Appunti di Aritmetica

http://poisson.dm.unipi.it/~daurizio/Aritmetica2010.pdf

Jacopo D'Aurizio
elianto84@gmail.com

11 Gennaio 2010

1 Divisori e numeri primi

Dati due numeri interi d ed n, diciamo che d è un divisore di n, in simboli $d|n$, se

$$\exists q \in \mathbb{Z} : \ q \cdot d = n.$$

Denotiamo con $d(n)$ la *funzione dei divisori*, definita come:

$$d(n) = |\{m \in \mathbb{N} : \ m|n\}|,$$

e diciamo che un numero naturale p è *primo* se ammette esattamente due divisori, ossia se verifica:

$$d(p) = 2.$$

Diciamo inoltre che due numeri naturali a e b sono *coprimi* se non ammettono divisori comuni all'infuori di 1, e denotiamo con $\mathcal{P}$ l'insieme dei numeri primi:

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\}.$$

Valgono i seguenti fatti:

- $\mathcal{P}$ è un insieme infinito;
- $p \in \mathcal{P}, p|(ab) \longrightarrow p|a \quad \text{o} \quad p|b$;
- $p_i \in \mathcal{P}, n = \prod_{i=1}^{\omega(n)} p_i^{\alpha_i} \longrightarrow d(n) = \prod_{i=1}^{\omega(n)}(\alpha_i + 1)$;
- a, b coprimi $\longrightarrow d(ab) = d(a) \cdot d(b)$;
- $\forall n \geq 2 \quad \exists p \in \mathcal{P} \cap (n, 2n)$;
- $\lim_{n\to\infty} \frac{\log(n)}{n} \cdot |\mathcal{P} \cap (1, n)| = 1$;
- Se a e b sono numeri naturali coprimi, $\mathcal{P} \cap (a + b\mathbb{N})$ è un insieme infinito.

2 Algoritmo di Euclide e lemma di Bézout

Dati due numeri interi a e b, il loro *massimo comun divisore* è definito come:

$$\gcd(a, b) = \max\{d \in \mathbb{N} : d|a, d|b\},$$

da cui a, b coprimi $\longleftrightarrow \gcd(a, b) = 1$.
Qual è un algoritmo efficiente per la determinazione del massimo comun divisore?
Chiaramente la complessità del calcolo è limitata da $\min(a, b)$ test di divisibilità, in quanto

$$\gcd(a, b) \leq \min(a, b),$$

ma è possibile essere più astuti, semplicemente considerando il seguente

Lemma 2.1.

$$a > b,\ d|a,\ d|b \longrightarrow d|(a-b).$$

Dimostrazione.

$$d|a \longrightarrow a = d \cdot a_1,$$
$$d|b \longrightarrow b = d \cdot b_1,$$
$$a - b = d \cdot (a_1 - b_1).$$

□

Nelle ipotesi del lemma si ha dunque:

$$\gcd(a,b) = \gcd(a-b,b) = \gcd(a \bmod b, b)$$

Osservazione che dà luogo all'algoritmo di Euclide:

$$\gcd(101,75) = \gcd(75,26) = \gcd(26,23) = \gcd(23,3) = \gcd(3,2) = 1,$$

tramite il quale è possibile calcolare il massimo comun divisore in tempo logaritmico.
Vale il seguente risultato:

Lemma 2.2 (Bézout)**.** *Comunque dati due numeri naturali a e b per cui si abbia* $\gcd(a,b) = 1$*, esistono due numeri naturali c e d che realizzano:*

$$\begin{cases} c \cdot a - d \cdot b &= 1 \\ c &< b \\ d &< a \end{cases}$$

Dimostrazione. Portiamo a termine l'algoritmo di Euclide per il calcolo del massimo comun divisore tenendo traccia dei quozienti parziali: quel che otteniamo è una scrittura del numero razionale $\frac{a}{b}$ in forma di frazione continua. Ad esempio:

$$\gcd(101,75) \overset{1}{=} \gcd(75,26) \overset{2}{=} \gcd(26,23) \overset{1}{=} \gcd(23,3) \overset{7}{=} \gcd(3,2) \overset{1}{=} \gcd(2,1) \overset{2}{=}$$

$$\frac{101}{75} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7 + \frac{1}{1 + \frac{1}{2}}}}} \doteq [1,2,1,7,1,2]$$

Tuttavia, se $\frac{x}{y}$ e $\frac{z}{w}$ sono convergenti successivi di una qualsiasi frazione continua, allora:

$$|x \cdot w - y \cdot z| = 1, \quad x < z, \quad y < w.$$

Nel nostro caso otteniamo, senza colpo ferire, una soluzione del sistema iniziale:

$$[1,2,1,7,1] = \frac{35}{26},$$

$$26 \cdot 101 - 35 \cdot 75 = 1;$$

e nel caso avessimo ottenuto una soluzione per $c \cdot a - d \cdot b = -1$ sarebbe stato sufficiente operare le sostituzioni $c \leftarrow (b-c), d \leftarrow (a-d)$. Notiamo inoltre che tutte le soluzioni (u,v) dell'equazione diofantea

$$u \cdot a - v \cdot b = 1$$

dipendono dalla soluzione fondamentale (c,d) attraverso le relazioni:

$$u = c + k \cdot b, \quad v = d + k \cdot a.$$

□

3 Nozioni fondamentali sui gruppi

Un *gruppo* è un insieme G dotato di un'operazione binaria associativa $\circ : G \times G \to G$, ove

- $\exists e \in G :\ \forall g \in G,\ e \circ g = g \circ e = g$;
- $\forall (g,h) \in G \times G,\ g \circ h \in G$;
- $\forall g \in G\ \exists h \in G :\ g \circ h = e$.

Un gruppo si dice *commutativo* (o *abeliano*) se tale è l'operazione $\circ$, ossia se

$$\forall (g,h) \in G \times G, \quad g \circ h = h \circ g.$$

L'*ordine* di un gruppo è la sua cardinalità; H si dice *sottogruppo* di G, in simboli $H \leq G$, se è al contempo un gruppo rispetto a $\circ$ e un sottoinsieme di G. Il sottogruppo generato da un elemento g, in simboli $< g >$, è dato da[1]:

$$< g >= \{\ldots, g^{-1} \circ g^{-1},\ g^{-1}, e,\ g,\ g \circ g,\ g \circ g \circ g, \ldots\}.$$

L'*ordine di un elemento* è l'ordine del sottogruppo generato, e un gruppo si dice *ciclico* se è generato da un certo elemento g, che in tal caso viene detto *generatore*. Uno strumento fondamentale nella teoria dei gruppi è il

Teorema 3.1 (Lagrange)**.** *Se G è un gruppo finito, l'ordine di ogni suo elemento divide l'ordine del gruppo:*

$$o(g) \mid o(G).$$

Dimostrazione. Osserviamo preliminarmente che $o(g)$ è finito, e che

$$g^a = g^b,\ a > b \ \longrightarrow\ g^{a-b} = e$$

garantisce che valga l'identità:

$$o(g) = \min\{n \in \mathbb{N} \setminus \{0\} :\ g^n = e\}.$$

Proviamo ora che $g^{o(G)} = e$. Nel caso di gruppi abeliani è sufficiente considerare che, fissato $g \in G$, la mappa

$$x \to x \circ g$$

manda iniettivamente G in se stesso, alché il prodotto degli elementi nell'immagine coincide con il prodotto degli elementi del dominio:

$$\prod_{h \in G} h = \prod_{h \in G} h \circ g = g^{o(G)} \prod_{h \in G} h$$

e la tesi segue immediatamente. A questo punto:

$$g^{o(g)} = e,\ g^{o(G)} = e\ \to g^{\gcd(o(g),o(G))} = e\ \to o(g) = \gcd(o(g), o(G))\ \to o(g) \mid o(G).$$

Nel caso di gruppi non abeliani è opportuno definire il concetto di *laterale sinistro*:

$$aH \doteq \{a \circ h : h \in H\}.$$

Per ogni elemento $a \in G$, il laterale $a < g >$ consta di $o(g)$ elementi; ogni elemento di G appartiene ad un laterale della suddetta forma (in particolare $h \in (hg^{-1}) < g >$) e, inoltre:

$$a \in b < g > \to a = b \circ g^m \to a < g >= b < g >;$$

segue che tutti i possibili laterali sinistri distinti della forma $a < g >$ partizionano G come insieme, e dunque:

$$o(g) \mid o(G)$$

come voluto. □

[1] Denotiamo con g^{-1} l'inverso di g, ossia l'unico $h \in G :\ h \circ g = e$.

