1 Divisioni e numeri primi.

Indicheremo con $\mathbb{Z}$ l'insieme dei numeri interi, con $\mathbb{N}$ quello dei numeri naturali (cioè interi non negativi), e con $\mathbb{N}^*$ l'insieme dei numeri naturali diversi da 0 ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono rispettivamente gli insiemi dei numeri razionali, dei numeri reali, e dei numeri complessi). Inizieremo richiamando proprietà ben note dei numeri interi, anche al fine di fissare le notazioni.

1.1 Divisione euclidea

Ricordiamo l'assioma del **buon ordinamento** per l'insieme $\mathbb{N}$: esso afferma che *ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ha un elemento minimo.*

Teorema 1.1 (Divisone euclidea.) *Siano* a, b *numeri interi, con* $b \geq 1$. *Allora esistono degli unici interi* q, r *tali che*

$$a = bq + r$$

$$0 \leq r \leq b - 1 \ .$$

Dimostrazione. Sia S l'insieme di tutti i numeri naturali che della forma $a - bt$, con $t \in \mathbb{Z}$. Osserviamo che S non è vuoto; infatti, se $a \geq 0$ allora $a = a - b0 \in S$; se $a < 0$, allora, poiché $b \geq 1$, $a - b(a-1) \in S$. Dunque, per il principio del buon ordinamento, S ha un elemento minimo r, ed esiste un $q \in \mathbb{Z}$ tale che $a = bq + r$.
Se fosse $r \geq b$, allora

$$0 \leq r - b = a - bq - b = a - b(q+1) \in S$$

contro la minimalità di r. Dunque $0 \leq r < b$.
La dimostrazione dell'unicità di q ed r è lasciata per esercizio. ∎

Esercizio 1. Siano a, b numeri interi, con $b \geq 1$. Si provi che esistono unici interi t, s tali che $a = bt + s$ e $-\frac{b}{2} < s \leq \frac{b}{2}$.

Siano $a, b \in \mathbb{Z}$. Con la scrittura $a|b$ intendiamo che a *divide* b, cioè che esiste un $c \in \mathbb{Z}$ tale che $ac = b$.

Siano m, n numeri interi non entrambi nulli. Ricordiamo che un elemento $d \in \mathbb{Z}$ si dice un *Massimo Comun Divisore* di m e n se $d|m$, $d|n$, e per ogni intero c, se $c|m$ e $c|n$ allora $c|d$. Ogni coppia di interi non entrambi nulli ammette due massimi comun divisori, che differiscono per il segno. Denotiamo con (m, n) il Massimo Comun Divisore *positivo* di m e n. I numeri m, n si dicono **coprimi** se $(m, n) = 1$.

Proposizione 1.2 *Siano a, b interi non entrambi nulli. Allora il massimo comun divisore (a, b) è il minimo numero intero positivo (non zero) d, che si può scrivere nella forma $d = ua + wb$, con $u, w \in \mathbb{Z}$.*

DIMOSTRAZIONE. Poichè a e b non sono entrambi nulli, l'insieme

$$\{z = xa + yb \mid x, y \in \mathbb{Z},\ z \geq 1\}$$

è non vuoto e pertanto ha un minimo $d = ua + wb$. Dividiamo a per d, $a = qd + r$, con $0 \leq r \leq d - 1$. Ora

$$0 \leq r = a - qd = (1 - qu)a + (-qw)b,$$

e quindi, per la scelta di d, deve essere $r = 0$. Dunque d divide a. Analogamente si prova che d divide b. Infine, se c è un divisore comune di a e b, chiaramente c divide anche d. Pertanto $d = (a, b)$. ∎

Esercizio 2. Trovare due numeri interi a e b tali che $19a + 21b = 1$.

Esercizio 3. Siano $a_1, a_2, \ldots, a_s$ numeri interi non tutti nulli. Si dimostri che $MCD(a_1, a_2, \ldots, a_s) = 1$ se e solo se esistono interi $x_1, x_2, \ldots, x_s$ tali che

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = 1.$$

Algoritmo di Euclide. L'algoritmo di Euclide consente di determinare, con un numero finito di operazioni, il Massimo Comun Divisore di due interi non nulli (ma si applica anche ad altri contesti, come ad esempio con polinomi) a e b.

Siano quindi a e b interi non nulli (e possiamo assumere $b \geq 1$).
Si pone $a_0 = a$, e $a_1 = b$. Il primo passo è dividere a_0 per a_1:

$$a_0 = q_1a_1 + a_2 \quad \text{con} \quad 0 \leq a_2 < a_1$$

quindi, se $a_2 \neq 0$, si divide a_1 per a_2, ottenendo un resto a_3 con $0 \leq a_3 < a_2$. Si prosegue quindi con tale ccatena di divisioni successive; ovvero, arrivati ad a_i si definisce a_{i+1} come il resto della divisione di a_{i-1} per a_i :

$$\begin{aligned}
&a_0 = q_1a_1 + a_2\\
&a_1 = q_2a_2 + a_3\\
&a_2 = q_3a_3 + a_4\\
&\ldots\ldots\\
&a_{i-1} = q_ia_i + a_{i+1}\\
&\ldots\ldots
\end{aligned}$$

In questo modo, si ottiene una sequenza di resti positivi

$$b = a_1 > a_2 > a_3 > \ldots > a_{i-1} > a_i > a_{i+1} > \ldots > a_{n+1} = 0$$

Questa sequenza, costituita da numeri naturali, arriva a zero dopo un numero finito di passi (che ho indicato con n). Sia quindi a_n l'ultimo resto non nullo; allora

a_n *è il massimo comun divisore positivo tra* a e b.

Cosa che si dimostra facilmente utilizzando induttivamente la seguente osservazione:

Lemma 1.3 *Siano a e b interi non nulli, e sia r il resto della divisione di a per b. Allora $(a, b) = (b, r)$.*

Osserviamo che l'algoritmo di Euclide, oltre a determinare (a, b), fornisce (ripercorso a ritroso) i coefficienti u, w come nella Proposizione 1.2, tali che $(a, b) = ua + wb$.

Esempio. Siano $a = 6468$ e $b = 2275$. Si ha

$$\begin{aligned}
6468 &= 2 \cdot 2275 + 1918 \\
2275 &= 1 \cdot 1918 + 357 \\
1918 &= 5 \cdot 357 + 133 \\
357 &= 2 \cdot 133 + 91 \\
133 &= 1 \cdot 91 + 42 \\
91 &= 2 \cdot 42 + 7 \\
42 &= 6 \cdot 7 + 0
\end{aligned}$$

Quindi $(6468, 2275) = 7$. Ora

$$\begin{aligned}
7 \quad &= 91 - 2 \cdot 42 = 91 - 2(133 - 91) = 3 \cdot 91 - 2 \cdot 133 = \\
&= 3(357 - 2 \cdot 133) - 2 \cdot 133 = -8 \cdot 133 + 3 \cdot 357 = \\
&= 43 \cdot 357 - 8 \cdot 1918 = \\
&= -51 \cdot 1918 + 43 \cdot 2275 = \\
&= -51 \cdot 6468 + 145 \cdot 2275.
\end{aligned}$$

Esercizio 4. Calcolare $(1001, 4485)$, e quindi scriverlo come combinazione a coefficienti interi dei due numeri dati.

1.2 Fattorizzazioni

Un intero p è un *primo* se $p \neq 0, 1, -1$ e l'insieme dei divisori di p è $\{1, -1, p, -p\}$.

Esercizio 5. Sia $p \in \mathbb{Z}$, $p \neq 0, 1, -1$. Si provi che sono equivalenti

(i) p è un numero primo.

(ii) Per ogni $a, b \in \mathbb{Z}$, se $p|ab$ allora $p|a$ oppure $p|b$.

Lemma 1.4 *Sia n un numero intero diverso da $0, 1, -1$. Allora esiste un numero primo che divide n.*

Dimostrazione. Esercizio. ∎

Utilizzando questo Lemma si dimostra che ogni intero (diverso da $0, 1, -1$) ammette una fattorizzazione essenzialmente unica come prodotto di numeri primi.

Teorema 1.5 (Teorema Fondamentale dell'Aritmetica). *Sia $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Allora esistono primi $p_1, p_2, \ldots, p_s$ tali che*

$$a = p_1 p_2 \cdots p_s \ .$$

Se inoltre $q_1, q_2, \ldots, q_t$ sono primi tali che $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_s$, allora $s = t$ ed esiste una permutazione σ di $\{1, 2, \ldots, s\}$ tale che, per ogni $i = 1, 2, \ldots, s$, $q_i = \pm p_{\sigma(i)}$.

Denotiamo con $\mathbb{P}$ l'insieme di tutti i numeri primi positivi. Dal Teorema precedente segue che ogni intero $a \neq 0$ si scrive come il prodotto

$$a = \pm \prod_{p \in \mathbb{P}} p^{r_p(a)}$$

dove gli $r_p(a)$ sono numeri naturali univocamente determinati, e quasi tutti nulli (cioè $r_p(a) \neq 0$ per un numero finito di primi p.

Teorema 1.6 (Euclide) *Esistono infiniti numeri primi.*

DIMOSTRAZIONE. Supponiamo, per assurdo, che l'insieme dei numeri primi sia finito, e che $p_1, p_2, \ldots, p_k$ siano tutti i numeri primi distinti. Consideriamo $n = p_1 p_2 \cdots p_k$. Per il Lemma 1.4, il numero intero $n + 1$ ammette un divisore primo, che deve essere pertanto uno dei p_i (con $i \in \{1, 2, \ldots, k\}$). Ma allora si avrebbe che tale primo divide sia n che $n + 1$, il che è chiaramente impossibile. ∎

Esercizio 6. Sia $1 < n \in \mathbb{N}$. Si provi che

$$u = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

non è un numero intero.

Soluzione. Sia 2^k la massima potenza di 2 minore o uguale a n (cioè $2^k \leq n < 2^{k+1}$), e sia m il minimo comune multiplo tra gli tutti gli interi $1, 2, \ldots, n$ escluso 2^k. Allora la massima potenza di 2 che divide m è 2^{k-1}. Ora abbiamo

$$mu = m + \frac{m}{2} + \cdots + \frac{m}{n}$$

dove ogni addendo del termine di destra è un intero con l'eccezione di $\frac{m}{2^k}$. Poiché, per quanto sopra osservato, $\frac{m}{2^k}$ non è un intero, ne segue che mu non è un intero, e quindi che u non è un intero.

Esercizio 7. Sia $1 < n \in \mathbb{N}$. Si provi che

$$v = 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$$

non è un numero intero.

1.3 Numeri primi

Vediamo ora alcune elementari osservazioni sui numeri primi che ci saranno utili nel prossimo capitolo; ulteriori risultati riguardanti la distribuzione dei numeri primi verranno esposti in seguito.

Lemma 1.7 *Siano $a, n, m \in \mathbb{N}^*$, con $a \neq 1$. Allora*

$$(a^n - 1, a^m - 1) = a^{(n,m)} - 1 \ .$$

DIMOSTRAZIONE. Siano $d = (a^n - 1, a^m - 1)$ e $c = (n, m)$. Allora, $a^c - 1$ divide d per una ben nota e facile proprietà delle somme di serie geometriche.
Viceversa, siano $u, -v \in \mathbb{Z}$, tali che $c = un + (-v)m = un - vm$. Allora, scambiando eventualmente n e m, u, v sono positivi. Ancora per le proprietà delle serie geometriche, abbiamo che d divide $a^{nu} - 1$ e $a^{mv} - 1$. Quindi d divide la diffrenza di questi, $a^{nu} - a^{mv} = a^{mv}(a^{nu-mv} - 1) = a^{mv}(a^c - 1)$. Poichè chiaramente d e a sono coprimi, si conclude che d divide $a^c - 1$. ∎

Proposizione 1.8 *Siano $n \in \mathbb{N}^*$, $n > 1$.*

(1) *Sia $a \in \mathbb{N}^*$; se $a^n - 1$ è un primo, allora $a = 2$ e n è un primo.*

(2) *Sia p un primo; se $p^n + 1$ è un primo, allora $p = 2$ e $n = 2^m$ per qualche $m \in \mathbb{N}^*$.*

DIMOSTRAZIONE. (1) Poichè $a^n - 1 = (a - 1)(a^{n-1} + \ldots + a + 1)$, se $a^n - 1$ è primo allora $a = 2$ e, per la stessa consoderazione, n è primo.
(1) Se $p^n + 1$ è primo allora deve essere dispari e quindi $p = 2$. Supponiamo che n abbia un divisore primo dispari q, e scriviamo $n = mq$. Allora $2^n + 1 = (2^m + 1)(2^{m(q-1)} - (2^{m(q-1)} + \ldots - 2^m + 1)$ non è primo. Dunque, se $2^n + 1$ è primo, n deve essere una potenza di 2. ∎

I numeri primi del tipo (2) sono detti primi di Fermat. In generale, per $m \in \mathbb{N}$, l'intero $F_m = 2^{2^m} + 1$ è detto *m-esimo numero di Fermat*. I primi cinque numeri di Fermat

$$F_0 = 3, \ F_1 = 5, \ F_2 = 17, \ F_3 = 257, \ F_4 = 65537$$

sono numeri primi. Sulla base di questa osservazione, P. Fermat affermò che ogni intero di questo tipo è primo. Fu L. Eulero a scoprire come il termine successivo $F_5 = 2^{32} + 1$ non sia primo (vedi proposizione seguente). Di fatto, oltre ai cinque detti, nessun altro primo di Fermat è stato a tutt'oggi trovato; e neppure è noto se ne esistano un numero infinito o finito, né se esistano infiniti numeri non-primi nella serie F_n (è stato verificato che, per $5 \leq m \leq 21$, F_m non è un primo).

Proposizione 1.9 (Eulero) *F_5 non è un numero primo.*

DIMOSTRAZIONE. Proviamo che $641 | F_5$. Infatti, $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$; dunque

$$2^{32} = 2^4 \cdot 2^{28} = (641 - 5^4) \cdot 2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 = 641 \cdot 2^{28} - (641 - 1)^4$$

e quindi esiste un intero positivo t tale che $2^{32} = 641t - 1$, cioè $641 | 2^{32} + 1 = F_5$
(si verifica che $F_5 = 641 \cdot 6700417$, e 641 e 6700417 sono numeri primi). ∎

Esercizio 8. (a) Per $n \in \mathbb{N}$, sia $F_n = 2^{2^n} + 1$. Si provi che se $n \neq m$ allora $(F_n, F_m) = 1$ (si osservi che, se $n < m$, allora F_n divide $F_m - 2$).

Similmente, non tutti i numeri del tipo $M_p = 2^p - 1$ (con p primo) sono primi. Essi sono detti *numeri di Mersenne*; il più piccolo numero di Mersenne a non essere primo è $M_{11} = 23 \cdot 89$. Anche in questo caso non è tuttora noto se esistano infiniti primi di Mersenne. Al maggio 2002, risultano noti 39 primi di Mersenne, il maggiore dei quali è M_p con $p = 13466917$ (M. Cameron, Woltman e Kurowski, dicembre 2001. Questo è, al momento, anche il più grande numero primo conosciuto: la sua espansione decimale comprende 4.053.946 cifre. Chi fosse interessato può consultare il sito internet: www.mersenne.org/prime.htm).

Esistono molte altre congetture aperte riguardanti i numeri primi (sui quali torneremo nel capitolo 5). Due fra le più famose sono:

Twin prime conjecture: esistono infinite coppie di numeri primi p e q 'consecutivi' (ovvero tali che $p - q = 2$).

Congettura di Goldbach: Ogni numero intero pari si può scrivere come somma di due numeri primi.

Esercizio 9. Sia $n \in \mathbb{N}$. Si provi che $n,\ n+2,\ n+4$ sono primi se e solo se $n = 3$. Si dimostri che la stessa conclusione vale assumedo che $n,\ n+4,\ n+8$ siano primi.

Esercizio 10. Siano $n, k \in \mathbb{N}$, con $k \geq 3$. Si provi che se $n,\ n+k,\ n+2k, \ldots, n+(k-2)k$ sono tutti numeri primi allora $n = k - 1$.

1.4 Equazioni diofantee

Con *equazione diofantea* (dal matematico alessandrino Diofanto) si intende genericamente una equazione algebrica le cui soluzioni sono cercate in prefissate classi di numeri; in particolare quando le soluzioni cercate sono numeri interi. Allo studio della risolubilità (e delle soluzioni) di particolari equazioni diofantee è riconducibile una considerevole parte della teoria dei numeri, così come sono molteplici gli strumenti sviluppati nel corso dei secoli per affrontare simili questioni. Un esempio è il capitolo 4 di questi appunti, dove studieremo la possibilità di rappresentare i numeri naturali come somme di quadrati.

Un primo facile caso di equazione diofantea è collegato alla Proposizione 1.2

Proposizione 1.10 *Siano a, b ed n numeri interi (con a e b non entrambi nulli); allora l'equazione*

$$ax + by = n$$

ammette soluzioni in $\mathbb{Z}$ se e solo se $(a, b)|n$. In generale, se $a_1, a_2, \ldots, a_k$ sono interi non tutti nulli, l'equazione $a_1x_1 + a_2x_2 + \cdots + a_kx_k = n$ ammette soluzioni intere se e solo se $(a_1, a_2, \ldots, a_k)$ divide n.

Dimostrazione. Esercizio. ∎

Esercizio 11. Sia $n \in \mathbb{N}^*$ e siano a, b interi non nulli tali che $(a,b)|n$. Sia (x_o, y_o) una soluzione dell'equazione diofantea $ax + by = n$. Si provi che l'insieme delle soluzioni di tale equazione è

$$\left\{ \left(x_o + t\frac{b}{(a,b)},\, y_o - t\frac{a}{(a,b)} \right) \;\middle|\; t \in \mathbb{Z} \right\}.$$

Un poco più complicata è la situazione in cui si richiede l'esistenza di soluzioni non negative. Anche la dimostrazione del seguente risultato è lasciata per esercizio.

Lemma 1.11 *Siano $a, b \in \mathbb{N}^*$ tali che $(a,b) = 1$. Se $n \geq a(b-1)$, allora esistono interi non negativi x, y tali che $ax + by = n$.*

Un esempio assai famoso di equazione diofantea è il cosiddetto *ultimo teorema di Fermat*, che fu enunciato da P. Fermat nel 1637. Fermat scrisse di averne trovato una dimostrazione 'mirabile', ma di non avere lo spazio per riportarla (egli stava appunto annotando un testo di Diofanto). Dopo secoli di sforzi (inefficaci a dimostrare l'asserzione di Fermat, ma importantissimi per lo sviluppo di molte idee matematiche), l'ultimo teorema di Fermat è stato finalmente dimostrato da Andrew Wyles verso la fine del secolo scorso, utilizzando metodi assai profondi di geometria algebrica.

Teorema 1.12 (Fermat - Wyles). *Sia n un numero naturale. Se $n \geq 3$, non esistono soluzioni intere dell'equazione*

$$x^n + y^n = z^n$$

tali che $xyz \neq 0$.

Il caso invece in cui l'esponente n è uguale a 2 è del tutto elementare.

Proposizione 1.13 *Ogni soluzione intera dell'equazione*

$$x^2 + y^2 = z^2$$

si scrive nella forma $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$, dove $(m,n) = 1$.

Dimostrazione. Si verifica facilmente che per ogni $k, n, m \in \mathbb{N}^*$, con $(n,m) = 1$, la terna $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$ è una soluzione dell'equazione data (ed è detta, per ovvî motivi, *terna pitagorica*).
Vicevarsa, siano $x, y, z \in \mathbb{N}^*$ tali che $x^2 + y^2 = z^2$, e sia $k = (x,y)$. Osserviamo che allora $k = (x,z) = (y,z)$. Siano $a, b, c \in \mathbb{N}^*$, con

$$x = ka, \quad y = kb, \quad z = kc\ .$$

Allora $(a,b) = (a,c) = (b,c) = 1$ e $a^2 + b^2 = c^2$. Dunque

$$c^2 = a^2 + b^2 = (a+b)^2 - 2ab\ .$$

a e b non sono entrambi pari. Se fossero entrambi dispari, allora $a+b$ e c sarebbero pari, e quindi $4|c^2$ e $4|(a+b)^2$, da cui segue la contraddizione $4|2ab$. Possiamo quindi assumere che a sia dispari e b sia pari (e quindi c è dispari). Sia $d=(c+a,c-a)$; allora $2|d$, ed inoltre $d|(c+a)+(c-a)=2c$ (analogamente $d|2a$), e dunque, poiché a e c sono coprimi, $d=2$. Siano ora $u,v\in\mathbb{N}^*$ tali che

$$c+a=2u \qquad c-a=2v\ .$$

Per quanto appena osservato $(u,v)=1$. Inoltre

$$b^2=c^2-a^2=(c+a)(c-a)=4uv\ ;$$

e dunque u e v sono quadrati: sia $u=m^2$ e $v=n^2$. Allora,

- $b^2=4m^2n^2$, e quindi $b=2mn$, e $y=2kmn$.
- $2c=2(u+v)=2(m^2+n^2)$, e quindi $c=m^2+n^2$, e $z=k(m^2+n^2)$.
- $2a=2(u-v)=2(m^2-n^2)$, e quindi $a=m^2-n^2$, e $x=k(m^2-n^2)$. ∎

Esercizio 12. Provare che l'equazione $x^4+y^4=z^2$ non ha soluzioni intere non banali (cioè tali che $xyz\neq 0$). In particolare, quindi, il Teorema di Fermat è vero per l'esponente $n=4$ (si veda l'appendice al Capitolo 4 per la soluzione del caso $n=3$).

Esercizio 13. Si provi che le sole soluzioni intere, con $x\geq 2$, dell'equazione

$$(x-1)!=x^y-1$$

sono $x=2$, $y=1$; $x=3$, $y=1$ e $x=5$, $y=2$.

Esercizio 14. La successione di *Fibonacci* è definita da:

$$u_0=0,\ u_1=1,\ \text{ e }\ u_{n+2}=u_{n+1}+u_n$$

(i primi termini di essa sono $0,1,1,2,3,5,8,13,21,33\ldots$). Provare i seguenti fatti

1) se $x=(1+\sqrt{5})/2$ e $y=(1-\sqrt{5})/2$, allora $u_n\sqrt{5}=x^n-y^n$ (x,y sono le radici reali dell'equazione t^2-t-1)
2) $(u_n,u_{n+1})=1$
3) $u_{m+n}=u_{n-1}u_m+u_nu_{m+1}$
4) se $r\in\mathbb{N}^*$, u_n divide u_{nr}
5) se $(m,n)=d$, allora $(u_m,u_n)=u_d$.

Esercizio 15. Sia $n\in\mathbb{N}^*$. Si provi che l'equazione diofantea $x+2xy+y=n$ ha soluzioni non banali (cioè $x\neq 0\neq y$) se e solo se $2n+1$ non è un numero primo.

L'importanza delle equazione diofantee non risiede tanto nella loro applicabilità 'pratica' (anche all'interno della matematica stessa), quanto nel proflufio di idee - a volte molto sofisticate - a cui il loro studio ha dato e dà luogo (ad esempio la teoria degli anelli e degli ideali è nata da un tentativo di attaccare la congettura di Fermat), e nella

suggestione esercitata da problemi i cui enunciati sono comprensibili anche ad un livello assolutamente elementare.
Un esempio curioso è la congettura di Catalan (che a tutt'oggi è ancora irrisolta)[1].

Congettura di Catalan: *Siano* $2 \leq n, m \in \mathbb{N}^*$. *La sola soluzione non banale intera dell'equazione*

$$x^n = y^m - 1$$

si ha per $n = 2$, $m = 3$, $x = 3$, $y = 2$.

(Ovvero i soli numeri naturali consecutivi che sono potenze non banali di numeri interi sono 8 e 9. Chi fosse interessato può consultare il testo di P. Ribenboim "Catalan's Conjecture".)

1.5 Appendice I: un test di primalità per i numeri di Mersenne.

Descriviamo un test di primalità per numeri di Mersenne che fu trovato da Lehmer nel 1930, ed è tuttora utilizzato nelle computazioni. Esso è una applicazione di una tecnica più generale, quella delle *sequenze di Lucas* (si veda l'interessante testo di P. Ribenboim, *The Book of Prime Numeber Records*).

Cominciamo col definire induttivamente una successione $(S_i)_{i\in\mathbb{N}^*}$ di numeri naturali, ponendo

$$S_1 = 4 \qquad \text{e} \qquad S_{n+1} = S_n^2 - 2 \ .$$

Denotiamo con $M_n = 2^n - 1$, l'n-esimo numero di Mersenne.

Test di Lucas-Lehmer. *M_n è primo se e solo se* $S_{n-1} \equiv 0 \, (mod \, M_n)$.

Dimostrazione. Ci limitiamo a dimostrare la sufficienza (che è poi quella che interessa maggiormente): ovvero che se M_p divide S_{p-1}, allora M_p è un numero primo.

Siano $w = 2 + \sqrt{3}$, e $v = 2 - \sqrt{3}$. Allora, per ogni $2 \geq n \in \mathbb{N}^*$,

$$S_n = w^{2^{n-1}} + v^{2^{n-1}}$$

(lo si verifichi per induzione). Quindi, se M_n divide S_{n-1}, esiste un intero r tale che

$$w^{2^{n-2}} + v^{2^{n-2}} = rM_n.$$

Moltiplicando per $w^{2^{n-2}}$ e sottraendo 1, si ha

$$w^{2^{n-1}} = rM_n w^{2^{n-2}} - 1 \ , \tag{1}$$

e quindi, elevando al quadrato,

$$w^{2^n} = (rM_n w^{2^{n-2}} - 1)^2 \ . \tag{2}$$

[1]Nella scorsa primavera, il matematico romeno Preda Mihailescu ha annunciato una dimostrazione di questa congettura.

Supponiamo, per assurdo, che M_n non sia primo; allora M_n ha un divisore primo q tale che $q \leq \sqrt{M_n}$.
Consideriamo il campo

$$F = \frac{\mathbb{Z}}{q\mathbb{Z}}[\sqrt{3}] \ ,$$

e sia $G = F^*$ il gruppo moltiplicativo dei suoi elementi non nulli. Poiché $\sqrt{3}$ è un elemento di grado al più 2 su $\mathbb{Z}/q\mathbb{Z}$, l'ordine di G è al più $q^2 - 1$.
Ora, le equazioni 1 e 2 di sopra, modulo q diventano

$$\begin{cases} w^{2^{n-1}} = -1 \\ w^{2^n} = 1 \end{cases}$$

Dunque, l'ordine di w nel gruppo moltiplicativo G è 2^n. Pertanto

$$2^n \leq |G| \leq q^2 - 1 < M_n = 2^n - 1$$

e questa è una contraddizione. ∎

1.6 Appendice II: una dimostrazione topologica del Teorema di Euclide.

(Fürstenberg) Dati $a, b \in \mathbb{Z}$, $b \geq 1$, sia

$$N_{a,b} = \{\ a + zb \mid z \in \mathbb{Z}\ \}.$$

Definiamo una topologia in $\mathbb{Z}$, definendo gli insiemi aperti non vuoti come i sottoinsiemi A di $\mathbb{Z}$ tali che per ogni $a \in A$ esiste $b \geq 1$ tale che $N_{a,b} \subseteq A$. Si verifica facilmente che ciò definisce una topologia su $\mathbb{Z}$. In questa topologia è immediato verificare che

- ogni insieme aperto non vuoto è infinito;

- ogni insieme $N_{a,b}$ è chiuso.

La prima è ovvia dalla definizione. Per la seconda basta osservare che

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}.$$

Ora, poiché ogni numero intero diverso da $1, -1$ ha almeno un divisore primo, si ha che

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Se, per assurdo $\mathbb{P}$ fosse finito, si avrebbe che $\mathbb{Z} \setminus \{1, -1\}$ sarebbe una unione finita di insiemi chiusi, e quindi esso stesso chiuso. Di conseguenza $\{1, -1\}$ sarebbe aperto, contro quanto osservato sopra.

1.7 Appendice III: la serie $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge.

(Erdös) Sia $p_1, p_2, p_3, \ldots$ la successione di tutti i numeri primi positivi in ordine crescente, e supponiamo per assurdo che $\sum_{p\in\mathbb{P}} \frac{1}{p}$ converge. Allora esiste un k tale che $\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}$; quindi, per un qualunque numero intero $N \geq 1$,

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Dato $N \geq 1$, sia N_0 il numero di interi positivi $n \leq N$ che sono divisibili per almeno un primo p_j con $j \geq k+1$, e con N_1 il numero di numeri di interi positivi $n \leq N$ che sono divisibili solo da primi p_t con $t \leq k$. Chiaramente, per definizione, $N_0 + N_1 = N$.
Osserviamo che il numero di interi $1 \leq n \leq N$ che sono multipli del primo p_i è al più $\frac{N}{p_i}$. Quindi

$$N_0 \leq \sum_{j\geq k+1} \frac{N}{p_j} < \frac{N}{2}.$$

Stimiamo ora N_1. Osserviamo che ogni numero naturale n può essere scritto in modo univoco come $n = a_n b_n^2$, dove b_n^2 è il massimo quadrato che divide n, e a_n è un prodotto di primi *distinti*. Ora, se i divisori primi di $n \leq N$ sono tutti compresi tra $p_1, p_2, \ldots, p_k$, si ha che il numro di possibili fattori a_n per tali interi n, è 2^k. D'altra parte, sempre per tali n, $b_n \leq \sqrt{n} \leq \sqrt{N}$, e dunque ci sono al più $\sqrt{N}$ possibilità per il fattore b_n. In conclusione,

$$N_1 \leq 2^k \sqrt{N}.$$

Poiché $N = N_0 + N_1$ vale per ogni $N \geq 1$, si ha

$$N < \frac{N}{2} + 2^k \sqrt{N}.$$

Ma tale relazione è falsa per $N \geq 2^{2k+2}$, e questa contraddizione dimostra che la serie $\sum_{p\in\mathbb{P}} \frac{1}{p}$ deve essere divergente.

Soluzione di alcuni esercizi.

Esercizio 8. Siano $n < m$ interi positivi. Proviamo per induzione su $k = m - n$ che F_n divide $F_m - 2$. Se $k = 1$

$$F_{n+1} - 2 = 2^{2^n 2} - 1 = (2^{2^n})^2 - 1 = (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n} - 1)F_n \ ;$$

se $k > 1$, l'ipotesi induttiva, ed il caso $m - n = 1$ ci dicono che F_n divide F_{m-1}, e che questo a sua volta divide F_m.
Sia ora $d = (F_n, F_m)$. Allora, per quanto sopra dimostrato, d divide 2. Poiché F_n è dispari, si conclude che $d = 1$.

Esercizio 9. Siano $n \in \mathbb{N}$, tale che $n, n+2, n+4$ sono numeri primi, e supponiamo, per assurdo, che $n \neq 3$. Allora, chiaramente, 3 non divide $n+2$ (che è primo). Quindi 3 divide $n+1$. Ma allora 3 divide $n+4$, che è un assurdo.

Esercizio 13. Siano $x, y \in \mathbb{N}$ tali che $(x-1)! = x^y - 1$. Se $x = 2, 3$ allora $y = 1$. Se $x > 2$ è pari, allora $(x-1)!$ è pari, mentre $x^y - 1$ è dispari, per ogni $y \geq 1$. Dunque x è dispari. Se $x = 5$, allora $y = 2$. Supponiamo ora, per assurdo, che esista una soluzione con x dispari $x \geq 7$. Allora, $x-1$ è pari, e $2 < \frac{x-1}{2} < x-2$. Quindi

$$x - 1 = 2 \cdot \frac{x-1}{2} \text{ divide } (x-2)!$$

Ora, poiché

$$(x-2)!(x-1) = (x-1)! = x^y - 1 = (x-1)(x^{y-1} + x^{y-2} + \ldots + x + 1) \ ,$$

se ne deduce che $x-1$ divide $b = x^{y-1} + x^{y-2} + \ldots + x + 1$. Ma ciò comporta che $x-1$ divide y (infatti $x-1$ divide anche $(x^{y-1}-1)+(x^{y-2}-1)+\ldots+(x-1)+(1-1) = b-y$). In particolare, si ha $x - 1 \leq y$, e di conseguenza si ottiene la contraddizione

$$x^y - 1 \geq x^{x-1} - 1 > (x-1)!$$

(l'ultima disuguaglianza essendo soddisfatta - lo si provi per induzione - per ogni $x \geq 3$).

