Esercizi di Aritmetica

Alessandro Beraducci

Versione del 21 Dicembre 2010

1 Induzione

Esercizio 1. Consideriamo un percorso automobilistico circolare. Per compiere un giro occorrono cento litri di benzina. Lungo il percorso si trovano un certo numero di taniche di benzina che cumulativamente contengono cento litri. Non sappiamo però quanta benzina contenga ciascuna tanica, e dove esse siano disposte. Dimostrate che esiste un punto del percorso a partire dal quale, a serbatoio inizialmente vuoto, si riesce a completare il giro.

Esercizio 2. Togliamo una casella d'angolo da una scacchiera di $2^n \times 2^n$ caselle. Dimostrare che è possibile ricoprire la parte rimanente con tessere a forma di L che ricoprono 3 caselle ciascuna.

Esercizio 3. Calcolate la somma di tutti i numeri dispari compresi nell'intervallo tra 1000 e 2000.

Esercizio 4. Dimostrare che, per ogni $n \in \mathbb{N}$ e per ogni numero reale $x > -1$ vale

$$(1+x)^n \geq 1 + nx$$

Come applicazione si consideri il problema seguente. Da un fagiolo magico germoglia una piantina alta un centimetro, che ogni giorno cresce di 1/30 della sua altezza. Dimostrare che dopo un anno la piantina avrà superato i 40 metri di altezza.

Esercizio 5. Sia f_n il numero delle stringhe binarie di lunghezza n che non contengono mai due 1 consecutivi. Si dimostri che $f_{n+2} = f_{n+1} + f_n$ e che per ogni n sufficientemente grande $f_n \geq n^2$.

Esercizio 6. Si dimostri che $\Sigma_{i=1}^{2^n} 1/i \geq 1 - n/2$.

2 Calcolo combinatorio

Esercizio 7. Quante sono le possibili mani di full a Poker ? Quanti colori? Coppie? Doppie coppie?

Esercizio 8. Quante sono le soluzioni intere non negative di $x + y + z = k$? Generalizzate con n variabili.

Esercizio 9. Quanti sono gli anagrammi della parola SUCCESSO? Ovvero quante stringhe di simboli si possono formare con tre S due C una U una E e una O?

Esercizio 10. Quante sono le funzioni surgettive da un insieme di m elementi ad un insieme di n elementi? Caso speciale $m = 5, n = 3$ e caso generale.

Esercizio 11. Quanti sono in modi di disporre i numeri da uno a 64 su una scacchiera in modo che su ogni riga ci siano 4 numeri dispari?

Esercizio 12. Dimostrare che $\Sigma_{i=1}^{n} i\binom{n}{i} = n2^{n-1}$.

Soluzione: $i\binom{n}{i}$ conta il numero di modi di scegliere una coppia (t, R) dove R è un sottoinsieme di i elementi presi da $\{1, \ldots, n\}$ e $t \in R$. Ponendo $S = R \setminus \{t\}$ si vede che questo è la stessa cosa che scegliere una coppia (t, S) dove $t \in \{1, \ldots, n\}$ (n possibilità) ed S è un sottoinsieme di $i - 1$ elementi presi dai rimanenti $n - 1$ elementi ($\binom{n-1}{i-1}$ possibilità). Abbiamo così dimostrato che

$$i\binom{n}{i} = n\binom{n-1}{i-1},$$

come si può anche verificare scrivendo i coefficienti binomiali in termini di fattoriali e semplificando. Il primo termine dell'uguaglianza da dimostrare diventa $\Sigma_{i=1}^{n} n\binom{n-1}{i-1}$, che può essere riscritto come $\Sigma_{j=0}^{n-1} n\binom{n-1}{j} = n(\Sigma_{j=0}^{n-1}\binom{n-1}{j})$. Applicando la formula del binomio di Newton, $\Sigma_{j=0}^{n-1}\binom{n-1}{j}$ diventa $(1 + 1)^{n-1} = 2^{n-1}$, da cui la tesi. Una seconda dimostrazione che non usa il binomio di Newton consiste nell'osservare che $n2^{n-1}$ conta il numero dei modi di scegliere una coppia (t, S) dove $t \in \{1, \ldots, n\}$ ed S è un sottoinsieme dei rimanenti $n-1$ elementi di $\{1, \ldots, n\}$. Distinguendo i vari casi a seconda del numero di elementi di S riotteniamo la sommatoria $\Sigma_{j=0}^{n-1} n\binom{n-1}{j}$. □

Esercizio 13. Quante sono le terne di numeri interi (x, y, z) tali che si possa formare un triangolo di perimetro 100 i cui lati abbiano lunghezza x, y, z?

Soluzione: Il problema equivale a contare le terne (x, y, z) con $x + y + z = 100$ e $x, y, z < 50$. Passando al complementare dobbiamo sottrarre dal totale delle terne con $x + y + z = 100$, che sappiamo essere $\binom{100+2}{2}$, quelle in cui $x \geq 50$ o $y \geq 50$ o $z \geq 50$. Se $x \geq 50$ possiamo scrivere $x = 50 + x'$, quindi il numero delle terne con $x \geq 50$ è uguale al numero delle soluzioni di $x' + y + z = 50$, ovvero $\binom{50+2}{2}$. Similmente ci sono $\binom{50+2}{2}$ terne con $y \geq 50$, e altrettante con $z \geq 50$. Sottraendo otteniamo $\binom{100+2}{2} - 3\binom{50+2}{2}$, che però ancora non è il risultato giusto in quanto abbiamo contato due volte le tre terne $(50, 50, 0)$, $(50, 0, 50)$ e $(0, 50, 50)$ corrispondenti al caso in cui due variabili sono ≥ 50. In base al principio di inclusione-esclusione, la soluzione è dunque $\binom{100+2}{2} - 3\binom{50+2}{2} + 3$. □

3 Algoritmo di Euclide, teorema di Bezout

Notazioni: scriviamo (a, b) oppure $MCD(a, b)$ per indicare il massimo comun divisore di a e b. Diamo alcuni richiami di teoria.

Algoritmo di Euclide: Il massimo comun divisore (a, b) di due numeri interi $a, b \in \mathbb{Z}$ si può ottenere riconducendosi a numeri sempre più piccoli usando l'equazione $(a, b) = (a, b - a)$. Per applicazione ripetuta di questa regola ne segue che

$$(a, b) = (a, b - ka),$$

ovvero il massimo comun divisore non cambia sottrando ad uno dei due numeri un multiplo dell'altro. In particolare, ricordando che il resto r della divisione euclidea di a per b si può scrivere nella forma $r = b - ka$ (per un certo k), otteniamo

$$(a, b) = (a, r)$$

Visto inoltre che $(a, b) = (b, a)$, valgono le analoghe equazioni a ruoli scambiati di a e b, ovvero: $(a, b) = (a - b, b) = (a - kb, b)$.

Teorema di Bezout: Il massimo comun divisore (a, b) si può ottenere come combinazione lineare di a e b.

Esercizio 14. Calcolare $(252, 198)$ e trovare x, y interi tali che $(252, 198) = 252x + 198y$.