Altri risultati notevoli sono i seguenti:

Teorema 3.2. *Se $H \leq G$, $o(H) \mid o(G)$.*

Dimostrazione. E' sufficiente partizionare G in laterali di H come già fatto per il Teorema di Lagrange. □

Teorema 3.3. *Ogni gruppo avente per ordine un numero primo è ciclico.*

Dimostrazione. Preso $g \in G$ diverso dall'elemento neutro, $o(g) = p$ per il Teorema di Lagrange, dunque $< g >= G$. □

Teorema 3.4 (Cauchy)**.** *Se G è un gruppo finito, per ogni primo p che divida l'ordine di G esiste un elemento $g \in G$ che realizza $o(g) = p$.*

Dimostrazione. Si proceda per induzione sull'ordine di G: se G ammette un sottogruppo H di ordine m, con $p|m$, allora la tesi è verificata banalmente. Viceversa, supponiamo che H sia un sottogruppo di G con ordine non multiplo di p. Se G è abeliano, l'insieme G/H dei laterali di H in G è un sottogruppo di G avente per ordine un multiplo di p, ed è nuovamente possibile ricorrere all'ipotesi induttiva. Nel caso G non sia abeliano, è necessario ricorrere alla formula delle classi, che riportiamo senza dimostrazione:

$$o(G) = o(Z(G)) + \sum_{C(a) \neq G} \frac{o(G)}{o(C(a))} \quad \begin{cases} Z(G) &= \{g \in G : \ \forall h \in G, g \circ h = h \circ g\} \leq G \\ C(a) &= \{g \in G : \ g \circ a = a \circ g\} \leq G \end{cases}$$

Se $p|o(G)$ e $p \nmid C(a)$, allora $p|o(Z(g))$, ma il *centro* $Z(g)$ è un gruppo abeliano, e ci siamo ricondotti al caso precedente. □

4 Gruppi notevoli e congruenze

Una *relazione di equivalenza* $\sim$ su un insieme A è una relazione

- riflessiva: $\forall a \in A, \ a \sim a$;
- simmetrica: $a \sim b \longrightarrow b \sim a$;
- transitiva: $a \sim b, b \sim c \longrightarrow a \sim c$.

Dato un insieme A e una relazione di equivalenza $\sim$ su di esso, l'*insieme quoziente* $A/_\sim$ è definito come:

$$A/_\sim \doteq \{[a] : a \in A\}.$$

Gli elementi dell'insieme quoziente sono detti *classi di equivalenza*:

$$[a] = \{b \in A : \ b \sim a\}.$$

Preso un numero naturale $m \geq 2$, consideriamo la relazione di equivalenza[2] $\equiv_m$ su $\mathbb{Z}$ definita come segue:

$$a \equiv_m b \ \longleftrightarrow m|(a - b);$$

l'insieme quoziente

$$\mathbb{Z}/_{\equiv_m} = \{[0], [1], \ldots, [m-1]\}$$

si denota usualmente con

$$\mathbb{Z}/_{m\mathbb{Z}},$$

inoltre la relazione[3] $a \equiv_m b$ si scrive più comunemente come

$$a \equiv b \pmod{m}$$

e le classi di equivalenza sono anche dette *classi residue modulo m*. Quello che ha rilevanza cruciale è che

$$(\mathbb{Z}/_{m\mathbb{Z}}, +)$$

è un gruppo ciclico (dunque abeliano) di ordine m, in quanto

[2] *Semel in vita*, è opportuno verificare che sia tale.
[3] "a e b hanno in medesimo resto nella divisione per m", ossia $(a - b) \in [0]$.

- l'usuale operazione di somma è *compatibile* con il passaggio al quoziente, ossia $x \in [y], z \in [w] \to (x+z) \in [y+w]$;
- la classe $[0] = [m]$ è elemento neutro;
- l'inverso della classe $[a]$ è la classe $[m-a]$;
- $[1]^k = [1] + [1] + \ldots + [1] = [k]$.

Se ora introduciamo la funzione *totient* di Eulero attraverso

$$\phi(n) = |\{1 \leq a < n : \ \gcd(a,n) = 1\}|$$

abbiamo che nel gruppo additivo $\mathbb{Z}/_{m\mathbb{Z}}$ vi sono esattamente $\phi(d)$ elementi di ordine d per ogni intero d che divida m, ordine del gruppo, da cui:

- $(\mathbb{Z}/_{m\mathbb{Z}}, +)$ ha esattamente $\phi(m)$ generatori;
- $\forall m \in \mathbb{N}, \ m = \sum_{d|m} \phi(d)$.

Analogamente, preso un numero naturale m, l'insieme dei numeri coprimi con m, quozientato rispetto alla relazione $\equiv_m$, si denota con

$$\mathbb{Z}/_{m\mathbb{Z}}{}^*$$

e tale insieme risulta un gruppo abeliano rispetto all'usuale prodotto, in quanto:

- il prodotto di due interi coprimi con m è coprimo con m (supposto infatti $d|m$ e $p|m|ab$ si ha $p|a$ o $p|b$, entrambe impossibili in quanto $p|a, p|m \to p|\gcd(a,m) = 1$) e tale condizione non muta sommando o sottraendo multipli di m;
- il prodotto è compatibile con $\equiv_m$ in quanto $(k_1 m + a) \cdot (k_2 m + b) = (k_1 k_2 m + a k_2 + b k_1) \cdot m + ab$ ed è dunque lecito scrivere $[a] \cdot [b] = [ab]$;
- la classe $[1]$ è elemento neutro per il prodotto;
- l'inverso della classe $[a]$ è rintracciabile attraverso l'algoritmo di Euclide: per il lemma di Bézout esistono infatti $k_1 < a$ e $k_2 < m$ per cui $k_1 \cdot m - k_2 \cdot a = -1$, e da tale identità si deduce $m|(k_2 a - 1)$, ossia $[k_2 a] = [1]$, ossia $[k_2] = [a]^{-1}$.