Esercizio 14. Osserviamo che $x = (1+\sqrt{5})/2$ e $y = (1-\sqrt{5})/2$ sono le radici reali del polinomio $t^2 - t - 1$.

1) Per induzione su $n \in \mathbb{N}$. Per $n = 0$ la cosa è banale. Se $n = 1$: $x - y = \sqrt{5} = u_1\sqrt{5}$. Supposta l'uguaglianza vera per ogni $k < n \geq 2$, abbiamo

$$u_n\sqrt{5} = u_{n-1}\sqrt{5} + u_{n-1}\sqrt{5} = x^{n-1} - x^{n-1} + x^{n-2} - y^{n-2} =$$

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

2) Per induzione su n, tenendo conto che se d divide (u_n, u_{n+1}), allora d divide $u_{n+1} - u_n = u_{n-1}$.

3) e 4) si provano anche facilmente per induzione.

5) Possiamo supporre $m > n$. Per l'algoritmo della divisione $m = nq + r$, con $0 \leq r \leq n-1$. Per il punto 2),

$$u_m = u_{nq-1}u_r + u_{nq}u_{r+1}$$

da cui deriva che $(u_m, u_n) = (u_n, u_r)$. Continuando come nell'algoritmo di Euclide, si ricava il risultato.

2 Funzioni Moltiplicative

2.1 Proprietà generali

Sia A un dominio d'integrità (che in generale, ma non sempre, sarà l'anello $\mathbb{C}$ dei numeri complessi). Una funzione aritmetica (cioè con dominio un sottoinsieme di $\mathbb{Z}$)

$$f : \mathbb{N}^* \longrightarrow A$$

si dice **moltiplicativa** se, per ogni $n, m \in \mathbb{N}^*$

$$(n, m) = 1 \quad \Rightarrow \quad f(nm) = f(n)f(m) \ .$$

Osservazioni 1) Se f è una funzione moltiplicativa, $f(1) = 1_A$. Infatti, $f(1) = f(1)f(1)$ e ciò implica (poichè A è un dominio d'integrità) $f(1) = 1_A$.

2) Sono moltiplicative la funzione costante $f(n) = 1_A$, e la funzione identica $f(n) = n$ (quest'ultima definita con dominio in $\mathbb{Z}$).

Vediamo un utile strumento per definire funzioni moltiplicative.

Teorema 2.1 *Sia* $f : \mathbb{N}^* \longrightarrow A$ *una funzione moltiplicativa, e sia* $F : \mathbb{N}^* \longrightarrow A$, *definita ponendo, per ogni* $n \in \mathbb{N}^*$

$$F(n) = \sum_{d|n} f(d) \ .$$

Allora F *è moltiplicativa.*

Dimostrazione. Siano $n, m \in \mathbb{N}^*$ tali che $(n, m) = 1$. Osserviamo allora che i divisori di nm sono in corrispondenza biunivoca con le coppie (d_1, d_2), dove d_1 e d_2 sono, rispettivamente divisori di n e di m: ogni divisore d di nm si scrive infatti *in modo unico* come prodotto $d = d_1d_2$ con dove $d_1|n$ e $d_2|m$. Quindi, tenendo presente che ogni divisore di n è coprimo con ogni divisore di m,

$$F(nm) = \sum_{d|nm} f(d) = \sum_{d_1|n\, d_2|m} f(d_1d_2) = \sum_{d_1|n\, d_2|m} f(d_1)f(d_2) =$$

$$= \sum_{d_1|n} f(d_1) \left(\sum_{d_2|m} f(d_2) \right) = \sum_{d_1|n} f(d_1) \cdot \sum_{d_2|m} f(d_2) = F(n)F(m) \ .$$

■

Definiamo ora alcune prime interessanti funzioni moltiplicative (a valori in $\mathbb{Z}$). Sia $n \in \mathbb{N}^*$; si pone

$$\tau(n) = \text{ numero di divisori positivi di } n$$

$$\sigma(n) = \text{ somma dei divisori positivi di } n$$

τ e σ sono moltiplicative. Infatti,

$$\tau(n) = \sum_{d|n} 1 \qquad \sigma = \sum_{d|n} d$$

sono moltiplicative per il Teorema 2.1.

La moltiplicatività di una funzione consente di deternminarne i valori a partire da quelli che assume sulle potenze dei numeri primi. Infatti, se f è una funzione moltiplicativa, e $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ dove i p_i sono primi distinti e gli α_i interi maggiori o uguali a 1, allora chiaramente

$$f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_k}) \ .$$

Ad esempio, se p è un primo e $\alpha \in \mathbb{N}^*$, allora si osserva che

$$\tau(p^\alpha) = 1 + \alpha \quad \text{ e } \quad \sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1} \ .$$

Possiamo dunque concludere con la seguente

Proposizione 2.2 *Sia $n \in \mathbb{N}^*$, e sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la fattorizzazione in primi di n; allora*

$$\tau(n) = \prod_{i=1}^{k} (1 + \alpha_i) \quad \text{ e } \quad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \ .$$

Esercizi. 1. Siano f e g funzioni moltiplicative (a valori in $\mathbb{C}$). Si provi che la funzione $f * h$ definita da

$$(f * h)(n) = \sum_{d|n} f(d) g(n/d)$$

è moltiplicativa. Si dimostri quindi che l'operazione $*$ (detta prodotto di convoluzione) è un'operazione associativa e commutativa nell'insieme delle funzioni moltiplicative a valori in $\mathbb{C}$.

2. Si provi che per ogni $n \geq 1$

$$\sum_{d|n} \tau^3(d) = \left(\sum_{d|n} \tau(d) \right)^2$$

3. Si provi che per ogni $n \geq 1$

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

4. Provare che se $\sigma(n)$ è dispari, allora $n = a^2$ oppure $n = 2a^2$, per qualche $a \in \mathbb{N}$.

5. (Olimpiadi Matematiche 1998) Sia $k \in \mathbb{N}^*$. Provare che esiste $n \in \mathbb{N}$ tale che

$$\frac{\tau(n^2)}{\tau(n)} = k$$

se e solo se k è dispari.

2.2 Numeri perfetti

Un numero $n \in \mathbb{N}^*$ si dice *perfetto* se è uguale alla somma dei suoi divisori diversi da sé. In altri termini, n è perfetto se e solo se $2n = \sigma(n)$.

Teorema 2.3 *Un numero pari n è perfetto se e solo se $n = 2^{p-1}(2^p - 1)$, dove p e $2^p - 1$ sono primi.*

Dimostrazione. Supponiamo prima che $n = 2^{p-1}(2^p - 1)$, con p e $2^p - 1$ numeri primi. Allora

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = 2n$$

e dunque n è perfetto.
Viceversa, sia n un numero perfetto pari. Allora $n = 2^{k-1}m$ con $k \geq 2$ e m dispari. Inoltre

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m) \ .$$

Quindi, $2^k - 1$ divide m. Sia $m = (2^k - 1)m'$; allora

$$\sigma(m) = \frac{2^k m}{2^k - 1} = 2^k m' \ .$$

Poichè m e m' sono distinti e dividono entrambi m si ha

$$\sigma(m) \geq m + m' = (2^k - 1)m' + m' = 2^k m' = \sigma(m)$$

da cui $m' = 1$. Quindi m è primo e $m = 2^p - 1$ per qualche primo p. ∎

Il Teorema precedente (parzialmente già noto ai matematici greci, e provato definitivamente da Eulero) riconduce quindi la descrizione dei numeri perfetti pari alla determinazione dei primi di Mersenne. In particolare se il numero di primi di Mersenne è finito, allora i numeri perfetti pari sono finiti. Il problema dell'esistenza di numeri perfetti dispari è invece tuttora aperto, anche se la congettura prevalente è che non ve ne siano (una cosa nota è che se esiste un numero perfetto dispari, esso deve avere almeno sette divisori primi distinti).

Esercizio 7. Si provi che l'ultima cifra dello sviluppo decimale di un numero perfetto pari è 6 o 8.

Esercizio 8. Si provi che se n è un numero perfetto dispari, allora n è diviso da almeno 3 primi distinti.

Esercizio 9. Fissato un intero $k \geq 2$, si dice che n è k-perfetto se $\sigma(n) = kn$. Si determinino tutti i numeri naturali n che sono 3-perfetti, con $1 \leq n \leq 150$.

Nel seguito di queste note, adotteremo la seguente convenzione. Se f è una funzione definita su $\mathbb{N}^*$, e $x \in \mathbb{R}$ un numero reale positivo, scriviamo

$$\sum_{i \leq x} f(i) = \sum_{i=1}^{[x]} f(i) \ .$$

Dove $[x]$ denota la *parte intera* di x, ovvero il massimo numero intero minore od uguale a x. Il Lemma seguente, la cui dimostrazione lascio per esercizio, riporta alcune proprietà elementari della parte intera.

Lemma 2.4 *Siano $x, y \in \mathbb{R}$. Allora*

1) $x - 1 \leq [x] < [x] + 1$*;*

2) $[x] + [y] \leq [x + y]$*;*

3) $|\{n \in \mathbb{N} \mid x < n \leq y\}| = [y] - [x]$.

Il seguente principio è spesso utile per derivare sommatorie più maneggevoli. Lo useremo qualche volta nel seguito anche senza richiamarlo esplicitamente.

Lemma 2.5 (Divisor Sum Identity) *Siano $f, g : \mathbb{N}^* \to \mathbb{C}$ funzioni aritmetiche. Allora per ogni $1 \leq x \in \mathbb{R}$,*

$$\sum_{i \leq x} f(i) \left(\sum_{d \mid i} g(d) \right) = \sum_{d \leq x} \left(g(d) \sum_{j \leq x/d} f(dj) \right) \ .$$

DIMOSTRAZIONE. Esercizio. ∎

Lemma 2.6 *Sia f una funzione aritmetica, e sia $F(n) = \sum_{d \mid n} f(d)$. Allora, per ogni $1 \leq x \in \mathbb{R}$,*

$$\sum_{i \leq x} F(i) = \sum_{i \leq x} \left[\frac{x}{i} \right] f(i) \ .$$

DIMOSTRAZIONE. Fissato $1 \leq x \in \mathbb{R}$, si ha, per la definizione di $F(i)$,

$$\sum_{i \leq x} F(i) = \sum_{i \leq x} \sum_{d|i} F(d) = \sum_{i \leq x} 1 \cdot \left(\sum_{d|i} F(d) \right) ,$$

e quindi, applicando il Lemma 2.5,

$$\sum_{i \leq x} F(i) = \sum_{d \leq x} \left(f(d) \sum_{j \leq x/d} 1 \right) = \sum_{d \leq x} \left[\frac{x}{d} \right] f(d) .$$

■

2.3 La funzione di Möbius

La *funzione di Möbius* classica è l'applicazione $\mu : \mathbb{N} \longrightarrow \{0, 1, -1\} \subset \mathbb{Z}$, definita nel modo seguente

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se esiste un primo } p \text{ tale che } p^2 | n \\ (-1)^s & \text{se } n = p_1 p_2 \dots p_s \text{ con i } p_i \text{ primi distinti} \end{cases}$$

La funzione di Möbius può essere generalizzata in modo da venire definita per insiemi parzialmente ordinati; quella che abbiamo esposto è la versione classica (in cui l'insieme parzialmente ordinato è $\mathbb{N}^*$ con la relazione di divisibilità.
Chiaramente μ è una funzione moltiplicativa. Inoltre si ha

Lemma 2.7

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & se \quad n = 1 \\ 0 & se \quad n > 1 \end{cases}$$

DIMOSTRAZIONE. Poniamo $\Delta(n) = \sum_{d|n} \mu(d)$. Allora Δ è moltiplicativa per il Teorema 2.1, e $\Delta(1) = 1$. Sia p un numero primo, e $a \geq 1$; allora

$$\Delta(p^a) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^a) = \mu(1) + \mu(p) = 1 - 1 = 0 ;$$

poichè Δ è moltiplicativa, si conclude che, se $n > 1$, $\Delta(n) = 0$. ■

L'importanza della funzione di Möbius risiede principalmente nella **Formula di Inversione di Möbius** che è il contenuto del prossimo Teorema.

Teorema 2.8 *Sia $f : \mathbb{N}^* \to A$ una funzione aritmetica, e per ogni $n \in \mathbb{N}$ definiamo $F(n) = \sum_{d|n} f(d)$. Allora, per ogni $n \in \mathbb{N}^*$*

$$f(n) = \sum_{d|n} \mu(n/d) F(d) = \sum_{d|n} \mu(d) F(n/d) .$$

DIMOSTRAZIONE. Sia $n \in \mathbb{N}^*$. Allora

$$\sum_{d|n} \mu(d)F(n/d) = \sum_{du=n} \mu(d)F(u) = \sum_{du=n} \left(\mu(d) \sum_{t|u} f(t) \right) = \sum_{dt|n} \mu(d)f(t)$$

e, applicando quindi il Lemma 2.7

$$\sum_{d|n} \mu(d)F(n/d) = \sum_{t|n} f(t) \cdot \sum_{d|n/t} \mu(d) = f(n) \ .$$

L'altra uguaglianza nell'enunciato è ovvia. ∎

Come primo esempio di applicazione di questa formula, vediamo come si possa invertire il Teorema 2.1.

Teorema 2.9 *Sia f una funzione aritmetica tale che la funzione F definita da $F(n) = \sum_{d|n} f(d)$ è moltiplicativa. Allora f è moltiplicativa.*

DIMOSTRAZIONE. Siano $n, m \in \mathbb{N}^*$ con $(n, m) = 1$. Tendendo conto che F e μ sono moltiplicative, ed applicando la formula di inversione di Möbius, si ha

$$f(mn) = \sum_{d|m,\, t|n} \mu\left(\frac{mn}{dt}\right) F(dt) = \sum_{d|m,\, t|n} F(d)\mu(m/d)F(t)\mu(n/t) =$$

$$= \sum_{d|m} F(d)\mu(m/d) \cdot \sum_{t|n} F(t)\mu(n/t) = f(m)f(n)$$

e dunque f è moltiplicativa. ∎

Esercizio 10. Si dimostrino le seguenti proprietà della funzione di Möbius

1) $\sum_{d^2|n} \mu(d) = |\mu(n)|$

2) $\sum_{i \le n} \mu(i)[n/i] = 1$ e quindi $\left| \sum_{i \le n} (\mu(i)/i) \right| \le 1$.

Esercizio 11. (La funzione λ di Liouville). Dato $n \in \mathbb{N}^*$, poniamo $\nu(1) = 0$, e per $n > 1$, $\nu(n)$ uguale al numero di fattori primi (non necessariamente distinti) di n (ad esempio, $\nu(24) = 4$). La funzione λ di Liouville è definita da

$$\lambda(n) = (-1)^{\nu(n)} \ .$$

Si provi che λ è moltiplicativa, e che per ogni $n \in \mathbb{N}^*$,

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ è un quadrato} \\ 0 & \text{altrimenti} \end{cases}$$

Esercizio 12. Si provi che per ogni $n \in \mathbb{N}^*$,

$$\sum_{d|n} |\mu(d)| = 2^{\nu(n)} \ .$$

2.4 La funzione di Eulero

Dato $n \in \mathbb{N}^*$, si indica con $\phi(n)$ il numero di interi compresi tra 1 e n che sono coprimi con n. La funzione ϕ così definita si chiama *funzione di Eulero*. Riscrivendo la definizione

$$\phi(n) = |\{a \in \mathbb{N} \ ; \ 1 \leq a \leq n \ \text{ e } \ (a,n) = 1\}| \ .$$

Lemma 2.10 *Per ogmi* $n \in \mathbb{N}^*$

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

Dimostrazione. Poniamo $A = \{1, 2, \ldots, n\}$ e $\Delta_n = \{1 \leq d \leq n \ ; \ d|n\}$. Definiamo una applicazione $c : A \to \Delta_n$ ponendo, per ogni $a \in A$, $c(a) = (a, n)$. Allora, chiaramente

$$n = \sum_{d|n} |c^{-1}(d)| \ .$$

D'altra parte, per ogni $d \in \Delta_n$,

$$|c^{-1}(d)| = |\{a \in A \ ; \ (a,n) = d\}| = |\{1 \leq a \leq n/d \ ; \ (a, n/d) = 1\}| = \phi(n/d) \ .$$

Dunque

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(d/n) = \sum_{d|n} |c^{-1}(d)| = n \ .$$

■

Teorema 2.11 *La funzione* ϕ *di Eulero è moltiplicativa. Inoltre, per ogni* $n \in \mathbb{N}^*$ *si ha*

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

Dimostrazione. La prima affermazione discende immediatamente dal Teorema 2.9, poichè la funzione $n = \sum_{d|n} \phi(d)$ è ovviamente moltiplicativa.
La seconda affermazione è un'altra facile applicazione della formula di inversione di Möbius all'uguaglianza del Lemma 2.10; infatti da queste si ha, per ogni $n \in \mathbb{N}^*$

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

■

La moltiplicatività della funzione di Eulero consente di determinarne i valori. Innanzi tutto supponiamo che $n = p^\alpha$ sia la potenza di un numero primo. Allora, per ogni $a \in \mathbb{N}^*$, $(a, n) = 1$ se e solo se $(a, p) = 1$; ora i multipli di p compresi tra 1 e p^α sono in numero di $p^{\alpha-1}$, e quindi

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) \ = p^\alpha \left(1 - \frac{1}{p}\right) \ .$$

Ne segue che se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ è la fattorizzazione in potenze di primi distinti di n, allora

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \ .$$

Osserviamo che, se p è un primo, il valore di ϕ in p^α si può anche ricavare immediatamente dall'uguaglianza del Teorema 2.11; infatti da questa si ha

$$\phi(p^\alpha) = p^\alpha \sum_{i=0}^{\alpha} \frac{\mu(p^i)}{p^i} = p^\alpha \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p}\right) = p^\alpha \left(1 - \frac{1}{p}\right) \ .$$

Eserciziof 13. Si provi che, per ogni $n \geq 2$,

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

dove p varia nell'insieme dei numeri primi che dividono n.

Esercizio 14. Si provi che, per ogni $n \geq 2$,

$$\sum_{i \leq n,\, (i,n)=1} i = \frac{1}{2} n \phi(n) \ .$$

Esercizio 15. Si provi che la disuguaglianza $\phi(x) \geq x - \sqrt{x}$ ha come sole soluzioni intere i numeri p e p^2, con p primo.

Esercizio 16. Si provi che, per ogni $n \in \mathbb{N}^*$,

$$\sum_{d=1}^{n} \phi(d) \left[\frac{n}{d}\right] = \frac{n(n+1)}{2} \ .$$

Esercizio 17. Per ogni $n \in \mathbb{N}^*$ sia $F(n) = \sum_{i \leq n}(n, i)$.

1) Si provi che $F(n)$ è una funzione moltiplicativa.
2) Per $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ si dia una esplicita espressione di $F(n)$.
3) Si provi che, per ogni $n \in \mathbb{N}^*$,

$$\phi(n) = \sum_{d|n} \mu(d) F(n/d) d.$$

4) Si provi che, per ogni $n \in \mathbb{N}^*$,

$$n\tau(n) = \sum_{d|n} F(d).$$

2.5 Media di $\tau(n)$

Se $n \in \mathbb{N}^*$, allora $1 \leq \tau(n) \leq n$, ma, in generale, il valore $\tau(n)$ è molto inferiore a n; in altri termini, la funzione $\max\{\tau(i) \mid 1 \leq i \leq n\}$ cresce lentamente. Ad esempio, si può verificare che per $n \leq 10^7$, $\tau(n) \leq 448$. D'altra parte, il comportamento di $\tau(n)$ è estremamante irregolare; così , ad esempio, se $n = 8.648.640$ allora $\tau(n-1) = 4$, $\tau(n) = 448$, $\tau(n+1) = 8$. Ci proponiamo allora di studiare la media di $\tau(n)$, ovvero la funzione definita per $1 \leq x \in \mathbb{R}$,

$$T(x) = \frac{1}{x} \sum_{i \leq x} \tau(i) \ .$$

Allo studio della media di τ, premettiamo alcune osservazioni che ci saranno utili. Considerando lo sviluppo in serie di e^x si ha che, per ogni $x > 0$, $e^x > 1 + x$. In particolare, per ogni $1 < x \in \mathbb{R}$,

$$\frac{1}{x} - \frac{1}{x^2} < \log \frac{x+1}{x} < \frac{1}{x} \ .$$

Per ogni intero $n \geq 1$ definiamo

$$\sigma_n = \frac{1}{n} - \log \frac{n+1}{n} = \frac{1}{n} - \int_n^{n+1} \frac{dt}{t} \ .$$

Per quanto osservato sopra, $0 < \sigma_n < \frac{1}{n^2}$; quindi la serie $\sum_{n=1}^{\infty} \sigma_n$ è maggiorata dalla serie convergente $\sum_{n=1}^{\infty} \frac{1}{n^2}$ che è convergente. Dunque esiste finita la somma

$$\gamma = \sum_{n=1}^{\infty} \sigma_n \ .$$

γ è chiamata costante di *Eulero - Mascheroni* e indicativamente il suo valore è $\gamma = 0,56\ldots$ Un altro modo per definirla (lo si verifichi per esercizio) è il seguente; per ogni $n \in \mathbb{N}^*$ sia γ_n definito da

$$\gamma_n + \log n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

allora

$$\gamma = \lim_{n \to \infty} \gamma_n \ .$$

(Un problema classico ancora aperto è stabilire se γ sia razionale o irrazionale).

Facciamo un'altra osservazione sulle serie. Sia $n \in \mathbb{N}^*$, allora

$$\sum_{i=n}^{\infty} \frac{1}{i(i+1)} = \sum_{i=0}^{\infty} \frac{1}{i(i+1)} - \sum_{i=0}^{n-1} \frac{1}{i(i+1)} = 1 - \frac{n-1}{n} = \frac{1}{n} \ .$$

Lemma 2.12 *Sia $1 \leq x \in \mathbb{R}$. Allora*

$$\sum_{i \leq x} \frac{1}{i} = \log x + \gamma + K(x)$$

dove $|K(x)| \leq 4/x$ (e $|K(n)| \leq 2/n$ se n è un intero).

DIMOSTRAZIONE. Supponiamo prima $x = n \in \mathbb{N}^*$. Utilizzando le notazioni introdotte precedentemente,

$$\log(n+1) = \int_1^{n+1} \frac{dt}{t} = \sum_{i=1}^{n} \left(\frac{1}{i} - \sigma_i \right) .$$

Quindi

$$\sum_{i=1}^{n} \frac{1}{i} = \log(n+1) + \sum_{i=1}^{n} \sigma_i = \log n + \gamma + K(n)$$

dove

$$K(n) = \log(n+1) - \log n - \sum_{i>n} \sigma_i = \log \frac{n+1}{n} - \sum_{i>n} \sigma_i \ .$$

Per quanto osservato sopra abbiamo

$$|K(n)| \leq \frac{1}{n} + \sum_{i>n} \frac{1}{i^2} \leq \frac{1}{n} + \sum_{i \geq n} \frac{1}{i(i+1)} = \frac{2}{n} \ .$$

Supponiamo ora x reale con $x > 1$. Allora

$$\sum_{i \leq x} \frac{1}{i} = \sum_{i \leq [x]} \frac{1}{i} = \log[x] + \gamma + K([x]) = \log x + \gamma + K(x)$$

dove $K(x) = K([x]) + \log[x] - \log x$; e dunque,

$$|K(x)| \leq \frac{2}{[x]} + \log \frac{x}{[x]} \leq \frac{2}{x-1} + \frac{1}{x-1} \leq \frac{2}{x-1} + \log \frac{x}{x-1} \leq \frac{3}{x-1} \leq \frac{4}{x}$$

dove l'ultima diseguaglianza vale per $x \geq 4$. D'altra parte, per $1 \leq x < 4$ l'identità nell'enunciato si verifica direttamente, completando la dimostrazione. ∎

Teorema 2.13 *Per ogni* $1 \leq x \in \mathbb{R}$*,*

$$\sum_{i \leq x} \tau(i) = x \log x + (2\gamma - 1)x + R(x)$$

dove $|R(x)| \leq 12\sqrt{x}$*.*

DIMOSTRAZIONE. Poichè $\tau(i) = \sum_{d|i} 1$, per il Lemma 2.5 possiamo scrivere

$$\sum_{i \leq x} \tau(i) = \sum_{i \leq x} \sum_{d|i} 1 = \sum_{d \leq x} \sum_{j \leq x/d} 1$$

dunque $\sum_{i \leq x} \tau(i)$ non è altro che il numero di coppie ordinate (d, j) di interi positivi e non nulli tali che $dj \leq x$. Denotiamo con D tale insieme di coppie, e poniamo

$$D_1 = \{(d,j) \in D \mid d \leq \sqrt{x}\}, \quad D_2 = \{(d,j) \in D \mid j \leq \sqrt{x}\} \ .$$

Allora chiaramente $|D_1| = |D_2|$ e quindi

$$|D| = |D_1| + |D_2| - |D_1 \cap D_2| = 2|D_1| - |D_1 \cap D_2| \ ;$$

Poichè $D_1 \cap D_2 = \{(d, j) \in D \mid d \leq \sqrt{x},\ j \leq \sqrt{x}\}$, questa uguaglianza di cardinalità si scrive

$$\sum_{i \leq x} \tau(i) = 2 \sum_{d \leq \sqrt{x}} \sum_{j \leq x/d} 1 - \sum_{d \leq \sqrt{x}} \sum_{j \leq \sqrt{x}} 1 = 2 \sum_{d \leq \sqrt{x}} \left[\frac{x}{d}\right] - [\sqrt{x}]^2.$$

Ora, per ogni $d \leq x$ sia

$$R_d = \left[\frac{x}{d}\right] - \frac{x}{d}$$

(allora $|R_d| < 1$). Inoltre sia $U = x - [\sqrt{x}]^2$, allora $U \leq x - (\sqrt{x} - 1)^2 < 2\sqrt{x}$. Scriviamo quindi

$$\sum_{i \leq x} \tau(i) = 2 \sum_{d \leq \sqrt{x}} \frac{x}{d} + 2 \sum_{d \leq \sqrt{x}} R_d - [\sqrt{x}]^2 = 2x \sum_{d \leq \sqrt{x}} \frac{1}{d} - x + U + 2 \sum_{d \leq \sqrt{x}} R_d;$$

e, applicando il Lemma 2.12, otteniamo

$$\sum_{i \leq x} \tau(i) = 2x \log \sqrt{x} + 2x\gamma - x + R(x) = x \log x + (2\gamma - 1)x + R(x)$$

dove

$$R(x) = 2xK(\sqrt{x}) + U + 2 \sum_{d \leq \sqrt{x}} R_d.$$

Per completare la dimostrazione occorre ora valutare il valore assoluto di $R(x)$. Per le osservazioni fatte sopra, e nel Lemma 2.12, abbiamo

$$|R(x)| \leq 2x \cdot \frac{4}{\sqrt{x}} + 2\sqrt{x} + 2\sqrt{x} \leq 12\sqrt{x}$$

e la dimostrazione è completa. ∎

Siano $f(x)$ e $g(x)$ funzioni reali a variabile reale; scriviamo

$$f(x) = O(g(x))$$

(e leggiamo f è *o-grande* g) se esiste una costante C ed un numero reale x_0 tali che

$$|f(x)| \leq C|g(x)| \quad \text{per ogni } x \geq x_0 \ .$$

Se $g(x)$ è una funzione nota, la notazione $O(g(x))$, da sola, rappresenta una funzione $f(x)$, che soddisfa $f(x) = O(g(x))$.
Ad esempio, con tale convenzione possiamo riscrivere l'enunciato del Teorema 2.13 come

$$\sum_{i \leq x} \tau(i) = x \log x + (2\gamma - 1)x + O(\sqrt{x})$$

Questa è una maniera di esprimere il comportamento asintotico di una funzione che è più frequente, ed anche più semplice da manipolare, piuttosto che scrivere direttamente un termine residuo ed una sua stima precisa, come invece abbiamo fatto nel Teorema 2.13.

Esercizio 18. Definiamo l'intero $\tau_2(n)$ come il numero di divisori di n che sono potenza di 2 ($2^0 = 1$ incluso). Quindi, per ogni $n \in \mathbb{N}^*$, $n = 2^{\tau_2(n)-1}m$ dove m è un numero primo (si osservi che τ_2 è una funzione moltiplicativa). Si provi che, per $1 \leq x \in \mathbb{R}$,

$$\sum_{i \leq x} \tau_2(i) = 2x + O(log_2 x) \ .$$

Si concluda che

$$\lim_{x \to \infty} \frac{1}{x} \sum_{i \leq x} \tau_2(i) = 2 \ .$$

[sugg. : si dimostri, procedendo per induzione, che se $2 \leq n \in \mathbb{N}^*$, allora $\sum_{i \leq n} \tau_2(i) = 2n + R(n)$, dove $|R(n)| \leq 1 + log_2 n$. Si passi quindi al caso generale.]

2.6 Media di $\phi(n)$

La funzione **Zeta di Riemann** ζ è definita per numeri complessi z tali che $Re(z) > 1$ da

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} \ .$$

Si tratta di una funzione estremamente importante in teoria dei numeri ed in altri settori della matematica. Ad esempio, L. Eulero ha dimostrato (chiaramente prima degli studi di B. Riemann) che, se $\mathbb{P}$ è l'insieme di tutti i numeri primi positivi, allora

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \ .$$

In questo paragrafo, siamo interessati al valore che essa assume in 2, che riporto senza, per il momento, fornire una dimostrazione.

Lemma 2.14

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \ .$$

DIMOSTRAZIONE. Vedi Appendice I. ∎

Lemma 2.15 *Se* $1 < s \in \mathbb{R}$, *allora*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \ .$$

DIMOSTRAZIONE. Poichè $s > 1$ la serie $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ è assolutamente convergente. Quindi

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \left(\sum_{m=1}^{\infty} \frac{1}{m^s} \right) \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right) = \sum_{m,n=1}^{\infty} \frac{\mu(n)}{(mn)^s} \ ;$$

ponendo $i = mn$ e ricordando il Lemma 2.7, possiamo scrivere

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{i=1}^{\infty} \left(\frac{1}{i^s} \sum_{d|i} \mu(d) \right) = 1$$

che è quello che si voleva. ■

Lemma 2.16

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} \ .$$

DIMOSTRAZIONE. L'ugualglianza discende immediatamente dai due Lemmi precedenti. ■

Vogliamo ora descrivere il comportamento (asintotico) della media della funzione ϕ di Eulero, ovvero dei valori $\frac{1}{n} \sum_{i \leq n} \phi(i)$. Chiaramente, possiamo studiare la funzione $\sum_{i \leq x} \phi(i)$, dove $1 \leq x \in \mathbb{R}$.

Teorema 2.17 *Per ogni* $1 \leq x \in \mathbb{R}$,

$$\sum_{i \leq x} \phi(i) = \frac{3x^2}{\pi^2} + R(x)$$

dove $|R(x)| \leq x + x \log(x+1)$.