Soluzione: Per prima cosa calcoliamo $(252, 198)$ usando l'algoritmo di Euclide.

$$\begin{gathered} 252 = 198 \cdot 1 + 54 \\ 198 = 54 \cdot 3 + 36 \\ 54 = 36 \cdot 1 + 18 \\ 36 = 18 \cdot 2 + 0 \end{gathered}$$

Dunque $(252, 198) = (198, 54) = (54, 36) = (36, 18) = 18$. Mostriamo ora come ottenere tutti questi numeri ome combinazioni lineari di 252 e 198:

$$\begin{array}{rcccccc} & & 252 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{0} \\ & & 198 & = & 252 \cdot \boxed{0} & + & 198 \cdot \boxed{1} \\ 252 - 198 & = & 54 & = & 252 \cdot \boxed{1} & + & 198 \cdot \boxed{(-1)} \\ 198 - 54 \cdot 3 & = & 36 & = & 252 \cdot \boxed{(-3)} & + & 198 \cdot \boxed{4} \\ 54 - 36 & = & 18 & = & 252 \cdot \boxed{4} & + & 198 \cdot \boxed{(-5)} \end{array}$$

Nella colonna centrale abbiamo scritto (dall'alto) 252, 198 e poi i resti ottenuti con l'algoritmo di Euclide. Di ognuno di questi numeri, nella colonna di destra è indicato come si può ottenere come combinazione di 252 e 198. Per passare dalla combinazione della terza riga a quella della quarta, visto che $36 = 198 - 54 \cdot 3$, abbiamo sommato la combinazione della seconda riga a quella della terza moltiplicata per -3. Similmente nei passaggi successivi ogni riga si ottiene dalle due precedenti sottraendo dalla prima un multiplo della seconda. Il risultato finale si legge dall'ultima riga ed è $x = 4, y = -5$. □

Richiami di teoria: i numeri che si possono ottenre come combinazioni lineari di a e b sono tutti e soli i multipli di (a, b).

Esercizio 15. Trovare tutte le soluzioni intere dell'equazione $54 = 252x + 198y$.

Soluzione: L'equazione ha soluzione in quanto $18 = (252, 198)$ divide 54. Dividendo tutto per 18 otteniamo l'equazione equivalente

$$3 = 14x + 11y.$$

Avendo diviso per il MCD per questa nuova equazione abbiamo $(14, 11) = 1$. Per il teorema di Bezout possiamo trovare x', y' tali che $1 = 14x' + 11y'$. Applicando l'algoritmo di Euclide si trova $x' = 4, y' = -5$. Moltiplicando per 3 si trova la soluzione particolare $x = 12, y = -15$. Le altre soluzioni si ottengono sommando alla soluzione particolare $(12, -15)$ le soluzioni (u, v) dell'equazione omogenea associata

$$0 = 14u + 11v,$$

ovvero le coppie della forma $(u, v) = (11k, -14k)$. Le soluzioni sono dunque $x = 12 + 11k, y = -15 - 14k$ al variare di $k \in \mathbb{Z}$. □

Esercizio 16. La successione di Fibonacci è definita da $f_0 = 1, f_1 = 1, f_{n+2} = f_{n+1} + f_n$. Si dimostri che per ogni n $(f_{n+1}, f_n) = 1$.

Soluzione: Abbiamo $(f_{n+2}, f_{n+1}) = (f_{n+1} + f_n, f_{n+1}) = (f_n, f_{n+1}) = (f_{n+1}, f_n)$, dove al primo passaggio abbiamo usato la definizione di f_{n+2}, e al secondo passaggio la regola secondo cui il massimo comun divisore di due interi non cambia sottrando ad uno dei due numeri un multiplo dell'altro. Ragionando per induzione otteniamo, per ogni n, $(f_{n+1}, f_n) = (f_1, f_0) = (1, 1) = 1$. □

4 Numeri primi

Esercizio 17. Si dimostri che in $\mathbb{N}$ esistono infiniti primi.

Soluzione: Siano $p_1, \ldots, p_n$ numeri primi. Basta mostrare che esiste un primo diverso da questi. Sia $a = p_1 \cdot \ldots \cdot p_n + 1$. Si noti che ciascun p_i non divide a perché il resto della divisione di a per p_i è 1. D'altra parte sappiamo anche che a deve avere un divisore primo q, che pertanto è diverso da ciascuno dei primi $p_1, \ldots, p_n$. □

Esercizio 18. Si dimostri che se $2^n - 1$ è primo, anche n è primo. Non si sa se esistono infiniti numeri primi della forma $2^n - 1$ (primi di Mersenne).

Soluzione: Supponiamo che $n = ab$ con $a, b \neq 1$. Ponendo $x = 2^a$ nell'identità $x^b - 1 = (x - 1)(x^{b-1} + x^{d-2} + \ldots + 1)$, e osservando che $(2^a)^b = 2^{(ab)}$, otteniamo una scomposizione di $2^{ab} - 1$. □

Esercizio 19. Si dimostri che se $2^c + 1$ è primo, allora c è una potenza di 2.

Soluzione: In caso contrario c ha un divisore dispari. Possiamo allora scrivere $c = k(2m+1)$ con $m > 0$. Usando l'identità

$$(b^{2m+1} + 1) = (b+1)(1 - b + b^2 - \ldots + b^{2m})$$

con $b = 2^k$ otteniamo la scomposizione $(2^c + 1) = (2^k + 1)(1 - 2^k + 2^{2k} - \ldots + 2^{2mk})$ e quindi $2^c + 1$ non è primo. □

In base all'esercizio tra i numeri della forma $2^c + 1$, gli unici candidati ad essere primi sono quelli della forma $F_n = 2^{2^n} + 1$. Tuttavia non tutti i numeri di questa forma sono primi, ad esempio si può mostrare che F_5 è composto. Il seguente esercizio illustra alcune proprietà degli F_n.

Esercizio 20. (Numeri di Fermat) Sia $F_n = 2^{2^n} + 1$. Si dimostri:

1. Se $n < m$, $F_n | F_m - 2$.
2. $(F_n, F_m) = 1$ per $n \neq m$.

Soluzione: (1) Sia $n < m$. Dobbiamo mostrare che $2^{2^n} + 1 | 2^{2^m} - 1$. Consideriamo d'apprima il caso $m = n + 1$. Applicando l'identità $x^2 - 1 = (x+1)(x-1)$ con $x = 2^{2^n}$ otteniamo

$$2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 = (2^{2^n} - 1)(2^{2^n} + 1).$$

La tesi desiderata si riduce ad osservare che il secondo fattore $2^{2^n} + 1$ di questo prodotto divide il termine di sinistra $2^{2^{n+1}} - 1$. Il caso generale è per induzione su m, partendo dal caso base $m = n + 1$ che abbiamo appena visto. Avendo già disposto del caso base possiamo assumere $m > n + 1$. Usando ancora una volta l'identità precedente con un cambiamento degli indici otteniamo

$$2^{2^m} - 1 = (2^{2^{m-1}})^2 - 1 = (2^{2^{m-1}} - 1)(2^{2^{m-1}} + 1).$$

Per ipotesti induttiva $2^{2^n} + 1$ divide il primo fattore $2^{2^{m-1}} - 1$ dell'equazione. Questo a sua volta in base all'equazione divide $2^{2^m} - 1$, da cui la tesi.

(2) Se un primo p divide F_n ed F_m, per la (1) p deve dividere 2, e quindi $p = 2$. D'altra parte 2 non divide F_n (F_n è dispari). □

5 Proprietà del massimo comun divisore e del minimo comune multiplo

Notazioni: Scriviamo $\mathbb{Z}\,a$ per l'insieme $\{na : n \in \mathbb{Z}\}$ dei multipli di a, e scriviamo $\mathbb{Z}\,a + \mathbb{Z}\,b$ per l'insieme $\{ma + nb : m, n \in \mathbb{Z}\}$ delle combinazioni lineari di a e b.

Per il teorema di Bezout sappiamo che $\mathbb{Z}(a,b) = \mathbb{Z}\,a + \mathbb{Z}\,b$, ovvero le combinazioni lineari di a e b sono esattamente i multipli del massimo comun divisore (a,b).

Il massimo comun divisore (a,b) e il minimo comune multiplo $[a,b]$ si calcolano facilmente conoscendo la scomposizione in primi degli interi a e b. Tuttavia in molti casi è possibile risolvere problemi riguardanti l'MCD e il MCM senza usare la scomposizione in primi, ma usando invece l'algoritmo di Bezout. Diamo un esempio:

Esercizio 21. Dati $m, x, y \in \mathbb{Z}$ con $m > 0$, si dimostri che $(mx, my) = m(x,y)$.