Nel caso in cui $m = p \in \mathcal{P}$ avvengono diversi fatti interessanti:

Lemma 4.1 (piccolo Teorema di Fermat)**.** $a^p \equiv a \pmod{p}$

Dimostrazione. $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è un gruppo di ordine $p-1$, dunque per il Teorema di Lagrange ogni intero a non divisibile per p realizza $a^{p-1} \equiv 1 \pmod{p}$. □

Lemma 4.2 (Wilson)**.** $n \in \mathcal{P} \leftrightarrow n|\left((n-1)! + 1\right)$

Dimostrazione. Supponiamo che un numero primo p divida propriamente n: in tal caso $p \leq n-1$ e dunque $p|(n-1)!$, da cui l'impossibilità di $p|n|\left((n-1)! + 1\right)$. Viceversa, consideriamo $\mathbb{Z}/_{p\mathbb{Z}}{}^*$: ogni classe $[a]$ è distinta dalla propria inversa, eccetto le classi $[1]$ e $[p-1]$, dunque

$$[(p-1)!] = [1] \cdot [2] \cdot \ldots \cdot [p-2] \cdot [p-1] = [1] \cdot [p-1]$$

$$(p-1)! \equiv -1 \pmod{p}$$

□

Lemma 4.3. *$\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è un gruppo ciclico.*

Dimostrazione. La tesi è semplice da provare nei casi $p = 2$ o $p = 3$ per diretta costruzione della tabella moltiplicativa, possiamo dunque supporre $p \geq 5$. Proviamo ora che in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ vi sono al più $\phi(d)$ elementi di ordine d per ogni numero naturale d che sia un divisore proprio dell'ordine del gruppo. Poiché possiamo dotare $\mathbb{Z}/_{\equiv_p}$ sia di struttura additiva che moltiplicativa, l'anello dei polinomi a coefficienti in $\mathbb{Z}/_{p\mathbb{Z}}$, che si denota con

$$\mathbb{F}_p[x]$$

eredita da $\mathbb{Z}[x]$, anello dei polinomi a coefficienti interi, la proprietà di essere *euclideo*:

$$\exists \partial : \mathbb{F}_p[x] \to \mathbb{N} \text{ tale che } \forall u, v \in \mathbb{Z}[x] \; \exists \, k, r \in \mathbb{Z}[x] : u - k \cdot v = r, \partial r < \partial v,$$

ove la funzione ∂ viene detta *grado*, e nel nostro caso coincide con l'usuale definizione di grado di un polinomio. Si ha in particolare che:

- $x^p - x \equiv \prod_{g \in \mathbb{Z}/_{p\mathbb{Z}}} (x - g) \pmod{p}$;
- per ogni elemento $u \in \mathbb{F}_p[x]$, il numero di radici in $\mathbb{Z}/_{p\mathbb{Z}}$ di u non supera il grado di u.

Proviamo ora che tutti gli elementi di ordine d in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, con d divisore proprio di $\phi(p) = p - 1$, sono radici di un elemento di $\mathbb{F}_p[x]$ di grado $\phi(d)$. Si ha infatti:

$$o(g) = d \longrightarrow g^d - 1 \equiv 0 \pmod{p} \text{ e } \forall q \neq d : q|d, \; g^q - 1 \not\equiv 0 \pmod{p}.$$

Tuttavia se u e v sono due elementi di un anello euclideo di polinomi, e le radici di u sono un sottoinsieme delle radici di v, allora u divide v, ossia esiste w tale che $v = u \cdot w$. Introduciamo ora la funzione di Möebius $\mu(n) : \mathbb{N} \to \{-1, 0, 1\}$:

$$\mu(1) = 1, \quad \forall p \in \mathcal{P} \; \mu(p) = -1 \text{ e } \forall n > 1 \; \mu(p^n) = 0, \quad \gcd(a, b) = 1 \to \mu(a \cdot b) = \mu(a) \cdot \mu(b).$$

Questa funzione gode di un'interessante proprietà:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{altrimenti} \end{cases},$$

dalla quale segue, per il principio di inclusione-esclusione, che ogni elemento di ordine d in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è radice del polinomio

$$p_d(x) = \frac{\prod_{q|d : \mu(q) = 1} (x^{d/q} - 1)}{\prod_{q|d : \mu(q) = -1} (x^{d/q} - 1)} \in \mathbb{F}_p[x].$$

Ora la funzione grado soddisfa $\partial(u \cdot v) = \partial u + \partial v$, dunque

$$\partial p_d = d \sum_{q|d} \frac{\mu(q)}{q},$$

ma è certamente lecito restringere la somma nel membro destro ai divisori di d della forma $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, in quanto la funzione di Möebius è nulla sugli interi che sono multipli di un quadrato di un primo. Segue:

$$d \sum_{q|d} \frac{\mu(q)}{q} = d \cdot \prod_{p \in \mathcal{P} : p|d} \left(1 - \frac{1}{p}\right) = \phi(d),$$

dunque in $G = \mathbb{Z}/_{p\mathbb{Z}}{}^*$ non possono esistere più di $\phi(d)$ elementi di ordine d. Ricordando ora che

$$o(G) = p - 1 = \sum_{d|(p-1)} \phi(d),$$

abbiamo che in G vi sono almeno $\phi(p - 1) > 1$ generatori, ed in realtà ve ne sono esattamente $\phi(p - 1)$, in quanto l'esistenza di un singolo generatore garantisce che in G vi siano esattamente $\phi(d)$ elementi di ordine d. In particolare:

$$o(g) = p - 1, \, \gcd(n, p - 1) = 1 \; \longrightarrow \; o(g^n) = p - 1.$$

□

Provata dunque l'esistenza di un generatore in ${\mathbb{Z}/_{p\mathbb{Z}}}^*$, ci chiediamo quale sia un algoritmo efficiente per determinarne esplicitamente uno. Al giorno d'oggi si ritiene che la scansione sequenziale delle classi $[2], [3], \ldots$ attraverso il criterio:

$$\forall q \in \mathcal{P} : q|(p-1) \quad g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \iff o(g) = p-1$$

sia la migliore strada perseguibile, in quanto Chen ha provato che, assumendo l'ipotesi di Riemann generalizzata, per p sufficientemente grande, esiste un generatore di ${\mathbb{Z}/_{p\mathbb{Z}}}^*$ entro le prime $2\log^2 p$ classi.

Rimuovendo ora l'ipotesi di primalità di m, resta il fatto che ${\mathbb{Z}/_{m\mathbb{Z}}}^*$ è un gruppo abeliano di ordine $\phi(m)$, da cui, come conseguenza del Teorema di Lagrange, il seguente

Lemma 4.4 (Eulero)**.**

$$m \nmid a \;\rightarrow\; a^{\phi(m)} \equiv 1 \pmod{m}.$$

E' inoltre interessante ricordare che:

Lemma 4.5. *Preso un numero naturale $m > 1$, nè pari nè divisibile per 5, la lunghezza del periodo dell'espressione decimale del numero $\frac{1}{m}$ è un divisore di $\phi(m)$, in particolare coincide con l'ordine della classe $[10]$ in ${\mathbb{Z}/_{m\mathbb{Z}}}^*$.*

Dimostrazione. Detta l la lunghezza del periodo si ha $m|(10^l - 1)$, ed anzi l è il minimo intero per cui ciò accade, da cui, immediatamente, la tesi. □

E' a questo punto lecito chiedersi se e quando ${\mathbb{Z}/_{m\mathbb{Z}}}^*$ sia un gruppo ciclico. Valgono i seguenti risultati:

Lemma 4.6. *${\mathbb{Z}/_{m\mathbb{Z}}}^*$ è un gruppo ciclico se e solo se $m = 2, 4, 2\,p^n$ o p^n per p primo dispari.*