DIMOSTRAZIONE. Per il Teorema 2.11, $\sum_{i \leq x} \phi(i) = \sum_{i \leq x} \left(i \cdot \sum_{d|i} \frac{\mu(d)}{d} \right)$; abbiamo quindi

$$\sum_{i \leq x} \phi(i) = \sum_{d \leq x} \frac{\mu(d)}{d} \sum_{i \leq x/d} di = \sum_{d \leq x} \left(\mu(d) \sum_{i \leq x/d} i \right) \ .$$

Ricordando che, per ogni $k \in \mathbb{N}^*$, $\sum_{i \leq k} i = k(k+1)/2$, si ha

$$\sum_{i \leq x} \phi(i) = \sum_{d \leq x} \frac{\mu(d)}{2} \left[\frac{x}{d} \right] \left(\left[\frac{x}{d} \right] + 1) \right) \ .$$

Ora, per ogni $d \leq x$,

$$\frac{x}{d} - 1 < \left[\frac{x}{d} \right] \leq \frac{x}{d}$$

quindi

$$\left(\frac{x}{d} \right)^2 - \frac{x}{d} = \left(\frac{x}{d} - 1 \right) \frac{x}{d} < \left[\frac{x}{d} \right] \left(\left[\frac{x}{d} \right] + 1 \right) \leq \frac{x}{d} \left(\frac{x}{d} + 1 \right) = \left(\frac{x}{d} \right)^2 + \frac{x}{d}$$

e quindi

$$\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right)=\left(\frac{x}{d}\right)^2+R_d$$

dove $R_d = R(x,d)$ è tale che

$$|R_d| \leq \frac{x}{d} \ .$$

Ritornando alla uguaglianza di sopra, si ha

$$\begin{aligned}\textstyle\sum_{i\leq x}\phi(i) &= \tfrac{1}{2}\textstyle\sum_{d\leq x}\mu(d)\left(\tfrac{x}{d}\right)+\tfrac{1}{2}\textstyle\sum_{d\leq x}\mu(d)R_d = \\ &= \tfrac{x^2}{2}\textstyle\sum_{d\leq x}\tfrac{\mu(d)}{d^2}+\tfrac{1}{2}\textstyle\sum_{d\leq x}\mu(d)R_d = \\ &= \tfrac{x^2}{2}\textstyle\sum_{d=1}^{\infty}\tfrac{\mu(d)}{d^2}+R(x)\end{aligned}$$

dove

$$R(x) = -\frac{x^2}{2}\sum_{d>x}\frac{\mu(d)}{d^2}+\frac{1}{2}\sum_{d\leq x}\mu(d)R_d \ .$$

Applicando il Lemma 2.16 si ha quindi

$$\sum_{i\leq x}\phi(i) = \frac{3x^2}{\pi^2}+R(x) \ .$$

Rimane da verificare la limitazione in modulo per $R(x)$. Osserviamo innanzi tutto il seguente fatto; per ogni $1 \leq x \in \mathbb{R}$,

$$\sum_{d\leq x}\frac{1}{d} \leq 1+\int_1^x\frac{dt}{t} = 1+\log(x+1) \ .$$

Ancora, si ha

$$\sum_{d>x}\frac{1}{d^2} \leq \frac{1}{x-1} \ .$$

Applicando queste disuguaglianze alla stima per $|R(x)|$, tenendo conto che, per ogni $n \in \mathbb{N}^*$, $|\mu(n)| \leq 1$, si ottiene (per $x \geq 2$)

$$|R(x)| \leq \frac{x^2}{2}\sum_{d>x}\frac{1}{d^2}+\frac{1}{2}\sum_{d\leq x}|R_d| \leq \frac{x^2}{2}\frac{1}{x-1}+\frac{x}{2}\sum_{d\leq x}\frac{1}{d} \leq x+x\log(x+1) \ .$$

La dimostrazione è completa. ■

Utilizzando la notazione con gli infiniti, possiamo dunque scrivere

$$\sum_{i\leq x}\phi(i) = \frac{3x^2}{\pi^2}+O(x\log x) \ .$$

Esercizio 19. Si descriva il comportamento (asintotico) della funzione

$$\sum_{i\leq n} \frac{\phi(i)}{i}.$$

Esercizio 20. Si provi che

$$\sum_{i\leq x} \frac{\sigma(i)}{i} = \frac{\pi^2}{6}x + O(\log x)\ .$$

Concludiamo questo capitolo con una interessante applicazione del Teorema 2.17

Corollario 2.18 *La probabilità che due interi positivi siano coprimi è* $6/\pi^2$.

DIMOSTRAZIONE. Fissato un $n \in \mathbb{N}^*$, il numero di coppie di interi (r, s) tali che $1 \leq r \leq s \leq n$ è $n(n+1)/2$. Il numero di tali coppie che sono costituite da numeri coprimi, è chiaramente $\sum_{i\leq x} \phi(i)$. Quindi, denotata con $P(n)$ la probabilità che due numeri interi minori di n siano coprimi, si ha

$$P(n) = \frac{2}{n(n+1)} \sum_{i\leq n} \phi(i)\ .$$

La probabilità che due interi positivi qualsiasi siano coprimi è

$$P = \lim_{n\to\infty} P(n) = \lim_{n\to\infty} \frac{2}{n(n+1)} \sum_{i\leq n} \phi(i)$$

per cui, applicando il Teorema precedente, si ha

$$P = \lim_{n\to\infty} \frac{6n^2}{\pi^2 n^2} = \frac{6}{\pi^2}\ .$$

■

2.7 Appendice I: dimostrazione che $\zeta(2) = \frac{\pi^2}{6}$.

[J. Hofbauer. American Mathematical Monthly 109 (2002)]

Ricordando che $\sin x = 2\sin\frac{x}{2}\cos\frac{x}{2}$, si ottiene la seguente identità,

$$\frac{1}{\sin^2 x} = \frac{1}{4\sin^2\frac{x}{2}\cos^2\frac{x}{2}} = \frac{1}{4}\left[\frac{1}{\sin^2\frac{x}{2}} + \frac{1}{\cos^2\frac{x}{2}}\right] = \frac{1}{4}\left[\frac{1}{\sin^2\frac{x}{2}} + \frac{1}{\sin^2\frac{\pi+x}{2}}\right].$$

In particolare

$$1 = \frac{1}{\sin^2\frac{\pi}{2}} = \frac{1}{4}\left[\frac{1}{\sin^2\frac{\pi}{4}} + \frac{1}{\sin^2\frac{3\pi}{4}}\right].$$

Applicando ripetutamente questa uguaglianza si prova (facendo induzione su n) che, per ogni $n \geq 2$,

$$1 = \frac{1}{4^n} \sum_{k=0}^{2^n-1} \frac{1}{\sin^2 \frac{(2k+1)\pi}{2^{n+1}}} = \frac{2}{4^n} \sum_{k=0}^{2^{n-1}-1} \frac{1}{\sin^2 \frac{(2k+1)\pi}{2^{n+1}}}.$$

Ora, per $0 < x < \pi/2$, si ha $\sin x < x < \tan x$, e quindi

$$\frac{1}{\sin^2 x} > \frac{1}{x^2} > \frac{1}{\tan^2 x} = \frac{1}{\sin^2 x} - 1.$$

Ponendo $N = 2^n$, e $x = (2k+1)\pi/2N$ (con $k = 0, 1, \ldots, N/2-1$), dalla identità di sopra segue

$$1 > \frac{8}{\pi^2} \sum_{k=0}^{N/2-1} \frac{1}{(2k+1)^2} > 1 - \frac{1}{N}.$$

Passando al limite per $n \to \infty$ si ottiene,

$$1 = \frac{8}{\pi^2} \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2}.$$

Da tale identità segue quella per $\zeta(2)$. Infatti

$$\zeta(2) = \sum_{i=1}^{\infty} \frac{1}{i^2} = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2} + \sum_{k=1}^{\infty} \frac{1}{(2k)^2} = \frac{\pi^2}{8} + \frac{1}{4}\zeta(2),$$

e quindi $\zeta(2) = \pi^2/6$.

Soluzione di alcuni esercizi.

Esercizio 2. Sia $1 \leq k \in \mathbb{N}$. Per induzione su k si dimostra che

$$\sum_{i=1}^{k} i^3 = \left(\sum_{i=1}^{k} i \right)^2 = \left(\frac{k(k+1)}{2} \right)^2.$$

Ora, le funzioni f, g date da

$$f(n) = \left(\sum_{d|n} \tau(d) \right)^2 \qquad g(n) = \sum_{d|n} \tau(d)^3$$

sono moltiplicative. Dunque è sufficiente provare l'asserto dell'esercizio per $n = p^k$ dove p è un numero primo. Utilizzando l'uguaglianza ricordata sopra, si ha in questo caso

$$f(p^k) = \left(\sum_{i=0}^{k} \tau(p^i)\right)^2 = \left(\sum_{i=0}^{k} (i+1)\right)^2 = \left(\sum_{i=1}^{k+1} i\right)^2 = \sum_{i=1}^{k+1} i^3 = \sum_{i=0}^{k} (i+1)^3 = g(p^k) \ .$$

Esercizio 3. Sia $n \in \mathbb{N}^*$; allora

$$n^{\tau(n)} = \prod_{d|n} n = \prod_{d|n} d\frac{n}{d} = \prod_{d|n} d \cdot \prod_{d|n} \frac{n}{d} = \left(\prod_{d|n} d\right)^2$$

per cui

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}} \ .$$

Esercizio 8. Sia $n = p^a q^b$ un numero dispari, con p e q primi distinti. Supponiamo, per assurdo, che n sia perfetto. Allora

$$\frac{p^{a+1}-1}{p-1} \cdot \frac{q^{b+1}-1}{q-1} = \sigma(n) = 2n = 2p^a q^b$$

e quindi, in particolare,

$$2p^a q^b < \frac{p^{a+1} q^{b+1}}{(p-1)(q-1)}$$

da cui segue l'assurdo

$$2 < \frac{p}{p-1} \cdot \frac{q}{q-1} \leq \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8}.$$

Esercizio 10. 1) Se $n = 1$ l'affermazione è ovvia. Se n è un prodotto di primi distinti, allora

$$\sum_{d^2|n} \mu(d) = \mu(1) = 1 = |\mu(n)| \ .$$

Se invece esiste un primo p tale che $p^2|n$, posto e il massimo intero positivo tale che $e^2|n$, si ha $e > 1$, e per il Lemma 2.7,

$$\sum_{d^2|n} \mu(d) = \sum_{d|e} \mu(d) = 0 = \mu(n) \ .$$

2) Per il Lemma 2.6,

$$\sum_{i \leq n} \mu(i)[n/i] = \sum_{i \leq x} F(i)$$

dove $F(i) = \sum_{d|n} \mu(d)$. Ma allora, per il Lemma 2.7,

$$\sum_{i \leq n} \mu(i)[n/i] = F(1) = 1 \ .$$

Ora, per ogni $1 \le i \le n$, $\frac{n}{i} = \left[\frac{n}{i}\right] + \epsilon_i$, con $0 \le \epsilon_i < 1$. Quindi

$$n\left|\sum_{i\le n}\frac{\mu(i)}{i}\right| = \left|\sum_{i\le n}\frac{n}{i}\mu(i)\right| \le \left|\sum_{i\le n}\left[\frac{n}{i}\right]\mu(i)\right| + \sum_{i=1}^{n-1}\epsilon_i|\mu(i)| \le 1 + (n-1) = n$$

da cui $\left|\sum_{i\le n}\frac{\mu(i)}{i}\right| \le 1$.

Esercizio 14. Se $n = 2$ l'affermazione è banale.
Sia quindi $n \ge 3$ e poniamo $D = \{1 \le i \le n \mid (i, n) = 1\}$. Si osservi che $i \in D$ se e solo se $n - i \in D$. Inoltre, poiché $n \ge 3$, $n - i \ne i$ per ogni $i \in D$. Pertanto,

$$\sum_{i\in D} i = \sum_{i\in D, i<n/2} i + (n-i) = \sum_{i\in D, i<n/2} n = \frac{1}{2}\phi(n)n\ .$$

Esercizio 20. Sia $F(x) = \sum_{i\le x}\frac{\sigma(i)}{i}$. Applicando la definizione di $\sigma(i)$ ed il Lemma 2.5, si ha

$$F(x) = \sum_{i\le x}\frac{1}{i}\sum_{d|i} d = \sum_{d\le x} d\sum_{j\le x/d}\frac{1}{dj} = \sum_{d\le x}\sum_{j\le x/d}\frac{1}{j} = \sum_{d\le x}\left[\frac{x}{d}\right]\frac{1}{d}.$$

Per ogni $d \le x$, poniamo $[x/d] = x/d + R_d$. Allora

$$F(x) = x\sum_{d\le x}\frac{1}{d^2} + \sum_{d\le x}\frac{R_d}{d} = x\zeta(2) + R(x) = \frac{\pi^2}{6}x + R(x)$$

dove $R(x) = -x\sum_{d>x}\frac{1}{d^2} + \sum_{d\le x}\frac{R_d}{d}$.

Tenedo conto che, per ogni d, $|R(d)| < 1$, utilizzando il Lemma 2.12, e una osservazione alla fine della dimostrazione del Teorema 2.17, si ottiene

$$|R(x)| \le \frac{x}{x-1} + \sum_{d\le x}\frac{1}{d} = \frac{x}{x-1} + \log x + \gamma + O(1/x)$$

e dunque $F(x) = \frac{\pi^2}{6}x + O(\log x)$.

3 Congruenze.

3.1 Proprietà generali

I fondamenti algebrici della teoria delle congruenze in $\mathbb{Z}$ sono parte del programma del corso di Algebra. Qui mi limito ad un rapido richiamo degli aspetti che ci interessano.

Sia $1 \leq m \in \mathbb{N}$. Due interi a e b si dicono **congrui modulo m** se m divide $a - b$. In tal caso si scrive

$$a \equiv b \ (mod\, m).$$

Per ogni $1 \leq m \in \mathbb{N}$, la congruenza modulo m è una relazione d'equivalenza su $\mathbb{Z}$. Per ogni $a \in \mathbb{Z}$ la classe di equivalenza di a (detta *classe di congruenza* di a modulo m) è l'insieme

$$a + m\mathbb{Z} = \{\ a + mz \mid z \in \mathbb{Z}\ \}$$

che, se non ci sono ambiguità sul valore di m, indicheremo di solito con la scrittura $\overline{a}$.
L'insieme di tutte la classi di congruenza modulo m (ovvero l'insieme quoziente) si denota con

$$\frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Usando la divisione euclidea si verifica facilmente che ogni intero a è congruo modulo m al resto della divisione di a per m. Da ciò segue subito che il quoziente $\mathbb{Z}/m\mathbb{Z}$ contiene esattamente m elementi, e che gli interi $0, 1, 2, \ldots, m-1$ costituiscono un insieme di rappresentanti delle classi di congruenza modulo m; ovvero

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \{\ 0 + m\mathbb{Z},\ 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\ \} = \{\overline{0},\ \overline{1}, \ldots, \overline{m-1}\}.$$

Inoltre, l'insieme $m\mathbb{Z}$ è un ideale dell'anello $\mathbb{Z}$, e quindi il quoziente $\mathbb{Z}/m\mathbb{Z}$ è un anello rispetto alle operazioni (che si verifica essere ben definite):

$$\overline{a} + \overline{b} = \overline{a + b}$$

$$\overline{a} \cdot \overline{b} = \overline{ab}\ ;$$

in cui lo zero è $\overline{0}$, e l'elemento identico è $\overline{1}$.

Ricordo, dal capitolo precedente, che, dato $m \in \mathbb{N}^*$, si indica con $\phi(m)$ (la funzione di Eulero) il numero di interi compresi tra 1 e m che sono coprimi con m.
Indichiamo quindi con

$$\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$$

l'insieme degli elementi **invertibili** dell'anello $\mathbb{Z}/m\mathbb{Z}$ (ovvero l'insieme delle classi di congruenza $\overline{a}$ modulo m tale che esiste $b \in \mathbb{Z}$ con $\overline{a}\overline{b} = \overline{1}$; esso è un gruppo rispetto alla moltiplicazione in $\mathbb{Z}/m\mathbb{Z}$. I suoi elementi sono facilmente descritti.

Lemma 3.1 *Sia $2 \leq m \in \mathbb{N}$, e sia $a \in \mathbb{Z}$. Allora $\overline{a} = a + m\mathbb{Z}$ è invertibile in $\mathbb{Z}/m\mathbb{Z}$ se e solo se $(a, m) = 1$.*

DIMOSTRAZIONE. Dopo aver osservato che $\overline{a}$ è invertibile in $\mathbb{Z}/m\mathbb{Z}$ se e solo se esiste un $b \in \mathbb{Z}$ tale che $ab \equiv 1\,(mod\, m)$; cioè se e solo se esiste anche un $c \in \mathbb{Z}$ per cui $ab = 1 + cm$, l'enunciato segue facilmente dalla Proposizione 1.2. ∎

Un caso particolare ma molto importante è quando $m = p$ è un numero primo. In tal caso ogni elemento non zero di $\mathbb{Z}/p\mathbb{Z}$ è invertibile, e quindi $\mathbb{Z}/p\mathbb{Z}$ è un **campo**.
Tornando al caso generale, poiché possiamo scegliere come insieme di rappresentanti di $\mathbb{Z}/m\mathbb{Z}$ gli elementi 0, 1, 2, ..., $m-1$, una conseguenza immediata del Lemma 3.1 è che iul numero di elementi invertibili di $\mathbb{Z}/m\mathbb{Z}$ è uguale a $\phi(m)$, ovvero

$$\left|\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*\right| = \phi(m).$$

Esempio. Gli interi $1 \leq a \leq 12$ che sono coprimi con 12, sono $1, 5, 7, 11$. Quindi $(\mathbb{Z}/12\mathbb{Z})^* = \{\ \overline{1},\ \overline{5},\ \overline{7},\ \overline{11}\ \}$.

Ricordiamo ora che se G è un gruppo finito moltiplicativo di ordine n, allora per ogni $g \in G$, risulta $g^n = 1_G$. Ora, $(\mathbb{Z}/m\mathbb{Z})^*$ è un gruppo moltiplicativo di ordine $\phi(m)$, e quindi, per ogni $\overline{a}$ in $(\mathbb{Z}/m\mathbb{Z})^*$, si ha $\overline{a^{\phi(m)}} = \overline{a}^{\phi(m)} = \overline{1}$, ovvero

$$a^{\phi(m)} \equiv 1\ (mod\, m).$$

Siccome gli elementi di $(\mathbb{Z}/m\mathbb{Z})^*$ sono le classi di congruenza degli interi a coprimi con m, ricaviamo il seguente

Teorema 3.2 (Eulero) *Sia $n \in \mathbb{N}^*$, e sia a un numero intero tale che $(n, a) = 1$. Allora n divide $a^{\phi(n)} - 1$, ovvero*

$$a^{\phi(n)} \equiv 1\,(mod\, n)$$

Il caso particolare in cui $m = p$ è un numero primo, è il cosiddetto "piccolo teorema di Fermat".

Corollario 3.3 *Sia p un numero primo, e sia $a \in \mathbb{Z}$. Se p non divide a,*

$$a^{p-1} \equiv 1\,(mod\, p).$$

In ogni caso, $a^p \equiv a\,(mod\, p)$.

Infatti, è possibile rendere del tutto esplicita la struttura algebrica del gruppo degli invertibili di $\mathbb{Z}/n\mathbb{Z}$. Per il momento, ci limitiamo al caso in cui $n = p$ è un numero primo.

Teorema 3.4 *Sia p un numero primo. Allora $(\mathbb{Z}/p\mathbb{Z})^*$ è un gruppo (moltiplicativo) ciclico di ordine $p - 1$.*

DIMOSTRAZIONE. Poniamo $G = (\mathbb{Z}/p\mathbb{Z})^*$. Allora $|G| = p-1$. Per un fatto già ricordato precedentemente, ogni elemento di G ha ordine che divide $p-1$. Per ogni divisore d di $p-1$, denotiamo con $\psi(d)$ il numero di elementi di G che hanno ordine esattamente d. Allora

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

Se $\psi(d) \neq 0$, esiste un elemento a di G tale che il sottogruppo ciclico $\langle a \rangle$ ha ordine d. Ogni elemento $g \in \langle a \rangle$ è tale che $g^d = 1$, e quindi è una radice in $\mathbb{Z}/p\mathbb{Z}$ del polinomio $x^d - 1$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un campo, il numero di tali elementi è al più d; quindi $\langle a \rangle$ è l'insieme di tutte le radici di $x^d - 1$.
Ora, $\langle a \rangle$ ammette $\phi(d)$ generatori distinti, tutti di ordine d.
In conclusione, per ogni $d|p-1$,

$$\psi(d) = 0 \quad \text{oppure} \quad \psi(d) \leq \phi(d).$$

Applicando ciò, ed il Teorema 2.11, si ottiene

$$p-1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \phi(d) = p-1.$$

Dunque, deve essere $\psi(d) = \phi(d)$ per ogni divisore d di $p-1$. In particolare, $\psi(p-1) \neq 0$, e quindi esiste un elemento in G di ordine $p-1$. Il gruppo ciclico generato da tale elemento è tutto G. ∎

Proviamo ora un risultato classico interessante (anche se non avremo nel seguito occasione di applicare).

Teorema 3.5 (Teorema di Wilson). *Sia p un numero primo. Allora*

$$(p-1)! \equiv -1 \, (mod\, p).$$

DIMOSTRAZIONE. Se $p = 2$ l'affermazione è banale. Sia $p > 2$. Osserviamo che $\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}$ sono tutti gli elementi non nulli del campo $\mathbb{Z}/p\mathbb{Z}$. Per il piccolo Teorema di Fermat (Corollario 3.3) queste sono tutte e sole le radici nel campo $\mathbb{Z}/p\mathbb{Z}$ del polinomio $x^{p-1} - \overline{1}$. Quindi

$$(x-\overline{1})(x-\overline{2})\ldots(x-\overline{p-1}) = x^{p-1} - \overline{1}$$

e, dal confronto dei termini noti, si ottiene

$$\overline{(p-1)!} = \overline{1} \cdot \overline{2}) \cdots \overline{p-1} = -\overline{1} = \overline{-1}$$

che significa proprio $(p-1)! \equiv -1 \, (mod\, p)$. ∎

(Per una diversa dimostrazione si veda l'esercizio 5 più in basso)

Esercizio 1. Determinare l'ultima cifra decimale di 7^{139}, e quella di 13^{2001}.

Esercizio 2. Siano a, m numeri interi. Si provi che se $(a, m) = 1 = (a-1, m)$, allora

$$1 + a + a^2 = \ldots + a^{\phi(m)-1} \equiv 0 \,(\text{mod } m).$$

Esercizio 3. Siano n, m numeri interi. Si provi che se $(m, n) = 1$ allora

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \,(\text{mod } mn).$$

Esercizio 4. Provare che se $m > 1$ e $(m-1)! \equiv -1 \,(\text{mod } m)$, allora m è primo.

Esercizio 5. Sia $G = \langle g \rangle$ un gruppo ciclico (moltiplicativo) di ordine pari n, e sia $a = 1 \cdot g \cdot g^2 \cdots g^{n-1}$. Si provi che $a \neq 1_G$ e che $a^2 = 1$. Si usi questo fatto ed il teorema 3.4 per dare una dimostrazione alternativa del Teorema di Wilson.

Esercizio 6. Per $n \in \mathbb{N}$, sia $F_n = 2^{2^n} + 1$ l'n-esimo numero di Fermat. Si provi che ogni divisore primo di F_n è del tipo $2^{n+1}k + 1$. Applicando l'esercizio 4 del Capitolo 1, si deduca che, per ogni $n \geq 1$, esistono infiniti numeri primi congrui a 1 modulo 2^n.

Esercizio 7. Si provi che un intero positivo è divisibile per 11 se e solo se la somma delle sue cifre decimali di posto pari è congrua alla somma di quelle di posto dispari modulo 11.

3.2 Congruenze

Sia $f(x)$ un polinomio a coefficienti interi, e sia $1 \leq n \in \mathbb{N}$. Siamo interessati a stabilire la risolubilità (ed a eventualmente determinare le "soluzioni") di congruenze del tipo

$$f(x) \equiv 0 \pmod{n} \tag{3}$$

Con "soluzione" di una tale congruenza si intende ovviamente un intero $a \in \mathbb{Z}$ tale che $f(a) \equiv 0 \pmod{n}$. Osserviamo subito che, poiché $f(x)$ ha coefficienti interi, se a è una soluzione di (3), e $b \equiv a \pmod{n}$, allora anche b è una soluzione di (3). Dunque, se esistono, le soluzioni sono infinite, ma corrispondono tuttavia ad un numero finito di classi di congruenza. Quindi potremo riferirci al *numero di soluzioni* di una congruenza del tipo (3), intendendo il numero di classi di congruenza distinte i cui elementi sono soluzioni vere e proprie (in altri termini, il numero di interi $0 \leq a \leq n-1$ tali che $f(a) \equiv 0 \pmod{n}$).

Una maniera spesso conveniente di trattare una congruenza del tipo (3) è quella di interpretarla come una "equazione" su un opportuno anello. Infatti, posto $A = \mathbb{Z}/n\mathbb{Z}$, al polinomio intero $f(x) = a_o + a_1 x + \ldots + a_k x^k$ possiamo univocamente associare la sua *riduzione* modulo n, $\overline{f}(x) = \overline{a_o} + \overline{a_1} x + \ldots + \overline{a_k} x^k$ (dove, per ogni $1 \leq i \leq k$, $\overline{a_i} = a_i + n\mathbb{Z}$), che è un polinomio in $A[x]$. È allora immediato osservare che se a è una soluzione della congruenza (3), allora $\overline{a} = a + n\mathbb{Z}$ è una radice in A del polinomio ridotto $\overline{f}(x)$ (ovvero, in termini più impropri ma usuali, è una "soluzione" in A dell'equazione $\overline{f}(x) = \overline{0}$). Viceversa, se $\overline{a}$ è una radice in A del polinomio ridotto $\overline{f}(x)$, allora ogni intero

appartenente alla classe di congruenza $\overline{a}$ (cioè ogni $b \equiv a \pmod{n}$) è una soluzione della congruenza (3).
Questo approccio risulta particolarmente adatto quando il modulo n è un numero primo, poiché in tal caso $\mathbb{Z}/n\mathbb{Z}$ è un campo, e la teoria delle radici di un polinomio a coefficienti su un campo è molto più agevole. Nelle sezioni successive vedremo come sia sempre possibile (mediante il teorema cinese del resto ed il lemma di Hensel) ricondursi a questa situazione; per il momento vediamo alcune osservazioni di carattere generale.
Il caso in cui $f(x)$ è lineare (cioè $f(x) = ax + b$, con $a, b \in \mathbb{Z}$) è relativamente semplice, ed è sostanzialmente contenuto nella Proposizione 1.10.

Proposizione 3.6 *Sia $1 \leq n \in \mathbb{N}$, e siano $a, b \in \mathbb{Z}$. La congruenza $ax \equiv b \pmod{n}$ ammette soluzioni se e solo se $(a, n)|b$.*

Ad esempio, la congruenza $15x \equiv 7 \pmod{6}$ non ha soluzioni intere.

Corollario 3.7 *Sia p un numero primo e $a, b \in \mathbb{Z}$. Allora la congruenza $ax \equiv b \pmod{p}$ ammette soluzioni se e solo se $p|b$ oppure $p \not| a$, e nel secondo caso la soluzione è una sola.*

Per risolvere congruenze di questo tipo si può quindi adoperare l'algoritmo di Euclide. Supponiamo, ad esempio, di voler risolvere la congruenza

$$57x \equiv 21 \pmod{12}.$$

Si trova, $57 = 4 \cdot 12 + 9$, e $12 = 1 \cdot 9 + 3$; dunque, andando a ritroso,

$$(57, 6) = 3 = (-1) \cdot 57 + 5 \cdot 12.$$

Ora $21 = 3 \cdot 7$ e pertanto si ha

$$21 = 7 \cdot 3 = 7 \cdot ((-1) \cdot 57 + 5 \cdot 12) = 57 \cdot (-7) + 12 \cdot 35.$$

Dunque -7 è una soluzione cercata, ed ogni intero ad essa congruo modulo 12 è tale. Ad esempio, 5 è una soluzione. Le altre eventuali soluzioni (si intende, come abbiamo spiegato sopra, modulo 12) si possono determinare mediante una applicazione dell'esercizio 11 del capitolo 1 (vedi esercizio seguente). Esse sono date da

$$5 + t\frac{12}{(57, 12)} = 5 + t \cdot 4$$

con $0 \leq t < 3$, ovvero sono 5, $5 + 4 = 9$ e $5 + 8 = 13$. In conclusione, le soluzioni della congruenza di partenza sono tutti e soli i numeri interi a tali che $a \equiv 1, 5, 9 \pmod{12}$.

Esercizio 8. Nelle ipotesi della Proposizione 3.6, sia a_o una soluzione della congruenza. Si provi che un sistema completo di rappresentanti modulo n di tutte le soluzioni è dato dagli interi

$$a_o + t\frac{n}{(a, n)} \qquad \text{con} \quad 0 \leq t < (a, n).$$

In particolare, il numero di soluzioni è (a, n).

Esercizio 9. Si determinino le soluzioni della congruenza

$$39x \equiv 5 \pmod{14}.$$

Esercizio 10. Si risolva il seguente sistema di congruenze:

$$\begin{cases} 4x - y \equiv 3 \pmod{13} \\ \\ 7x + 2y \equiv 5 \pmod{13} \end{cases}$$

Vediamo ora come il Corollario 3.7 si può agevolmente interpretare mediante la riduzione modulo p. Siano quindi p un numero primo ed $a, b \in \mathbb{Z}$. Risolvere la congruenza $ax \equiv b \pmod{p}$ equivale a trovare le radici nel campo $\mathbb{Z}/p\mathbb{Z}$ del polinomio $\overline{a}x + \overline{b}$. Supponiamo che p non divida a. Allora la classe di congruenza $\overline{a} = a + p\mathbb{Z}$ è un elemento invertibile del campo $\mathbb{Z}/p\mathbb{Z}$, dunque ammette un inverso $\overline{a}^{-1}$, e $\overline{b}\overline{a}^{-1}$ è un elemento di $\mathbb{Z}/p\mathbb{Z}$ (cioè una classe di congruennza modulo p) che è una radice del polinomio $\overline{a}x + \overline{b}$. Se $c \in \mathbb{Z}$ è un suo qualsiasi elemento, si ha $\overline{c} = \overline{b}\overline{a}^{-1}$, e quindi $\overline{ac} = \overline{b}$. Dunque c è una soluzione della congruenza $ax \equiv b \pmod{p}$. L'unicità degli inversi in un campo (ovvero il fatto che $\overline{a}x + \overline{b}$ abbia un'unica radice) assicura che la congruenza ha una sola soluzione.

Esercizio 11. Si dica per quali $x \in \mathbb{N}$ si ha $2^x \equiv 2 \pmod{7}$.

In linea di principio, per ogni congruenza del tipo che stiamo considerando è possibile determinare le eventuali soluzioni: se n è il modulo e $f(x)$ il polinomio intero, "basta" valutare $f(x)$ per tutti gli interi compresi tra 0 e $n-1$. Tuttavia, sia dal punto di vista astratto che da quello pratico, ciò è tutt'altro che soddisfacente. Da un lato si vorrebbero risultati generali che garantiscano la risolubilità (e possibilmente la determinazione delle soluzioni, come la Proposizione 3.6) di ampie classi di congruenze, senza dover "fare i conti", dall'altro la computazione diretta si rivela presto estremamente laboriosa. Questo vale già per le congruenze di secondo grado, che saranno l'argomento del prossimo capitolo, centrato sul famoso teorema di reciprocità quadratica di Gauss. Per il momento vediamo un altro risultato di esistenza, che nella sostanza ci dice, dati un primo p ed un intero positivo n, quante radice n-esime dell'unità sono contenute nel campo $\mathbb{Z}/p\mathbb{Z}$. Ne diamo due dimostrazioni, la seconda della quale adotta un approccio gruppale (che, se ben compreso, a mio avviso semplifica e chiarisce molto la situazione - ma il lettore giudicherà da sé).

Proposizione 3.8 *Sia p un primo, $n \in \mathbb{N}$ e $d = (n, p-1)$. Allora la congruenza*

$$x^n \equiv 1 \pmod{p}$$

ha esattamente d soluzioni.

Dimostrazione. Osserviamo preliminarmente che le soluzioni della congruenza $x^n \equiv 1 \pmod{p}$ sono tutte e sole quelle della congruenza $x^d \equiv 1 \pmod{p}$. Infatti, è chiaro che le soluzioni della seconda sono anche soluzioni della prima. Viceversa sia $a \in \mathbb{Z}$ tale che $a^n \equiv 1 \pmod{p}$, e siano $u, v \in \mathbb{Z}$ con $d = nu + (p-1)v$. Poiché p non divide a, applicando il piccolo teorema di Fermat (Corollario 3.3) si ha

$$a^d = a^{nu+(p-1)v} = a^{nu}a^{(p-1)v} \equiv (a^n)^u(a^{p-1})^v \equiv 1 \pmod{p}$$

(osserviamo che in questo calcolo abbiamo usato il fatto che, essendo $\mathbb{Z}/p\mathbb{Z}$ un campo ha senso elevare con esponente negativo - si veda anche l'esercizio che segue). Quindi a è soluzione di $x^d \equiv 1 \pmod{p}$.
Mostriamo ora che la congruenza $x^d \equiv 1 \pmod{p}$ (con d un divisore di $p-1$) ha esattamente d soluzioni.