Soluzione: Per il teorema di Bezout $\mathbb{Z}(mx, my) = \mathbb{Z}\,mx + \mathbb{Z}\,my$. Portando fuori m, il secondo termine dell'uguaglianza coincide con $m(\mathbb{Z}\,x + \mathbb{Z}\,y)$ (i numeri della forma mk con $k \in \mathbb{Z}\,x + \mathbb{Z}\,y$), che a sua volta coincide con $m(\mathbb{Z}(x,y))$, che riportando dentro il fattore m è uguale a $\mathbb{Z}\,m(x,y)$. Otteniamo così $\mathbb{Z}(mx,my) = \mathbb{Z}\,m(x,y)$, ovvero (mx,my) e $m(x,y)$ hanno gli stessi multipli. Concludiamo osservando che due numeri positivi con gli stessi multipli devono coincidere. □

Esercizio 22. Si dia una seconda dimostrazione dell'esercizio precedente usando la scomposizione in primi.

Esercizio 23. È sempre vero che $(a,b)(c,d) = (ac,bd)$ per $a,b,c \in \mathbb{Z}$?

Soluzione: No: $(2,3)(3,5) = 1$, ma $(2\cdot 3, 3\cdot 5) = 3$. □

Esercizio 24. Dati $x, y \in \mathbb{Z}$, $(x^2, y^2) = (x,y)^2$.

Soluzione: Dato un primo p, basta mostrare che esso compare con lo stesso esponente in entrambi i membri dell'uguaglianza. In effetti se p compare con esponente a in x, e con esponente b in y, esso compare con esponente $2a$ in x^2, $2b$ in y^2, e $\min\{2a, 2b\}$ in (x^2, y^2). Facendo il conto per $(x,y)^2$ si trova $2\min\{a,b\}$, che è la stessa cosa. □

Esercizio 25. Siano $a, b, n \in \mathbb{Z}$ tali che $(a,b) = 1$, $a|n$ e $b|n$. Si mostri che $ab|n$.

Soluzione: Per Bezout esistono $x, y \in \mathbb{Z}$ con $1 = ax + by$. Quindi $n = anx + bny$. Da $b|n$ segue $ab|an$. Da $a|n$ seque $ab|bn$. Quindi ab divide sia an che bn, e pertanto divide anche la combinazione lineare $anx + bny$, che è uguale ad n. □

Esercizio 26. Dati $x, y, z \in \mathbb{Z}$, $(x, [y,z]) = [(x,y),(x,z)]$. Similmente $[x,(y,z)] = ([x,y],[x,z])$.

Soluzione: Usiamo l'esistenza e l'unicità della scomposizione in primi. Dimostriamo la prima uguaglianza. Basta var vedere che ciascun primo compare con lo stesso esponente in entrambi i membri dell'uguaglianza. Indichiamo che $v_p(x)$ l'esponente con cui il primo p compare nella fattorizzazione di x. Sappiamo che $v_p((x,y)) = \min\{v_p(x), v_p(y)\}$, e $v_p([x,y]) = \max\{v_p(x), v_p(y)\}$. Quindi basta dimostrare che

$$\min\{a, \max\{b,c\}\} = \max\{\min\{a,b\}, \min\{a,c\}\}.$$

Se $a \leq b, c$ entrambi i termini sono $= a$. Se $b \leq c, a$ il primo termine diventa $\min\{a, c\}$, e il secondo $\max\{b, \min\{a, c\}\}$, che a sua volta è uguale a $\min\{a, c\}$ essendo $b \leq \min\{c, a\}$. L'ultimo caso da analizzare è quello in cui $c \leq a, b$ che si tratta come il precedente scambiando i ruoli di b e c. Per l'uguaglianza $[x, (y, z)] = ([x, y], [x, z])$ procediamo in modo simile usando il fatto che

$$\max\{a, \min\{b, c\}\} = \min\{\max\{a, b\}, \max\{a, c\}\}$$

(che si dimostra come prima scambiando $\leq$ con $\geq$, e min con max). □

Esercizio 27. È sempre vero che $(xy, z) = (x, z)(y, z)$?

Soluzione: In generale no, ad esempio $(6 \cdot 15, 3) = 3$, ma $(6, 3)(15, 3) = 9$. □

Esercizio 28. Si dimostri che $(xy, z) = (x, z)(y, z)$ se x, y sono coprimi.

Soluzione: Il minimo comune multiplo $[a, b]$ di due numeri coprimi coincide con il prodotto ab dei due numeri. Ora se x, y sono coprimi lo sono ovviamente anche (x, z) ed (y, z) (perché?). Quindi sotto l'ipotesi di coprimalità possiamo sostituire $[,]$ al posto del prodotto e ci siamo ricondotti a dimostrare che $([x, y], z) = [(x, z), (y, z)]$. Questo segue dall'Esercizio 26. □

L'esercizio precedente consente di semplificare il calcolo di (a, z) qualora si conosca una fattorizzazione $a = xy$ con $(x, y) = 1$.

6 Prove di divisibilità

Utilizzando il linguaggio delle congruenze possiamo in molti casi calcolare il resto della divisione euclidea senza effettuare la divisione. I prossimi esempi illustrano il caso in cui il divisore è $3, 9, 11, 4, 7$ e in particolare ci fanno ottenere dei criteri di divisibilità per tali numeri.

Ricordiamo che quando scriviamo un numero, ad esempio 1234567, implicitamente sottintendiamo che esso è scritto in base 10, ovvero:

$$1234567 = 1 \cdot 10^6 + 2 \cdot 10^5 + 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 6 \cdot 10 + 7$$

Esercizio 29. Trovare il resto della divisione di 1234564 per 3 e per 9.

Soluzione: Siccome $10 \equiv 1 \bmod 3$, nel fare le congruenze modulo 3 possiamo sostituire 10 con 1 nell'espansione decimale ottenendo: $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 1 \bmod 3$. Quindi il resto è 1. Se avessimo cercato il resto della divisione di 1234564 per 9, avremmo anche in questo caso sostituito il 10 con 1 ottenendo $1234564 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 4 \equiv 7 \bmod 9$. □

Esercizio 30. Trovare il resto della divisione di 1234567 per 11.

Soluzione: Siccome $10 \equiv -1 \bmod (11)$, nel fare le congruenze modulo 11 possiamo sostituire 10 con -1 nell'espansione decimale ottenendo: $1234567 \equiv 1-2+3-4+5-6+7 \equiv 4$. Quindi il resto è 4. □

Esercizio 31. Trovare il resto della divisione di 1234567 per 4.

Soluzione: Osserviamo che $100 = 25 \cdot 4 \equiv 0 \bmod (4)$. Quindi $1234567 = 12345 \cdot 100 + 67 \equiv 67 \equiv 3 \bmod (4)$. □

Esercizio 32. Trovare il resto della divisione di 1234567 per 7.

Soluzione: Osserviamo che $1000 = 7 \cdot 143 - 1 \equiv -1 \bmod (7)$. Quindi $1234567 = 1 \cdot 1000^2 + 234 \cdot 1000 + 567 \equiv 1 - 234 + 567 \equiv 334 \equiv 5 \bmod 7$. □

In generale nel calcolare il resto della divisione di n per 7 si può spezzare l'espansione decimale n in gruppi di tre cifre (il che equivale a scrivere n in base 1000) sommandoli con segni alterni (ovvero sostituendo 1000^k con $(-1)^k$) e prendendo il resto del risultato modulo 7.

Esercizio 33. Si dimostri che $\sqrt{1234567}$ non è un intero.