Dimostrazione. Forniamo solo uno sketch della dimostrazione, rimandando ai riferimenti bibliografici per ulteriori delucidazioni. Se m è prodotto di due distinti primi dispari p e q, per ogni intero a coprimo con m si ha:

$$a^{p-1} \equiv 1 \pmod{p} \qquad a^{q-1} \equiv 1 \pmod{q}$$

dunque $a^{\gcd(p-1,q-1)} \equiv 1 \pmod{m}$ e il massimo ordine di un elemento di ${\mathbb{Z}/_{m\mathbb{Z}}}^*$ è al più metà dell'ordine del gruppo. I casi $m = 2$ ed $m = 4$ sono banali e il caso $m = 2\,p^n$ è sostanzialmente analogo al caso $m = p^n$, mentre nel caso $m = p^n$ si fa ricorso alla tecnica del *sollevamento henseliano*: un generatore per ${\mathbb{Z}/_{p^h\mathbb{Z}}}^*$ può essere traslato fino a ottenere un generatore di ${\mathbb{Z}/_{p^{h+1}\mathbb{Z}}}^*$.
Proviamo il passo base dell'induzione: sia g un generatore (ossia un elemento di ordine massimo) di ${\mathbb{Z}/_{p\mathbb{Z}}}^*$. Si ha:

$$\left|{\mathbb{Z}/_{p^2\mathbb{Z}}}^*\right| = \varphi(p^2) = p(p-1).$$

Per ogni numero primo q che divide $(p-1)$ si ha:

$$g^{\frac{p(p-1)}{q}} \not\equiv 1 \pmod{p^2},$$

in quanto:

$$g^{\frac{p(p-1)}{q}} \equiv g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

è un'identità assicurata dal fatto che g è generatore di ${\mathbb{Z}/_{p\mathbb{Z}}}^*$. Tale identità continua inoltre ad essere verificata rimpiazzando g con $g + kp$. Consideriamo allora $g^{(p-1)} \pmod{p^2}$: se questa quantità è diversa da 1, g è un generatore per ${\mathbb{Z}/_{p^2\mathbb{Z}}}^*$. In caso contrario, facendo ricorso al binomio di Newton, si ha:

$$(g+kp)^{p-1} \equiv g^{p-1} + kp(p-1)g^{p-2} \equiv 1 - p\,k\,g^{-1} \pmod{p^2}.$$

In tal caso, appena $k \not\equiv 0 \pmod{p}$, l'ultimo addendo del membro destro è non nullo, e ciò permette di concludere che $g + kp$ è un generatore di ${\mathbb{Z}/_{p^2\mathbb{Z}}}^*$. La tecnica del sollevamento henseliano permette inoltre di provare che: □

Lemma 4.7. *Preso $n \geq 3$, il massimo ordine di un elemento di ${\mathbb{Z}/_{2^n\mathbb{Z}}}^*$ è pari a 2^{n-2}, ossia a metà dell'ordine del gruppo; inoltre la classe $[5]$ ha esattamente tale ordine, ed ogni elemento di ${\mathbb{Z}/_{2^n\mathbb{Z}}}^*$ può essere espresso come $[\pm 5^k]$.*

Esaminiamo ora, attraverso alcuni esempi, delle proprietà generali delle *congruenze*, ossia delle identità che hanno luogo dall'applicazione della relazione $\equiv_m$. Consideriamo in primo luogo equazioni di primo grado della forma $a \cdot x + b \equiv 0 \pmod{m}$:

$$2 \cdot x + 15 \equiv -1 \pmod{101}.$$

Per compatibilità del prodotto e della somma con la relazione di equivalenza $\equiv_{101}$ è lecito scrivere:

$$[2] \cdot [x] + [15] = [100], \qquad [2] \cdot [x] = [85].$$

Poiché 101 è un numero primo, ogni classe distinta dalla classe [0] è invertibile (moltiplicativamente), da cui:

$$[x] = [85] \cdot [2]^{-1}.$$

Per ogni p primo dispari, l'inversa della classe [2] in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è la classe $\left[\frac{p+1}{2}\right]$, dunque:

$$[x] = [85] \cdot [51] = [4335] = [93] \qquad x \equiv 93 \pmod{101},$$

risultato a cui saremmo potuti pervenire in maniera più rapida attraverso:

$$[x] = [-16] \cdot [2]^{-1} = [-8] = [93].$$

Ma come trattare le congruenze lineari nel caso in cui appaiano classi non invertibili?
I due risultati che seguono sono fondamentali:

Lemma 4.8.

$$a \cdot x \equiv 0 \pmod{ab} \longleftrightarrow x \equiv 0 \pmod{b}.$$

Lemma 4.9. *Se* $\gcd(a, b) = 1$*, allora*

$$x \equiv m \pmod{ab} \longleftrightarrow \begin{cases} x \equiv m \pmod{a} \\ x \equiv m \pmod{b} \end{cases}$$

Consideriamo, ad esempio, l'equazione

$$6x \equiv -11 \pmod{70}.$$

La classe [6] non appartiene al gruppo $\mathbb{Z}/_{70\mathbb{Z}}{}^*$ in quanto $\gcd(6, 70) = 2 \neq 1$, tuttavia l'equazione risulta equivalente al sistema

$$\begin{cases} 6x + 11 \equiv 0 \pmod{2} \\ 6x + 11 \equiv 0 \pmod{35} \end{cases}$$

che è impossibile, visto che la prima equazione si riduce a $1 \equiv 0 \pmod{2}$.
In generale, un'equazione della forma

$$ax + b \equiv 0 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}$$

risulta equivalente ad un sistema di equazioni del tipo

$$ax + b \equiv 0 \pmod{p_i^{\alpha_i}}.$$

Se $p_i \nmid a$, la classe $[a]$ appartiene a $\mathbb{Z}/_{p_i^{\alpha_i}\mathbb{Z}}{}^*$, e si ha $x \equiv -b \cdot a^{-1} \pmod{p_i^{\alpha_i}}$. Se $p_i | a$ ma $p_i \nmid b$, l'equazione è impossibile; se $p_i | a$ e $p_i | b$ l'equazione è equivalente a

$$\frac{a}{p_i} \cdot x + \frac{b}{p_i} \equiv 0 \pmod{p_i^{\alpha_i - 1}};$$

resta da provare il seguente fatto:

Teorema 4.10 (Teorema cinese del resto)**.** *Se* $\forall i \neq j$ *si ha* $\gcd(m_i, m_j) = 1$*, il sistema*

$$\begin{cases} x & \equiv & a_1 & (\text{mod } m_1) \\ x & \equiv & a_2 & (\text{mod } m_2) \\ & \dots & & \\ x & \equiv & a_k & (\text{mod } m_k) \end{cases}$$

è equivalente ad un'unica equazione della forma

$$x \equiv a \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_k}.$$

Dimostrazione. Detto M il prodotto di tutti gli m_i, chiamiamo S_1 il sistema

$$S_1 : \begin{cases} x & \equiv & a_1 & (\text{mod } m_1) \\ x & \equiv & 0 & (\text{mod } M/m_1) \end{cases}$$