(Prima dimostrazione) Consideriamo il polinomio intero $f(x) = x^d - 1$. Allora a è soluzione della congruenza di sopra se e solo se $\overline{a} = a + p\mathbb{Z}$ è radice del polinomio (ridotto modulo p) $\overline{f}(x) = x^d - \overline{1} \in (\mathbb{Z}/p\mathbb{Z})[x]$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un campo, tale polinomio ammette al più d radici. Sia ora $e \in \mathbb{N}$ tale che $p - 1 = de$. Allora

$$x^{p-1} - \overline{1} = (x^d - \overline{1})\overline{g}(x)$$

dove $g(x) = x^{d(e-1)} + \ldots + x^d + 1$. Ora, per il Corollario 3.3, $x^{p-1} - \overline{1}$ ha esattamente $p-1$ soluzioni in $\mathbb{Z}/p\mathbb{Z}$. Poiché le soluzioni di $\overline{g}(x)$ sono al piú $d(e-1) = p - 1 - d$, ne segue che $x^d - \overline{1}$ ha almeno d soluzioni. Dunque $x^d - \overline{1}$ ha esattamente d soluzioni in $\mathbb{Z}/p\mathbb{Z}$, e questo prova l'asserto.

(Seconda dimostrazione) Sappiamo che il gruppo moltiplicativo $F^* = (\mathbb{Z}/p\mathbb{Z})^*$ è ciclico di ordine $p-1$. Sia $\overline{u}$ un suo generatore, e sia $p - 1 = de$. Allora $\langle \overline{u}^e \rangle$ è un sottogruppo di F^* di ordine esattamente d. Se $\overline{a} \in \langle \overline{u}^e \rangle$; allora $\overline{a}^d = \overline{1}$, cioè $\overline{a}$ è radice di $x^d - \overline{1}$. Poiché $x^d - \overline{1}$ ha al più d radici, si conclude che $\langle \overline{u}^e \rangle$ è l'insieme di esse e, siccome $\langle \overline{u}^e \rangle$ contiene esattamente d elementi, la dimostrazione è conclusa. ∎

Esercizio 12. Siano p un primo, $n \in \mathbb{N}$ e $d = (n, p-1)$. Sia $q = n/d$. Utilizzando la fattorizzazione

$$x^n - 1 = (x^d - 1)(x^{d(q-1)} + \ldots + x^d + 1)$$

si provi che le soluzioni di $x^n \equiv 1 \pmod{p}$ coincidono con quelle di $x^d \equiv 1 \pmod{p}$.

Notiamo come la seconda dimostrazione della Proposizione, oltre a determinare il numero di soluzioni della congruenza, sembra anche fornire un metodo per trovarle. Da un punto di vista computazionale, questo è abbastanza apparente: la ragione è che non è noto alcun algoritmo efficiente che, dato un primo p, trovi un generatore del gruppo moltiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$ (tali generatori sono detti *elementi primitivi* di $\mathbb{Z}/p\mathbb{Z}$).
Il solo caso veramente facile è quando $n = 2$.

Lemma 3.9 *Sia p un numero primo dispari. Allora le radici in $\mathbb{Z}/p\mathbb{Z}$ di $x^2 - 1$ sono $\overline{1}$ e $-\overline{1}$. Equivalentemente, se $a \in \mathbb{Z}$ si ha $a^2 \equiv 1 \pmod{p}$ se e solo se $a \equiv \pm 1 \pmod{p}$.*

Sia $n \geq 1$ e $a \in \mathbb{Z}$ tale che $(a, n) = 1$. Allora $\overline{a} = a + n\mathbb{Z}$ è un invertibile nell'anello $\mathbb{Z}/n\mathbb{Z}$, e quindi è un elemento del gruppo moltiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$. L'ordine di $\overline{a}$ in tale gruppo si dice *ordine di a modulo n*. Esso è il minimo intero $\zeta \geq 1$ tale che $a^\zeta \equiv 1 \pmod{n}$. Per una proprietà nota dei gruppi finiti (il Teorema di Lagrange), l'ordine di a modulo n è un divisore dell'ordine del gruppo $(\mathbb{Z}/n\mathbb{Z})^*$, pertanto è un divisore di $\phi(n)$.
È chiaro che l'ordine di un intero modulo n dipende solo dalla sua classe di congruenza modulo n. Calcoliamo, ad esempio, l'ordine di 54 modulo 7. Posssiamo sostituire 54 con 5, dato che sono congrui modulo 7. Inoltre $\phi(7) = 6$, e quindi è sufficiente considerare

come esponenti i divisori di 6. Poiché $5^2 = 25 \equiv 4 \pmod 7$, e $5^3 = 125 \equiv 6 \pmod 7$, deduciamo che l'ordine di 5 (e quindi di 54) modulo 7 è 6.

Esercizio 13. Si calcoli l'ordine di 53 modulo, rispettivamente 3, 12, 15, 19.

Esercizio 14. Sia $n \geq 3$. Si provi che, l'ordine di ogni numero dispari modulo 2^n è un divisore di 2^{n-2} (si deduca che il gruppo $(\mathbb{Z}/2^n\mathbb{Z})^*$ non è ciclico). Si provi quindi che l'ordine di 5 modulo 2^n è 2^{n-2}.

3.3 Il Teorema Cinese del Resto

Il Teorema Cinese del Resto (così chiamato perché nella sostanza appare noto ad antichi matematici cinesi - come Sun Tze, vissuto nel 1^o secolo D.C.) consente di ridurre le congruenze al caso in cui il modulo sia una potenza di un numero primo. Iniziamo vedendone una formulazione "astratta".

Teorema 3.10 *Siano $m_1, m_2, \ldots, m_s$ elementi di $\mathbb{N}^*$ a due a due coprimi, e sia $n = m_1 m_2 \cdots m_s$. Allora l'applicazione definita da, per ogni $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$,*

$$a + n\mathbb{Z} \ \mapsto \ (a + m_1\mathbb{Z},\, a + m_2\mathbb{Z},\, \ldots,\, a + m_s\mathbb{Z})$$

è ben definita e stabilisce un isomorfismo (di anelli)

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_s\mathbb{Z}}.$$

Dimostrazione. Con le notazioni dell'enunciato, denotiamo con Γ l'applicazione data. Verifichiamo che Γ è ben definita. Siano $a, b \in \mathbb{Z}$ tali che $a + n\mathbb{Z} = b + n\mathbb{Z}$. Allora $n|a - b$, e quindi per ogni $i = 1, 2, \ldots, s$, $m_i|a - b$, e di consguenza $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$, provando che secondo la definizione $\Gamma(a + n\mathbb{Z}) = \Gamma(b + n\mathbb{Z})$.
Il fatto che Γ sia un omomorfismo d'anelli segue immediatamente dalla definizione degli anelli quoziente $\mathbb{Z}/k\mathbb{Z}$.
Proviamo che Γ è iniettiva. Siano $a+n\mathbb{Z}, b+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, tali che $\Gamma(a+n\mathbb{Z}) = \Gamma(b+n\mathbb{Z})$. Allora, per ogni $i = 1, 2, \ldots, s$, $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$; e quindi m_i divide $a - b$. Poiché gli interi m_i sono a due a due coprimi, da ciò segue che $n = m_1 m_2 \cdots m_s$ divide $a - b$, e dunque che $a + n\mathbb{Z} = b + n\mathbb{Z}$, provando l'iniettività di Γ.
Per la suriettività, si osservi che

$$\left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = n = \left|\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right| \times \cdots \times \left|\frac{\mathbb{Z}}{m_s\mathbb{Z}}\right| = \left|\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_s\mathbb{Z}}\right|.$$

Dunque Γ è una applicazione iniettiva tra insiemi finiti dello stesso ordine, e pertanto è anche suriettiva. ∎

Corollario 3.11 *Con le stesse ipotesi del Teorema precedente,*

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \simeq \left(\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{m_2\mathbb{Z}}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{m_s\mathbb{Z}}\right)^*.$$

Il Teorema 3.10 si può riformulare in termini di congruenze nel modo classico.

Teorema 3.12 (Cinese del resto). *Siano $m_1, m_2, \ldots, m_s$ elementi di $\mathbb{N}^*$ a due a due coprimi, e sia $n = m_1 m_2 \cdots m_s$. Per ogni $1 = 1, 2, \ldots, s$ siano dati $a_i, b_i \in \mathbb{Z}$. Allora, il sistema di congruenze*

$$\begin{cases} a_1 x \equiv b_1 \ (mod\, m_1) \\ a_2 x \equiv b_2 \ (mod\, m_2) \\ \ldots \\ a_s x \equiv b_s \ (mod\, m_s) \end{cases}$$

ammette soluzioni in $\mathbb{Z}$ se e solo se ciascuna congruenza $a_i x \equiv b_i \, (mod\, m_i)$ ammette soluzioni.

Dimostrazione. Supponiamo che, per ciascuno degli $i = 1, 2, \ldots, s$, la congruenza $a_i x \equiv b_i (mod\, m_i)$ ammetta soluzioni, e sia x_i una sua soluzione. Per il teorema 3.10 (la suriettività dell'applicazione nell'enunciato), esiste un intero y tale che

$$(y + m_1\mathbb{Z}, y + m_2\mathbb{Z}, \ldots, y + m_s\mathbb{Z}) = (x_1 + m_1\mathbb{Z}, x_2 + m_2\mathbb{Z}, \ldots, x_s + m_s\mathbb{Z}),$$

ovvero $y \equiv x_i (mod\, m_i)$, per ogni $i = 1, 2, \ldots, s$. Tale y è una soluzione del sistema delle congruenze. ∎

La dimostrazione che abbiamo dato del teorema cinese del resto è elegante ma astratta. In particolare non sembra suggerire un metodo per trovere le soluzioni del sistema (a partire da quelle delle singole congruenze). Non sarebbe difficile dare una dimostrazione più diretta e costruttiva, che tuttavia lasciamo per esercizio.
Assumendo le ipotesi e le notazioni dell'enunciato del Teorema 3.12, vediamo invece (invece ?) come è possibile ricavare una soluzione del sistema a partire dalle soluzioni x_i di ciascuna congruenza. Per ogni m_i, poniamo $m_i' = n/m_i$. Osserviamo che le ipotesi sugli m_i assicurano che, per ogni $i = 1, \ldots, s$, si ha $(m_i, m_i') = 1$ e $m_i' \equiv 0 \pmod{m_j}$ se $i \neq j$. Mediante l'algoritmo di Euclide, per ogni indice i, si trovano quindi interi u_i, c_i tali che $u_i m_m + c_i m_i' = 1$ (ovvero, $c_i m_i' \equiv 1 \pmod{m_i}$). Se $x_1, x_2, \ldots, x_s$ sono soluzioni delle singole congruenze, si pone

$$y = x_1 m_1' c_1 + x_2 m_2' c_2 + \ldots + x_s m_s' c_s.$$

Per la definizione degli m_i' e la scelta dei c_i, si ha che, per ogni $i = 1, \ldots, s$,

$$y \equiv x_i m_i' c_i \equiv x_i \pmod{m_i}.$$

Dunque y è una soluzione del sistema di congruenze.

Esercizio 15. Ispirandosi al procedimento descritto sopra si dia una dimostrazione diretta del Teorema Cinese dei resti.

A sua volta il Teorema Cinese del Resto può essere enunciato in termini (apparentemente) più generali (la dimostrazione è lasciata per esercizio).

Teorema 3.13 *Siano $m_1, m_2, \ldots, m_s$ elementi di $\mathbb{N}^*$ a due a due coprimi, e sia $n = m_1 m_2 \cdots m_s$. Sia f un polinomio non nullo a coefficienti in $\mathbb{Z}$. Le seguenti asserzioni sono equivalenti*

(1) *è risolubile in $\mathbb{Z}$ la congruenza*

$$f(x) \equiv 0 \ (mod\, n)$$

(2) *è risolubile in $\mathbb{Z}$ il sistema di congruenze*

$$\begin{cases} f(x) \equiv 0 \ (mod\, m_1) \\ f(x) \equiv 0 \ (mod\, m_2) \\ \ldots \\ f(x) \equiv 0 \ (mod\, m_s) \end{cases}$$

(3) *Per ogni $i = 1, 2, \ldots, s$, è risolubile in $\mathbb{Z}$ la congruenza*

$$f(x) \equiv 0 \ (mod\, m_i)$$

Esercizio 16. Si risolvano i seguenti sistemi di congruenze:

$$\begin{cases} x \equiv 3 \,(\text{mod } 6) \\ x \equiv 5 \,(\text{mod } 35) \\ x \equiv 7 \,(\text{mod } 143) \\ x \equiv 3 \,(\text{mod } 323) \end{cases}$$

$$\begin{cases} x \equiv 5 \,(\text{mod } 6) \\ 7x \equiv 5 \,(\text{mod } 12) \\ 17x \equiv 19 \,(\text{mod } 30) \end{cases}$$

Esercizio 17. Si provi che il sistema di congruenze

$$\begin{cases} x \equiv a \,(\text{mod } n) \\ x \equiv b \,(\text{mod } m) \end{cases}$$

ha soluzioni se e solo se $(n, m) | b - a$, e che in tal caso la soluzione è unica modulo m.c.m.(m, n).

3.4 Congruenze modulo un numero composto

Sia $f = a_o + a_1 x + \ldots + a_n x^n$ un polinomio non nullo (a coefficienti in un campo F). Il *polinomio derivato* di f è:

$$f' = a_1 + 2a_2 x = 3a_3 x^2 \ldots + n a_n x^{n-1}.$$

A volte, per rendere la notazione più agevole scriveremo $f' = D(f)$. Inoltre, come consuetudine, si pone $f^{(0)} = f$ e induttivamente, per $k \geq 2$, $f^{(k)} = (f^{(k-1)})'$. La seguente regola per il prodotto si verifica immediatamente.

Siano f, g, polinomi su un campo F. Allora $(fg)' = f'g + fg'$.

Lemma 3.14 *Sia $f = a_o + a_1 x + \ldots + a_n x^n$ un polinomio non nullo in $\mathbb{Z}[x]$, e sia $k \geq 1$. Allora*

$$f^{(k)} = k! \sum_{i=o}^{n-k} \binom{k+i}{i} a_{k+i} x^i.$$

In particolare, $\frac{1}{k!} f^{(n)} \in \mathbb{Z}[x]$.

DIMOSTRAZIONE. Procediamo per induzione su k. Se $k = 1$, la cosa è immediata per definizione. Sia $k \geq 1$; allora, applicando l'ipotesi induttiva,

$$f^{(k+1)} = (f^{(k)})' = D\left(k! \sum_{i=o}^{n-k} \binom{k+i}{i} a_{k+i} x^i\right) = k! \sum_{i=1}^{n-k} i \binom{k+i}{i} a_{k+i} x^{i-1}$$

Ponendo $j = i - 1$, si ha

$$f^{(k+1)} = (k+1)! \sum_{j=0}^{n-k+1} \frac{j+1}{k+1} \binom{k+1+j}{j+1} a_{k+1+j} x^j =$$

$$= (k+1)! \sum_{j=0}^{n-k+1} \binom{(k+1)+j}{j} a_{(k+1)+j} x^j.$$

Il lemma è quindi provato. ∎

Il Lemma che segue non è che un caso particolare della formula di Taylor.

Lemma 3.15 *Sia $f(x)$ un polinomio non nullo in $\mathbb{Z}[x]$, e sia $b \in \mathbb{Z}$. Allora*

$$f(x+b) = \sum_{k=0}^{n} \frac{b^k f^{(k)}(x)}{k!}.$$

In particolare, $f(x+b) = f(x) + f'(x)b + s_b(x)b^2$, dove $s_b(x)$ è un polinomio a coefficienti interi.

DIMOSTRAZIONE. Sia $f(x) = a_o + a_1 x + \ldots + a_n x^n$ un polinomio non nullo in $\mathbb{Z}[x]$. Sviluppando mediante la formula di Newton ciascun binomio $(x+b)^k$, per $0 \leq k \leq n$, ed applicando il Lemma 3.14, si ottiene

$$f(x+b) = \sum_{i=)}^{n} a_i (x+b)^i = \sum_{i=0}^{n} a_i \left(\sum_{k=0}^{i} \binom{i}{k} x^{i-k} b^k\right) = \sum_{k=0}^{n} \sum_{i=k}^{n} \binom{i}{k} a_i x^{i-k} b^k$$

$$= \sum_{k=0}^{n} \sum_{j=0}^{n-k} \binom{k+j}{k} a_{k+j} x^j b^k = \sum_{k=0}^{n} \left(b^k \sum_{j=0}^{n-k} \binom{k+j}{j} a_{k+j} x^j\right) = \sum_{k=0}^{n} \frac{b^k f^{(k)}(x)}{k!},$$

ed il Lemma è dimostrato. ∎

Teorema 3.16 (Lemma di Hensel) *Sia p un primo e $f \in \mathbb{Z}[x]$ un polinomio il cui coefficiente direttivo non sia multiplo di p. Supponiamo che esista un intero z_1 tale che*

$$\begin{cases} f(z_1) \equiv 0 \pmod{p} \\ \\ f'(z_1) \not\equiv 0 \pmod{p} \end{cases}$$

Allora, per ogni $n \geq 1$ esiste un intero z_n tale che

$$f(z_n) \equiv 0 \pmod{p^n} \qquad e \qquad z_{n+1} \equiv z_n \pmod{p^n}.$$

DIMOSTRAZIONE. Siano f e z_1 come nell'enunciato. Procedendo per induzione su n, proviamo l'esistenza di $z_n \in \mathbb{Z}$ con le proprietà desiderate, ed inoltre tale che $f'(z_n) \not\equiv 0 \pmod{p}$.
Poiché il passo $n = 1$ è dato, supponiamo, per ipotesi induttiva di aver già costruito $z_1, z_2, \ldots, z_n$. Sia t un numero intero. Allora, per il Lemma 3.15, esiste un polinomio intero $s(x)$, tale che

$$f(z_n + tp^n) = f(z_n) + f'(z_n)tp^n + s(z_n)t^2p^{2n}.$$

Quindi, in particolare,

$$f(z_n + tp^n) \equiv f(z_n) + f'(z_n)tp^n \pmod{p^{n+1}}.$$

Ora, siccome, per ipotesi induttiva, $f(z_n) \equiv 0 \pmod{p^n}$, $f(z_n)/p^n$ è un numero intero. Inoltre, $f'(z_n) \not\equiv 0 \pmod{p}$, e dunque esiste un $0 \leq t_o \leq p-1$ tale che

$$f'(z_n)t_o \equiv -\frac{f(z_n)}{p^n} \pmod{p}.$$

Ponendo $z_{n+1} = z_n + t_o p^n$, si ha subito $z_{n+1} \equiv z_n \pmod{p^n}$. Inoltre, sostituendo nella congruenza di sopra, si ottiene

$$f(z_{n+1}) \equiv f(z_n) + f'(z_n)t_o p^n \equiv 0 \pmod{p^{n+1}}.$$

Resta da provare che $f'(z_{n+1}) \not\equiv 0 \pmod{p}$. Ma questo è immediato dal fatto che $z_{n+1} \equiv z_n \pmod{p}$, e che $f'(z_n) \not\equiv 0 \pmod{p}$. ∎

Vediamo ora come questo Teorema (assieme al teorema cinese del resto) consente di ricondurre la soluzione di congruenze modulo un intero generico a congruenze modulo un numero primo.
Supponiamo dunque di voler risolvere la congruenza

$$f(x) \equiv 0 \pmod{n}$$

con $f(x) \in \mathbb{Z}[x]$, e $n \geq 2$. Per il teorema cinese del resto (nella versione 3.13) possiamo supporre che $n = p^k$ sia la potenza di un numero primo p, vogliamo cioè risolvere

$$f(x) \equiv 0 \pmod{p^k}. \tag{4}$$

Si considera allora la congruenza $f(x) \equiv 0 \pmod{p}$. Se questa non ammette soluzioni, allora chiaramente neppure la (4) ne ha. Supponiamo quindi che $f(x) \equiv 0 \pmod{p}$ sia risolubile e sia $y_1, y_2, \ldots, y_s$ (con $s \leq p$) un sistema di rappresentanti delle soluzioni di essa (i cui elementi sono a due a due non congrui modulo p, e che anzi possiamo prendere compresi tra 0 e $p-1$). Per ogni $i = 1, \ldots, s$, si calcola $f'(y_i)$

- Se $f'(z_1) \not\equiv 0 \pmod{p}$, allora per il Lemma di Hensel è possibile trovare soluzioni della congruenza (4) che sono congrue a x_i modulo p. Di fatto, in un primo passo, si trovano quelle della congruenza modulo p^2: la dimostrazione del Teorema 3.16 mostra che (modulo p^2) ce n'è una sola, e suggerisce anche come calcolarla.

- Se $f'(z_1) \equiv 0 \pmod{p}$, allora per il Lemma 3.15, per ogni intero t,

$$f(x_i + tp) \equiv f(x_i) \pmod{p^2};$$

dunque, è possibile sollevare la soluzione x_i ad una soluzione di $f(x) \equiv 0 \pmod{p^2}$ se e soltanto se x_i è già una soluzione di questa. In tal caso, tutti gli interi $x_i + tp$ con $0 \leq t \leq p-1$ sono soluzioni della congruenza modulo p^2.

In questo modo, dopo aver applicato la procedura descritta a tutti gli $x_1, \ldots, x_s$ si avrà trovato un sistema completo di rappresentanti delle soluzioni della congruenza $f(x) \equiv 0 \pmod{p^2}$ (detto un sollevamento di quello modulo p). Da questo, con lo stesso procedimento, si risale alle soluzioni modulo p^3, e così via, sino al modulo desiderato.
L'esempio che segue chiarirà forse meglio l'algoritmo.

Esempio. Determinare le soluzioni della congruenza

$$x^3 - 2x^2 + 3x + 9 \equiv 0 \pmod{27}.$$

Posto $f(x) = x^3 - 2x^2 + 3x + 9$, si ha $f'(x) = 3x^2 - 4x + 3$. Un sistema di rappresentanti delle soluzioni di $f(x) \equiv 0 \pmod{3}$ è dato da $x_1 = 0$, $x_2 = 2$. A partire da queste si determinano le soluzioni modulo 3^2.

- Per $x_1 = 0$, si ha $f'(0) = 3 \equiv 0 \pmod{3}$. Poiché $f(0) = 9 \equiv 0 \pmod{3^2}$, si ha che 0, $0+3$, $0+6$ sono soluzioni della congruenza $f(x) \equiv 0 \pmod{3^2}$.
- Per $x_2 = 2$, si ha $f(2) = 15$, e $f'(2) = 7 \not\equiv 0 \pmod{3}$. Per il lemma di Hensel x_2 si può sollevare ad un'unica soluzione modulo 3^2, che è data da $2 + 3t_o$, dove t_o è la soluzione di

$$f'(2)t_o \equiv -\frac{f(2)}{3} \pmod{3}.$$

Cioè $7t_o \equiv -5 \pmod{3}$, da cui si ricava $t_o = 1$. Quindi la soluzione modulo 3^2, associata (cioè ad essa congrua modulo 3) a $x_2 = 2$ è $x_2 + 3 \cdot 1 = 5$.
Pertanto, un sistema completo di rappresentanti delle soluzioni di $f(x) \equiv 0 \pmod{3^2}$ è $y_1 = 0$, $y_2 = 3$, $y_3 = 5$, $y_4 = 6$. Ad ognuna di queste si riapplica il procedimento.

- Per $y_1 = 0$. Si ha $f'(0) = 3 \equiv 0 \pmod{3}$, ma $f(0) = 9 \not\equiv 0 \pmod{3^3}$. Quindi, 0 non si solleva ad alcuna soluzione modulo 3^3.
- Per $y_2 = 3$. Si ha $f'(3) = 18 \equiv 0 \pmod{3}$, e $f(3) = 27 \equiv 0 \pmod{3^3}$. Quindi, $y_2 = 3$ si solleva alle soluzioni 3, $3 + 9 = 12$, $3 + 18 = 21$, di $f(x) \equiv 0 \pmod{3^3}$.
- Per $y_3 = 5$. Si ha $f'(5) = 58 \not\equiv 0 \pmod{3}$, e $f(5) = 99$. Per il Lemma di Hensel, $y_3 = 5$ si solleva alla soluzione $5 + 9t$, dove t è tale che $58t \equiv \frac{99}{9} \pmod{3}$; ovvero $t = 1$. La soluzione di $f(x) \equiv 0 \pmod{3^3}$ associata a y_3 è dunque $5 + 9 = 14$.

- Per $y_4 = 6$. Si ha $f'(6) = 87 \equiv 0 \pmod 3$, ma $f(6) = 171 \not\equiv 0 \pmod{3^3}$. Quindi, 6 non si solleva ad alcuna soluzione modulo 3^3.

In conclusione, un sistema completo di rappresentanti delle soluzioni della congruenza $x^3 - 2x^2 + 3x + 9 \equiv 0 \pmod{27}$ è dato da 3, 12, 14, 21.

Esercizio 18. Sia p un primo dispari, e sia $a \in \mathbb{Z}$ tale che p non divide a. Supponiamo che esista un intero b tale che $b^2 \equiv a \pmod p$. Si provi che, per ogni $s \geq 1$, la congruenza $x^2 \equiv a \pmod{p^s}$ ammette soluzioni.

Esercizio 19. Dire quale condizione deve essere soddisfatta dal primo p affinché la proprietà analoga a quella dell'esercizio precedente valga con la potenza terza, invece del quadrato.

Esercizio 20. Si risolvano le seguenti congruenze.

$$x^4 - 3x^2 + 11 \equiv 0 \pmod{5^3}$$

$$x^4 - 2x^2 + x - 3 \equiv 0 \pmod{5^3}$$

3.5 Appendice I: Pseudoprimi e numeri di Carmichel.

Sia n un intero positivo e supponiamo di voler determinare se n è un numero primo oppure è composto (questo è un probelma pratico che si presenta in modo importante in molte applicazioni, ad esempio in alcuni sistemi crittografici). La procedura più diretta è quella di dividere n per tutti gli interi positivi minori o uguali alla sua radice quadrata; n è un numero primo se e solo se nessuno di essi è un divisore di n. Questo può anche andar bene se n è piccolo, ma per numeri grandi questo semplice algoritmo si rivela del tutto inefficiente (a causa della crescita esponenziale del tempo necessario a svolgere tutte le operazioni). Il piccolo teorema di Fermat (Corollario 3.3) fornisce un criterio *necessario* affinché un intero $n \geq 2$ sia un numero primo: per ongi intero b con $(n, b) = 1$ deve essere

$$b^{n-1} \equiv 1 \pmod n. \tag{5}$$

Quindi se, dato un intero positivo n, troviamo un altro intero (detto base) b con $(b, n) = 1$ per cui la congruenza (5) non è soddisfatta, allora n è necessariamente un numero composto.

Una singola tale verifica è computazionalmente abbastanza agevole (perché moltiplicare è più facile che dividere). Vediamo, ad esempio che 319 non è un numero primo. Una procedura conveniente è quella di scrivere $319 - 1 = 318$ in base 2; si ha

$$318 = 2^8 + 2^5 + 2^4 + 2^3 + 2^2 + 2.$$

Quindi, tenendo conto che $b^{2^{k+1}} = (b^{2^k})^2$, e prendendo come base $b = 2$, otteniamo

$$\begin{aligned}
2^{2^2} &= 4 \\
2^{2^{2^2}} &= 16 \\
2^{2^{2^3}} &= 256 \\
2^{2^{2^4}} &= 65536 \equiv 141 \pmod{319} \\
2^{2^{2^5}} &\equiv 141^2 = 19881 \equiv 103 \pmod{319} \\
2^{2^{2^6}} &\equiv 103^2 \equiv 82 \pmod{319} \\
2^{2^{2^7}} &\equiv 82^2 \equiv 25 \pmod{319} \\
2^{2^{2^8}} &\equiv 25^2 \equiv 306 \pmod{319}
\end{aligned}$$

Dunque,

$$2^{318} = 2^{2^8}2^{2^5}2^{2^4}2^{2^3}2^{2^2}2^2 \equiv 306 \cdot 103 \cdot 141 \cdot 256 \cdot 16 \cdot 4 \equiv 193 \not\equiv 1 \pmod{319}$$

e pertanto 319 non è un numero primo (infatti $319 = 11 \cdot 29$).

Sia $b \in \mathbb{N}^*$; un intero $n \geq 2$ si dice *pseudo-primo* rispetto alla base b se $(n, b) = 1$ e la congruenza (5) è verificata.

Vediamo, ad esempio che $n = 341$ è uno pseudo-primo rispetto alla base $b = 2$ (per fare questo usiamo il fatto di conoscere già la fattorizzazione di $341 = 11 \cdot 31$ (cosa che facilita i calcoli, e che nel caso di sopra non sarebbe stata leale). Ora, $2^5 = 32 \equiv 1 \pmod{11}$, e quindi

$$2^{340} = (2^5)^{68} \equiv 1 \pmod{31}.$$

Inoltre, $2^5 \equiv -1 \pmod{11}$, dunque $2^{10} \equiv 1 \pmod{11}$, e

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}.$$

Poiché 11 e 31 sono coprimi si conclude che

$$2^{340} \equiv 1 \pmod{341}$$

e quindi che 341 è uno pseudo-primo rispetto alla base 2. Non è invece uno pseudo-primo rispetto alla base 3. Infatti, se, per assurdo fosse $3^{341} \equiv 1 \pmod{341}$, allora in particolare $3^{341} \equiv 1 \pmod{31}$, e dunque l'ordine di 3 modulo 31 sarebbe un divisore di 340; ma l'ordine di 3 modulo 31 è un divisore di $\phi(31) = 30$; poiché $(340, 30) = 10$, si dovrebbe avere $3^{10} \equiv 1 \pmod{31}$. Ma, da $3^5 = 243 \equiv 26 \equiv -5 \pmod{31}$ segue

$$3^{10} \equiv (-5)^2 \equiv 25 \pmod{31}$$

e dunque un assurdo.

A questo punto viene naturale congetturare che la condizione espressa dal teorema di Fermat sia anche sufficiente a ché n sia un numero primo; ovvero che se n è uno pseudo-primo rispetto ad ogni base b (con $(n, b) = 1$) allora n è un primo. Tuttavia, le cose non

stanno così. Esistono cioè numeri composti che sono pseudo-primi rispetto a qualunque base ad essi coprima. Tali interi sono denominati *numeri di Carmichel*.
Un esempio è il numero $n = 1105$. Infatti, $n = 5 \cdot 13 \cdot 17$, e $n - 1 = 1104 = 2^4 \cdot 3 \cdot 23$; osserviamo quindi che $n-1$ è un multiplo comune di $\phi(5) = 4$, $\phi(13) = 12$ e $\phi(17) = 16$. Sia b un intero coprimo con 1105, allora, per il Teorema di Fermat b^{1104} è congruo ad 1 modulo 5, 13 e 17. Poiché questi sono coprimi si conclude che

$$b^{1104} \equiv 1 \pmod{1105}$$

e dunque 1105 è un numero di Carmichel.

Esercizio 21. Si provi che 561 è un numero di Carmichel.

Esercizio 22. Sia $n = p_1 p_2 \cdots p_s$ un prodotto di primi distinti (almeno due), tale che, per ogni $i = 1, \ldots, s$, $p_i - 1$ divide $n - 1$. Si provi che n è un numero di Carmichel.

3.6 Appendice II: Un criterio di primalità.

Recentemente i matematici Agrawal, Kayal e Saxena hanno proposto un algoritmo che testa la primalità di un intero positivo n in un tempo polinomiale (rispetto ad n) risolvendo così un importante problema aperto. Il loro algoritmo (chi fosse interessato può consultare il sito www.cse.iitk.ac.in/news/primality.html) si basa sul seguente ed elementare criterio di primalità.

Teorema 3.17 *Sia n un intero positivo, e sia a un numero naturale coprimo con n. Allora n è un numero primo se e solo se per ogni $x \in \mathbb{Z}$*

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Dimostrazione. Sviluppando mediante la formula del binomio di Newton, si trova che, per $1 \leq i \leq n-1$, il coefficiente di x^i in $(x-a)^n - (x^n - a)$ è

$$(-1)^i \binom{n}{i} a^{n-1}.$$

Supponiamo che n sia un numero primo. Ricordo che allora, per ogni $1 \leq i \leq n-1$, n divide $\binom{n}{i}$; dunque il coefficiente di x^i in $(x-a)^n - (x^n - a)$ è un multiplo di n. Da ciò segue che

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Viceversa, supponiamo che n sia un numero composto, e sia q un divisore primo di n. Se q^k è la massima potenza di q che divide n (e scriviamo $n = q^k b$ con $(q, b) = 1$, allora q^k è coprimo con a^{p-q} e non divide

$$\binom{n}{q} = \frac{q^k b(q^k b - 1) \cdots (q^k b - q + 1)}{1 \cdot 2 \cdot 3 \cdots q}.$$

Da ciò segue che il coefficiente di x^q in $(x-a)^n - (x^n - a)$ non è un multiplo di n e dunque (lo si dimostri) il polinomio $(x-a)^n - (x^n - a)$ non assume valori identicamente uguali a zero modulo n. ∎

Soluzione di alcuni esercizi.