Soluzione: Per assurdo supponiamo che vi sia un intero x tale che $x^2 = 1234567$. Abbiamo precedentemente visto che $1234567 \equiv 3 \bmod 4$. Quindi basta mostrare che x^2 non può essere congruente a 3 modulo 4. Siccome x è congruo a $0, 1, 2$ o 3 modulo 4, ci sono solo quattro verifiche da fare:

$$\begin{aligned} 0^2 &\equiv 0 \bmod 4 \\ 1^2 &\equiv 1 \bmod 4 \\ 2^2 &\equiv 0 \bmod 4 \\ 3^2 &\equiv 1 \bmod 4 \end{aligned}$$

□

6.1 Tornei all'italiana (da sistemare)

Esercizio 34. n squadre di calcio, numerate con gli interi da 0 ad $n-1$, si incontrano per un torneo all'italiana. Se n è dispari il calendario è organizzato come segue. Le squadre $x, y \in \{0, \ldots, n-1\}$ si incontrano nella giornata numero r, dove r è il resto di $x + y$ diviso n. (Ad esempio se $n = 5$ le squadre 3 e 4 si incontrano nel giorno $r = 2$.)

1. Dimostrate che con queste regole, per n dispari, ogni giorno c'è esattamente una squadra che riposa.

2. Trovate una regola per organizzare il calendario quando n è pari, facendo in modo che in ogni giornata nessuma squadra riposi. Come mai non funziona la regola di prima?

Soluzione: Caso n dispari. Sia $n = 2m + 1$. In base alle regole date la squadra x riposa nel giorno r se e solo se $x + x \equiv r \bmod (2m + 1)$ (x non più giocare con se stessa!). Se r è pari scriviamo $r = 2s$ e sostituendo otteniamo $2x \equiv 2s \bmod (2m+1)$. Visto che 2 è invertibile modulo $2m + 1$ dividendo otteniamo $x \equiv s \bmod (2m + 1)$. Quindi l'unica squadra che riposa nel giorno $r = 2s$ è la squadra $x = s$. Se invece r è dispari, scriviamo $r = 2s + 1$, e osserviamo che x riposa nel giorno r se e solo se $2x \equiv 2s + 1 \bmod (2m + 1)$. Ma $1 \equiv 2m + 2 \bmod (2m + 1)$. Sostituendo otteniamo $2x \equiv 2s + 2m + 2 \bmod (2m + 1)$. Visto che 2 è invertibile modulo $2m + 1$ dividendo otteniamo $x \equiv s+m+1 \bmod (2m+1)$. Quindi l'unica squadra che riposa nel giorno $r = 2s + 1$, è data dal resto di $s + m + 1$ modulo $2m + 1$.

Caso n pari. Facciamo giocare le prime $n-1$ squadre (da 0 ad $n-2$) seguendo il calendario precedente per $n-1$ squadre (lo possiamo fare visto che $n-1$ è dispari). Rimane da stabilire con chi gioca l'ultima squadra (la numero $n-1$). Visto che nel calendario per un numero dispari di squadre ogni giorno c'è una squadra che riposa, possiamo far giocare la squadra $n-1$ con quella che avrebbe riposato. □

6.2 Teorema cinese dei resti

Esercizio 35. Dati $a_1, a_2, m_1, m_2 \in \mathbb{Z}$, il sistema

$$\begin{cases} x \equiv a_1 & (m_1) \\ x \equiv a_2 & (m_2) \end{cases}$$

è risolubile se e solo se $a_1 \equiv a_2 \bmod (m_1, m_2)$. (In particolare è sempre risolubile se m_1 ed m_2 sono coprimi.) Data una soluzione particolare x_0, le altre si ottengono aggiungendo ad x_0 un multiplo di $[m_1, m_2]$.

Soluzione: Sia $x = x_0$ una soluzione del sistema. Osserviamo che se due numeri sono congrui modulo m, lo sono anche modulo un divisore di m. Quindi x_0 è congruo sia ad a_1 che ad a_2 modulo (m_1, m_2), e pertanto a_1 ed a_2 sono congrui tra loro modulo (m_1, m_2). Viceversa supponiamo che $a_1 \equiv a_2 \bmod (m_1, m_2)$. Ne segue che $a_1 - a_2$ è divisibile per (m_1, m_2) e per il teorema di Bezout possiamo scrivere $a_1 - a_2 = z_1 m_1 - z_2 m_2$ con $z_1, z_2 \in \mathbb{Z}$. Ponendo $x_0 := a_1 - z_1 m_1 = a_2 - z_2 m_2$ otteniamo una soluzione del sistema. Data una soluzione x_0 del sistema, le altre soluzioni devono verificare

$$\begin{cases} x \equiv x_0 & (m_1) \\ x \equiv x_0 & (m_2) \end{cases}$$

che equivale a $x \equiv x_0 \bmod [m_1, m_2]$. □

Esercizio 36. Trovare le soluzioni $x \in \mathbb{Z}$ del sistema

$$\begin{cases} 2x \equiv 14 & (15) \\ 3x \equiv 6 & (35) \end{cases}$$

Soluzione: Siccome 2 è invertibile modulo 15 e 3 è invertibile modulo 35, dividendo ottengo il sistema equivalente:

$$\begin{array}{rcll} x & \equiv & 7 & (15) \\ x & \equiv & 2 & (35) \end{array}$$

Il sistema ha soluzione in quanto 7 e 2 sono congrui modulo $5 = (15, 35)$. Per il teorema di Bezout possiamo scrivere $7 - 2 = z_1 15 - z_2 35$. Applicando l'algoritmo di Euclide (o procedendo "ad occhio") otteniamo $z_1 = -2, z_2 = -1$. Ponendo $x_0 = 7 - z_1 15 = 2 - z_2 35 = 37$ otteniamo una soluzione del sistema. Le altre si ottengono sommando ad x_0 un multiplo di $[15, 35] = 3 \cdot 5 \cdot 7$. □

Esercizio 37. Trovare le soluzioni $x \in \mathbb{Z}$ del sistema

$$\begin{cases} 200x & \equiv & 1400 & (1500) \\ 30x & \equiv & 60 & (350) \end{cases}$$

Soluzione: Dividendo tutto per 100 (incluso il modulo) nella prima equazione, e dividendo tutto per 10 nella seconda, ci riconduciamo all'esercizio precedente. □

Diamo ora una forma del teorema cinese dei resti con un numero arbitrario di congruenze.

Teorema 38. *(Teorema cinese dei resti) Siano $a_0, a_1, \ldots, a_n$ numeri a due a due relativamente primi. Siano $b_0, b_1, \ldots, b_n$ numeri arbitrari. Allora esiste un numero x che per ogni $i \leq n$:*

$x \equiv b_i \pmod{a_i}$

(Il numero x è univocamente determinato modulo il prodotto degli a_i.)

Proof. Assumiamo dapprima che uno dei b_i sia 1 e tutti gli altri siano 0. Dato $i \leq n$ cerchiamo dunque un x_i tale che

$x_i \equiv 1 \pmod{a_i}$

$x_i \equiv 0 \pmod{a_j}$ $\forall j \neq i$.

Poichè a_i e $\Pi_{j \neq i} a_j$ sono relativamente primi, per il teorema di Bezout esistono α, β tali che $\alpha \cdot a_i + \beta \cdot \Pi_{j \neq i} a_j = 1$. Basta ora porre $x_i = \beta \cdot \Pi_{j \neq i} a_j$. Per risolvere il sistema originale basta scegliere $x = b_0 x_0 + b_1 x_1 + \ldots + b_n x_n$ (verificate!). □

7 Periodo e antiperiodo di una frazione (da sistemare)

Esercizio 39. Sia m/n una frazione. Allora possiamo scrivere m/n nella forma $A/2^a 5^b + B/n'$ con $(n', 10) = 1$.

Soluzione: Scriviamo $n = 2^a 5^b n'$ con $(n', 10) = 1$. Basta ora scegliere $A, B \in \mathbb{Z}$ tali che $m = An' + B 2^a 5^b$. Questo è possibile per il teorema di Bezout dato che $(n', 2^a 5^b) = 1$. □

Esercizio 40. Sia m/n una frazione. Allora possiamo scrivere m/n nella forma $m'/10^l n'$ dove $l \geq 0$, $(n', 10) = 1$, e 10 non divide m'.