Dalla seconda equazione abbiamo $x = k_1 \cdot \frac{M}{m_1}$, e affinché una siffatta x soddisfi anche la prima equazione dev'essere

$$k_1 \equiv a_1 \cdot \left(\frac{M}{m_1}\right)^{-1} \pmod{m_1},$$

dove l'ipotesi di coprimalità degli m_i garantisce l'esistenza della classe inversa di $\left[\frac{M}{m_1}\right]$ in ${\mathbb{Z}/_{m_1\mathbb{Z}}}^*$, che per brevità denominiamo K_1. Abbiamo che tutte e sole le x che risolvono S_1 sono della forma

$$x \equiv a_1 K_1 \frac{M}{m_1} \pmod{M},$$

denominiamo dunque X_1 il più piccolo numero naturale congruo a $a_1 K_1 \frac{M}{m_1}$ modulo M, e procediamo analogamente per $X_2, X_3, \ldots, X_k$. Poiché

$$x \equiv 0 \pmod{M/m_i} \longrightarrow \forall j \neq i \quad x \equiv 0 \pmod{m_j},$$

il numero $a \doteq X_1 + X_2 + \ldots + X_k$ è soluzione del sistema iniziale, e tutte le soluzioni sono della forma $a + kM$, in quanto:

- $x \equiv a \,(\text{mod } M)$ implica $x \equiv a \,(\text{mod } m_i)$ per ogni i;
- $\forall j \neq i \; X_i \equiv 0 \,(\text{mod } m_j)$ e $X_i \equiv a_1 \,(\text{mod } m_i)$ garantiscono che, $\forall i$, $a \equiv a_i \,(\text{mod } m_i)$;
- se U e V sono due distinte soluzioni del sistema iniziale, $\forall i \quad U - V \equiv 0 \,(\text{mod } m_i)$, e dunque $M|(U - V)$.

□

Dal Teorema cinese del resto discende un importante risultato di struttura:

Lemma 4.11. *Se* $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$*, l'ordine moltiplicativo della classe* $[a]$ *in* ${\mathbb{Z}/_{m\mathbb{Z}}}^*$ *è pari al minimo comune multiplo di* $(n_1, \ldots, n_k)$*, dove* n_i *è l'ordine della classe* $[a]$ *in* ${\mathbb{Z}/_{p_i^{\alpha_i}\mathbb{Z}}}^*$*.*

4.1 Criteri di divisibilità

Muniti delle più importanti nozioni di teoria dei gruppi, analizziamo ora alcuni criteri di divisibilità. Assumendo che $a_1 a_2 \ldots a_{l(n)}$ sia la rappresentazione decimale del numero naturale

$$n = a_1 \cdot 10^{l(n)-1} + a_2 \cdot 10^{l(n)-2} + \ldots + 10 \cdot a_{l(n)-1} + a_{l(n)},$$

allora:

$$2|n \longleftrightarrow a_{l(n)} = 0, 2, 4, 6, 8 \qquad 3|n \longleftrightarrow 3\left|\left(\sum_{i=1}^{l(n)} a_i\right)\right.$$

$$4|n \longleftrightarrow 4\left|\left(2\, a_{l(n)-1} + a_{l(n)}\right)\right. \quad 5|n \longleftrightarrow a_{l(n)} = 0, 5 \qquad ,$$

$$9|n \longleftrightarrow 9\left|\left(\sum_{i=1}^{l(n)} a_i\right)\right. \qquad 11|n \longleftrightarrow 11\left|\left(\sum_{i=1}^{l(n)} (-1)^i\, a_i\right)\right.$$

in quanto:

- $n \equiv a_{l(n)} \pmod{10}$ implica $n \equiv a_{l(n)} \pmod{2}$ e $n \equiv a_{l(n)} \pmod{5}$;
- $10^k \equiv 1 \pmod{3}$ e $10^k \equiv 1 \pmod{3}$ implicano $n \equiv \sum_{i=1}^{l(n)} a_i \pmod{3}$ e $n \equiv \sum_{i=1}^{l(n)} a_i \pmod{9}$;
- $10^k \equiv (-1)^k \pmod{11}$ implica $n \equiv \pm \sum_{i=1}^{l(n)} (-1)^i a_i \pmod{11}$;
- $\forall j \geq k$, $10^k \equiv 0 \pmod{2^k}$ e $\pmod{5^k}$ implicano che 2^k (5^k) divide n se e solo se le ultime k cifre dell'espressione decimale di n costituiscono un multiplo di 2^k (5^k).

Notiamo inoltre che:

$$7|(10 \cdot a + b) \longrightarrow 7|(50 \cdot a + 5 \cdot b) \longrightarrow 7|(a - 2 \cdot b),$$

segue che n è un multiplo di 7 se e solo se lo è

$$\left\lfloor \frac{n}{10} \right\rfloor - 2 \cdot a_{l(n)},$$

e ciò costituisce un criterio di divisibilità per 7:

$$12334 \to 1225 \to 112 \to 7, \qquad 7 \,|\, 12334,$$

$$12345 \to 1224 \to 114 \to 3, \qquad 7 \nmid 12345.$$

Analogamente per il 13:

$$13|(10 \cdot a + b) \longrightarrow 13|(40 \cdot a + 4 \cdot b) \longrightarrow 13|(a + 4 \cdot b),$$

$$13 \,|\, n \longleftrightarrow 13 \,|\, \left(\left\lfloor \frac{n}{10} \right\rfloor + 4 \cdot a_{l(n)} \right)$$

$$12324 \to 1248 \to 156 \to 39, \qquad 13 \,|\, 12324,$$

$$12345 \to 1254 \to 141 \to 18 \qquad 13 \nmid 12345.$$

Per il 17 si ha:

$$17|(100 \cdot a + b) \longrightarrow 17|(1600 \cdot a + 16 \cdot b) \longrightarrow 13|(2 \cdot a - b),$$

$$17 \,|\, n \longleftrightarrow 17 \,|\, \left(2 \cdot \left\lfloor \frac{n}{100} \right\rfloor - a_{l(n)} \right)$$

$$12342 \to 204 \to 0, \qquad 17 \,|\, 12342,$$

$$12345 \to 201 \to 3 \qquad 17 \nmid 12345.$$

Per il 19 si ha:

$$19|(10 \cdot a + b) \longrightarrow 19|(20 \cdot a + 2 \cdot b) \longrightarrow 19|(a + 2 \cdot b),$$

$$19 \,|\, n \longleftrightarrow 19 \,|\, \left(\left\lfloor \frac{n}{10} \right\rfloor + 2 \cdot a_{l(n)} \right)$$

$$12331 \to 1235 \to 133 \to 19, \qquad 19 \,|\, 12331,$$

$$12345 \to 1244 \to 132 \to 17 \qquad 19 \nmid 12345.$$

Per il 23 si ha:

$$23|(10 \cdot a + b) \longrightarrow 23|(70 \cdot a + 7 \cdot b) \longrightarrow 23|(a + 7 \cdot b),$$

$$23 \,|\, n \longleftrightarrow 23 \,|\, \left(\left\lfloor \frac{n}{10} \right\rfloor + 7 \cdot a_{l(n)} \right)$$

$$12351 \to 1242 \to 138 \to 69 \qquad 23 \,|\, 12351,$$

$$12345 \to 1269 \to 189 \to 81 \qquad 23 \nmid 12345.$$

Lasciamo al lettore il compito di generalizzare quanto esposto ad altri primi e a basi differenti da quella decimale.

