \sum_{i=0}^{p} \binom{p}{i} b^i p^{ai} = 1 + bp^{a+1} \underbrace{\binom{p}{2} b^2 p^{a2} + \ldots + b^p p^{ap}}_{\equiv 0 \bmod\ p^{a+1}} - 1 \equiv bp^{a+1} \bmod p^{a+1}.$$

Poiché $p \not| b$, abbiamo che $v_p(x^p - 1) = a + 1$.

Applichiamo questo fatto all'elemento $x = 1 + p$:

$v_p(x-1) = 1$;

$v_p(x^p - 1) = 2$;

$v_p(x^{p^i} - 1) = i + 1$;

$\cdots \quad \cdots \quad \cdots$

$v_p(x^{p^{k-1}} - 1) = k$.

Questo dice precisamente che

$$x^{p^{k-1}} \equiv 1 \bmod p^k$$

e l'elemento $x = \overline{1+p}$ ha ordine esattamente p^{k-1}.

Esempio. Un generatore di $\mathbf{Z}_{3^4}$ è $\overline{1+3} = \bar{4}$.

Infatti:

3 divide 4-1

3^2 divide esattamente $4^3 - 1$

3^3 divide esattamente $4^{3^2} - 1$

3^4 divide esattamente $4^{3^3} - 1$

in altre parole

$$4^{3^3} \equiv 1 \bmod 3^4$$

e nessuna potenza inferiore di 4 è congrua a 1 modulo 3^4.

(2) Sia $p = 2$.
$\mathbf{Z}_2^* = \{\bar{1}\}$;
$\mathbf{Z}_4^* = \{\bar{1}, \bar{3}\} \cong \mathbf{Z}_2$ è un gruppo ciclico;
$\mathbf{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. La sua tabella moltiplicativa è data da

	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Da essa si vede che il gruppo $\mathbf{Z}_8^*$ non è ciclico: tutti gli elementi hanno ordine 2.
Ed infatti $\mathbf{Z}_8^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.
In generale $\mathbf{Z}_{2^k}^* \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{k-2}}^*$ e non è ciclico.
Sia $p = 2$.
Per poter ripetere l'argomento del teorema precedente, consideriamo l'omomorfismo di gruppi $\phi\colon \mathbf{Z}_{2^k}^* \to \mathbf{Z}_4^*$. Da ciò segue che

$$\mathbf{Z}_{2^k}^* \cong \mathbf{Z}_4^* \times \{\bar{x} \in \mathbf{Z}_{p^k}^* \mid \bar{x} \equiv \bar{1} \bmod 4\},$$

dove il secondo è un gruppo ciclico di ordine 2^{k-2}, generato da $\bar{1} + \bar{4} = \bar{5}$.

Osservazione. Dalla dimostrazione del teorema della radice primitiva si deduce anche che in $\mathbf{Z}_p^*$, gli elementi di ordine minore o uguale ad m, con m divisore di $p-1$, sono tutti e soli quelli della forma

$$\{\bar{x}^{\frac{p-1}{m}}, \quad \bar{x} \in \mathbf{Z}_p^*\}.$$

Inoltre

$$m = \sum_{d|m} \varphi(d).$$