Soluzione: Possiamo supporre che m/n sia ridotta ai minimi termini. Scomponiamo il denominatore n nella forma $n = 2^a 5^b n'$ con $(n', 10) = 1$. Moltiplicando numeratore e denominatore per un'opportuna potenze di 2 o di 5 possiamo scrivere $m/n = m'/10^l n'$ dove $l = \max\{a, b\}$, $(n', 10) = 1$ e 10 non divide m'. Ad esempio se $a \leq b$, $m/n = m2^{b-a}/n2^{b-a} = m2^{b-a}/10^b n'$. Se 10 dividesse $m' = m2^{b-a}$, allora 5 dividerebbe m, contraddicendo il fatto che m/n fosse ridotta ai minimi termini. □

Esercizio 41. Siano $a, n \in \mathbb{Z}$ coprimi. Allora esiste $t \in \mathbb{N}$ tale che $a^t \equiv 1 \bmod n$.

Soluzione: Consideriamo i resti di a^t modulo n. Siccome ci sono solo n possibilià per i resti, prima o poi si devono ripetere, ovvero esistono $s, t \in \mathbb{N}$ con $t > 0$ tali che $a^s \equiv a^{s+t} \bmod n$. Poiché $(a, n) = 1$, anche $(a^s, n) = 1$, e quindi a^s è invertibile modulo n. Dividendo entrambi i membri della congruenza per l'inverso di a^s modulo n otteniamo $1 \equiv a^t \bmod n$. □

Dati due interi m, n, lo sviluppo decimale di m/n è finito (a meno degli zeri finali), o termina con un "periodo", ovvero un gruppo di cifre che si ripetono indefinitamente. Ad esempio $1/84 = 0, 01\overline{190476}$ dove la barra indica il periodo che si ripete e 01 è l'antiperiodo.

Esercizio 42. (Periodo e antiperiodo di una frazione) Data una frazione razionale vogliamo calcolarne la lunghezza del periodo e dell'antiperiodo. Usando l'Esercizio 40 possiamo scrivere la frazioen nella forma $m/10^l n$ dove $l \geq 0$, $(n, 10) = 1$, e 10 non divide m. Si dimostri:

1. (Caso $n \neq 1$) Se $n \neq 1$, $m/10^l n$ ha un antiperiodo di lunghezza l seguito da un periodo di lunghezza t, dove t è il minimo intero positivo tale che $10^t \equiv 1 \bmod n$. In particolare il periodo e l'antiperiodo dipendono solo dal denominatore.

2. (Caso $n = 1$) La frazione $m/10^l$ ha uno sviluppo decimale finito di lunghezza l con l'ultima cifra diversa da zero (assumendo che 10 non divida m).

Soluzione: Il punto (2) è ovvio. Dimostriamo il punto (1). Consideriamo prima il caso $l = 0$. Abbiamo quindi una frazione m/n con $(n, 10) = 1$. Dall'Esercizio 41 segue che esiste t tale che $10^t \equiv 1 \bmod n'$. Fissato un tale t, possiamo scrivere $nk = 10^t - 1$ per un certo k. Abbiamo allora $m/n = mk/nk = a/(10^t - 1)$ dove $a = mk$. Ci siamo dunque ricondotti a trattare il caso di frazioni della forma $a/(10^t - 1)$. Osserviamo che $1/(10^t - 1) = \Sigma_{i=1}^{\infty} 1/(10^t)^i = 0, \overline{0 \ldots 01}$ ha un periodo di lunghezza l (con il primo 1 al t-esimo posto dopo la virgola). Lo sviluppo di $a/(10^t - 1)$ si ottiene moltiplicando per a. È facile fare i conti se $0 \leq a < 10^t - 1$ perché in questo caso non ci sono "riporti". (Ad esempio sapendo che $1/10^2 - 1 = 1/99 = 0, \overline{01}$, ne segue che $64/99 = 0, \overline{64}$.) Possiamo ricondurci al caso facile rimpiazzando a con il

resto r della divisione di a per $10^t - 1$. Infatti $r/(10^t - 1)$ differisce da $a/(10^t - 1)$ per un numero intero, e quindi ha lo stesso periodo e antiperiodo. Abbiamo così dimostrato che se $10^t \equiv 1 \bmod n$, m/n ha uno sviluppo con un periodo di lunghezza t (senza antiperiodo). Il minimo t che verifica la congruenza è quindi la lunghezza del periodo minimo. (Ad esempio $0, \overline{123}$ può anche essere scritto nella forma $0, \overline{123123}$, ma il periodo minimo è di lunghezza 3 non 6.)

Consideriamo ora il caso generale $m/10^l n$. Per il caso $l = 0$ sappiamo che m/n ha periodo la cui lunghezza è il minimo t tale che $10^t \equiv 1 \bmod n$. Moltiplicando per $1/10^l$ spostiamo la virgola di l passi, creando un antiperiodo, sequito da un perido di lunghezza t. (Una seconda deduzione del caso generale dal caso $l = 0$ si basa sull'esercizio 39.) □

8 Inversi modulo n

Per definizione $x \in \mathbb{Z}$ è invertibile modulo n se e solo se esiste $y \in \mathbb{Z}$ tale che $xy \equiv 1 \bmod n$.

Esercizio 43. x è invertibile modulo n se e solo se $(x, n) = 1$.

Soluzione: Se $(x, n) = 1$ per Bezout troviamo $a, b \in \mathbb{Z}$ con $ax + bn = 1$. Riducendo questa equazione modulo n ne seque che a è un inverso di x modulo n. Viceversa se x è invertibile modulo n, esiste per definizione un $a \in \mathbb{Z}$ con $ax \equiv 1 \bmod n$. In base alla definizione delle congruenze questo significa che esiste $b \in \mathbb{Z}$ con $ax + bn = 1$, da cui discende $(x, n) = 1$ (un eventuale fattore comune di a, b deve dividere $ax + bn$, e quindi divide 1). □

9 Funzione di Eulero

Sia $\phi(n)$ la cardinalità dell'insieme dei numeri interi x coprimi con n e compresi nell'intervallo da 0 ad $n - 1$. Equivalentemente, in base all'Esercizio 43, $\phi(n)$ è la cardinalità degli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$. Ad esempio $\phi(12) = 4$ in quanto gli elementi invertibili di $\mathbb{Z}/12\mathbb{Z}$ sono le classi di $1, 5, 7, 11$.

Esercizio 44. Se p è primo, $\phi(p^n) = p^n - p^{n-1}$.

Soluzione: $\phi(p^n)$ conta il numero degli elementi invertibili di $\mathbb{Z}/p^n\mathbb{Z}$. In totale $\mathbb{Z}/p^n\mathbb{Z}$ ha p^n elementi, e di questi ve ne sono esattamente p^{n-1} che non sono invertibili (i multipli di p). □

Il seguente esercizio sarà risolto in seguito utilizzando i gruppi, ma esistono anche dimostrazioni dirette.

Esercizio 45. Se $(x, y) = 1$, $\phi(xy) = \phi(x)\phi(y)$.

Gli esercizi precedenti ci consentono di calcolare $\phi(n)$ conoscendo la scomposizione in primi di n. Ad esempio $\phi(3^4 5^7) = \phi(3^4)\phi(5^7) = (3^4 - 3^3)(5^7 - 5^6)$.

Esercizio 46. $\Sigma_{d|n}\phi(d) = \Sigma_{d|n}\phi(n/d) = n$.