5 Residui quadratici

Dato un gruppo moltiplicativo e abeliano G, $g \in G$ si dice *residuo quadratico* se appartiene all'immagine dell'applicazione $f : G \to G$ definita da

$$f(g) = g \cdot g.$$

Tale applicazione è un *automorfismo* di G, ossia una mappa da G in G compatibile con l'operazione di gruppo:

$$f(g \cdot h) = f(g) \cdot f(h),$$

da cui segue che l'insieme dei residui quadratici è un sottogruppo di G:

$$Q \doteq \operatorname{Im} f \leq G.$$

Nel caso di gruppi di ordine dispari, Q coincide con G, in quanto:

$$o(g) = n \longrightarrow n | o(G), n \equiv 1 \pmod 2 \longrightarrow \left(g^{\frac{n+1}{2}}\right)^2 = g^n \cdot g = g \longrightarrow \forall g \in G, g \in \operatorname{Im} f.$$

Incidentalmente, ciò prova anche che in un gruppo di ordine pari ogni elemento di ordine dispari appartiene a Q. Nel caso di gruppi ciclici di ordine pari, preso un qualunque generatore g si ha

$$Q = < g^2 >,$$

in quanto ogni elemento di $< g^2 >$ appartiene all'immagine di f, $o(< g^2 >) = \frac{o(G)}{2}$, e se Q contenesse elementi distinti da quelli di $< g^2 >$, in quanto sottogruppo di G, dovrebbero coincidere con G, dunque contenere anche g, il che è assurdo, dato che il massimo ordine di un elemento di $< g^2 >$ è pari a $\frac{o(G)}{2}$. Tale fenomeno ha una conseguenza importante:

$$g, h \in (G \setminus Q) \longrightarrow g \cdot h \in Q,$$

nelle ipotesi, infatti, g e h risultano "potenze dispari" di un generatore, ragion per cui il loro prodotto è una "potenza pari", ossia un elemento di Q. A questo punto abbiamo un criterio potente per verificare l'appartenenza di una classe $[a]$ al sottogruppo dei residui quadratici in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, per p primo dispari:

$$[a] \in Q \longleftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Preso infatti un generatore g, se $[a] \in Q$ è della forma $[g^{2k}]$, e dunque $a^{\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1^k \pmod p$; in caso contrario si ha

$$a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

in quanto il termine centrale è distinto dalla classe $[1]$, poiché $[g^k] = [1]$ implica $(p-1)|k$, mentre il suo quadrato è esattamente la classe $[1]$. Da tale criterio segue un celebre fatto:

Lemma 5.1. $[-1]$ *è un residuo quadratico in* $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ *se e solo se* $p \equiv 1 \pmod 4$*: in tal caso il Teorema di Wilson garantisce che si abbia*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p.$$

Risultati analoghi si hanno per le classi $[2]$ e $[-3]$:

Lemma 5.2. $[2]$ *è un residuo quadratico in* $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ *se e solo se* $p \equiv \pm 1 \pmod 8$.

Dimostrazione.

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv 2 \cdot 4 \cdot \ldots \cdot p-1 \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)!.$$

□

Lemma 5.3. $[-3]$ *è un residuo quadratico in* $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ *se e solo se* $p \equiv 1 \pmod 3$.

Dimostrazione. Se $p \equiv 1 \pmod 3$, in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ esiste, per il Teorema di Cauchy, un elemento di ordine 3, che denominiamo ω. Si ha

$$\omega^2 + \omega + 1 \equiv 0 \pmod p,$$

in quando $[\omega] \neq [1]$ e $[\omega^3] = [1]$. Consideriamo allora $\omega - \omega^2$:

$$\left(\omega - \omega^2\right)^2 \equiv \omega^2 - 2\omega^3 + \omega^4 \equiv (\omega^2 + \omega + 1) - 3 \equiv -3 \pmod p.$$

Viceversa, supponiamo che in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, per $p \equiv 2 \pmod 3$, esista una classe $[q]$ che realizzi $[q^2] = [-3]$. Si ha:

$$\left[\frac{-1+q}{2}\right] \neq [1] \qquad \left(\frac{-1+q}{2}\right)^3 \equiv \frac{q^3 + 3q + 8}{8} \equiv 1 \pmod p,$$

da cui l'esistenza di un elemento di ordine 3, assurda poiché 3 non è un divisore dell'ordine del gruppo. □

Per la determinazione della radice quadrata di un residuo quadratico in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$ è possibile adoperare un algoritmo di *crivello*: se $[a]$ è residuo quadratico (ossia realizza $a^{\frac{p-1}{2}} \equiv 1 \pmod p$) esiste un numero naturale $b < p/2$ per cui vale $b^2 \equiv a \pmod p$, ovvero

$$b^2 = k \cdot p + a.$$

In tali ipotesi si ha $1 \leq k < p/4$, e la determinazione di k comporta la determinazione di b: chiediamoci dunque quale sia un metodo efficiente per identificare l'unico quadrato nella sequenza

$$m_j = j \cdot p + a, \qquad 1 \leq j < p/4.$$

Prendiamo a titolo di esempio il caso $p = 101, a = 5$. Se m_j è un quadrato, in particolare realizza:

$$m_j \not\equiv 2, 3, 5, 6, 7 \pmod 8,$$

che è come dire:

$$101 \cdot j \not\equiv -3, -2, 0, 1, 2 \pmod 8,$$

condizione a sua volta equivalente (previa moltiplicazione per l'inverso di $[101]$ in $\mathbb{Z}/_{8\mathbb{Z}}{}^*$) a:

$$j \not\equiv 0, 1, 2, 5, 6 \pmod 8.$$

Segue:

$$k \in \{3, 4, 7, 11, 12, 15, 19, 20, 23\}.$$

Inoltre:

$$m_k = b^2 \longrightarrow k \not\equiv 0 \pmod 3,$$

dunque

$$k \in \{4, 7, 11, 19, 20, 23\}.$$

Ed ancora:

$$m_k = b^2 \longrightarrow k \not\equiv 2, 3 \pmod 5,$$
$$k \in \{4, 11, 19, 20\},$$
$$m_k = b^2 \longrightarrow k \not\equiv 0, 4, 5 \pmod 7,$$
$$k \in \{20\},$$

per cui una radice quadrata della classe $[5]$ in $\mathbb{Z}/_{101\mathbb{Z}}{}^*$ è

$$[\sqrt{101 \cdot 20 + 5}] = [45]$$

e l'altra è la classe opposta, $[-45] = [56]$.
Certamente, se abbiamo necessità di generare tutti i $\frac{p-1}{2}$ residui quadratici in $\mathbb{Z}/_{p\mathbb{Z}}{}^*$, è sufficiente ricordare che:

$$Q = \left\{[1^2], [2^2], \ldots, \left[\left(\frac{p-1}{2}\right)^2\right]\right\},$$

in quanto:

$$a \neq b,\ p|(a^2 - b^2) \longrightarrow [a] = [b] \text{ o } [a] = [-b]$$

e il membro destro non può essere soddisfatto da due distinti elementi interi dell'intervallo $\left(0, \frac{p}{2}\right)$.
A questo punto il Teorema cinese del resto rientra prepotentemente nella discussione, comunicandoci, ad esempio, che:

- poiché i residui quadratici sono un sottogruppo, $[-6]$ è un residuo quadratico in ${\mathbb{Z}/_{p\mathbb{Z}}}^*$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$;
- se $n = a^2 + 6b^2$ è un intero libero da quadrati, ogni divisore primo di n è della forma $24k + 1$, $24k + 5, 24k + 7$ o $24k + 11$;
- se $\gcd(m, n) = 1$, la classe $[a]$ è un residuo quadratico in ${\mathbb{Z}/_{mn\mathbb{Z}}}^*$ se e solo se lo è sia in ${\mathbb{Z}/_{n\mathbb{Z}}}^*$ che in ${\mathbb{Z}/_{m\mathbb{Z}}}^*$.