Esercizio 1. Si osservi che l'ultima cifra decimale di $n = 7^{139}$ è il resto della divisione di n per 10, ovvero quell'intero $0 \leq k \leq 9$, tale che $7^{139} \equiv k\,(mod\,10)$. Poiché $\phi(10) = 4$, per il Teorema di Eulero-Fermat si ha, $7^4 \equiv 1\,(mod\,10)$. Ora, $139 = 4 \cdot 34 + 3$. Quindi

$$7^{139} = (7^4)^{34} \cdot 7^3 \equiv 7^3 \equiv 3\,(mod\,10)\ .$$

Dunque $k = 3$.

Esercizio 3. Poiché $(n, m) = 1$, si ha $m^{\phi(n)} \equiv 1 \pmod{n}$ e $n^{\phi(m)} \equiv 1 \pmod{m}$. Da ciò segue $n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{m}$ e $n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{n}$. Siccome n ed m sono coprimi, da questo segue l'asserto.

Esercizio 6. Sia p un divisore primo di F_n. Allora $2^{2^n} \equiv -1\,(mod\,p)$ da cui anche $2^{2^{n+1}} \equiv 1\,(mod\,p)$. Poichè $2^{p-1} \equiv 1\,(mod\,p)$, se ne deduce che $2^{n+1}|p-1$, e quindi che $p = 2^{n+1}k + 1$ per qualche $k \in \mathbb{N}$.
Per la seconda parte, è sufficiente considerare tutti i numeri di Fermat F_m con $m \geq n-1$, e scegliere per ognuno di essi un divisore primo p_m. Per quanto visto sopra ogni p_m è congruo ad 1 modulo 2^n, e per l'esercizio 4 del capitolo 1 i primi p_m sono tutti distinti.

Esercizio 14. Sia a un numero dispari, e sia $n \geq 3$. Proviamo, per induzione su n che

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

Poiché a è dispari, almeno uno tra in numeri pari $a-1$ e $a+1$ è divisibile per 4; quindi $a^2 - 1 = (a-1)(a+1)$ è divisibile per 8, e questo prova il caso $n = 3$. Sia $n \geq 4$ ed assumiamo la proprietà vera per ogni $n-1$. Allora

$$a^{2^{n-2}} = (a^{2^{n-3}} - 1)(a^{2^{n-3}} + 1);$$

siccome $a^{2^{n-3}} + 1$ è pari, dall'ipotesi induttiva segue che $2^{n-1} = 2^(n-2) \cdot 2$ divide $a^{2^{n-2}}$, provando così l'asserto. Poiché $\phi(2^n) = 2^{n-1}$, da ciò segue che l'odine di a modulo 2^n divide 2^{n-2}.
In particolare, $(\mathbb{Z}/2^n\mathbb{Z})^*$ non è ciclico, perché se lo fosse, ammetterebbe un generatore $\overline{a}$, il cui ordine è $\phi(2^n) = 2^{n-1}$, e questo comporterebbe che il numero intero a avrebbe ordine 2^{n-1} modulo 2^n.

Proviamo ora che (con $n \geq 3$) l'ordine di 5 modulo 2^n è esattamente 2^{n-2}. Per fare questo è sufficiente provare che

$$5^{2^{n-3}} \not\equiv 1 \pmod{2^n}.$$

A sua volta, ciò segue facilmente dal seguente fatto, che dimostriamo per induzione su k: per ogni $k \geq 1$,

$$5^{2^k} \equiv 1 + 3 \cdot 2^{k+2} \pmod{2^{k+4}}.$$

Per $k = 1$ si ha $5^2 = 25 = 1 + 3 \cdot 2^3$, e l'asserto è vero. Sia $k \geq 2$; allora, per ipotesi induttiva, esiste un intero b tale che

$$5^{2^{k-1}} = 1 + 3 \cdot 2^{k+1} + b2^{k+3} = 1 + (3 + 4b)2^{k+1}.$$

Dunque

$$5^{2^k} = (5^{2^{k-1}})^2 = 1 + (3+4b)2^{k+2} + (3+4b)^2 2^{2k+2} = 1 + 3 \cdot 2^{k+2} + b \cdot 2^{k+4} + (3+4b)^2 2^{2k+2}$$

e, poiché $2k + 2 \geq k + 4$ (dato che $k \geq 2$), si conclude.

Esercizio 16. Per il primo sistema (se non ho sbagliato i conti) $x = -2846265$ (e tutti gli interi congrui ad esso modulo $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$). Per il secondo sistema, $x = 47$ (modulo 60).

Esercizio 17. Supponiamo che il sistema dato sia risolubile, e sia x_o una sua soluzione. Allora $n|x_o - a$ e $m|x_o - b$. Quindi (n, m) divide $x_o - a - (x_o - b) = b - a$. Viceversa, supponiamo che $(n, m)|b - a$. Allora, è risolubile la congruenza $nx \equiv b - a \pmod{m}$. Sia x_1 una sua soluzione, e sia $x_2 = a + nx_1$. Allora, per scelta, $x_2 \equiv a \pmod{n}$; inoltre $x_2 - b = a + nx_1 - b = nx_1 - (b - a) \equiv 0 \pmod{m}$. Dunque x_2 è una soluzione del sistema. Infine, supponiamo che u e v siano soluzioni del sistema. Allora u è congruo a v sia modulo n che modulo m, e quindi m.c.m.$(n, m)|u - v$.

Esercizio 19. $p \neq 3$.

4 Residui Quadratici.

Sia p un primo dispari, e siano $a, b, c \in \mathbb{Z}$ con $p \not| a$. Risolvere la congruenza quadratica

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

equivale a risolvere nel campo $\mathbb{Z}/p\mathbb{Z}$ l'equazione

$$\overline{a}x^2 + \overline{b}x + \overline{c} = \overline{0} \tag{6}$$

(deove il soprassegno indica, come usuale, la classe di congruenza modulo p del numero intero sottostante). Ora, le eventuali soluzioni della (6) soddisfano alla medesima formula che si usa per risolvere equazioni reali di secoondo grado (e la dimostrazione è la stessa: la si svolga per esercizio). Quindi, la (6) è risolubile in $\mathbb{Z}/p\mathbb{Z}$ (e pertanto la congruenza in alto è risolubile in $\mathbb{Z}$) se e soltanto se il *discriminante* $\Delta = \overline{b}^2 - 4\overline{a} \cdot \overline{c}$ è un quadrato in $\mathbb{Z}/p\mathbb{Z}$, ovvero se e soltanto se la congruenza

$$x^2 \equiv \Delta \pmod{p}$$

è risolubile. Questo capitolo è dedicato a risultati classici che riguardano tali congruenze. Prima, un paio di esercizi di prova.

Esercizio 1. Calcolare le eventuali soluzioni della congruenza

$$x^2 - 3x + 11 \equiv 0 \pmod{13}.$$

Esercizio 2. Calcolare le eventuali soluzioni della congruenze $x^2 \equiv 2 \pmod{17}$, e $x^2 \equiv 2 \pmod{43}$.

4.1 Il simbolo di Legendre

Definizione. Siano $a, b \in \mathbb{Z}$, con $b \neq 1$. a si dice un **Residuo Quadratico (R.Q.) modulo** b se esiste un $c \in \mathbb{Z}$ tale che

$$c^2 \equiv a \,(mod\, b)$$

(ovvero se $\overline{a} = a + b\mathbb{Z}$ è un quadrato nell'anello $\mathbb{Z}/b\mathbb{Z}$).

Il caso in cui $b = p$ è un numero primo è particolarmente interessante. Se $p = 2$, allora ogni elemento di $\mathbb{Z}/2\mathbb{Z}$ è un quadrato, e quindi ogni intero è un residuo quadratico modulo 2. Se invece p è un primo dispari le cose sono più complicate, ed è conveniente introdurre il seguente

SIMBOLO DI LEGENDRE. *Sia p un numero primo dispari, e $a \in \mathbb{Z}$. Si pone*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p|a; \\ 1 & \text{se } p \not| a \text{ ed } a \text{ è un R.Q. modulo } p; \\ -1 & \text{se } a \text{ non è un R.Q. modulo } p. \end{cases}$$

Sia p un primo dispari, e sia $a \in \mathbb{Z}$. Per definizione a è un R.Q. modulo p se e soltanto se la classe di congruenza $\overline{a}$ di a modulo p è un quadrato nel campo $\mathbb{Z}/p\mathbb{Z}$. Ora, siccome p è dispari, per ogni $0 \neq \overline{a}$ in $\mathbb{Z}/p\mathbb{Z}$, si ha $-\overline{a} \neq \overline{a}$ e $(\overline{a})^2 = \overline{a}^2$. Ne segue che esattamnente la metà degli elementi non nulli di $\mathbb{Z}/p\mathbb{Z}$ è un quadrato. Ovvero (contando anche lo 0): *il numero di quadarti in* $\mathbb{Z}/p\mathbb{Z}$ *è* $1 + (p-1)/2 = (p+1)/2$.
Una maniera più astratta (e forse migliore) di provare questo semplice fatto, consiste nell'osservare che, per il teorema 3.4, il gruppo moltiplicativo $G = (\mathbb{Z}/p\mathbb{Z})^*$ è ciclico di ordine $p-1$; sia α un suo generatore. Poiché $2|p-1$, il sottogruppo $Q = \langle \alpha^2 \rangle$ è un sottogruppo di G, di ordine $\frac{p-1}{2}$. Se $x \in Q$, allora, per qualche $0 \leq n \leq p-2$,

$$x = (\alpha^2)^n = (\alpha^n)^2$$

e dunque x è un quadrato. Viceversa, sia $y \neq 0$ un quadrato in $\mathbb{Z}/p\mathbb{Z}$. Allora y è il quadrato di un elemento in G, e quindi, per qualche m intero $y = (\alpha^m)^2 = (\alpha^2)^m \in Q$. Dunque, Q è l'insieme dei quadrati non nulli di $\mathbb{Z}/p\mathbb{Z}$, e si ritrova la formula di sopra.

Prima di vedere un'importante applicazione di questa osservazione alla teoria dei residui quadratici, dimostriamo un Lemma che ci sarà utile nei capitoli successivi.

Lemma 4.1 *Sia p un numero primo. Allora ogni elemento del campo $\mathbb{Z}/p\mathbb{Z}$ è una somma di due quadrati.*

DIMOSTRAZIONE. Se $p = 2$ non c'e nulla da dimostrare. Sia dunque p un primo dispari, e sia Q_o l'insieme dei quadrati di $\mathbb{Z}/p/Z$. Per quanto visto sopra $|Q_o| = (p+1)/2$.
Sia $a \in Z/p\mathbb{Z}$. Consideriamo l'applicazione σ_a da Q_o in $Z/p\mathbb{Z}$, definita da

$$\sigma_a(y) = a - y$$

per ogni $y \in Q_o$. Poiché $Z/p\mathbb{Z}$ è un gruppo additivo, σ_a è iniettiva, e quindi, posto $Q_1 = \sigma_a(Q_o)$, si ha $|Q_1| = |Q_o| = \frac{p+1}{2}$. D'altra parte Q_o e Q_1 sono sottoinsiemi di $Z/p\mathbb{Z}$, e quindi $|Q_o \cup Q_1| \leq |Z/p\mathbb{Z}| = p$. Dunque

$$p \geq |Q_o \cup Q_1| = |Q_o| + |Q_1| - |Q_o \cap Q_1| = p + 1 - |Q_o \cap Q_1|;$$

da cui segue che l'intersezione $Q_o \cap Q_1$ non è vuota. Dunque esiste un $y \in Q_o$ tale che $a - y \in Q_o$, provando che $a = y + (a-y)$ è una somma di due quadrati. ∎

Torniamo ora al nostro argomento principale, provando il *Criterio di Eulero.*

Proposizione 4.2 (Eulero) *Sia p un primo dispari, ed $a \in \mathbb{Z}$, con $(a,p)=1$. Allora.*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \,(mod\, p).$$

DIMOSTRAZIONE. Sia p un primo dispari, e sia $a \in \mathbb{Z}$, con $(a,p)=1$. Dal Corollario 3.3 segue che $a^{\frac{p-1}{2}}$ è una soluzione dell'equazione

$$x^2 \equiv 1 \,(mod\, p),$$

e poiché tale equazione ha esattamente due soluzioni modulo p, che sono 1 e -1 si ha

$$a^{\frac{p-1}{2}} \equiv \pm 1 \,(mod\, p).$$

Se $\left(\frac{a}{p}\right) = 1$, a è un R.Q. modulo p, cioè esiste $c \in \mathbb{Z}$ tale che $c^2 \equiv a \,(mod\, p)$. Ma allora, ancora per il Corollario 3.3,

$$a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1 \,(mod\, p).$$

Ora, per quanto osservato in precedenza, il numero di quadrati non nulli modulo p è esattamente $\frac{p-1}{2}$; e quindi essi sono tutte e sole le soluzioni dell'equazione

$$x^{\frac{p-1}{2}} = \overline{1}$$

in $\mathbb{Z}/p\mathbb{Z}$ (si ricordi che, poichè $\mathbb{Z}/p\mathbb{Z}$ è un campo l'equazione di sopra ha al più $\frac{p-1}{2}$ soluzioni). Dunque, se $a \in \mathbb{Z}$ (con $(a,p)=1$) non è un R.Q. modulo p, allora $\overline{a}$ non è una soluzione dell'equazione di sopra, quindi, per quanto prima osservato, deve essere

$$a^{\frac{p-1}{2}} \equiv -1 \,(mod\, p),$$

provando così la Proposizione. ∎

Non è ora difficile verificare che valgono le seguenti proprietà elementari.

Lemma 4.3 *Sia p un primo dispari, e siano $a, b \in \mathbb{Z}$. Allora*

(1) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *se* $a \equiv b \,(mod\, p)$*;*

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*;*

(3) $\left(\frac{a^2}{p}\right) = 1$*;*

(4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

DIMOSTRAZIONE. I punti (1) e (3) discendono immediatamente dalle definizioni. Per il punto (3), la cosa è ovvia se p divide ab. Altrimenti, per il criterio di Eulero,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \,(mod\, p)$$

provando così l'affermazione (essendo p dispari).
Anche il punto (4) segue dal criterio di Eulero; infatti

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \ (mod\, p)$$

e quindi l'asserto. ∎

Osserviamo che se p è un primo dispari, allora $p \equiv 1, 3\, (mod\, 4)$. Il punto (4) del Lemma precedente può quindi essere riformulato affermando che, per un primo dispari p,

$$\left(\frac{-1}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1\, (mod\, 4).$$

Sia $1 \geq n$. Allora l'insieme dei numeri interi x con $-n/2 < x \leq n/2$ è un sistema di rappresentanti delle classi di congruenza modulo n. Dato un intero a chiamiamo *residuo assoluto* di a modulo n quell'unico intero $-n/2 < b \leq n/2$ tale che $a \equiv b\, (mod\, n)$.

Lemma 4.4 (Lemma di Gauss) *Sia p un primo dispari, e sia $1 \leq a \in \mathbb{N}$ tale che $(a, p) = 1$. Sia t il numero di elementi nell'insieme*

$$Q = \{\ a,\, 2a, \ldots,\, ((p-1)/2)a\ \}$$

il cui residuo assoluto modulo p è negativo. Allora

$$\left(\frac{a}{p}\right) = (-1)^t.$$

Dimostrazione. Osserviamo che, poiché $(a, p) = 1$, gli elementi di Q sono a due a due non congrui modulo p.
Sia $k = (p-1)/2 - t$. Siano $r_1, r_2, \ldots, r_k$ i residui assoluti positivi degli elementi di Q, e siano $-s_1, -s_2, \ldots, -s_t$ quelli negativi. Supponiamo che esistano $1 \leq i \leq k$ e $1 \leq j \leq t$ tali che $r_i \equiv s_j\, (mod\, p)$. Ora, esistono $1 \leq n_i, n_j \leq (p-1)/2$, tali che $an_i \equiv r_i\, (mod\, p)$ e $an_j \equiv -s_j\, (mod\, p)$. Ma allora

$$a(n_i - n_j) \equiv 0\, (mod\, p)$$

e quindi p divide $n_i - n_j$, il che è possibile solo se $n_i = n_j$, che invece non è. Dunque gli elementi dell'insieme $R = \{r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_t\}$ sono a due a due non congrui modulo p, e di conseguenza $R = \{\ 1, 2, \ldots, (p-i)/2\ \}$. Da ciò segue che

$$a^{\frac{p-1}{2}}((p-1)/2)! = a \cdot 2a \cdots ((p-1)/2)a \equiv (-1)^t((p-1)/2)!\ (mod\, p);$$

e quindi, poiché p non divide $((p-1)/2)!$,

$$a^{\frac{p-1}{2}} \equiv (-1)^t\ (mod\, p)$$

e la dimostrazione si completa applicando il criterio di Eulero. ∎

Il Lemma di Gauss può essere impiegato per calcolare il valore del simbolo di Legendre. Ad esempio, determiniamo $\left(\frac{5}{13}\right)$ (nella tabella di sotto i residui assoluti sono ovviamente intesi modulo 13).

	res. ass.
$1 \cdot 5 = 5$	5
$2 \cdot 5 = 10$	-3
$3 \cdot 5 = 15$	2
$4 \cdot 5 = 20$	-6
$5 \cdot 5 = 25$	-1
$6 \cdot 5 = 30$	4

quindi il numeri t di residui assoluti negativi per i multipli di 5 da considerare è 3 e pertanto, per il Lemma di Gauss,

$$\left(\frac{3}{13}\right) = (-1)^3 = -1.$$

Esercizio 3. Calcolare, usando il Lemma di Gauss, $\left(\frac{7}{17}\right)$ e $\left(\frac{3}{23}\right)$.

Proposizione 4.5 *Sia p un primo dispari. Allora*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dimostrazione. Applichiamo il Lemma di Gauss (e le stesse notazioni) con $a = 2$, e quindi $Q = \{2, 4, \ldots, p-1\}$. In questo caso, gli elementi di Q il cui residuo assoluto modulo p è negativo sono quelli maggiori di $p/2$, ovvero (in ordine decrescente)

$$p-1,\ p-3,\ \ldots,\ p-(2t-1)$$

dove quindi t è il massimo tale che $p-(2t-1) > p/2$, e cioè

$$t = \left[\frac{p+2}{4}\right]$$

dove le parentesi quadre denotano la parte intera.
Se $p \equiv \pm 1 \,(mod\, 8)$, allora $\frac{p^2-1}{8}$ è pari; inoltre, per qualche k, $p = 8k \pm 1$, e quindi

$$t = \left[\frac{p+2}{4}\right] = 2k$$

è pari, e dunque

$$\left(\frac{2}{p}\right) = (-1)^t = 1 = (-1)^{\frac{p^2-1}{8}}.$$

Se invece $p \equiv 3, 5 \,(mod\, 8)$, allora $\frac{p^2-1}{8}$ è dispari, $p = 8k+3$ oppure $p = 8k+5$, e quindi

$$t = \left[\frac{p+2}{4}\right] = 2k+1$$

è dispari, e dunque

$$\left(\frac{2}{p}\right) = (-1)^t = -1 = (-1)^{\frac{p^2-1}{8}}.$$

concludendo la dimostrazione. ∎

Vediamo una applicazione di quest'ultimo risultato ai numeri di Mersenne.

Proposizione 4.6 *Sia $1 \leq k \in \mathbb{N}$, tale che $p = 4k + 3$ sia un numero primo. Allora*

(i) $2p + 1$ *è primo* $\Leftrightarrow$ $2^p \equiv 1 \pmod{2p+1}$.

(ii) Se $2p + 1$ *è primo, allora* $M_p = 2^p - 1$ *non è un numero primo.*

DIMOSTRAZIONE. (i) Osserviamo che $2p + 1 \equiv 7 \pmod 8$. Se $2p + 1$ è un primo, allora, per la Proposizione 4.5,

$$\left(\frac{2}{2p+1}\right) = (-1)^{\frac{(2p+1)^2-1}{8}} = (-1)^{\frac{49-1}{8}} = 1,$$

e quindi, dal criterio di Eulero,

$$2^p = 2^{\frac{(2p+1)-1}{2}} \equiv 1 \pmod{(2p+1)}.$$

Viceversa, supponiamo che $2^p \equiv 1 \pmod{(2p+1)}$. Allora, poiché $(2, 2p+1) = 1$, si ha che p divide l'ordine di 2 modulo $2p+1$, e quindi p divide $\phi(2p+1) = \prod_{i=1}^{s} p_i^{a_1-1}(p_i - 1)$, dove $2p + 1 = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ è la fattorizzazione di $2p + 1$ in potenze di primi distinti. Quindi, $p|p_i$ per qualche $i = 1, 2, \ldots, s$. Sia, per assurdo, $2p+1 \neq p_i$, allora $2p+1 = p_i m$ con $m \geq 3$, e quindi (essendo $p = neq2$) $2p + 1 \geq (p_i - 1)3 > 3p$, una contraddizione. Pertanto, $2p + 1 = p_i$ è un numero primo.

(ii) Segue subito dal punto (i), tenendo conto che, poiché $p > 3$, $2p + 1 \neq 2^p - 1$. ∎

Esercizio 4. Sia $F_n = 2^{2^n} + 1$ l'n-esimo numero di Fermat, e sia p un suo divisore primo. Nell'esercizio 6 del capitolo 3 si è provato che $p \equiv 1 \pmod{2^{n+1}}$. Usando tale fatto, e la Proposizione 4.5, si provi che se $n \geq 2$, allora esiste un intero a tale che

$$a^{2^{n+1}} \equiv -1 \pmod p$$

e si deduca da questo che $p \equiv 1 \pmod{2^{n+2}}$.

4.2 La Legge di Reciprocità Quadratica

Siano p e q numeri primi dispari distinti. Allora, p è un residuo quadratico modulo q se la congruenza

$$x^2 \equiv p \pmod q$$

è risolubile. A prima vista, la risolubilità di tale congruenza non ha molto legame con la risolubilità di quella che si ottiene scambiando p con q, ovvero $x^2 \equiv q \pmod p$. Invece, esiste un legame molto stretto, stabilito dal teorema seguente, che deve considerarsi come uno dei vertici della teoria dei numeri classica.

Teorema 4.7 (**Legge di reciprocità quadratica di Gauss**). *Siano p, q due primi dispari distinti. Allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Esempio. Proviamo che la congruenza $x^2 \equiv 257 \, (mod \, 269)$ non ha soluzioni. Infatti, $269 = 257 + 12$; inoltre 257 e 259 sono numeri primi e possiamo applicare il Teorema di Reciprocità Quadratica, ottenendo

$$\left(\frac{257}{269}\right) = \left(\frac{269}{257}\right) = \left(\frac{12}{257}\right) = \left(\frac{3}{257}\right)\left(\frac{4}{257}\right) = \left(\frac{3}{257}\right) = \left(\frac{257}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Esistono molte dimostrazioni diverse del Teorema di reciprocità Quadratica (pare che ne siano state proposte più di 150), e lo stesso Gauss ne fornì sette distinte. Quella che vedremo è prossima ad una delle dimostrazioni di Gauss; pur non essendo forse la più accessibile, dato che richiede qualche prerequisito algebrico non banale (una dimostrazione di carattere più elementare si trova nell'appendice del capitolo), è piuttosto elegante, e fornisce delle indicazioni sulle possibili generalizzazioni (reciprocità biquadratica, cubica, etc.).

Lemma 4.8 *Sia p un primo dispari, e sia A un sistema di rappresentanti delle classi di congruenza modulo p. Allora*

$$\sum_{a \in A} \left(\frac{a}{p}\right) = 0.$$

Dimostrazione. Il Lemma discende immediatamente dal fatto che, essendo p dispari, esattamente la metà degli elementi di $(\mathbb{Z}/p\mathbb{Z})^*$ è un quadrato (e contribuisce con 1 alla somma), e l'altra metà non lo è (e contribuisce con -1), mentre il contributo alla somma del rappresentante in A della classe nulla è zero. ∎

Dimostrazione *(della legge di reciprocità quadratica).* Siano p e q primi dispari distinti, e sia E un campo di caratteristica q che contenga le radici p-esime dell'unità (ad esempio, si può prendere come E il campo di spezzamento del polinomio $x^p - 1$ sul campo $\mathbb{Z}/q\mathbb{Z}$), e sia $\omega \in E$ una radice primitiva p-esima. Quindi, $\{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$ sono tutte le radici (distinte) del polinomio $x^p - 1 = (x-1)(x^{p-1} + \ldots + x + 1)$ nel campo E. In particolare ω è radice del fattore di destra, e quindi

$$1 + \omega + \omega^2 + \ldots + \omega^{p-1} = 0. \tag{7}$$

Osserviamo che per ogni $z \in \mathbb{Z}$, il valore ω^z dipende solo dalla classe di congruenza di z modulo p. Quindi ha senso definire la potenza ω^a per ogni $a \in \mathbb{Z}/p\mathbb{Z}$ (evitiamo di usare il soprassegno per non appesantire le noatazioni). Se $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$, allora la applicazione $x \mapsto ax$ al variare di $x \in (\mathbb{Z}/p\mathbb{Z})^*$ è una permutazione di $(\mathbb{Z}/p\mathbb{Z})^*$. Dalla formula (7) segue pertanto che, per ogni $a \in (\mathbb{Z}/p\mathbb{Z})^*$,

$$\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} \omega^{ax} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} \omega^x = \omega + \omega^2 + \ldots + \omega^{p-1} = -1. \tag{8}$$

Definiamo ora l'applicazione $\tau : \mathbb{Z}/p\mathbb{Z} \longrightarrow E$, ponendo, per ogni $a \in \mathbb{Z}/p\mathbb{Z}$,

$$\tau(a) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{x}{p}\right) \omega^{ax}.$$

Nel seguito, per non scrivere troppo, indicheremo con F il campo $\mathbb{Z}/p\mathbb{Z}$. Proviamo che, per ogni $a \in (\mathbb{Z}/p\mathbb{Z})^* = F^*$,

$$\tau(a) = \left(\frac{a}{p}\right)\tau(1). \tag{9}$$

Infatti,

$$\begin{aligned}\tau(a) &= \sum_{x\in F^*}\left(\frac{x}{p}\right)\omega^{ax} = \sum_{x\in F^*}\left(\frac{a^{-1}xa}{p}\right)\omega^{ax} = \left(\frac{a^{-1}}{p}\right)\sum_{x\in F^*}\left(\frac{xa}{p}\right)\omega^{ax} = \\ &= \left(\frac{a}{p}\right)\sum_{x\in F^*}\left(\frac{t}{p}\right)\omega^{t} = \left(\frac{a}{p}\right)\tau(1).\end{aligned}$$

Ora, dimostriamo che

$$\tau(1)^2 = (-1)^{(p-1)/2}p. \tag{10}$$

Infatti, applicando la formula (9), si ha

$$\begin{aligned}\tau(1)^2 &= \tau(1)\sum_{x\in F^*}\left(\frac{x}{p}\right)\omega^{x} = \sum_{x\in F^*}\tau(x)\omega^{x} = \sum_{x\in F^*}\left[\sum_{y\in F^*}\left(\frac{y}{p}\right)\omega^{xy}\right]\omega^{x} = \\ &= \sum_{x\in F^*}\sum_{y\in F^*}\left(\frac{y}{p}\right)\omega^{x(y+1)} = \sum_{y\in F^*}\left[\left(\frac{y}{p}\right)\sum_{x\in F^*}\omega^{x(y+1)}\right];\end{aligned}$$

Ora, per la formula (8), se $y \in F^*$ e $y+1 \neq 0$, si ha

$$\sum_{x\in F^*}\omega^{x(y+1)} = -1.$$

Quindi, applicando il Lemma 4.8 ed il Lemma 4.3,

$$\begin{aligned}\tau(1)^2 &= -\sum_{y\in F^*}\left(\frac{y}{p}\right) + \left(\frac{-1}{p}\right) + \left(\frac{-1}{p}\right)\sum_{x\in F^*}\omega^{0} = \\ &= \left(\frac{-1}{p}\right)(1+(p-1)) = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p.\end{aligned}$$

Completiamo ora la dimostrazione del Teorema. Applicando la formula (10), sia ha

$$\tau(1)^{q-1} = (\tau(1)^2)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}$$

e quindi, per il criterio di Eulero (tenendo conto che in E moltiplicare per q da zero),

$$\tau(1)^{q-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{11}$$

D'altra parte, poichè E è un campo di caratteristica q, l'elevazione alla q-esima potenza è un omomorfismo di E in se stesso. In particolare,

$$\tau(1)^q = \left(\sum_{x\in F^*}\left(\frac{x}{p}\right)\omega^{x}\right)^q = \sum_{x\in F^*}\left(\frac{x}{p}\right)^q\omega^{qx} = \tau(q).$$

Confrontando quest'ultima eguaglianza (nel campo E) con la (11), ed applicando la formula (9), si ricava

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \tau(1)^{q-1} = \tau(q)\tau(1)^{-1} = \left(\frac{q}{p}\right) \tag{12}$$

Questa è un'uguaglianza nel campo E, nella quale quindi gli interi vanno intesi come multipli dell'identità. D'altra parte, i simboli di Legendre $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$ appartengono a $\{1, -1\}$ e, siccome q (che è la caratteristica di E) è dispari, in E, $-1 \neq 1$. Ne segue che dalla uguaglianza (12) deriva l'uguaglianza in $\mathbb{Z}$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

concludendo così la dimostrazione del Teorema. ■

Esercizio 5. Si dica se la congruenza

$$17x^2 + 28x - 11 \equiv 0 \pmod{503}$$

ammette soluzioni.

Esercizio 6. Si dica se la congruenza

$$7x^2 + 12x - 19 \equiv 0 \pmod{1067}$$

ammette soluzioni (si faccia attenzione che 1067 non è un numero primo).

Esercizio 7. Sia p un primo dispari. Si provi che 3 è un residuo quadratico modulo p se e solo se $p \equiv \pm 1 \pmod{12}$.

Esercizio 8. Si caratterizzino tutti i primi dispari p, tali che 5 è un residuo quadratico modulo p.

Esercizio 9. Si provi che la congruenza

$$(x^2 - 5)(x^2 - 6) \equiv 0 \pmod{p}$$

è risolubile per ogni primo p.

Esercizio 10. Sia p un primo dispari. Si provi che la congruenza

$$3x^2 + y^2 \equiv 0 \pmod{p}$$

ha soluzioni non banali (cioè con $x, y \not\equiv 0 \pmod{p}$) se e solo se $p \equiv 1 \pmod{3}$.

4.3 Il simbolo di Jacobi

Il **simbolo di Jacobi** estende al caso dei numeri dispari il simbolo di Legendre per i numeri primi.

Definizione. Sia $1 < b$ un intero dispari, e sia $b = p_1 p_2 p_3 \cdots p_k$, come prodotto di numeri primi (non necessariamente distinti). Per ogni $a \in \mathbb{Z}$ si pone

$$\left(\frac{a}{b}\right)_J = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{p_3}\right)\cdots\left(\frac{a}{p_k}\right)$$

dove, per ogni $i = 1, 2, \ldots, k$

$$\left(\frac{a}{p_i}\right)$$

è l'usuale simbolo di Legendre.

Osserviamo subito che, diversamente dal simbolo di Legendre, il simbolo di Jacobi non individua i residui quadratici modulo b. Infatti, se a è un R.Q. modulo b, allora a è un R.Q. modulo ogni primo p_i e dunque

$$\left(\frac{a}{b}\right)_J = 1;$$

ma è possibile che il simbolo di Jacobi calcolato in a sia uguale ad 1 senza che a sia un R.Q. modulo b. Ad esempio, se $b = 9$, ed $a = -1$,

$$\left(\frac{-1}{9}\right)_J = \left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right) = (-1)(-1) = 1$$

mentre -1 non è un R.Q. modulo 9.