Soluzione: La prima uguaglianza è ovvia: la seconda somma è uguale alla prima scritta in ordine inverso. Dimostriamo $\Sigma_{d|n}\phi(n/d) = n$. Sia X_d l'insieme degli interi x tra 1 ed n con $(x, n) = d$. Chiaramente $n = \Sigma_{d|n}\,\mathrm{Card}(X_d)$ in quanto l'insieme degli interi tra 1 ed n è l'unione disgiunta degli X_d al variare di d tra i divisori di n. Per finire basta mostrare che $\mathrm{Card}(X_d) = \phi(n/d)$. Per definizione $\phi(n/d)$ è la cardinalità dell'insieme Y_d costituito dagli interi y compresi tra 1 ed n/d con $(y, n/d) = 1$. Abbiamo: $(y, n/d) = 1$ se e solo se $d(y, n/d) = d$ se e solo se $(yd, n) = d$ (valendo in generale $m(u, v) = (mu, mv)$ per $m > 0$). Ne segue che la funzione che manda $x \in X_d$ in $y = xd$ è una bigezione tra X_d ed Y_d, da cui la tesi. □

10 Congruenze esponenziali

Esercizio 47. È possibile definire x^y negli interi modulo n?

Esercizio 48. Siano $a, n \in \mathbb{Z}$ coprimi. Allora $a^{\phi(n)} \equiv 1 \bmod n$.

Soluzione: Sappiamo che $(\mathbb{Z}/n\,\mathbb{Z})^*$ ha $\phi(n)$ elementi. Possiamo dunque scrivere $(\mathbb{Z}/n\,\mathbb{Z})^* = \{a_1, \ldots, a_{\phi(n)}\}$, dove ciascun a_i è una classe resto modulo m. Sia $b = \Pi_{i=1}^{\phi(n)} a_i \in (\mathbb{Z}/n\,\mathbb{Z})^*$. Fissato $g \in (\mathbb{Z}/n\,\mathbb{Z})^*$, il prodotto $\Pi_{i=1}^{\phi(n)} g a_i$ coincide con $g^{\phi(n)} b$. D'altra parte l'insieme $\{ga_1, \ldots, ga_{\phi(n)}\}$ coincide con $\{a_1, \ldots, a_{\phi(n)}\}$, salvo che gli elementi sono enumerati in ordine differente. Dunque il prodotto $\Pi_{i=1}^{\phi(n)} g a_i$ coincide anche con b. Abbiamo mostrato che $g^{\phi(n)} b = b$. Dividento per b otteniamo $g^{\phi(n)} = 1$ per ogni g in $(\mathbb{Z}/n\,\mathbb{Z})^*$. Prendendo come g la classe di a modulo m, abbiamo $a^{\phi(n)} \equiv 1 \bmod n$. □

Esempio 49. Trovare il resto della divisione euclidea di 2^{99} per 7. Soluzione: $2^{99} = 2^{3 \cdot 33} = 8^{33}$. Ora, 8 è congruo a 1 modulo 7 dunque possiamo continuare sostituendo: $8^{33} \equiv 1^{33} \equiv 1 \bmod 7$. Quindi il resto è 1.

Esempio 50. Trovare il resto della divisione di 3^{11} per 5. Soluzione: Modulo 5 abbiamo le seguenti congruenze: $3^{11} \equiv 3^2 3^2 3^2 3^2 3 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \equiv (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot (-1) \cdot 3 \equiv -3 \equiv 2 \bmod (5)$. Quindi il resto è 2.

Esercizio 51. Stabilire per quali valori del parametro a esistono soluzioni del seguente sistema:

$$\begin{cases} 5^{5x} & \equiv & 4 & \bmod(21) \\ 2x & \equiv & a & \bmod(15) \end{cases}$$

Esercizio 52. (Dal compito del 7 giugno 2006, soluzioni sul sito di Dvornicich) Al variare di $a \in \mathbb{Z}$ risolvere il seguente sistema di congruenze:

$$\begin{cases} ax & \equiv & 1 & \mod(9) \\ a^x & \equiv & 1 & \mod(9) \end{cases}$$

Esercizio 53. Trovare le soluzioni $x \in \mathbb{Z}$ della congruenza $x^3 \equiv 0 \bmod (64)$.

Soluzione: $64 = 2^6$. Se 2^6 divide x^3 se e solo se 2^2 divide x. Quindi la congruenza equivale a $x \equiv 0 \bmod 4$. □

11 Gruppi

Esercizio 54. Gli elementi di $\mathbb{Z}/n\mathbb{Z}$ formano un gruppo rispetto all'addizione. L'elemento neutro è la classe dello zero.

Esercizio 55. Il sottoinsieme $(\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}$ constituito dagli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$, forma un gruppo rispetto alla moltiplicazione. L'elemento neutro di $(\mathbb{Z}/n\mathbb{Z})^*$ è la classe di 1.

Esercizio 56. Il gruppo moltiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$ ha $\phi(n)$ elementi, dove ϕ è la funzione di Eulero. Ad esempio $(\mathbb{Z}/12\mathbb{Z})^*$ consiste delle classi resto di $1, 3, 5, 7$ con l'operazione di moltiplicazione.

Abbiamo visto che x è invertibile modulo n se e solo se è coprimo con n. Diamo ora un'altra caratterizzazione degli elementi invertibili modulo n.

Esercizio 57. Un elemento $x \in \mathbb{Z}/n\mathbb{Z}$ è invertibile (cioè esiste $y \in \mathbb{Z}/n\mathbb{Z}$ con $xy = 1$) se e solo se è un generatore del gruppo additivo $\mathbb{Z}/n\mathbb{Z}$.

Soluzione: Per definizione x genera $\mathbb{Z}/n\mathbb{Z}$ se ogni $y \in \mathbb{Z}/n\mathbb{Z}$ è un multiplo di x, ovvero y è della forma $kx = x + \ldots + x$ (k volte) per un certo $k \in \mathbb{Z}$. Ovviamente la classe resto di 1 genera il gruppo, ma non è in generale l'unico generatore. Si noti che presi due generatori, ciascuno di essi deve essere un multiplo dell'altro. Se x genera il gruppo, in particolare deve esistere k tale che $kx = 1$ in $\mathbb{Z}/n\mathbb{Z}$, e quindi x è invertibile. Viceversa se x è invertibile, allora posso scrivere $1 = kx = x + \ldots + x$ e quindi x genera il gruppo (in quanto da x ottengo 1 e da 1 tutti gli altri elementi del gruppo). □

Sapevamo già che $\mathbb{Z}/n\mathbb{Z}$ ha esattamente $\phi(n)$ elementi invertibili. In base all'esercizio precedente ne segue che $\mathbb{Z}/n\mathbb{Z}$ ha esattamente $\phi(n)$ generatori come gruppo additivo. Ad esemio $\mathbb{Z}/12\mathbb{Z}$ ha 4 generatori, consistenti nelle classi di $1, 5, 7, 11$.

Esercizio 58. Se $d|n$ il gruppo ciclico $\mathbb{Z}/n\mathbb{Z}$ ha uno e un solo sottogruppo di ordine k, e precisamente il sottogruppo generato da n/d.

Visto che ogni gruppo ciclico di ordine n è isomorfo a $\mathbb{Z}/n\mathbb{Z}$, lo stesso risultato si estende a tutti i gruppi ciclici di ordine n. Ne diamo comunque qui sotto (Esercizio 60) una dimostrazione indipendente (in notazione moltiplicativa anziché additiva). Iniziamo con un esercizio preliminare.

Esercizio 59. Sia G un gruppo abeliano. Dato un elemento $x \in G$ di ordine finito $o(x)$, e dato un divisore t di $o(x)$, abbiamo $o(x^t) = o(x)/t$. In particolare se G ha un elemento x di ordine n, ne ha uno per ogni divisore d di n (basta prendere x^t con $t = n/d$).

Se G è scritto in notazione additiva anziché moltiplicativa, l'esercizio precedente prende la forma $o(tx) = o(x)/t$. Ad esempio nel gruppo $\mathbb{Z}/12\mathbb{Z}$ l'elemento 4 (che possiamo scrivere nella forma $4 \cdot x$ con $x = 1$) ha ordine $3 = 12/4 = o(x)/4$.