Abbiamo a questo punto tutti gli strumenti necessari alla risoluzione di equazioni della forma

$$ax^2 + bx + c \equiv 0 \pmod{m}$$

meno che uno: un algoritmo per l'estrazione della radice quadrata in un gruppo moltiplicativo ciclico. Esistono due approcci, che pur avendo la medesima efficienza sono concettualmente molto diversi: il primo, dovuto a Cipolla e Lehmer, sfrutta le proprietà dell'automorfismo di Frobenius in campi finiti, riconducendo il problema a quello del calcolo di una potenza di una matrice; il secondo, dovuto a Daniel Shanks, è fondato sulle seguenti osservazioni:

- Se $p - 1 = 2^k \cdot q$ con q dispari, per ogni b che non sia un residuo quadratico in ${\mathbb{Z}/_{p\mathbb{Z}}}^*$, b^q risulta una radice primitiva 2^k-esima dell'unità;
- Per ogni residuo quadratico a, a meno di moltiplicare per un'opportuna radice 2^k-esima dell'unità, si ha che $a^{\frac{q+1}{2}}$ è radice quadrata di a.

Per i dettagli consigliamo nuovamente di consultare la bibliografia.
Introducendo ora il *simbolo di Legendre*:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{se} \quad [a] \text{ è residuo quadratico in } {\mathbb{Z}/_{p\mathbb{Z}}}^* \\ 0 & \text{se} \quad p|a \\ -1 & \text{se} \quad [a] \text{ non è residuo quadratico in } {\mathbb{Z}/_{p\mathbb{Z}}}^* \end{cases}$$

possiamo facilmente verificare che valgono le seguenti proprietà:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;
- $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$;
- Se $p \nmid q$, $\left(\frac{q^2}{p}\right) = 1$,

e formulare il *Teorema di Reciprocità Quadratica*:

Teorema 5.4 (Gauss)**.** *Se p e q sono primi dispari,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Stupefacente risultato, la cui dimostrazione esula certamente dallo scopo di queste dispense: nuovamente, rimandiamo alla bibliografia. Tornando, per modo di dire, con i piedi per terra, chiediamoci cosa si possa dire, più in generale, della mappa

$$f : G \to G, \qquad f(x) = x^q,$$

se q è un primo dispari e G è un gruppo moltiplicativo abeliano. Come prima, f risulta un automorfismo di G, dunque

$$\operatorname{Im} f \leq G,$$

inoltre

$$o(g) = qk \implies o(g^q) = k, \qquad q \nmid o(g) \implies o(g^q) = o(g),$$
$$q \nmid o(g) \implies \exists\, h \in < g >:\ g = h^q \implies g \in \operatorname{Im} f,$$

Si ha conseguentemente che, nei gruppi ciclici, l'ordine di $\operatorname{Im} f$ è esattamente pari a $\frac{o(G)}{q}$ oppure a $o(G)$ a seconda che $q|o(G)$ o $q \nmid o(G)$, rispettivamente. Nel caso in cui q divida $o(G)$ si ha inoltre:

$$g \in \operatorname{Im} f \iff g^{\frac{o(G)}{q}} = e,$$

in quanto, preso un generatore g, l'elemento $g^{\frac{o(G)}{q}}$ risulta radice primitiva q-esima dell'unità.

6 Gruppi di permutazioni

Se $\sigma : A \to A$ è una mappa biettiva su un insieme finito, è detta *permutazione*. Le permutazioni su un insieme di cardinalità n formano un gruppo (in generale non abeliano) rispetto alla composizione, usualmente denominato *gruppo simmetrico* su n elementi, in simboli S_n, di ordine $n!$. Sussistono due differenti notazioni per le permutazioni:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

$$\sigma = (a_1\ a_2\ \dots\ a_k),$$

dove con la seconda si intende che σ agisce su $\{a_1, a_2, \dots, a_k\}$ in modo ciclico (*è una permutazione ciclica*, o, più semplicemente, un *ciclo*):

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \dots\ \sigma(a_k) = a_1,$$

lasciando fissi gli elementi di $\{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_k\}$.
L'insieme dei punti fissi di una permutazione si denota con

$$\mathrm{Fix}(\sigma) = \{i : \sigma(i) = i\},$$

e due permutazioni σ_1, σ_2 si dicono *disgiunte* se

$$(\{1, 2, \dots, n\} \setminus \mathrm{Fix}(\sigma_1)) \cap (\{1, 2, \dots, n\} \setminus \mathrm{Fix}(\sigma_2)) = \emptyset.$$

Una permutazione di ordine 2, ossia un 2-ciclo, è detta *trasposizione*. Sussistono i seguenti fatti:

- permutazioni disgiunte commutano;
- ogni permutazione è prodotto di cicli disgiunti;
- ogni m-ciclo è prodotto di $(m-1)$ trasposizioni;
- l'ordine di un m-ciclo è m;

è dunque particolarmente semplice calcolare l'ordine di una permutazione; presa, ad esempio, $\sigma \in S_7$ della forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 3 & 7 & 5 \end{pmatrix},$$

si ha:

$$\sigma = (1\ 4\ 2)(3\ 6\ 7\ 5), \qquad o(\sigma) = \frac{3 \cdot 4}{\gcd(3,4)} = 12.$$

Inoltre, se una permutazione σ realizza:

$$\sigma = \tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_j = \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_k$$

con τ_x e ρ_y trasposizioni, allora $j - k$ è pari. Se infatti definiamo la *segnatura* (o *segno*) di una generica permutazione σ attraverso

$$s(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{|\sigma(i) - \sigma(j)|} = \pm 1$$

l'applicazione segno risulta un *omomorfismo*, ossia una mappa che realizza $s(\sigma_1 \cdot \sigma_2) = s(\sigma_1) \cdot s(\sigma_2)$: di conseguenza, il nucleo di tale applicazione

$$\ker s = \{\sigma \in S_n : s(\sigma) = 1\}$$

risulta un sottogruppo di S_n di ordine $\frac{n!}{2}$, detto gruppo *alterno* su n elementi, in simboli A_n.
Si noti che A_n, in generale, non coincide con l'insieme dei quadrati in S_n, per ragioni legate alle decomposizione di una permutazione in cicli disgiunti:

Lemma 6.1. *Se $\sigma = (1\ 2)(3\ 4\ 5\ 6) \in A_6$, non vi è alcun elemento ρ di A_6 per cui si abbia $\sigma = \rho^2$. Infatti il quadrato di un $2k$-ciclo è il prodotto di due k-cicli disgiunti, mentre il quadrato di un ciclo di ordine dispari è un ciclo del medesimo ordine: se fosse $\rho^2 = \sigma$ nella decomposizione in cicli di ρ dovrebbe far capolino un 8-ciclo, assurdo.*

Lemma 6.2. *Se $\sigma_1 = (1\ 4\ 2\ 5\ 3\ 6), \sigma_2 = (1\ 5\ 2\ 6\ 3\ 4), \sigma_3 = (1\ 6\ 2\ 4\ 3\ 5)$ si ha:*

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = (1\ 2\ 3)(4\ 5\ 6).$$

Lemma 6.3. *Se $\sigma \in A_n$ ed L_m è il numero di m-cicli che compaiono nella decomposizione di σ,*

$$\exists \rho \in S_n : \ \sigma = \rho^2 \quad \leftrightarrow \quad \forall k, \ \ L_{2k} \equiv 0 \pmod 2.$$

Se ora chiamiamo *isomorfismo* un omomorfismo iniettivo tra due gruppi finiti di pari cardinalità, abbiamo:

Teorema 6.4 (Cayley)**.** *Ogni gruppo finito G è isomorfo ad un sottogruppo di $S_{o(G)}$.*