Tuttavia, il simbolo di Jacobi è utile per semplificare diversi argomenti. Ne vedremo un esempio con il Teorema 4.11. Prima elenchiamo alcune immediate proprietẹl simbolo di Jacobi; esse discendono dalla definizione e dalle analoghe proprietà del simbolo di Legendre (Lemma 4.3).

Lemma 4.9 *Siano b, b_1, b_2 numeri naturali dispari maggiori di 1, e siano a, a_1, a_2 interi. Allora*

1) $\left(\frac{a_1}{b}\right)_J = \left(\frac{a_2}{b}\right)_J$ *se* $a_1 \equiv a_2 \,(mod\, b)$
2) $\left(\frac{a_1 a_2}{b}\right)_J = \left(\frac{a_1}{b}\right)_J \left(\frac{a_2}{b}\right)_J$
3) $\left(\frac{a}{b_1}\right)_J \left(\frac{a}{b_2}\right)_J = \left(\frac{a}{b_1 b_2}\right)_J$
4) $\left(\frac{-1}{b}\right)_J = (-1)^{\frac{b-1}{2}}$
5) $\left(\frac{2}{b}\right)_J = (-1)^{\frac{b^2-1}{8}}$.

Dimostrazione. I punti 1), 2) e 3) si deducono immediatamente dalla definizione di simbolo di Jacobi e dalla moltiplicativitẹl simbolo di Legendre.

Per i rimanenti punti osserviamo preliminarmente che se m e n sono numeri naturali dispri allora

$$mn-1 \equiv (m-1)+(n-1) \ (mod\, 4)$$

e quindi

$$\frac{mn-1}{2} \equiv \frac{m-1}{2}+\frac{n-1}{2} \ (mod\, 2).$$

Dunque, se $b = p_1 p_2 \cdots p_k$, per il Lemma 4.3,

$$\left(\frac{-1}{b}\right)_J = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i-1}{2}} = (-1)^{\sum \frac{p_i-1}{2}} = (-1)^{\frac{b-1}{2}}$$

provando il punto (4). Dalla stessa osservazione di sopra segue anche che, se n e m sono dispari

$$\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8}+\frac{n^2-1}{8} \ (mod\, 2).$$

Dunque, per la Proposizione 4.5,

$$\left(\frac{2}{b}\right)_J = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum \frac{p_i^2-1}{8}} = (-1)^{\frac{b^2-1}{8}}$$

provando il punto (5). ■

Dal teorema di reciprocità quadratica di Gauss discende inoltre un analogo risultato per il simbolo di Jacobi.

Lemma 4.10 *Siano b_1, b_2 due interi positivi dispari. Allora*

$$\left(\frac{b_1}{b_2}\right)_J\left(\frac{b_2}{b_1}\right)_J = (-1)^{\frac{b_1-1}{2}\frac{b_2-1}{2}}.$$

Esempio. Consideriamo $b = 803 = 11 \cdot 73$;

$$\left(\frac{403}{803}\right)_J = -\left(\frac{803}{403}\right)_J = -\left(\frac{-3}{403}\right) = \left(\frac{3}{403}\right) = -\left(\frac{403}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Teorema 4.11 *Un numero intero $a \in Z$ è un quadrato in $\mathbb{Z}$ se e solo se $\left(\frac{a}{p}\right) = 1$ per ogni primo dispari p che non divide a.*

Dimostrazione. Se a è un quadrato in $\mathbb{Z}$, allora è ovvio che è un R.Q. modulo ogni primo dispari che non lo divide.
Viceversa, proviamo che se a non è un quadrato in $\mathbb{Z}$, allora esiste un primo p con $(a,p) = 1$, tale che a non è un R.Q. modulo p. Distinguiamo tre casi.

(1) $a = -b^2$ per qualche $b \in \mathbb{N}$.

Scegliamo un intero $k > 0$ tale che $(b,k) = 1$ e $k \equiv 1\,(mod\,4)$. Allora, applicando il lemma 4.9,

$$\left(\frac{a}{k}\right)_J = \left(\frac{-b^2}{k}\right)_J = \left(\frac{-1}{k}\right)_J = (-1)^{\frac{k-1}{2}} = -1$$

e quindi, per la definizione del simbolo di Jacobi, esiste un divisore primo p di k tale che $\left(\frac{a}{p}\right) = -1$, cioè a non è un R.Q. modulo p.

(2) $a = \pm 2^t b$, con t e b numeri naturali dispari.
Per il Teorema Cinese del Resto, esiste un intero positivo k tale che

$$\begin{cases} k \equiv 5\,(mod\,8) \\ k \equiv 1\,(mod\,b). \end{cases}$$

Per tale k si ha, essendo t dispari,

$$\left(\frac{2^t}{k}\right)_J = \left(\frac{-2^t}{k}\right)_J = -1,$$

ed anche, applicando il Lemma 4.10,

$$\left(\frac{b}{k}\right)_J = \left(\frac{k}{b}\right)_J = \left(\frac{1}{b}\right)_J = 1.$$

Quindi

$$\left(\frac{a}{k}\right)_J = \left(\frac{\pm 2^t}{k}\right)_J \left(\frac{b}{k}\right)_J = -1,$$

e dunque esiste un divisore primo di k, rispetto al quale a non è un R.Q.

(3) $a = \pm 2^{2n} q^t b$, con b numero naturale dispari, q un primo dispari tale che $(q,b) = 1$, e $t \geq 1$.
Poiché q è dispari, esiste un naturale c tale che $\left(\frac{c}{q}\right) = -1$. Per il Teorema Cinese del Resto, esiste un intero positivi k tale che

$$\begin{cases} k \equiv 1\,(mod\,4b) \\ k \equiv c\,(mod\,q). \end{cases}$$

Per tale intero k si ha

$$\left(\frac{2^{2n}}{k}\right)_J = \left(\frac{-2^{2n}}{k}\right)_J = 1,$$

e, applicando il Lemma 4.10,

$$\left(\frac{b}{k}\right)_J = \left(\frac{k}{b}\right)_J = \left(\frac{1}{b}\right)_J = 1,$$

inoltre, poiché t è dispari,

$$\left(\frac{q^t}{k}\right)_J = \left(\frac{q}{k}\right)_J = \left(\frac{k}{q}\right)_J = \left(\frac{c}{q}\right)_J = -1.$$

Quindi

$$\left(\frac{a}{k}\right)_J = \left(\frac{\pm 2^t}{k}\right)_J \left(\frac{b}{k}\right)_J \left(\frac{q^t}{k}\right)_J = -1,$$

e dunque esiste un divisore primo di k, rispetto al quale a non è un R.Q.

Poiché ogni intero a rientra in uno dei tre casi (1), (2), (3), il Teorema è dimostrato. ∎

Esercizio 11. Siano p un primo dispari ed a un intero non divisibile per p. Si provi che, per ogni $n \geq 1$, a è un R.Q. modulo p^n se e solo se a è un R.Q. modulo p.

Esercizio 12. Questo esercizio caratterizza i numeri interi positivi n tali che -1 è un R.Q. modulo n. Sia $2 \leq n \in \mathbb{N}$, e denotiamo con $\nu(n)$ il numero di soluzioni distinte (modulo n) della congruenza

$$x^2 \equiv -1 \pmod{n}.$$

Si provi che $\nu(n) = 0$ se $4|n$ oppure n ha un divisore primo p con $p \equiv 3 \pmod 4$. Se invece $n = 2^e p_1^{a_1} \cdots p_s^{a_s}$, con $e = 0, 1$, e p_i primi distinti e tali che $p \equiv 1 \pmod 4$, allora $\nu(n) = 2^s$.

4.4 Appendice I: Un'altra dimostrazione della Legge di Reciprocità Quadratica.

Quella che vediamo è una dimostrazione di carattere più elementare di quella fornita nel testo, ed è sostanzialmente la terza delle dimostrazioni proposte da Gauss.

Siano quindi p e q numeri primi dispari distinti. Poniamo

$$P = \{1, 2, \ldots, (p-1)/2\} \qquad \text{e} \qquad Q = \{1, 2, \ldots, (q-1)/2\}.$$

Sia s il numero di elementi dell'insieme $Pq = \{xq \mid x \in P\}$ il cui residuo assoluto modulo p è negativo, e sia t il numero di elementi dell'insieme $Qp = \{xp \mid x \in Q\}$ il cui residuo assoluto modulo q è negativo. Per il Lemma di Gauss, (Lemma 4.4)

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

La Legge di reciprocità quadratica equivale quindi ad affernare che

$$s + t \text{ è dispari} \quad \Leftrightarrow \quad p \equiv q \equiv 3 \pmod 4.$$

Consideriamo l'insieme N di tutte le coppie $(u, v) \in P \times Q$ tali che

$$-q/2 < vp - uq < 0. \tag{13}$$

Queste sono i punti a coordinata intera che (in un usuale piano cartesiano) giacciono all'interno del trapezio di coordinate

$$A_0 = (0, 0) \quad A_1 = (p/2,\, q/2) \quad B_1 = (0,\, 1/2) \quad B_2 = (p/2,\, q(p-1)/2p).$$

La condizione (13) implica che se $(u, v) \in N$, allora il residuo assoluto di vp modulo q è negativo. Pertanto $|N| \leq t$.
Viceversa, se $j \in Q$ è tale che il residuo assoluto di jp modulo q è negativo, allora esiste un intero k tale che $-q/2 < jp - kq < 0$. Quindi, $jp < kq < jp + q/2$; siccome $1 \leq j \leq (q-1)/2$ si ha

$$p < kq < \frac{(q-1)p}{2} + \frac{q}{2}$$

da cui segue,

$$\frac{p}{q} < k < \frac{q-1}{q} \cdot \frac{p}{2} + \frac{1}{2} < \frac{p+1}{2}$$

ed essendo k intero e p dispari

$$1 \leq k \leq (p-1)/2$$

ovvero $k \in P$. In conclusione per ogni $j \in Q$ tale che il residuo assoluto di jp modulo q è negativo esiste uno ed un solo punto $(j, k) \in N$.
Pertanto $|N| \geq t$, e dunque $|N| = t$.

Allo stesso modo si prova che il numero di coppie $(u, v) \in P \times Q$ tali che

$$-p/2 < uq - vp < 0 \tag{14}$$

è uguale a s. In questo caso si tratta dei punti a coordinate intere che giacciono all'interno del trapezio di vertici

$$A_0 = (0, 0) \quad A_1 = (p/2,\, q/2) \quad C_1 = (0, 0) \quad C_2 = (p/2,\, p(q-1)/2q).$$

Quindi, $s + t$ è uguale alla cardinalità dell'insieme U di tutti i punti a coordinata intera che giacciono all'interno dell'esagono di vertici A_0, B_1, B_2, A_1, C_2, C_1.

Ora, si verifica facilmente che $X = (x_0, y_0) \in U$ se e solo se $\sigma(X) = (x_1, y_1) \in U$, dove

$$\begin{cases} x_1 = \frac{p+1}{2} - x_0 \\ \\ y_1 = \frac{q+1}{2} - y_0. \end{cases}$$

Dunque, σ definisce una biezione involutoria su U (cioè $\sigma(\sigma(X)) = X$ per ogni $X \in U$). Supponiamo che $X = (x_0, y_0)$ sia un punto fisso per σ (ovvero $\sigma(X) = X$). Allora

$$\begin{cases} 2x_0 = \frac{p+1}{2} \\ \\ 2y_0 = \frac{q+1}{2} \end{cases}$$

Ne segue, in particolare, che esiste al più un punto fisso per σ. Siccome σ è una involuzione, il numero di elementi di U che non sono fissati da σ è pari. Quindi, un punto fisso esiste se e solo se $|U| = s + t$ è dispari. D'altra parte, dalle due equazioni che lo caratterizzano, si conclude che, essendo x_0 e y_0 numeri interi, un punto fisso per σ esiste se e solo se $p \equiv q \equiv 3 \pmod 4$.
Ciò conclude la dimostrazione.

Soluzione di alcuni esercizi.

Esercizio 1. Le soluzioni sono 7, 9 (e tutti gli interi congrui ad una di esse modulo 13).

Esercizio 4. Sia p un divisore primo di F_n. Poiché $p = 1 + k2^{n+1}$ (per qualche $k \geq 1$) ed essendo $n \geq 2$, si ha che, 2^4 divide $p^2 - 1$. Quindi, per la Proposizione 4.5, 2 è un R.Q. modulo p, e quindi esiste una intero a tale che $a^2 \equiv 2 \pmod{p}$, e quindi

$$a^{2^{n+1}} = (a^2)^{2^n} \equiv 2^{2^n} \equiv -1 \pmod{p}.$$

Inoltre $a^{2^{n+2}} \equiv 1 \pmod{p}$. Pertanto, l'ordine di a modulo p è un divisore di 2^{n+2}, ma non è 2^{n+1}, e dunque è proprio 2^{n+2}. In particolare 2^{n+2} divide $\phi(p) = p - 1$, e quindi $p \equiv 1 \pmod{2^{n+2}}$.

Esercizio 6. Poiché $1067 = 11 \cdot 97$, per il Teorema Cinese del Resto, la congruenza data è risolubile se e solo se sono risolubili le stesse congruenze modulo 11 e 97. Questo si verifica se e solo se il discriminante, $\Delta = 12^2 - 4 \cdot 7 \cdot (-19) = 676$ del polinomio $7x^2 + 12x - 19$ è un R.Q. modulo 11 e modulo 97. Applicando le proprietà del simbolo di Legendre, tenendo conto che $169 \equiv 4 \pmod{11}$, si ha

$$\left(\frac{676}{11}\right) = \left(\frac{4 \cdot 169}{11}\right) = \left(\frac{4}{11}\right)\left(\frac{169}{11}\right) = \left(\frac{169}{11}\right) = \left(\frac{4}{11}\right) = 1.$$

Inoltre, tenendo conto che $169 \equiv -3 \pmod{97}$, e del criterio di Eulero,

$$\left(\frac{676}{97}\right) = \left(\frac{169}{97}\right) = \left(\frac{-1}{97}\right)\left(\frac{3}{97}\right) = (-1)^{48}\left(\frac{3}{97}\right) = \left(\frac{3}{97}\right).$$

Applicando la legge di reciprocità quadratica

$$\left(\frac{676}{91}\right) = (-1)^{1\cdot 45}\left(\frac{97}{3}\right) = -\left(\frac{97}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Quindi la congruenza di partenza non è risolubile.

Esercizio 7. Sia p un primo dispari, e $p \neq 3$. Allora, per il Teorema di reciprocità quadratica,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Pertanto 3 è un R.Q. modulo p se e solo se $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$.
Se $p \equiv 1 \pmod{3}$, allora $\left(\frac{p}{3}\right) = 1$, e quindi la condizione è soddisfatta se e solo se $4|p-1$, ovvero se e solo se $p \equiv 1 \pmod{12}$.
Altrimenti, $p \equiv 2 \pmod{3}$, e $\left(\frac{p}{3}\right) = -1$. In tal caso la condizione è soddisfatta se e solo se 4 non divide $p - 1$ (cioè, essendo p dispari, $p \equiv -1 \pmod{4}$), ovvero se e solo se $p \equiv -1 \pmod{12}$.

Esercizio 10. La congruenza data ha soluzioni non banali se e solo se esistono interi x e y non divisibili per p tali che, nel campo $\mathbb{Z}/p\mathbb{Z}$, $3\overline{x}^2 = -\overline{y}^2$, ovvero

$$-\overline{3} = (\overline{y} \cdot \overline{x}^{-1})^2.$$

Quindi, la congruenza è risolubile se e solo se -3 è un residuo quadratico modulo p. Applicando il criterio di Eulero e il Teorema di reciprocità quadratica, si ha

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right),$$

concludendo che -3 è un residuo quadratico modulo p se e solo se $p \equiv 1 \pmod 3$.

Esercizio 11. In un senso la cosa è ovvia. Per il viceversa, applicare il Lemma di Hensel.

5 Teoria additiva.

Con Teoria Additiva dei Numeri si intende compendiare in modo generico quelle questioni che riguardano la possibilità di rappresentare ogni numero naturale (o ogni numnero naturale sufficientemente grande, oppur appartenente ad un certo sottoinsieme notevole) come somma di elementi di un fissato sottoinsieme S dei numeri interi.
Un tipico probelma di teoria additiva dei numeri è la famosa *congettura di Goldbach*, la quale afferma che ogni numero naturale pari è somma di due numeri primi (o, equivalentemente, che ogni numero naturale è somma di al più tre primi).

5.1 Somme di 2 quadrati

Teorema 5.1 (Eulero). *Sia p un numero primo. Allora l'equazione*

$$x^2 + y^2 = p$$

è risolubile se e solo se $p = 2$ oppure $p \equiv 1 \, (mod\, 4)$.

Di questo Teorema vedremo due dimostrazioni. La prima, simile a quella originale, utilizza il cosiddetto "metodo della discesa", introdotto da P. Fermat, che riapplicheremo più avanti per dimostrare il Teorema di Lagrange sulla somma di quattro quadrati; la seconda, più moderna, utilizza le proprietà algebriche dell'anello degli interi di Gauss. Vediamo la prima dimostrazione

Dimostrazione. Poichè $2 = 1 + 1 = 1^2 + 1^2$, l'affermazione è vera per $p = 2$. Inoltre, per ogni intero a, si ha $a^2 \equiv 0, 1 \, (mod\, 4)$, quindi, per ogni $a, b \in \mathbb{N}$,

$$a^2 + b^2 \equiv 0, 1, 2 \, (mod\, 4) \ ;$$

dunque $x^2 + y^2 = p$ non è risolubile se $p \equiv 3 \, (mod\, 4)$.

Supponiamo ora $p \equiv 1 \, (mod\, 4)$. Allora, $4|p - 1$ e dunque esiste un intero $0 < t < p/2$ tale che $t^2 \equiv -1 \, (mod\, p)$. Pertanto (prendendo ad esempio $x_0 = t, \ y_0 = 1$) esistono interi x_0, y_0, k, con $0 < k < p$, tali che

$$x_0^2 + y_0^2 = kp \ . \tag{15}$$

Tra le possibili terne di questo tipo, scegliamo una in modo che k sia minimo, e supponiamo per assurdo che sia $k > 1$.
Utilizzeremo la seguente identità

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2. \tag{16}$$

Poniamo

$$\begin{aligned} x_0 &= bk + x_1 \\ y_0 &= ck + y_1 \end{aligned}$$

dove b, c sono interi, e x_1, y_1 sono rappresentanti di x_0, y_0 modulo k che possiamo trovare in modo che

$$-\frac{k}{2} \leq x_1,\ y_1 \leq \frac{k}{2}\ .$$

Allora,

$$x_1^2 + y_1^2 = (x_0 - bk)^2 + (y_0 - ck)^2 \equiv x_0^2 + y_0^2 \equiv 0\,(mod\,k)\ ;$$

dunque $x_1^2 + y_1^2 = k_1 k$, con $k_1 < k$, perchè, per la scelta di x_1, y_1,

$$x_1^2 + y_1^2 \leq 2(k/2)^2 = k^2/2\ .$$

Applicando le formula (2) otteniamo

$$(x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0x_1 + y_0y_1)^2 + (x_0y_1 - x_1y_0)^2 = k_1k^2p\ .$$

Ora,

$$x_0x_1 + y_0y_1 = x_0(x_0 - bk) + y_0(y_0 - ck) \equiv x_0^2 + y_0^2 \equiv 0\,(mod\,k)$$

e, similmente

$$x_0y_1 - x_1y_0 = x_0(y_0 - ck) - (x_0 - bk)y_0 \equiv x_0y_0 - x_0y_0 \equiv 0\,(mod\,k)\ ;$$

per cui, ponendo

$$x_2 = \frac{x_0x_1 + y_0y_1}{k} \qquad\qquad y_2 = \frac{x_0y_1 - x_1y_0}{k}$$

si ha

$$x_2^2 + y_2^2 = k_1p$$

comtro la scelta di k. ∎

Prima di esaminare brevemente la seconda dimostrazione di questo risultato, vediamone una conseguenza.

Teorema 5.2 *Sia $n \in \mathbb{N}^*$. Allora l'equazione*

$$x^2 + y^2 = n$$

è risolubile se e solo se per ogni primo $p \equiv 3\,(mod\,4)$, la massima potenza di p che divide n ha esponente pari.

Dimostrazione. Sia $Q = \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$; l'identità (2) della dimostrazione precedente assicura che Q è moltiplicativamente chiuso. Quindi se $n = 2^{\alpha_0}p_1^{\alpha_1}\dots p_n^{\alpha_n}$ con α_k pari per i primi $p_k \equiv 3\,(mod\,4)$, allora $n \in Q$ per il teorema precedente.
Viceversa, sia $p \equiv 3\,(mod\,4)$, e supponiamo che $n = p^{2k+1}m$ appartenga a Q con $(p, m) = 1$ e k minimale. Siano $x, y \in \mathbb{N}$ tali che $x^2 + y^2 = n$. Si ha che p non divide xy, perchè se p divide x o y, allora p^2 divide $x^2 + y^2 = n$ e quindi anche $p^{2k-1}m$ appartiene a Q, contro la scelta di k. Allora y è invertibile modulo p e dunque, da $x^2 \equiv -y^2\,(mod\,p)$ comporta

$$\left(\frac{x}{y}\right)^2 \equiv -1\,(mod\,p)$$

e dunque

$$\left(\frac{-1}{p}\right) = 1$$

che è assurdo. ■

Ricordiamo ora la definizione dell'anello degli interi di Gauss; esso è il sottonisieme del campo $\mathbb{C}$,

$$\mathbb{Z}[i] = \{\ a + ib \mid a, b \in \mathbb{Z}\ \}\ .$$

La usuale *norma* su $\mathbb{C}$ (definita da, per ogni $z \in \mathbb{C}$, $N(z) = z \cdot \overline{z}$ induce una norma su $\mathbb{Z}[i]$, quindi, per ogni $z = a + ib \in \mathbb{Z}[i]$

$$N(z) = (a + ib)(a - ib) = a^2 + b^2$$

è un numero intero positivo. Richiamiamo due proprietà elementari ma importanti della norma,

$N(uv) = N(u)N(v)$, per ogni $u, v \in \mathbb{C}$;

$N(u) = 0$ se e solo se $u = 0$.

È ben noto che, mediante la norma, $\mathbb{Z}[i]$ è un dominio Euclideo; pertanto è un dominio a ideali principali e a fattorizzazione unica. Gli elementi primi di $\mathbb{Z}[i]$ sono chiamati *primi di Gauss* (mentre, in questa parte, chiameremo primi *razionali* i primi di $\mathbb{Z}$).

Lemma 5.3 *Gli elementi invertibili di* $\mathbb{Z}[i]$ *sono* $1, -1, i, -i$.

Dimostrazione. Esercizio. Si prrovi innanzi tutto che gli elementi invertibili di $\mathbb{Z}[i]$ sono tutti e soli quelli di norma 1. ■

Lemma 5.4 *Sia* π *un primo di Gauss; allora* $N(\pi) = p, p^2$ *per un primo razionale* p.

Dimostrazione. Sia π un primo di Gauss. Allora, $\pi\overline{\pi} = N(\pi) > 1$, e quindi esiste un primo razionale p che divide $N(\pi)$. Quindi

$$\pi\overline{\pi} = p \cdot b$$

per qualche $b \in \mathbb{Z}$. Poichè π è un primo in $\mathbb{Z}[i]$ si ha allora che

$$\pi | p \qquad \text{oppure} \qquad \overline{\pi} | p\ .$$

Se $\pi | p$, allora $p = \pi u$ per qualche $u \in \mathbb{Z}[i]$, e quindi

$$p^2 = N(p) = N(\pi)N(u)$$

e dunque $N(\pi) = p$ oppure $N(\pi) = p^2$. Similmente se $\overline{\pi} | p$. ■

Proposizione 5.5 *Sia* p *un numero primo razionale. Allora le seguenti condizioni sono equivalenti.*

1) $p = N(\pi)$ *per qualche primo di Gauss* π*;*

2) $p = a^2 + b^2$ *con* $a, b \in \mathbb{Z}$*;*

3) $p \equiv 1 \,(mod\, 4)$ *oppure* $p = 2$*.*

DIMOSTRAZIONE. 1) $\Rightarrow$ 2) è chiara.

2) $\Rightarrow$ 3) è vista all'inizio dell dimostrazione del Teorema 5.1.

3) $\Rightarrow$ 1) Se $p = 2$, allora $2 = N(1 + i)$.
Sia ora $p \equiv 1 \,(mod\, 4)$; allora $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$. Quindi esistono $a, k \in \mathbb{N}$, tali che $a^2 + 1 = kp$. Nell'anello $\mathbb{Z}[i]$, si ha quindi

$$(a + i)(a - i) = kp$$

Poiché $a \neq 0$, $a + i$ non è invertibile in $\mathbb{Z}[i]$, ed esiste un elemento irriducibile (cioè un primo di Gauss) π di $\mathbb{Z}[i]$, che divide $a + i$ (oppure $a - i$) e divide p. Ora, $\overline{\pi}$ divide $\overline{p} = p$, e quindi, dato che π e $\overline{\pi}$ non sono associati in $\mathbb{Z}[i]$, si deduce che

$$N(\pi) = \pi\overline{\pi} \text{ divide } p;$$

poiché $1 < N(\pi)$, si conclude che $N(\pi) = p$. ∎

Esercizio 1. Sia p un numero primo. Si provi che ognuna delle seguenti equazioni diofentee

$$x^2 - xy + y^2 = p \qquad x^2 + 3y^2 = p$$

è risolubile se e solo se $p = 3$ oppure $p \equiv 1 \,(mod\, 3)$.

Esercizio 2. per ogni $n \in \mathbb{N}^*$, sia $\nu(n)$ il numero di soluzioni di $x^2 \equiv -1 \,(mod\, n)$. Si provi che il numero di soluzioni dell'equazione $x^2 + y^2 = n$ con $(x, y) = 1$ è uguale a $4\nu(n)$.

5.2 Problema di Waring. Somme di 4 quadrati

Teorema 5.6 (Lagrange). *Ogni numero naturale è somma di* 4 *quadrati.*

DIMOSTRAZIONE. Useremo la seguente identità (dovuta ad Eulero)

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{17}$$

dove

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \ . \end{aligned}$$

Il risultato è banalmente vero per $n = 0, 1, 2$; l'identità 17 assicura quindi che è sufficiente dimostrarlo per un primo $p \geq 3$. Sia dunque p un primo dispari.
Sappiamo che ogni intero è congruo modulo p ad una somma di due quadrati. Dunque, esistono x_0, y_0 tali che $x^2 + y^2 \equiv -1 \, (mod\, p)$. Tali interi x, y possono essere presi in modo che $0 \leq x, y \leq \frac{p-1}{2}$. Dunque sistono interi positivi x, y ed m tali che

$$1 + x^2 + y^2 = mp \tag{18}$$

ed inoltre $0 < 1 + x^2 + y^2 < 1 + 2(\frac{p}{2})^2 < p^2$; e quindi

$$0 < m < p \ .$$

Sia ora m_0 il più piccolo intero positivo tale che $m_0 p$ è somma di quattro quadrati. Vogliamo provare che $m_0 = 1$. Per la (4), si ha $0 < m_0 < p$.
Siano x_1, x_2, x_3, x_4 interi tale che

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \ . \tag{19}$$

Supponiamo per assurdo, $m_0 \geq 2$, ed analizziamo separatamente i due casi: I) m_0 è pari; II) m_0 è dispari.

I) Se m_0 è pari, allora $x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p$ è pari; quindi $x_1 + x_2 + x_3 + x_4$ è pari. Dunque si verifica una delle seguenti posssibilità:
i) x_1, x_2, x_3, x_4 sono tutti pari;
ii) x_1, x_2, x_3, x_4 sono tutti dispari;
iii) x_1, x_2, x_3, x_4 sono due pari e due dispari; in questo caso possiamo assumere che x_1, x_2 siano pari, e x_3, x_4 siano dispari.
In tutti e tre i casi si ha che

$$x_1 + x_2, \ x_1 - x_2, \ x_3 + x_4, \ x_3 - x_4$$

sono interi pari. Ma allora

$$\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

il che, poichè $\frac{m_0}{2}$ è un intero, contraddice la scelta di m_0.

II) Sia m_0 dispari; e quindi $m_0 \geq 3$. Allora, dividendo gli x_i per m_0; è possibile trovare interi b_i e y_i, per $i = 1, 2, 3, 4$, tali che

$$y_i = x_i - b_i m_0 \qquad \text{con} \ \ |y_i| < \frac{m_0}{2} \ .$$

Osserviamo che, poichè m_0 non divide p, almeno uno degli x_i non è divisibile per m_0, e quindi che almeno uno degli y_i è diverso da 0. Dunque

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 = 4\left(\frac{m_0}{2}\right)^2 = m_0^2$$

ed inoltre

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \, (mod\, m_0)$$

ovvero, mettendo insieme queste due proprietà,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0 \tag{20}$$

per qualche $0 < m_1 < m_0$. Moltiplicando membro a membro l'uguaglianza (5) e la (6), otteniamo

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p$$

dove gli z_i sono dati dall'identità di Eulero (3). Ora, si osserva che

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i(x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \,(mod\, m_0) \ .$$

Analogamente si prova che, per $i = 1, 2, 3, 4$, si ha $z_i \equiv 0 \,(mod\, m_0)$. Esistono quindi interi positivi t_1, t_2, t_3, t_4 tali che

$$z_i = m_0 t_i \qquad \text{per} \ \ i = 1, 2, 3, 4 \ .$$

ma allora

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p$$

che, ancora una volta, è in contraddizione con la scelta di m_0.
Pertanto, deve essere $m_0 = 1$, e dunque p è somma di quattro quadrati, completando così la dimostrazione del Teorema. ∎

Il precedente teorema, enunciato da Fermat, fu dimostrato da Lagrange nel 1770 (grosso modo con la stessa tecnica che abbiamo utilizzato sopra). In quello stesso anno, nel suo libro *Meditationes Algebricae*, Edward Waring affermò, senza provarlo, che ogni numero intero può essere espresso come somma di al più 9 cubi, e di al più 19 quarte potenze. Più tardi, nell'edizione del 1782, egli aggiunse la congettura che per ogni $k \geq 2$, esiste un intero s tale che ogni numero naturale può scriversi come somma di al più s potenze k-esime. Nella letteratura moderna, fissato un k, si suole indicare con $g(k)$ il minimo valore possibile di tale s. La dimostrazione della congettura, ovvero dell'esistenza di $g(k)$ per ogni $k \geq 2$, fu data da Hilbert nel 1909. La determinazione dei valori esatti di $g(k)$ (che viene comunemente chiamato *problema di Waring*), richiese più tempo, e lo sforzo combinato di diversi studiosi e tecniche.

Il Teorema di Lagrange risolve il caso $k = 2$.

Corollario 5.7 $g(2) = 4$.

Dimostrazione. Per il Teorema di Lagrange $g(2) \leq 4$. D'altra parte si vede subito che $n = 7$ non è somma di 3 quadrati. Dunque $g(2) = 4$. ∎

Il caso $n = 3$ fu risolto indipendentemente da Wieferich e da Kemper nel 1909-1912; essi provarono che $g(3) = 9$, ovvero che ogni numero naturale può essere espresso come somma di 9 cubi interi, e che esistono numeri naturali che non sono somma di otto cubi. Più tardi, Dickson provò che 23 e 239 sono i soli numeri naturali che richiedono almeno nove cubi, e nel 1943 Linnik dimostrò che ogni numero naturale sufficientemente grande può essere rappresentato come somma di 7 cubi.

Questo porta a definire una nuova funzione $G(k)$, come il minimo valore s, tale che ogni numero naturale sufficientemente grande può essere espresso come somma di s potenze k-esime. Dal teorema di Lagrange scende che $G(2) = 4$ (vedi la proposizione seguente). Il citato risultato di Linnik dice inoltre che $G(3) \leq 7$. La determinazione dei valori di $G(k)$ è un problema in larga parte ancora aperto; i soli valori esatti conosciuti sono $G(2) = 4$, e $G(4) = 16$ (Davemport 1939).

Proposizione 5.8 $G(2) = 4$.

DIMOSTRAZIONE. Proviamo che nessun numero naturale congruo a 7 modulo 8 si può scrivere come somma di tre quadrati. Infatti, sia $x \in \mathbb{N}$;

- se $x = 2m$ è pari: $x^2 = 4m^2 \equiv 0\,(mod\,4)$;
- se $x = 2m = 1$ è dispari: $x^2 = (2m = 1)^2 = 4m(m + 1) + 1 \equiv 1\,(mod\,8)$.