Esercizio 60. Sia G un gruppo ciclico finito di ordine n generato da $x \in G$. Ogni sottogruppo H di G è ciclico e il suo ordine divide n. Inoltre per ogni divisore d di n, G ha un unico sottogruppo H di ordine d, e precisamente il sottogruppo generato da $x^{n/d}$.

Soluzione: Abbiamo $G = \{1, x, x^2, \ldots, x^{n-1}\}$. Sia H un sottogruppo di G. Se $H \neq \{e\}$, sia $r > 0$ minimo tale che $x^r \in H$. Dico che: (i) r divide n; (ii) x^r genera H; (iii) $o(H) = o(x^r) = o(x)/r$; (iv) H è l'unico sottogruppo di G di ordine n/r. Per dimostrare il punto (i) scriviamo $n = rq + s$ con $0 \leq s < r$ (divisione euclidea). Ne segue che $1 = x^n = x^{rq} \cdot x^s$. Siccome x^{rq} ed 1 sono in H, anche x^s lo deve essere (essendo l'inverso di x^{rq}). Dalla minimalità di r segue che $s = 0$ e quindi r divide n. Un simile ragionamento mostra il punto (ii). Infatti dato $y \in H$, sia m tale che $y = x^m$. Essendo anche x^r in H, si vede facilmente che lo deve essere anche x^s dove s è il resto della divisione euclidea di m per r. Per la minimalità di r, s deve essere zero, e pertanto scrivendo $m = rq$ si ha $y = x^m = x^{rq} \in \langle x^r \rangle$. Nel punto (iii), l'uquaglianza $o(H) = o(x^r)$ segue dal fatto che x^r genera H, e l'uguaglianza $o(x^r) = o(x)/r = d$ segue dall'Esercizio 59. Il punto (iv) seque dai punti precedenti. Consideriamo infatti un sottogruppo H' di G di ordine n/r. Sia $r' > 0$ minimo tale che $x^{r'} \in H'$. Ragionando come sopra, r' divide n e $x^{r'}$ genera H'. Inoltre, poiché $n/r = o(H') = o(x^{r'}) = o(x)/r' = n/r'$, abbiamo $r = r'$ e $H = H'$. □

Esercizio 61. In un gruppo abeliano finito G, dati due elementi x, y di ordini m, n coprimi tra loro, il prodotto xy ha ordine mn. Più in generale dati elementi $x_1, \ldots, x_k$ di ordini a due a due coprimi, il prodotto $x_1 \cdot \ldots \cdot x_k$ ha come ordine il prodotto degli ordini.

Soluzione: Dimostriamolo per due fattori, il caso generale si deduce per induzione. Siano dunque x, y, m, n come nell'enunciato. Poiché il gruppo è abeliano, $(xy)^{mn} = x^{mn}y^{mn}$, e ovviamente $x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1$. Pertanto l'ordine t di xy divide mn. Per dimostrare che $t = mn$ basta mostrare che $m|t$ ed $n|t$ (da cui segue $mn|t$ usando la coprimalità). A tal fine osserviamo che $1 = (xy)^{mt} = x^{mt}y^{mt} = y^{mt}$, da cui $n = o(y)|mt$, e quindi $n|t$ (essendo $(m, n) = 1$). Similmente, scambiando i ruoli di x, y, otteniamo $m|t$. □

Esercizio 62. In un gruppo abeliano finito G, dati due elementi x, y di ordine n, m, esiste un elemento $z \in G$ di ordine $[n, m]$ (che in generale non è il prodotto di x ed y).

Soluzione: Conosciamo già il risultato nel caso particolare $(m, n) = 1$. Per ridurci al caso particolare scomponiamo n, m in primi: $n = \Pi_i p_i^{e_i}$, $m = \Pi_i p_i^{f_i}$. Sia $t_i = \max(e_i, f_i)$. Usando la formula $o(z^t) = o(z)/t$, possiamo trovare $r_1, \ldots, r_n \in G$ con $o(r_i) = p_i^{t_i}$. (Se $t_i = e_i$ prendiamo come r_i una opportuna potenza di x, e se $t_i = f_i$ prendiamo come r_i un'opportuna potenza di y.) Ne seque che $o(r_1 \cdot \ldots \cdot r_n) = \Pi_i p_i^{t_i} = [m, n]$. □

Esercizio 63. Ogni sottogruppo H di $(\mathbb{Z}, +)$ è della forma $a\,\mathbb{Z} = \{an : n \in \mathbb{Z}\}$ per qualche $a \in \mathbb{Z}$.

Soluzione: Se H si riduce al solo 0, prendiamo $a = 0$. Altrimenti sia a il minimo elemento strettamente positivo di H. Dato $b \in H$, usiamo la divisione euclidea per scrivere $b = an + r$ con $q \in \mathbb{Z}$ e $0 \leq r < a$. Poichè $a \in H$, anche $an = a + a + \ldots + a$ è in H. Quindi anche $r = b - an$ è in H (in $b \in H$ e $-an$ è l'inverso di an nel gruppo). Ne seque che $r \in H$ ed essendo $r < a$ deve essere $r = 0$. Abbiamo dimostrato che ogni $b \in H$ è un multiplo di a, da cui $H = a\,\mathbb{Z}$. □

Possiamo facilmente calcolare l'intersezione e il prodotto di due sottogruppi di $(\mathbb{Z}, +)$ tramite la formula: $a\,\mathbb{Z} \cap b\,\mathbb{Z} = [a, b]\,\mathbb{Z}$ e $a\,\mathbb{Z} + b\,\mathbb{Z} = (a, b)\,\mathbb{Z}$.

12 Prodotti di gruppi

Esercizio 64. Esiste una bigezione tra $\mathbb{Z}/15\,\mathbb{Z}$ e $\mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/5\,\mathbb{Z}$ che manda $x + 15\,\mathbb{Z}$ in $(x + 3\,\mathbb{Z}, x + 5\,\mathbb{Z})$. Tale bigezione è in effetti un isomorfismo di gruppi.

Soluzione: Se $x + 15\,\mathbb{Z} = y + 15\,\mathbb{Z}$, allora x ed y sono congrui modulo 15, e pertanto lo sono sia modulo 3 che modulo 5, ovvero $(x + 3\,\mathbb{Z}, x + 5\,\mathbb{Z}) = (y + 3\,\mathbb{Z}, y + 5\,\mathbb{Z})$. Ne segue che la funzione è ben posta. Essa è inoltre iniettiva in quanto se $(x + 3\,\mathbb{Z}, x + 5\,\mathbb{Z}) = (y + 3\,\mathbb{Z}, y + 5\,\mathbb{Z})$, allora x ed y sono congrui sia modulo 3 che modulo 5 e pertanto lo sono modulo 15, ovvero $x + 15\,\mathbb{Z} = y + 15\,\mathbb{Z}$ (qui si usa il fatto che 3 e 5 sono coprimi). Essendo la funzione iniettiva, ed avendo il dominio lo stesso numero di elementi del codominio (15 elementi), essa deve essere biunivoca. La verifica che è un isomorfismo è facile. □

Più in generale abbiamo:

Esercizio 65. Siano $a, b \in \mathbb{Z}$ coprimi. Allora la funzione f che manda $x \bmod (ab)$ nella coppia $(x \bmod a, x \bmod b)$ è un isomorfismo tra $\mathbb{Z}/ab\,\mathbb{Z}$ e $\mathbb{Z}/a\,\mathbb{Z} \times \mathbb{Z}/b\,\mathbb{Z}$. Inoltre la restrizione di f agli elementi invertibili $(\mathbb{Z}/ab\,\mathbb{Z})^* \subset \mathbb{Z}/ab\,\mathbb{Z}$, è una bigezione su $(\mathbb{Z}/a\,\mathbb{Z})^* \times (\mathbb{Z}/b\,\mathbb{Z})^*$ (e in effetti è un isomorfismo di gruppi moltiplicativi).