Dimostrazione. E' sufficiente associare ad ogni $g \in G$ la permutazione σ_g definita attraverso $\sigma_g(h) = h \cdot g$; si ha:

$$\sigma_g \cdot \sigma_h = \sigma_{h \cdot g} \qquad (\sigma_g)^{-1} = \sigma_{g^{-1}}.$$

□

7 Esercizi

1. Si determini il più piccolo numero naturale non nullo avente esattamente 12 divisori;
2. Si provi che la cifra delle decine di un numero naturale della forma 3^k è sempre pari;
3. Si determinino tutte le soluzioni naturali dell'equazione $\phi(n) = 12$;
4. Si dica per quali numeri interi a il rapporto tra $a^2 + 30a$ e $3a + 2$ è un numero intero;
5. Sia A un insieme con un numero finito di elementi, munito di un'operazione binaria associativa $\circ : A \times A \to A$ per cui valga la legge di cancellazione $a \circ b = a \circ c \longrightarrow b = c$. Si provi che $(A, \circ)$ è un gruppo.
6. Si studi il comportamento dei coefficienti binomiali modulo un primo p
   e se ne deduca il *Teorema di Lucas*;
7. Dal punto precedente si deduca una dimostrazione alternativa del piccolo Teorema di Fermat;
8. Si determini il massimo comun divisore degli infiniti elementi non nulli dell'insieme
   $\{n^3 - 2n^2 + 2n - 2 : n \in \mathbb{N}\}$;
9. Si provi che, per ogni numero naturale m, 3^{m+1} divide $7^{3^m} - 1$;
10. Si provi che non esistono cubi di interi che differiscono di 7004, nè di 35020;
11. Si provi che la somma di tre quadrati consecutivi non è mai un quadrato;
12. Si provi che l'insieme dei residui quadratici in ${\mathbb{Z}/_{2^n\mathbb{Z}}}^*$, per $n \geq 3$, è il sottogruppo generato dalla classe [25];
13. Si provi che esistono infiniti numeri naturali n tali che $\forall (a, b, c) \in \mathbb{N}^3, \ n \neq a^2 + b^2 + c^2$;
14. Si provi che ogni primo p per cui si abbia $p \equiv 1 \pmod 4$ può essere espresso come somma di due quadrati di interi in modo sostanzialmente univoco; si provi inoltre che, nonostante ciò, non tutti gli interi della forma $4k + 1$ possono essere espressi come somma di due quadrati;
15. Si determinino le ultime due cifre nell'espressione decimale di 2^{2010};

16. Si provi che ogni successione di interi $\{a_i\}_{i\in\mathbb{N}}$ definita attraverso

$$a_{n+k} = b_1 \cdot a_{n+k-1} + b_2 \cdot a_{n+k-2} + \ldots + b_k \cdot a_n,$$

con ogni b_j intero, è periodica modulo m per ogni numero naturale m; se ne deduca l'esistenza di numeri di Fibonacci la cui espressione decimale termina con una quantità arbitraria di zeri;

17. Si determini qual è la massima potenza di un primo p che divide $n!$;

18. Si provi o si smentisca l'esistenza di una coppia di numeri primi (p, q) per cui si abbia $5|(2^p+3^q+2)$;

19. Si provi che un polinomio a coefficienti interi che realizza $p(a) = p(b) = p(c) = p(d) = 11$ per quattro distinti interi (a, b, c, d) non può assumere il valore 8 su alcun intero;

20. Si provi che la somma delle k-esime potenze dei primi m numeri naturali è un polinomio di k+1-esimo grado in m i cui coefficienti possono essere dedotti attraverso l'*interpolazione di Lagrange*;

21. Si provi che per qualunque intero k la funzione aritmetica

$$\sigma_k(n) = \sum_{d|n} d^k$$

è moltiplicativa, ossia realizza $\gcd(a, b) = 1 \ \rightarrow \ \sigma_k(a \cdot b) = \sigma_k(a) \cdot \sigma_k(b)$;

22. Si provi che l'insieme dei numeri naturali che sono somma di due quadrati è un semigruppo (ossia un gruppo a meno dell'esistenza degli inversi) rispetto al prodotto, e che tale risultato vale anche per le somme di quattro quadrati, ma non di tre;

23. Si provi che, se l'equazione $x^2 - Dy^2 = -1$, con $D \in \mathbb{N} \setminus \{0, 1\}$, ha una soluzione $(x, y) \in \mathbb{N}^2$, allora ne ha infinite;

24. Si provi che, se l'equazione $Ax^2+By^2 = z^2$, con $(A, B) \in \mathbb{N}_0^2$, è risolta da una terna (x, y, z) di numeri naturali mutuamente coprimi, allora è risolta da infinite terne aventi le medesime caratteristiche;

25. Si provi che, contrariamente a quanto sostenuto da alcuni manuali di disegno tecnico, il lato dell'ettagono regolare inscritto in una circonferenza non è pari a metà del lato del triangolo equilatero inscritto nella medesima;

26. Si provi che esiste un unico numero razionale q con la proprietà che sia $q^2 + 5$ che $q^2 - 5$ risultano quadrati di numeri razionali (*problema di Fibonacci*);

27. (*Teorema di Erdös-Ginzburg-Ziv*) Si provi che tra $2n - 1$ distinti numeri naturali è sempre possibile sceglierne n la cui somma risulti multipla di n;

28. (*Problema 6 Cesenatico 2007*) Data la successione

$$\begin{cases} x_1 &= 2 \\ x_{n+1} &= 2\,x_n^2 - 1 \end{cases}$$

si provi per ogni numero naturale $n > 1$ si ha $\gcd(n, x_n) = 1$;

29. Definito l'n-esimo numero armonico H_n come $H_n = \sum_{m=1}^{n} \frac{1}{m}$, si provi che, se p è un numero primo maggiore o uguale a 5, allora p^2 divide il numeratore di H_{p-1};

30. Si provi che S_7 ammette un sottogruppo di ordine 12 non isomorfo [4] ad alcun sottogruppo di S_n per $n < 7$.

[4] Un *isomorfismo* di gruppi è un omomorfismo suriettivo.

Riferimenti bibliografici

[1] Elementary Number Theory, A Computational Approach, William Stein,
`http://modular.math.washington.edu/edu/2007/spring/ent/ent-html/ent-html.html`;

[2] Elementary Theory of Numbers, 2nd ed., W. Sierpinski,
PWN-Polish Scientific Publishers, North-Holland, 1988;

[3] Algebra, I.N. Hernstein,
Editori Riuniti, Roma, 1999;

[4] Pell's Equations $X^2 - mY^2 = -1, -4$ and Continued Fractions, P. Kaplan, K.S. Williams,
Journal Of Number Theory, Volume 23 (1986) 169-182;

[5] A remark on the computation of square roots in finite fields, N.Nishihara et alia,
`http://eprint.iacr.org/2009/457.ps`;

[6] Efficient Finite Fields in the Maxima C.A.S., F.Caruso, J.D'Aurizio, A.McAndrew,
Lecture Notes in Computer Science Volume 5130,62-76, Springer Verlag 2008;

[7] Lecture notes on elementary group theory, W.Miller,
`http://ima.umn.edu/~miller/sgatach1.pdf`;

[8] Primes of the form $x^2 + n\,y^2$, D.A.Cox,
John Wiley and Sons, 1997,
Esercizi presso `http://www.math.ucsb.edu/~stopple/BQF.exercises.pdf`;