Dunque, per ogni $x \in \mathbb{N}$,

$$x^2 \equiv 0,\ 1,\ 4\ (mod\,8)\ .$$

Da ciò segue subito che se $x, y, z \in \mathbb{N}$,

$$x^2 + y^2 + z^2 \not\equiv 7\,(mod\,8)$$

che è quello che si voleva. ∎

Torniamo alla funzione $g(k)$, e proviamo una limitazione inferiore per essa.

Teorema 5.9 *Sia $k \geq 2$, e sia $q = [(\frac{3}{2})^k]$; allora*

$$g(k) \geq 2^k + q - 2\ .$$

DIMOSTRAZIONE. Con le notazioni dell'enunciato, sia $n = 2^k q - 1$. Allora

$$n \leq 2^k(\frac{3}{2})^k - 1 = 3^k - 1 < 3^k\ .$$

Dunque, in una espressione di n come somma di potenze k-esime i soli addendi non nulli che compaiono sono 1^k e 2^k. Chiaramente, il numero minimo necessario di addendi del tipo 2^k si ottiene come quoziente della divisione di n per 2^k:

$$n = (q - 1)2^k + (2^k - 1)1^k\ .$$

Ne segue che per ottenere n come somma di potenze k-esime sono necessari almeno $q-1$ addendi uguali a 2^k e $2^k - 1$ addendi uguali a $1 = 1^k$. Pertanto

$$g(k) \geq q - 1 + 2^k - 1 = 2^k + q - 2\ .$$

∎

Osservazione. Per $n = 2, 3, 4$ la disuguaglianza del Teorema precedente fornisce

$$g(3) \geq 9,\quad g(4) \geq 19,\quad g(5) \geq 37$$

che sono, di fatto, i valori corretti. Se $k \geq 7$ e $r = 3^k - q2^k$ (quindi $1 \leq r \leq 2^k - 1$), è stato provato che $2^k + q - 2$ è effetivamente il valore di $g(k)$ se risulta soddisfatta la disuguaglianza

$$r + q \leq 2^k \ .$$

È noto che tale disuguaglianza non è soddisfatta per al più un numero finito di interi n, ma non se ne conoscono controesempi.

Esercizio 3. Sfruttando la seguente identità

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4+ \\ &\quad (a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4+ \\ &\quad (a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4 \end{aligned}$$

si provi che $g(4) \leq 50$.

Vediamo ora un risultato che riguarda la funzione $G(k)$.

Lemma 5.10 *Sia $1 \leq h \in \mathbb{N}$ fissato. Allora, per ogni $1 \leq n \in \mathbb{N}$,*

$$\sum_{j=0}^{n} \frac{(j+1)\dots(j+h)}{h!} = \frac{(n+1)\dots(n+h+1)}{(h+1)!}.$$

Dimostrazione. Esercizio (induzione su n). ∎

Teorema 5.11 *Per ogni numero naturale $k \geq 2$,*

$$G(k) \geq k+1.$$

Dimostrazione. Fissato $k \geq 2$, per ogni naturale N denotiamo con $A(N)$ il numero di numeri naturali $n \leq N$ che sono rappresentabili nella forma

$$n = x_1^k + x_2^k + \ldots + x_k^k, \tag{21}$$

dove $x_i \in \mathbb{N}$, per $i = 1, 2, \ldots, k$. Osserviamo $A(N) \leq B(N)$, dove $B_k(N)$ è il numero di k-uple intere $(x_1, x_2, \ldots, x_k)$ tale che

$$0 \leq x_1 \leq x_2 \leq \ldots \leq x_k \leq N^{\frac{1}{k}}.$$

Proviamo, per induzione su k, che

$$B_k(N) = \frac{1}{k!} \prod_{r=1}^{k} \left(\left[N^{\frac{1}{k}} \right] + r \right).$$

Per $N = 1$ si trova subito che $B_1(N) = [N^{\frac{1}{k}}] + 1$ (stiamo contando anche lo zero), che è ciò che fornisce anche la formula da provare.

Sia $k \geq 2$, e poniamo $t = [N^{\frac{1}{k}}]$. Allora, applicando l'ipotesi induttiva (e chiamando $j = x_k$),

$$B(N) = \sum_{j=0}^{t} B_{k-1}(j^k) = \sum_{j=0}^{t} \frac{1}{(k-1)!} \prod_{r=1}^{k-1}(j+r) = \frac{1}{(k-1)!} \sum_{j=0}^{t} \left(\prod_{r=1}^{k-1}(j+r) \right).$$

Pertanto, per il Lemma 5.10

$$B(N) = \frac{(t+1)(t+2)\dots(t+k)}{k!}$$

come si voleva. Osserviamo a questo punto che

$$\lim_{N\to\infty} \frac{B(N)}{N/k!} = 1. \tag{22}$$

Supponiamo, per assurdo, che si abbia $G(k) \leq k$, cioè che tutti i numeri naturali n, tranne un numero finito siano rappresentabili nella forma (21). In tal caso, esiste un $C \geq 0$, indipendente da N, tale che

$$B(N) \geq A(N) > N - C.$$

Ma ciò implica in particolare

$$\lim_{N\to\infty} \frac{N}{B(N)} \leq 1,$$

in contraddizione con il limite (22). Dunque $G(k) \geq k+1$. ∎

Esercizio 4. Si provi che $G(4) \geq 16$.

5.3 Somme di 3 quadrati

In questa sezione completiamo la parte dedicata alle somme di quadrati, dimostrando un Teorema di Gauss che descrive i numeri interi che sono somme di tre quadrati (5.17). La dimostrazione di questo risultato richiede metodi diversi e meno elementari di quelli utilizzati per i teoremi di Eulero e di Lagrange; essi riguardano alcune proprietà delle matrici a coefficienti interi che richiameremo tra poco, ed un profondo risultato di Dirichlet che sarà dimostrato nel capitolo seguente.

Teorema 5.12 (Dirichlet). *Siano a e b due numeri interi tali che $a \geq 1$ e $(a,b) = 1$. Allora esistono infiniti numeri primi della forma $an + b$ con $n \in \mathbb{Z}$.*

Ricordiamo ora, rinviando ad un testo di algebra lineare per le dimostrazioni, alcune proprietà delle forme quadratiche (a coefficienti interi), limitandoci al caso di matrici quadrate di ordine 3, anche se ciò che diremo vale per qualunque ordine. Sia

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

una matrice *simmetrica* a coefficienti in $\mathbb{Z}$, e sia $x \in \mathbb{Z}^3$ il vettore colonna

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} .$$

Si chiama *forma quadratica* associata alla matrice A la funzione nelle tre variabili intere x_1, x_2, x_3 data da

$$x^T A x = \sum_{i=1}^{3} \sum_{j=1}^{3} a_{i,j} x_i x_j \ ,$$

e diciamo che la forma quadratica è *definita positiva* se, per ogni $0 \neq x \in \mathbb{Z}^3$, si ha

$$x^T A x \geq 1 \ .$$

Allo stesso modo in cui si trattano le più familiari forme quadratiche sui reali, non è difficile provare che la forma associata ad A è definita positiva se e solo se i minori principali di A (che, nel nostro caso, sono $a_{1,1}$, $\det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ e $\det(A)$) sono positivi.
Dato un intero n, si dice che la matrice A *rappresenta* n se esiste un $x \in \mathbb{Z}^3$ tale che $x^T A x = n$ (ovvero se n appartiene all'immagine della forma quadratica associata ad A su $\mathbb{Z}^3$). Due matrici simmetriche a coefficienti in $\mathbb{Z}$ dello stesso ordine si dicono *equivalenti* se esiste una matrice a coefficienti interi U con determinante uguale ad 1 tale che

$$B = U^T A U \ .$$

Si verifica facilmente che se una matrice simmetrica intera rappresenta n, allora ogni altra matrice ad essa equivalente rappresenta n. Inoltre, vale il seguente risultato (che è l'analogo del teorema spettrale nel caso di matrici a coefficienti interi).

Proposizione 5.13 *Sia A una matrice simmetrica a coefficienti interi tale che la forma quadratica ad essa associata è definita positiva. Allora A è equivalente alla matrice identica I_3, e quindi gli interi rappresentati da A sono tutti e soli quelli rappresentati da I_3, ovvero quelli del tipo $x_1^2 + x_2^2 + x_3^2$.*

Lemma 5.14 *Sia $n \geq 2$ un numero naturale. Se esiste un numero naturale $d \geq 1$ tale che $-d$ è un residuo quadratico modulo $dn - 1$, allora n è somma di tre quadrati interi.*

Dimostrazione. Se $-d$ è un residuo quadratico modulo $dn - 1$ (con $d \geq 1$), allora esistono $a_{1,1}, a_{1,2} \in \mathbb{Z}$ tali che

$$a_{1,2}^2 + d = a_{1,1}(dn - 1) = a_{1,1} a_{2,2}$$

dove

$$a_{2,2} = dn - 1 \geq 2d - 1 \geq 1$$

e quindi anche $a_{1,1} \geq 1$.
Ora, la matrice simmetrica

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{2,1} & a_{2,2} & 0 \\ 1 & 0 & a_{3,3} \end{pmatrix}$$

ha determinante

$$\det(A) = (a_{1,1}a_{2,2} - a_{1,2}^2)n - a_{2,2} = dn - a_{2,2} = 1 \ .$$

Inoltre i tre minori principali di A sono positivi, e dunque la forma quadratica associata ad A è definita positiva. Per la proposizione richiamata sopra, A è equivalente alla matrice identica I_3. Si osserva anche che A rappresenta n, infatti

$$(0\ 0\ 1)A(0\ 0\ 1)^T = n \ .$$

Ne segue che anche I_3 rappresenta n, ovvero che n può essere scritto come la somma di tre quadrati interi. ∎

Lemma 5.15 *Se n è un numero naturale tale che*

$$n \equiv 2 \, (mod \, 4)$$

allora n è somma di tre quadrati interi.

Dimostrazione. Sia n un numero naturale tale che $n \equiv 2 \, (mod \, 4)$. Allora

$$(4n, n-1) = 1 \ .$$

Per il teorema di Dirichlet la progressione aritmetica $\{4nj + (n-1) \mid J \in \mathbb{N}^*\}$ contiene infiniti numeri primi. È dunque possibile scegliere $j \in \mathbb{N}^*$ tale che

$$p = 4nj + n - 1 = (4j+1)n - 1$$

sia un numero primo. Poniamo $d = 4j + 1$, ed osserviamo che

$$p = dn - 1 \equiv 1 \, (mod \, 4) \ .$$

Per il Lemma 5.14 è ora sufficiente mostrare che $-d$ è un residuo quadratico modulo p. Sia

$$d = \prod_{i=1}^{k} q_i^{s_i} \ ,$$

dove i q_i sono i primi distinti che dividono d. Ora

$$p = dn - 1 \equiv -1 \, (mod \, q_i)$$

per ogni tale q_i. Inoltre

$$d \equiv \prod_{q_i \equiv 3 \, (mod \, 4)} (-1)^{s_i} \, (mod \, 4) \ ,$$

e quindi

$$\prod_{q_i \equiv \, 3 (mod \, 4)} (-1)^{s_i} = 1 \ .$$

Ora, poichè $p \equiv 1 \, (mod \, 4)$, si ha che -1 è un residuo quadratico modulo p, ovvero

$$\left(\frac{-1}{p} \right) = 1$$

e dunque, applicando il Teorema di Reciprocità Quadratica,

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right) = \prod_{i=1}^{k}\left(\frac{q_i}{p}\right)^{s_i} = \prod_{i=1}^{k}\left(\frac{p}{q_i}\right)^{s_i} =$$

$$= \prod_{i=1}^{k}\left(\frac{-1}{q_i}\right)^{s_i} = \prod_{q_i \equiv 3 (mod\, 4)} (-1)^{s_i} = 1 \ .$$

Dunque $-d$ è un residuo quadratico modulo p, e la dimostrazione è completa. ∎

Lemma 5.16 *Se n è un numero naturale tale che*

$$n \equiv 1,\, 3,\, 5\, (mod\, 8)$$

allora n è somma di tre quadrati interi.

DIMOSTRAZIONE. Possiamo chiaramente supporre $n \geq 2$. Poniamo

$$c = \begin{cases} 1 & \text{se } n \equiv 3\, (mod\, 8) \\ \\ 3 & \text{se } n \equiv 1,\, 5\, (mod\, 8) \end{cases}$$

Allora, in ogni caso (lo si verifichi),

$$\left(4n,\, \frac{cn-1}{2}\right) = 1 \ .$$

Quindi, per il teorema di Dirichlet, esiste un primo p della forma

$$p = 4nj + \frac{cn-1}{2}$$

per qualche intero positivo j. Sia $d = 8j + c$; allora

$$2p = (8j + c)n - 1 = dn - 1 \ .$$

Per il Lemma 5.14, è ora sufficiente provare che $-d$ è un residuo quadratico modulo $2p$. Per quasto è sufficiente provare che $-d$ è un residuo quadratico modulo p. Infatti, se questo è il caso, allora esiste un intero a tale che

$$(a + p)^2 + dn \equiv a^2 + d \equiv 0\, (mod\, p) \ ;$$

se a è dispari si pone $u = a$, se a è pari si pone $u = a + p$. Allora u è dispari, e $u^2 + d$ è pari, e pertanto

$$u^2 + d \equiv 0\, (mod\, 2p)$$

cioè $-d$ è un residuo quadratico modulo $2p$.

Proviamo dunque che $-d$ è un residuo quadratico modulo p. Siano $q_1, \ldots, q_k$ i primi distinti che dividono d, e sia

$$d = \prod_{i=1}^{k} q_i^{s_i} \ .$$

Poiché $2p \equiv -1\,(mod\,d)$, si ha che, per ogni $i = 1, \ldots, k$,

$$2p \equiv -1\,(mod\,q_i) \quad \text{e} \quad (p, q_i) = 1\ .$$

Sia $n \equiv 1,\ 3\,(mod\,8)$. Allora $p \equiv 1\,(mod\,4)$, e

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right) = \prod_{i=1}^{k}\left(\frac{q_i}{p}\right)^{s_i}.$$

Sia $n \equiv 5\,(mod\,8)$; allora $p \equiv 3\,(mod\,4)$, e $d \equiv 3\,(mod\,8)$. denotiamo con U l'insieme dei divisori primi di d che sono congrui a 3 modulo 4; e con T quelli che sono congrui a 1 modulo 4. Allora

$$-1 \equiv d \equiv \prod_{q_i \in U} q_i^{s_i} \equiv \prod_{q_i \in U} (-1)^{s_i}\ (mod\,4)$$

e quindi

$$\prod_{q_i \in U} (-1)^{s_i} = -1\ .$$

Allora, applicando opportunamente il Teorema di Reciprocità Quadratica,

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = -\left(\frac{d}{p}\right) = -\prod_{q_i \in T}\left(\frac{q_i}{p}\right)^{s_i}\prod_{q_i \in U}\left(\frac{q_i}{p}\right)^{s_i} =$$

$$= -\prod_{q_i \in T}\left(\frac{p}{q_i}\right)^{s_i}\prod_{q_i \in U}\left(\frac{p}{q_i}\right)^{s_i}\prod_{q_i \in U}(-1)^{s_i} = \prod_{q_i \in T}\left(\frac{p}{q_i}\right)^{s_i}\prod_{q_i \in U}\left(\frac{p}{q_i}\right)^{s_i} = \prod_{q_i | d}\left(\frac{p}{q_i}\right)^{s_i}.$$

In entrambi i casi, e denotando nei prodotti i primi in congruenza modulo 8,

$$\left(\frac{-d}{p}\right) = \prod_{q_i | d}\left(\frac{p}{q_i}\right)^{s_i} = \prod_{q_i | d}\left(\frac{2}{q_i}\right)^{s_i}\left(\frac{2p}{q_i}\right)^{s_i} = \prod_{q_i | d}\left(\frac{2}{q_i}\right)^{s_i}\prod_{q_i | d}\left(\frac{-1}{q_i}\right)^{s_i} =$$

$$\prod_{q_1 \equiv 3,5 (mod\,8)} (-1)^{s_i} \prod_{q_1 \equiv 3,7 (mod\,8)} (-1)^{s_i} = \prod_{q_1 \equiv 5,7 (mod\,8)} (-1)^{s_i}.$$

Per concludere, è dunque sufficiente provare che

$$\sum_{q_1 \equiv 5,7 (mod\,8)} s_i \equiv 0\ (mod\,2).$$

Osserviamo che, modulo 8,

$$d = \prod_{q_1 \equiv 1} q_i^{s_i} \prod_{q_1 \equiv 3} q_i^{s_i} \prod_{q_1 \equiv 5} q_i^{s_i} \prod_{q_1 \equiv 7} q_i^{s_i} \equiv \prod_{q_1 \equiv 3} 3^{s_i} \prod_{q_1 \equiv 5} (-3)^{s_i} \prod_{q_1 \equiv 7} (-1)^{s_i} \equiv$$

$$\equiv \prod_{q_1 \equiv 3,5} 3^{s_i} \prod_{q_1 \equiv 5,7} (-1)^{s_i}\ \ (mod\,8).$$

Se $n \equiv 1,\ 5\,(mod\,8)$; allora $c = 3$, e

$$d = 8j + 3 \equiv 3\ (mod\,8).$$

Questo, per la congruenza di sopra, implica in particolare,

$$\sum_{q_1 \equiv 5,7 (mod\, 8)} s_i \equiv 0 \ (mod\, 2).$$

Se invece $n \equiv 3\,(mod\, 8)$; allora $c = 1$, e

$$d = 8j + 1 \equiv 1 \ (mod\, 8).$$

Anche questo, dal confronto con la congruenza di sopra, implica

$$\sum_{q_1 \equiv 3,5 (mod\, 8)} s_i \equiv 0 \ (mod\, 2),$$

e quindi

$$\sum_{q_1 \equiv 5,7 (mod\, 8)} s_i \equiv 0 \ (mod\, 2).$$

La dimostrazione è così completata. ∎

Siamo ora in grado di dimostrare il teorema di Gauss.

Teorema 5.17 (Gauss). *Un intero $n \geq 0$ non può essere scritto come somma di 3 quadrati se e solo se esso è del tipo*

$$n = 4^s(8t + 7)$$

con $s, t \in \mathbb{N}$.

Dimostrazione. Sia Ω l'insieme dei numeri naturali che si possono scrivere come somma di tre quadrati. Abbiamo visto nella Proposizione 5.8 che, per ogni $t \in \mathbb{N}$, $8t + 7 \notin \Omega$.
Sia ora $m \in \mathbb{N}$ tale che $4m \in \Omega$; allora

$$4m = x^2 + y^2 + z^2$$

dove x, y, z sono tutti numeri pari, e quindi

$$m = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 .$$

Quindi $m \in \Omega$ se e solo se $4m \in \Omega$. Da ciò scende immediatamente che nessun numero della forma

$$4^s(8t + 7)$$

con $s, t \in \mathbb{N}$, appartiene ad Ω (cioè può essere scritto come somma di tre quadrati).

Viceversa, sia $n \in \mathbb{N}$. Possiamo scrivere $n = 4^s m$, con $s, m \in \mathbb{N}$ univocamente determinati. Per i due Lemmi precedenti, se

$$m \equiv 2\,(mod\, 4) \qquad \text{oppure} \qquad m \equiv 1,\, 3,\, 5\,(mod\, 8)$$

allora m e quindi n appartiene ad Ω. Dunque, se $n \notin \Omega$, deve essere

$$m \equiv 7 \, (mod \, 8)$$

e ciò completa la dimostrazione. ■

Esercizio 5. Si provi che ogni numero naturale n con $n \equiv 3 \, (mod \, 8)$, è somma di tre quadrati dispari.

5.4 Appendice I: Il metodo di Schnirelmann.

Il metodo si Schnirelmann è uno strumento molto utile nella teoria additiva. Esso è stato sviluppato negli anni 30, è consentì al suo scopritore di ottenere uno dei primi risultati significativi intorno alla congettura di Goldbach. Schnirelmann provò infatti che esiste un intero k tale che ogni numero naturale è somma di k numeri primi.
Noi ci limitiamo ad illustrare il metodo, suggerendo la consultazione di uno dei testi consigliati a chi volesse vederlo applicato (anche alla soluzione del problema di Waring).

Nel seguito, indicheremo con A e B sottoinsiemi di numeri naturali del tipo

$$\{ \, 0, \, a_1, \, a_2, \ldots \mid 0 < a_1 < a_2 < \ldots \, \}.$$

Dato un insieme A di tal tipo, ed un $n \in \mathbb{N}$, poniamo

$$A(n) = |\{a \in A \mid 0 < a \leq n \, \}| \, .$$

Si osservi quindi che, per ogni $n \in \mathbb{N}$, $0 \leq A(n) \leq n$ e pertanto, se $n \geq 1$,

$$0 \leq \frac{A(n)}{n} \leq 1.$$

Definizione. Dato un sottonsieme A dei numeri naturali (contenente 0) si dice *densità di Schnirelmann* di A

$$d(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

È quindi chiaro che, per ogni insieme A,

$$0 \leq d(A) \leq 1.$$

Poiché inoltre $d(A) = 1$ se e soltanto se $A(n)/n = 1$ per ogni $n \geq 1$, si ha immediatamente la seguente

Proposizione 5.18 *$d(A) = 1$ se e solo se $A = \mathbb{N}$.*

Inoltre,

Proposizione 5.19 *Sia A tale che $1 \in A$ e $d(A) = 0$. Allora per ogni numero reale $\epsilon > 0$ ed ogni numero naturale $n \geq 1$, esiste un numero naturale $N \geq n$ tale che $A(N)/N < \epsilon$.*

DIMOSTRAZIONE. Poiché $1 \in A$, per ogni naturale $n \geq 1$ si ha

$$\frac{A(n)}{n} \neq 0.$$

Questo significa che 0 è l'estremo inferiore, ma non il minimo dell'insieme

$$\{\ A(n)/n \mid n \geq 1\ \},$$

e da ciò segue la tesi. ∎

Definizione. Dati due sottoinsiemi A e B dei numeri naturali si definisce la *somma* $A+B$ come l'insieme di tutti i numeri naturali della forma $a+b$, con $a \in A$ e $b \in B$ (che, così come per A e B, intenderenmo scritti in oredine crescente). Analogamente, dati k insiemi $A_1,\ A_2, \ldots,\ A_k$ si definisce la loro somma $A_1 + A_2 + \ldots + A_k$. In particolare, se $A_1 = A_2 = \ldots = A_k = A$, si pone $A_1 + A_2 + \ldots + A_k = kA$.

Teorema 5.20 (Schnirelmann). *Per ogni coppia di insiemi A e B si ha*

$$d(A+B) \geq d(A) + d(B) - d(A)d(B).$$

DIMOSTRAZIONE. Sia $A = \{a_0 = 0, a_1, a_2, \ldots\}$. Per ogni numero naturale i poniamo

$$l_i = a_{i+1} - a_i - 1.$$

Osserviamo che, se $l_i \geq 1$, allora

$$a_i + 1,\ a_1 + 2, \ldots, a_i + l_i \notin A.$$

D'altra parte, nell'insieme $\{1, 2, \ldots, l_i\}$ ci sono $B(l_i)$ elementi di B; e quindi nell'insieme $\{a_i + 1,\ a_1 + 2, \ldots, a_i + l_i\}$ ci sono almeno $B(l_i)$ elementi di $A + B$. Da ciò segue che, per ogni numero naturale $n \geq 1$,

$$(A+B)(n) \geq A(n) + \sum_{i=0}^{A(n)-1} B(l_i) + B(n - a_{A(n)}).$$

Per la definizione di densità di Schnirelmann, si ha quindi

$$\begin{aligned}(A+B)(n) &\geq A(n) + d(B)\left\{\sum_{i=0}^{A(n)-1} l_i + n - a_{A(n)}\right\} = \\ &= A(n) + d(B)(n - A(n)) = A(n)(1 - d(B)) + nd(B) \\ &\geq nd(A)(1 - d(B)) + nd(B).\end{aligned}$$

Ma allora, per ogni numero naturale $n \geq 1$

$$\frac{(A+B)(n)}{n} \geq d(A) + d(B) - d(A)d(B),$$

e quindi

$$d(A+B) \geq d(A) + d(B) - d(A)d(B),$$

come si voleva. ∎

Corollario 5.21 *Per ogni insieme A, ed ogni numero naturale $n \geq 1$,*

$$d(nA) \geq 1 - (1 - d(A))^n.$$

DIMOSTRAZIONE. Per induzione su n. Se $n = 1$ la tesi è ovvia. Per $n \geq 2$, segue dal Teorema 5.20 che

$$\begin{aligned} d(nA) - 1 = d((n-1)A + A) - 1 &\geq d((n-1)A) + d(A) - d((n-1)A)d(A) - 1 \\ &= (d((n-1)A) - 1)(1 - d(A)), \end{aligned}$$

ed applicando l'ipotesi induttiva

$$d(nA) - 1 \geq -(1 - d(A))^{n-1}(1 - d(A)) = -(1 - d(A))^n$$

come si voleva. ∎

Definizione. Un insieme A si dice **base** di $\mathbb{N}$ se esiste un intero $n \geq 1$ tale che $nA = \mathbb{N}$.

Teorema 5.22 (Schnirelmann). *Se A è un insieme tale che $d(A) > 0$, allora A è una base di $\mathbb{N}$.*

DIMOSTRAZIONE. Sia $d(A) > 0$. Per il Corollario 5.21

$$\lim_{n\to\infty} d(nA) \geq \lim_{n\to\infty} \{1 - (1 - d(A))^n\} = 1.$$

Per definizione di limite, esiste quindi un numero naturale $n \geq 1$ tale che

$$d(nA) > \frac{1}{2}.$$

Da ciò segue, per definizione di densità, che, per ogni numero naturale $m \geq 1$

$$\frac{(nA)(m)}{m} \geq \frac{1}{2}.$$

Sia $nA = \{\ a_0 = 0, a_1, a_2, \dots\ \}$, e si osservi che, per ogni numero naturale $m \geq 1$, ed ogni $i = 1, 2, \dots, (nA)(m)$

$$0 \leq m - a_i < m.$$

Allora

$$a_0 = 0, a_1, \dots, a_{(nA)(m)}, m - a_1, \dots, m - a_{(nA)(m)}$$

sono $2(nA)(m) + 1$ numeri naturali contenuti nell'intervallo $[0, m]$. Poiché

$$2(nA)(m) + 1 > m + 1$$

tali numeri non possono essere tutti distinti. D'altra parte, i numeri

$$a_0 = 0, a_1, \dots, a_{(nA)(m)},$$

sono tutti distinti; quindi esistono $i \geq 0$ e $j \geq 1$, tali che

$$a_i = m - a_j$$

cioè

$$m = a_i + a_j.$$

Quindi

$$\mathbb{N} = nA + nA = 2nA$$

e dunque A è una base di $\mathbb{N}$. ∎

Utilizzando questo Teorema, assieme ad altri risultati sulla distribuzione dei numeri primi, Schnirelmann fu in grado di provare che, posto $\mathbb{P}$ l'insieme dei numeri primi, allora $d(\{0\} \cup \mathbb{P}) > 0$, e dunque che ogni numero naturale è somma di un numero fissato c di numeri primi. A tutt'oggi, il risultato migliore in tal senso è dovuto a Vinogradov, ed asserisce che ogni numero dispari sufficientemente grande è la somma di tre numeri primi (e quindi ogni numero naturale sufficientemente grande è la somma di quattro numeri primi).

5.5 Appendice II: La Congettura abc.

Ottenuta la dimostrazione del Teorema di Fermat, la cosiddetta **congettura abc** è da molti ritenuta uno dei problemi più importanti della teoria dei numeri. Si tratta di una congettura molto potente, che collega la struttura additiva dei numeri interi con quella moltiplicativa; se dimostrata, da essa seguirebbe la correttezza di diverse singole congetture ancora aperte.

Sia z un intero non nullo. Il **radicale** di z è il massimo divisore positivo di z privo di quadrati; ovvero il prodotto dei primi positivi distinti che dividono z,

$$rad(z) = \prod_{p|z} p$$

(e, di conseguenza, $rad(1) = rad(-1) = 1$).

Cogettura abc. Per ogni numero reale $\epsilon > 0$ esiste un numero $K(\epsilon)$ tale che, se a, b e c sono interi non nulli e $a + b + c = 0$, allora

$$\max\{|a|, |b|, |c|\} \leq K(\epsilon)\, rad(abc)^{1+\epsilon}.$$

Illustriamo con qualche esempio la forza di questa congettura, cominciando con il Teorema di Fermat. Per $n \geq 2$, chiamiamo n-esima equazione di Fermat:

$$x^n + y^n = z^n.$$

Il Teorema di Fermat afferma che per $n \geq 3$ la n-esima equazione di Fermat non ammette soluzioni intere con $xyz \neq 0$.

Proposizione 5.23 *La congettura abc implica che esiste un intero $N \geq 3$ tale che per ogni $m \geq N$, l'equazione m-esima di Fermat non ha soluzioni intere non banali.*

DIMOSTRAZIONE. Osserviamo, innanzi tutto, che se una equazione di Fermat ha una soluzione $x^k + y^k = z^k$, e p è un divisore primo comune di x, y e z, allora anche $x/p, y/p, z/p$ è una soluzione della stessa equazione¿ Possiamo quindi limitarci a provere, assumendo la congettura abc, che esiste N tale che per $m \geq N$ l'equazione m-esima di Fermat non ha soluzioni con interi positivi tra loro coprimi.
Supponiamo che, per un qualche $n \geq 3$, esistano interi coprimi x, y e z tali che

$$x^n + y^n = z^n.$$

Allora

$$rad\,(x^n y^n z^n) = rad(xyz) \leq xyz \leq z^3.$$

Osserviamo che, poiché $n \geq 3$, deve essere $z \geq 3$. Applichiamo la congettura abc, con $\epsilon = 1$: esiste un numero $K = \max\{1, K(1)\}$ tale che

$$z^n = \max\{x^n, y^n, z^n\} \leq K\, rad(x^n y^n z^n)^2 < K z^6.$$

Da ciò segue

$$n < 6 + \log_z K \leq 6 + \log_3 K.$$

Dunque, per $m \geq 6 + \log_3 K$ l'equazione m-esima di Fermat non ammette soluzioni coprime. ∎

Il nostro secondo esempio riguarda la congettura di Catalan (vedi la fine del capitolo 1).

Proposizione 5.24 *La congettura abc implica che la congettura di Catalan ha un numero finito di soluzioni.*

DIMOSTRAZIONE. L'equazione di Catalan è

$$y^m - x^n = 1$$

dove si cercano soluzioni non banali (con $n, m \geq 2$, e $xy \neq 0$) in x, y, n, m.
È noto che non esistono soluzioni con $n = 2$, e che la sola soluzione con $m = 2$ è $n = 3$, $x = 2$, $y = 3$.
Supponiamo dunque che (x, y, m, n) sia una soluzione dell'equazione di Catalan, con $\min\{m, n\} \geq 3$. Chiaramente, x e y sono coprimi.
Applichiamo la congettura abc, con $\epsilon = \frac{1}{4}$: esiste un numero $K = K(1/4)$ tale che

$$x^n < y^m \leq K\, rad\,(y^m x^n)^{\frac{5}{4}} = K\, rad(yx)^{\frac{5}{4}} \leq K(yx)^{\frac{5}{4}}.$$

Da ciò seguono le diseguaglianze

$$n \log x < \log K + \frac{5}{4} \log y + + \frac{5}{4} \log x$$

$$m \log y \leq \log K + \frac{5}{4} \log y + + \frac{5}{4} \log x.$$

E da queste,

$$n \log x + m \log y < 2 \log K + \frac{5}{2}(\log x + \log y),$$

e di conseguenza,

$$(n - 5/2)\log x + (m - 5/2)\log y < 2\log K.$$

Poiché $x, y \geq 2$, si ricava

$$(n + m - 5)\log 2 < 2\log K$$

e quindi

$$m + n < \frac{2\log K}{\log 2} + 5.$$

Dunque l'equazione di Catalan ha un numero finito di soluzioni, dato che per fissati $m \geq 3$ e $n \geq 3$, l'equazione $y^m - x^n = 1$ ha un numero finito di soluzioni intere. ∎

6 Caratteri di gruppi abeliani.

6.1 Costruzione di caratteri

Sia G un gruppo abeliano (cioè commutativo) finito. Un **carattere** di G è un omomorfismo di gruppi moltiplicativi

$$\chi \ : \ G \ \longrightarrow \ \mathbb{C}^*.$$

Dove $\mathbb{C}^*$ è il gruppo moltiplicativo dei numeri complessi diversi da zero.