Soluzione: La funzione f è ben definita ed iniettiva in quanto $x \bmod (ab) = y \bmod (ab)$ se e solo se $(x \bmod a, y \bmod a) = (x \bmod b, y \bmod b)$. Essendo il dominio e il codominio di f della stessa cardinalità ab, f è anche surgettiva (alternativamente si può dimostrare la surgettività usando il teorema cinese dei resti, ma si noti che la dimostrazione data fornisce una dimostrazione alternativa del teorema cinese dei resti).

La seconda parte dell'esercizio si risolverebbe meglio passando al linguaggio degli anelli, ma ce la possiamo anche cavare rimanendo ai gruppi.

Ovviamente se x ha un inverso u modulo ab, allora u è un inverso di x anche modulo a e modulo b. Quindi f manda $(\mathbb{Z}/ab\mathbb{Z})^*$ in $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$. Resta da dimostrare che ogni elemento di $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ proviene da un elemento di $(\mathbb{Z}/ab\mathbb{Z})^*$. Sia dunque $(i \bmod a, j \bmod b)$ un elemento di $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$. Visto che a, b sono coprimi, per il teorema cinese dei resti esiste $x \in \mathbb{Z}$ con $x \equiv i \bmod a$ ed $x \equiv j \bmod b$. Dobbiamo mostrare che x è invertibile modulo ab. In effetti se indichiamo con i^{-1} e j^{-1} gli inversi di i e j modulo a e b rispettivamente, e se in base al teorema cinese dei resti scegliamo v che risolve il sistema $v \equiv i^{-1} \bmod a$ e $v \equiv j^{-1} \bmod b$, allora si verifica facilmente che v è l'inverso di x modulo ab. □

Esercizio 66. Se a, b sono coprimi, $\phi(ab) = \phi(a)\phi(b)$.

Soluzione: Visto che $\phi(n)$ è la cardinalità di $(\mathbb{Z}/n\mathbb{Z})^*$, il risultato è conseguenza dell'Esercizio 65. □

Esercizio 67. Siano H, K gruppi abeliani finiti. L'ordine di $(x, y) \in H \times K$ è il minimo comune multiplo degli ordini di $x \in H$ ed $y \in K$.

Soluzione: Usiamo le notazioni moltiplicative e indichiamo con 1_H l'elemento neutro di H e con 1_K quello di K. Allora $(1_H, 1_K)$ è l'elemento neutro di $H \times K$. Abbiamo $(x, y)^m = (x^m, y^m)$. Quindi: $(x, y)^m = (1_H, 1_K)$ se e solo se $x^m = 1_H$ ed $y^m = 1_K$, se e solo se $o(x)|m$ e $o(y)|m$, se e solo se $[o(x), o(y)]|m$. Ne segue che l'ordine di (x, y) è $[o(x), o(y)]$. □

Se vogliamo applicare l'esercizio precedente a $H = \mathbb{Z}/n\mathbb{Z}$ e $K = \mathbb{Z}/m\mathbb{Z}$ conviene usare le notazioni additive anziché moltiplicative. Dobbiamo allora scrivere 0 invece di 1, ed mx invece di x^m.

Esercizio 68. Contare il numero degli elementi di ordine 4 nel gruppo additivo $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Contare poi il numero dei sottogruppi ciclici di G di ordine 4.

Soluzione: L'ordine di $(x, y) \in G$ è il minimo comune multiplo $[o(x), o(y)]$ tra l'ordine di $x \in \mathbb{Z}/4\mathbb{Z}$ e quello di $y \in \mathbb{Z}/6\mathbb{Z}$ (come gruppi additivi). Siccome l'ordine di x deve dividere 4 e l'ordine di y deve dividere 6, affinché $[o(x), o(y)]$ sia 4, le uniche possibilità sono $o(x) = 4$ ed $o(y) = 1$ o 2. Quindi $x = 1$ o 3 (gli unici due elementi di ordine 4), ed $y = 0$ o 3 (di ordine 1 e 2 rispettivamente). Gli elementi (x, y) di ordine 4 sono dunque $(1, 0), (1, 3), (3, 0), (3, 3)$. Di questi 4 elementi di ordine 4, si vede facilmente che $(1, 0)$ ed $(3, 0)$ generano lo stesso sottogruppo, e similmente $(1, 3)$ e $(3, 3)$ generano lo stesso sottogruppo. Quindi vi sono 4 elementi di ordine 4 e due sottogruppi ciclici di ordine 4. □

13 Esercizi astratti sui gruppi

Esercizio 69. Siano H, K sottogruppi di un gruppo finito G. Indichiamo con HK l'insieme $S = \{xy : x \in H, y \in K\}$. Allora $o(HK) = o(H)o(K)/o(H \cap K)$.

Soluzione: Definiamo una relazione di equivalenza $\sim$ su $H \times K$ ponendo $(x, y) \sim (a, b)$ se e solo se $xy = ab$. L'insieme delle classi di equivalenza è in bigezione con HK. Per ottenere l'uguaglianza desiderata basta mostrare che ogni classe di equivalenza ha $o(H \cap K)$ elementi. A tal fine osserviamo che per ogni $z \in H \cap K$ abbiamo $xy = xzz^{-1}y$, ovvero $(x, y) \sim (xz, z^{-1}y)$. Basta mostrare che le coppie della forma $(xz, z^{-1}y)$ sono le uniche che sono in relazione con (x, y). Infatti se $(x, y) \sim (a, b)$ ne segue che l'elemento $z := x^{-1}a = yb^{-1}$ è nell'intersezione $H \cap K$, e possiamo scrivere a, b nella forma $a = xz, b = z^{-1}y$. □

Dato $H < G$ indichiamo con G/H l'insieme delle classi laterali sinistre xH al variare di x in G.

Esercizio 70. Dato $H < G$ esiste una bigezione tra l'insieme delle classi laterali sinistre e destre di H.

Soluzione: Basta mandare la classe xH nella classe Hx^{-1}. Questa è una funzione ben definita ed iniettiva tra le classi sinistre e destre grazie alle equivalenze seguenti: $Hx^{-1} = Hy^{-1}$ se e solo se $H = Hy^{-1}x$ se e solo se $y^{-1}x \in H$ se e solo se $y^{-1}xH = H$ se e solo se $xH = yH$. Per finire osserviamo che ogni classe destra Hg è della forma Hx^{-1} (prendo $x = g^{-1}$) e quindi la funzione è biunivoca. □

Dato un sottogruppo $H < G$ definiamo l'indice $[G : H]$ di H in G come la cardinalità dell'insieme $G/H = \{xH : x \in G\}$ delle classi laterali sinistre di H in G. (Otterrei lo stesso valore per l'indice usando le classi destre.)

Esercizio 71. Se $K < H < G$ allora esiste una funzione surgettiva da G/K a G/H che manda xK in xH. Quindi l'indice di H in G è minore o uguale all'indice di K in G.

Esercizio 72. Siano H, K sottogruppi di G di indice finito. Allora $H \cap K$ è anch'esso di indice finito in G.

Soluzione: Basta osservare che la funzione $G/(H \cap K) \to G/H \times G/K$ che manda $a(H \cap K)$ in (aH, aK) è iniettiva. Infatti se $(aH, aK) = (bH, bK)$ allora $b^{-1}a \in H \cap K$, da cui $b^{-1}a(H \cap K) = H \cap K$ e quindi $a(H \cap K) = b(H \cap K)$. □

Esercizio 73. Siano $K, N < G$ sottogruppi di G. Sia $KN = \{xy : x \in K, y \in N\}$. Allora esiste una bigezione tra $N/(N \cap K)$ e NK/K.

Soluzione: Basta mandare $x(N \cap K) \in N/(N \cap K)$ in $xK \in NK/K$ e controllare che questa funzione è biunivoca. □

Esercizio 74. Ogni sottogruppo di indice 2 è normale.