Ricordo che se G è un gruppo abeliano finito, e $g \in G$, allora esiste un intero $k \geq 1$ tale che $g^k = 1_G$, ed il minimo $k \geq 1$ per cui ciò avviene si dice *ordine* dell'elemento g. Inoltre, del noto Teorema di Lagrange, discende che l'ordine di ciascun elemento di G divide la cardinalità di G.
Sia χ un carattere di G, e sia $g \in G$ un elemento di ordine k; allora, poiché χ è un omomorfismo

$$\chi(g)^k = \chi(g^k) = \chi(1_G) = 1$$

e quindi $\chi(g)$ deve essere una radice k-esima dell'unità. Pertanto, per ogni carattere χ di un gruppo abeliano finito, l'immagine $\Im(\chi)$ è contenuta (difatti ne è un sottogruppo) nel gruppo moltiplicativo U di tutte le radici dell'unità del campo complesso $\mathbb{C}$.

Esempio 1. Sia $G = \langle x \rangle$ un gruppo ciclico di ordine $n \geq 1$, e sia g un suo generatore. Allora

$$G = \{ \ 1, \ g, \ g^2, \ \ldots, \ g^{n-2}, \ g^{n-1} \ \}.$$

Sia U_n l'insieme delle radici n-esime dell'unità in $\mathbb{C}$. Quindi

$$U_n = \{ \ \zeta_{n,k} = e^{\frac{2\pi i}{n}k} \mid 0 \leq k \leq n-1 \ \}.$$

Ricordo che U_n è un gruppo moltiplicativo ciclico di ordine n, e che i suoi generatori sono le radici *primitive* n-esime, ovvero le radici $\zeta_{n,m}$ con $(m, n) = 1$. Inoltre se $\zeta_k \in U_n$, e $m \in \mathbb{Z}$, $(\zeta_{n,k})^m = \zeta_{n,r}$, dove r è il resto della divisione di km per n.
Fissata una radice n-esima $\zeta_{n,k}$, definiamo, $\chi_k(g) = \zeta_{n,k}$, e per ogni $g^m \in G$,

$$\chi_k(g^m) = (\zeta_{n,k})^m.$$

Si riconosce subito che tale applicazione χ_k così definita è un omomorfismo $G \longrightarrow \mathbb{C}^*$, cioè un carattere di G.
Viceversa, sia χ un carattere di $G = \langle g \rangle$. Per quanto osservato sopra, $\chi(g)$ deve essere un elemento di U_n; dunque $\chi(g) = \zeta_{n,k}$, per qualche $0 \leq k \leq n$. Ma allora, poiché χ è un omomorfismo, per ogni $g^m \in G$, si ha

$$\chi(g^m) = \chi(g)^m (\zeta_{n,k})^m.$$

Quindi χ coincide con $\chi_{n,k}$. In conclusione, l'insieme dei caratteri di G coincide con l'insieme dei $\chi_{n,k}$ con $0 \leq k \leq n-1$ (e questi sono tutti distinti).

La discussione dell'esempio contiene in particolare la dimostrazione del seguente

Lemma 6.1 *Sia G un gruppo ciclico di ordine n. Allora il numero di caratteri distinti di G è n.*

Osserviamo che, come emerge dall'esempio di sopra, non tutti i caratteri sono omomorfismi iniettivi.

Esercizio 1. Sia G un gruppo ciclico di ordine 12, sia fissato con generatore g di G, e sia $\zeta = \zeta_{12,2} = e^{\frac{2\pi i}{6}}$ una radice 12-esima dell'unità come definita nell'esempio 1. Si determini il nucleo $\ker(\chi_2)$ del carattere χ_2, associato a ζ rispetto al generatore g.

Esempio 2. Sia $G = A \times B$, il prodotto diretto di due gruppi ciclici di ordine primo p. Allora G ha ordine p^2, e non è ciclico (ogni suo elemento non identico ha ordine p). Siano a e b rispettivamente generatori di A e di B. Quindi

$$G = \{\ (a^r, b^s) \mid 0 \leq r, s \leq p-1\ \}.$$

Siano ζ e ξ due fissate radici p-esime dell'unita. Allora, definendo per ogni $(a^r, b^s) \in G$,

$$\chi_{\zeta,\xi}((a^r, b^s)) = \zeta^r \xi^s$$

si ottiene, come si vede facilmente, un carattere di G. Viceversa, ogni carattere di G è di questo tipo (e dunque il numero di caratteri distinti di G è uguale a $p^2 = |G|$.

Eserrcizio 2. Si provi che nessun carattere del gruppo G dell'esempio 2 è iniettivo.

Lasciamo quindi per esercizio la dimostrazione della seguente

Proposizione 6.2 *Sia $G = G_1 \times G_2 \times \ldots \times G_n$ un gruppo prodotto diretto di gruppi abeliani finiti. Siano $\chi_1, \chi_2, \ldots, \chi_n$ caratteri di $G_1, G_2, \ldots, G_n$ rispettivamente. Allora l'applicazione*

$$\chi(g_1, g_2, \ldots, g_n) = \chi_1(g_1)\chi_2(g_2)\cdots\chi_n(g_n)$$

definita per ogni $(g_1, g_2, \ldots, g_n) \in G$, è un carattere di G. Viceversa ogni carattere di G si ottiene in tal modo, per un'unica scelta dei caratteri $\chi_1, \chi_2, \ldots, \chi_n$.

Enunciamo ora, senza dimostrazione, un importante teorema di struttura per gruppi abeliani finiti (una dimostrazione di questo fatto si trova nell'appendice al capitolo).

Teorema 6.3 *Ogni gruppo abeliano finito è isomorfo ad un prodotto diretto di gruppi ciclici.*

Da questo Teorema, insieme con la Proposizione 6.2 ed il Lemma 6.1, si deduce immediatamente la seguente osservazione.

Proposizione 6.4 *Sia G un gruppo abeliano finito. Allora il numero di caratteri distinti di G è uguale all'ordine di G.*

6.2 Prodotto di caratteri

Sia G un gruppo finito. D'ora in avanti denoteremo con $\widehat{G}$ l'insieme dei caratteri di G. Fissato il gruppo G, l'applicazione

$$\chi_0 : G \longrightarrow \mathbb{C}^*$$

definita ponendo, per ogni $g \in G$, $\chi_)(g) = 1$, è un carattere di G, ed è chiamato il *carattere principale* di G. Noi lo indicheremo sempre con χ_0.

Siano ora χ e ψ due caratteri del gruppo G. Definiamo il loro *prodotto* ponendo, per ogni $g \in G$,

$$\chi\psi(g) = \chi(g)\psi(g).$$

Si verifica immediatamente che l'applicazione $\chi\psi$ così definita è un carattere di G, e che l'operazione di prodotto è un'operazione associativa e commutativa sull'insieme $\widehat{G}$ dei caratteri di G. Inoltre, chiaramente, il carattere principale χ_0 è l'elemento neutro per il prodotto. Vediamo ora che in $\widehat{G}$ esistono anche gli elementi inversi.
Sia χ un carattere di G. Definiamo il carattere *coniugato* $\overline{\chi}$ di χ, ponendo, per ogni $g \in G$,

$$\overline{\chi}(g) = \overline{\chi(g)}$$

dove $\overline{\chi(g)}$ è il coniugato in $\mathbb{C}$ del numero complesso $\chi(g)$. Si vede subito che anche $\overline{\chi}$ è un carattere di G. Inoltre, per ogni $g \in G$, tenendo conto che $\chi(g)$ è una radice dell'unità (e quindi ha modulo uguale ad 1),

$$\chi\overline{\chi}(g) = \chi(g)\overline{\chi(g)} = |\chi(g)| = 1 = \chi_0(g),$$

dunque, in $\widehat{G}$, $\chi\overline{\chi} = \chi_o$; pertanto $\overline{\chi}$ è l'inverso di χ rispetto al prodotto di caratteri. Abbiamo dunque provato il seguente risultato.

Teorema 6.5 *Sia G un gruppo abeliano finito. Allora, con l'operazione di prodotto, $\widehat{G}$ è un gruppo abeliano dello stesso ordine di G.*

Il gruppo $\widehat{G}$ è chiamato il *duale* del gruppo G.
Osserviamo che, per ogni $g \in G$, ed ogni $\chi \in \widehat{G}$,

$$\overline{\chi}(g) = \chi(g)^{-1} = \chi(g^{-1}).$$

Esercizio 3. Sia G un gruppo ciclico di ordine n. Si provi che $\widehat{G}$ è un gruppo ciclico di ordine n (si dimostri che G è isomorfo a $\widehat{G}$).

Di fatto, utilizzando l'esercizio precedente, ed i Teoremi 6.2 e 6.3, non è difficile provare che se G è un gruppo abeliano finito, allora il gruppo duale $\widehat{G}$ è isomorfo a G.
Osserviamo che sia la definizione di carattere, che l'operazione di prodotto tra caratteri definita sopra, hanno senso anche se G è un gruppo abeliano infinito, ed anche in tal caso si ottiene che $\widehat{G}$ è un gruppo abeliano. Tuttavia, se G non è finito, non è in generale vero che $\widehat{G}$ è isomorfo a G (chi è interessato può provare per proprio conto ad analizzare

il caso in cui G è un gruppo ciclico infinito - ad esempio, il gruppo additivo $(\mathbb{Z}, +)$ dei numeri interi).

Ora, un'altra osservazione che ci sarà utile

Lemma 6.6 *Sia G un gruppo abeliano finito, e sia $1_G \neq g \in G$. Allora esiste un carattere χ di G tale che $\chi(g) \neq 1$.*

DIMOSTRAZIONE. Se G è un gruppo ciclico, allora la proprietà segue immediatamente dalla costruzione dat nell'esempio 1. Fissato un generatore x di G, ogni carattere χ che associa ad x una radice primitiva $|G|$-esima dell'unità è iniettivo, e quindi $\chi(g) \neq 1$ per ogni $1_G \neq g \in G$.
Altrimenti, G è (isomorfo ad) un prodotto diretto di gruppi ciclici, per il Teorema 6.3. La proprietà segue ora facilmente (i dettagli per esercizio) dal Teorema 6.2 e dal caso ciclico. ∎

Esercizio 4. Sia H un sottogruppo del gruppo abeliano finito G. Si provi che ogni carattere χ di G/H si può "sollevare" ad un carattere χ^G di G.

Un carattere χ di G si dice *reale* se, per ogni $g \in G$, $\chi(g) \in \mathbb{R}$. Dalla definizione segue subito che χ è un carattere reale se e solo se $\chi = \overline{\chi}$. Inoltre, se χ è un carattere reale, allora, per ogni $g \in G$, $\chi(g) = \pm 1$ (dato che 1 e -1 sono le sole radici dell'unità che appartengono a $\mathbb{R}$).

Esercizio 5. Si provi che un gruppo abeliano finito G ammette un carattere reale diverso dal carattere principale se e solo se 2 divide l'ordine di G.

6.3 Relazioni di ortogonalità

Le relazioni di ortogonalità sono importanti proprietà dei caratteri, che hanno svariate applicazioni. Noi le utilizzeremo nel prossimo capitolo nel corso della dimostrazione del Teorema di Dirichlet.

Teorema 6.7 *Sia G un gruppo abeliano finito, e sia $\widehat{G}$ il gruppo dei caratteri di G.*

Per ogni $g \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & se \quad g = 1_G \\ 0 & se \quad g \neq 1_G. \end{cases}$$

Per ogni $\chi \in \widehat{G}$,

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & se \quad \chi = \chi_o \\ 0 & se \quad \chi \neq \chi_o. \end{cases}$$

DIMOSTRAZIONE. Poiché $\chi(1_G) = 1$ per ogni $\chi \in \widehat{G}$, e, per la Proposizione 6.4, $|\widehat{G}| = |G|$, si ha

$$\sum_{\chi\in\widehat{G}} \chi(1_G) = |G|.$$

Sia quindi $1_G \neq g \in G$. Allora, per il Lemma 6.6 esiste un carattere ψ tale che $\psi(g) \neq 1$. Dunque, tenendo conto che, essendo $\widehat{G}$ un gruppo: $\{\psi\chi \mid \chi \in \widehat{G}\} = \widehat{G}$,

$$\psi(g)\sum_{\chi\in\widehat{G}} \chi(g) = \sum_{\chi\in\widehat{G}} \psi(g)\chi(g) = \sum_{\chi\in\widehat{G}} \psi\chi(g) = \sum_{\chi\in\widehat{G}} \chi(g)$$

e poiché $\psi(g) \neq 1$, deve essere

$$\sum_{\chi\in\widehat{G}} \chi(g) = 0.$$

La seconda parte è analoga. Per il carattere principale si ha

$$\sum_{g\in G} \chi_o(g) = \sum_{g\in G} 1 = |G|.$$

Se $\chi \neq \chi_o$, allora esiste un elemento $a \in G$ tale che $\chi(a) \neq 1$. Ora

$$\chi(a)\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(a)\chi(g) = \sum_{g\in G} \chi(ag) = \sum_{g\in G} \chi(g)$$

e di conseguenza $\sum_{g\in G} \chi(g) = 0$. ∎

Teorema 6.8 (Relazioni di ortogonalità) *Con le stesse notazioni del Teorema precedente.*

Per ogni $a, b \in G$,

$$\sum_{\chi\in\widehat{G}} \chi(a)\overline{\chi}(b) = \begin{cases} |G| & se \;\; a = b \\ 0 & se \;\; a \neq b. \end{cases}$$

Per ogni $\chi_1, \chi_2 \in \widehat{G}$,

$$\sum_{g\in G} \chi_1(g)\overline{\chi_2}(g) = \begin{cases} |G| & se \;\; \chi_1 = \chi_2 \\ 0 & se \;\; \chi_1 \neq \chi_2. \end{cases}$$

DIMOSTRAZIONE. Le identità seguono immadiatamente da quelle del Teorema precedente. Infatti, se $a, b \in G$,

$$\sum_{\chi\in\widehat{G}} \chi(a)\overline{\chi}(b) = \sum_{\chi\in\widehat{G}} \chi(ab^{-1}).$$

Mentre, se $\chi_1, \chi_2 \in \widehat{G}$,

$$\sum_{g\in G} \chi_1(g)\overline{\chi_2}(g) = \sum_{g\in G} \chi_1\chi_2^{-1}(g).$$

∎

6.4 Appendice: la struttura dei gruppi abeliani finiti.

Ci proponiamo di dimostrare il Teorema 6.3.

Innanzi tutto, ricordiamo il seguente criterio per prodotti diretti.

Proposizione 6.9 *Siano N e M sottogruppi normali del gruppo G. Se avviene che $NM = G$ e $N \cap M = \{1_G\}$, allora*

$$G \simeq N \times M.$$

In particolare, se G è un gruppo abeliano ogni sottogruppo è normale, quindi la Proposizione di sopra si applica a qualunque coppia di sottogruppi. Osserviamo anche che, se H e K sono sottogruppi di un gruppo abeliano G, allora il prodotto

$$HK = \{xy \mid x \in H,\, y \in K\}$$

è sempre un sottogruppo di G.

D'ora in avanti con G intendiamo un gruppo abeliano finito.

Lemma 6.10 *Siano H e K sottogruppi di G, con K massimale tale che $H \cap K = \{1_G\}$. Sia $x \in G$, e supponiamo che esista un numero primo p tale che $x^p \in K$. Allora $x \in HK = H \times K$.*

Dimostrazione. Osserviamo, innanzi tutto che, siccome $H \cap K = \{1_G\}$, dalla Proposizione 6.9 segue che $HK = H \times K$.
Sia $x \in G$ come nelle ipotesi. Se $x \in K$, non c'è nulla da provare. Supponiamo quindi che $x \notin K$. Allora K è un sottogruppo proprio di $\langle K, x\rangle = K\langle x\rangle$, e quindi, per l'assunzione su K, $K\langle x\rangle \cap H \neq \{1_G\}$. Dunque, esistono $y \in K$, $h \in H$, e un intero $t \neq 0$ tali che

$$yx^t = h \neq 1_G.$$

Allora, $x^t = y^{-1}h \in KH$. Se fosse $p|t$, si avrebbe $y^{-1}h = (x^p)^{t/p} \in K$, e pertanto $h \in K$, che, siccome $H \cap K = \{1_G\}$, conduce alla contraddizione $h = 1_G$. Dunque p non divide t, quindi $(p, t) = 1$ ed esistono interi a, b tali che $1 = pa + tb$. Ma allora

$$x = x^{pa+tb} = (x^p)^a(x^t)^b = (x^p)^a(y^{-1}h)^b = (x^{pa}y^{-b})h^b \in KH,$$

come si voleva. ∎

Per ogni elemento $g \in G$ si denota con $o(g)$ l'ordine di g (abbiamo già ricordato che $o(g)$ è il minimo intero positivo non nullo tale che $g^{o(g)} = 1_G$). Allora, $o(g)$ è la cardinalità del sottogruppo ciclico $\langle g\rangle$ generato da g; quindi, per il Teorema di Lagrange,

$$o(g) \text{ divide } |G|.$$

Inoltre, se $n \geq 1$, allora

$$g^n = 1_G \text{ se e solo se } o(g)|n.$$

Infatti, se $d = (n, o(g))$, ed a e b sono interi tali che $na + o(g)b = d$, si ha

$$g^d = g^{na+o(g)b} = g^{na}g^{o(g)b} = (g^n)^a(g^{o(g)})^b = 1_G^a 1_G^b = 1_G$$

e quindi, $o(g) \leq d$, che comporta $o(g) = d$, cioè $o(g)|n$. Viceversa, se n è un multiplo di $o(g)$, è chiaro che $g^n = 1_G$.
Infine ricordiamo che, se $o(g) = n$ e $t \in \mathbb{Z}$, allora si ha

$$o(g^t) = \frac{n}{(n,t)}$$

(la dimostrazione di ciò è lasciata per esercizio); in particolare, se $t|n$ allora $o(g^t) = n/t$.

Lemma 6.11 *Siano g e h elementi di G i cui ordini sono coprimi. Allora*

$$o(gh) = o(g)o(h).$$

DIMOSTRAZIONE. Esercizio (si cerchi anche di provare che la tesi non vale se gli ordini di g e di h non sono coprimi)[2] ∎

Lemma 6.12 *Sia g un elemento di G il cui ordine è il massimo possibile. Allora, per ogni $x \in G$, $o(x)|o(g)$.*

DIMOSTRAZIONE. Sia g un elemento di G di ordine massimo, e sia $n = o(g)$. Sia $x \in G$ e sia $r = o(x)$. Poniamo $d = (n, r)$, allora $(n/d, r/d) = 1$. Sia t il massimo fattore di n che è coprimo con n/d, ed u il massimo fattore di r coprimo con r/d. Allora n/t ed r/u sono coprimi, e inoltre $(n/t)(r/u) = [n, r]$ (il minimo comune multiplo).
Ora, per quanto ricordato sopra, $o(g^t) = n/t$, e $o(x^u) = r/u$; quindi, per il Lemma 6.11

$$o(g^t x^u) = \frac{n}{t} \cdot \frac{r}{u} = [n, r].$$

Ma allora, per la scelta di g deve essere $n = o(g) \geq o(g^t x^u) = [n, r]$. Quindi $n = [n, r]$ che significa che r divide n. ∎

Lemma 6.13 *Sia g un elemento di G del massimo ordine possibile. Allora esiste un sottogruppo K di G tale che $G \simeq \langle g \rangle \times K$.*

DIMOSTRAZIONE. Sia $g \in G$ un elemento di ordine massimo possibile, e $n = o(g)$. Sia $K \leq G$ un sottogruppo di G, massimale tra quelli per cui $\langle g \rangle \cap K = \{1_G\}$. Proviamo che $G = \langle g \rangle K = \langle g \rangle \times K$.
Sia $x \in G$, allora esiste un $m \geq 1$ tale che $x^m \in \langle g \rangle K$. Per induzione su m proviamo che $x \in \langle g \rangle K$. Se $m = 1$ la cosa è data. Sia quindi $m \geq 1$ e sia p un divisore primo di n. Allora $(x^{m/p})^p = x^m \in \langle g \rangle K$, e quindi, se $p < m$ si conclude per ipotesi induttiva che $x \in \langle g \rangle K$. Dunque, possiamo supporre che $m = p$ sia un numero primo.
Ora, esiste un elemento $k \in K$ ed un numero intero t tali che $x^p = g^t k$. Osserviamo anche che, per il Lemma 6.12, $x^n = 1_G$.

[2] Nè tantomeno il Lemma è vero per gruppi non abeliani.

Supponiamo che p non divida n. In tal caso $(p,n)=1$ ed esistono interi a,b tali che $1=pa+nb$. Si ha allora

$$x = x^{pa+nb} = (x^p)^a (x^n)^b = (x^p)^a = g^{ta}k^a \in \langle g\rangle K.$$

Possiamo quindi assumere che $p|n$. Allora

$$1_G = x^n = (x^p)^{n/p} = g^{tn/p}k^{n/p}$$

e quindi $g^{tn/p} = (k^{n/p})^{-1} \in \langle g\rangle \cap K = \{1_G\}$. Dunque $g^{tn/p} = 1_G$, e pertanto $n = o(g)$ divide tn/p, da cui segue che p divide t. Allora, posto $y = x^{-1}g^{t/p}$, si ha

$$y^p = (x^p)^{-1}g^t = k^{-1} \in K$$

e quindi, per il Lemma 6.10, $x^{-1}g^{t/p} = y \in \langle g\rangle K$. Da ciò segue subito che x appartiene a $\langle g\rangle K$, completando così la dimostrazione. ∎

Teorema 6.14 (Teorema 6.3) *Sia G un gruppo abeliano finito. Allora esistono elementi $g_1,\dots,g_n$ di G, tali che*

$$G \simeq \langle g_1\rangle \times \langle g_2\rangle \times \cdots \times \langle g_n\rangle.$$

Dimostrazione. Procediamo per induzione sull'ordine di G. Se $G = \{1_G\}$ non c'è nulla da dimostrare. Sia quindi $|G| > 1$, e sia g_1 un elemento di G del massimo ordine possibile. Per il Lemma 6.13, esiste un sottogruppo K di G tale che

$$G \simeq \langle g_1\rangle \times K.$$

Ora $|K| = |G|/|\langle g\rangle| = |G|/o(g) < |G$, e quindi, per ipotesi induttiva, esistono elementi $g_2,\dots,g_n$ di K tali che

$$K \simeq \langle g_2\rangle \times \cdots \times \langle g_n\rangle.$$

Quindi si ha

$$G \simeq \langle g_1\rangle \times K \simeq \langle g_1\rangle \times \langle g_2\rangle \times \cdots \times \langle g_n\rangle$$

e la dimostrazione è completa. ∎

7 Numeri primi.

Sia x un numero reale maggiore di 1. Denotiamo con $\pi(x)$ il numero di numeri primi positivi minori od uguali ad x. Il più importante risultato concernente la funzione $\pi(x)$ è il Teorema dei Numeri Primi, congetturato da Legendre e da Gauss e provato, indipendentemente da Hadamard e La Vallee Poussin nel 1896. Esso afferma che

$$\pi(x) \sim \frac{x}{\log x}$$

dove con la scrittura $f(x) \sim g(x)$ si intende che $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

In questo capitolo ci accontentiamo di provare un precedente risultato di Čebichev (1860), che afferma che esistono due costanti $A, B > 0$ tali che

$$A\frac{x}{\log x} \leq \pi(x) \leq B\frac{x}{\log x} \ .$$

La seconda parte del capitolo sarà invece dedicata alla dimostrazione del Teorema di Dirichlet sui numeri primi di successioni aritmetiche, che abbiamo già utilizzato nel capitolo precedente.

Iniziamo facendo alcune osservazioni sulla massima potenza di un primo che divide un intero. Siano quindi n un intero positivo, e p un numero primo. Denotiamo con $r_p(n)$ il massimo intero s (maggiore o uguale a zero) tale che p^s divide n. Dunque

$$n = \prod_{p\leq n} p^{r_p(n)}$$

è la decomposizione di n come prodotto di potenze di primi distinti. Dalla definizione si ha subito le seguente ovvia

Osservazione: Per ogni $n, m \in \mathbb{N}^*$, si ha $r_p(nm) = r_p(n) + r_p(m)$.

Meno evidente, ma molto importante è la formula seguente.

Lemma 7.1 *Sia $n \geq 2$, e sia p un numero primo (minore od uguale a n). Allora*

$$r_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] \ .$$

(Osserviamo che la sommatoria del membro di destra è di fatto una somma finita; infatti se $i > [\log_p n]$ allora $[n/p^i] = 0$.)

DIMOSTRAZIONE. Sia $n \in \mathbb{N}^*$ e p un numero primo. Denoto con $I = \{1, 2, \ldots, [\log_p n]\}$, l'insieme dei numeri naturali compresi tra 1 e $[\log_p n]$, con $T = \{1, 2, \ldots, n\}$, e considero l'insieme delle coppie,

$$S = \{ (i, m) \in I \times T \mid p^i \text{ divide } m \} .$$

Sia $i \in I$; allora il numero di elementi di S che hanno i come prima componente è uguale al numero di interi minori o uguali ad n che sono multipli di p^i, cioè $[n/p^i]$. Dunque, il numero di elementi di S (che si può ottenere sommando, per ogni $i \in I$ il numero di coppie di cui essa è la prima componente) è

$$|S| = \sum_{i=1}^{[\log_p n]} \left[\frac{n}{p^i}\right] .$$

Viceversa, fissato un $m \in T$, il numero di elementi di S che hanno m come seconda componente è il numero di potenze di p che dividono m, cioè $r_p(m)$; quindi

$$|S| = \sum_{m=1}^{n} r_p(m) .$$

Poichè, per l'osservazione fatta sopra,

$$\sum_{m=1}^{n} r_p(m) = r_p\left(\prod_{m=1}^{n} m\right) = r_p(m!)$$

dal confronto delle due espressioni di $|S|$ si ottiene l'enunciato. ∎

Lemma 7.2 *Sia $n \in \mathbb{N}^*$. Allora*

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} < 2^{2n} .$$

DIMOSTRAZIONE. Sia $n \in \mathbb{N}^*$. Allora

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} > \binom{2n}{n} .$$

Viceversa, tenendo conto del fatto che per ogni $1 \leq i \leq n$, $\binom{2n}{i}$ è minore di $\binom{2n}{n}$ (lo si dimostri per esercizio), si ha

$$2^{2n} = 2 + \sum_{i=1}^{2n-1} \binom{2n}{i} \leq 2 + (2n-1)\binom{2n}{n} \leq 2n\binom{2n}{n}$$

che dà la prima disuguaglianza. ∎

Esercizio 1. Sia $n \in \mathbb{N}^*$, e per ogni primo p denotiamo con $p^{s_p(2n)}$ la massima potenza di p minore o uguale a $2n$. Si provi che

(*a*) $\prod_{n<p\leq 2n} p$ divide $\binom{2n}{n}$;

(*b*) $\binom{2n}{n}$ divide $\prod_{p\leq 2n} p^{s_p(2n)}$.

7.1 Il Teorema di Čebichev

Definiamo ora le seguenti due funzioni ('theta' e 'psi' di Čebichev). Sia x un numero reale maggiore di 1; poniamo

$$\theta(x) = \sum_{p \le x} \log p$$

$$\psi(x) = \sum_{p^m \le x} \log p \ .$$

Ad esempio, si ha

$$\theta(10) = \log 2 + \log 3 + \log 5 + \log 7$$

$$\psi(10) = 3\log 2 + 2\log 3 + \log 5 + \log 7$$

Osservazione. Per ogni $x > 1$ si ha

$$\psi(x) = \sum_{p^m \le x} \log p = \sum_{p \le x} \left[\frac{\log x}{\log p} \right] \log p \le \sum_{p \le x} \frac{\log x}{\log p} \log p = \pi(x) \log x \ .$$

Esercizio 2. Provare che $\psi(x) = logU(x)$, dove $U(x)$ è il Minimo Comune Multiplo di tutti gli interi minori od uguali a x.

Esercizio 3. Sia $1 < x \in \mathbb{R}$, e sia $t = [\log_2 x] = [\log x / \log 2]$. Si provi che

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \ldots + \theta(x^{1/t}) \ .$$

Esercizio 4. Si provi che $\psi(x) = \theta(x) + O(\sqrt{x}\log x)^2)$.

Proposizione 7.3 *Per ogni* $1 < x \in \mathbb{R}$,

$$\theta(x) < 2x \log 2 \ .$$

Dimostrazione. Poichè $\theta(x) = \theta([x])$, è chiaro che è sufficiente provare l'affermazione per $x = n \in \mathbb{N}^*$.
Premettiamo una osservazione. Sia $m \in \mathbb{N}^*$, e sia

$$M = \binom{2m+1}{m} = \binom{2m+1}{m+1} = \frac{(2m+1)2m(2m-1)\cdots(m+2)}{m!} \ .$$

Ora, M è un intero che compare due volte come addendo nell'espansione binomiale $(1+1)^{2m+1} = 2^{2m+1}$. Quindi $2M < 2^{2m+1}$, cioè $M < 2^{2m}$. Se p è un primo tale che $m+1 < p \le 2m+1$, allora p divide il numeratore ma non il denominatore nell'espressione di M come frazione; quindi divide M. Dunque

$$\prod_{m+1 < p \le 2m+1} p \ \text{ divide } \ M \ .$$

Da ciò segue

$$\theta(2m+1) - \theta(m+1) = \sum_{m+1<p\leq 2m+1} \log p \leq \log M < 2m \log 2 \ .$$

Proviamo ora la Proposizione procedendo per induzione su n. Se $n = 2$ l'affermazione è banale. Sia $n \geq 3$ e assumiamo la proposizione vera per $m \leq n-1$.
- Se n è pari, n non è un numero primo e, applicando l'ipotesi induttiva,

$$\theta(n) = \theta(n-1) < 2(n-1)\log 2 < 2n \log 2 \ .$$

- Se $n = 2m+1$ è dispari, $m+1 < n$; applicando l'ipotesi induttiva e l'osservazione di sopra,

$$\theta(n) = \theta(2m+1) - \theta(m+1) + \theta(m+1) < 2m \log 2 + 2(m+1)\log 2 = 2n \log 2 \ ;$$

come si voleva. ∎

Esercizio 5. Sia $n \in \mathbb{N}^*$; si provi che

$$\prod_{p\leq n} p < 4^n \ .$$

Proposizione 7.4 *Per ogni* $1 < x \in \mathbb{R}$,

$$\psi(x) \geq \frac{1}{4} x \log 2 \ .$$

Dimostrazione. Sia $n \in \mathbb{N}^*$, e sia

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p\leq 2n} p^{r_p(N)} \ .$$

Per il Lemma 7.1 e l'osservazione che lo precede,

$$r_p(N) = r_p((2n)!) - 2r_p(n!) = \sum_{m\geq 1} \left(\left[\frac{2n}{p^m} \right] - 2 \left[\frac{n}{p^m} \right] \right) \ .$$

Ora, si vede facilmente che ciascun termine $\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]$ è uguale a 0 o ad 1 a seconda che $\left[\frac{2n}{p^m}\right]$ sia pari o dispari. Quindi

$$r_p(N) \leq \log_p(2n) \leq \left[\frac{\log 2n}{\log p} \right]$$

da cui segue

$$\log N = \sum_{p\leq 2n} r_p(N) \log p \leq \sum_{p\leq 2n} \left[\frac{\log 2n}{\log p} \right] \log p = \psi(2n) \ .$$

D'altra parte, $N \geq 2^n$ e quindi

$$\psi(2n) \geq n \log 2 \ .$$

Sia ora $2 \leq x \in \mathbb{R}$. Allora, $n = \left[\frac{x}{2}\right] \geq 1$, e per quanto visto sopra si ha

$$\psi(x) \geq \psi(2n) \geq n \log 2 \geq \frac{1}{4} x \log 2 \ ,$$

completando la dimostrazione. ∎

Teorema 7.5 (Čebichev). *Per ogni* $2 \leq x \in \mathbb{R}$*,*

$$\frac{\log 2}{4} \frac{x}{\log x} \leq \pi(x) \leq (2 + 4 \log 2) \frac{x}{\log x} \ .$$

Dimostrazione. Sia $1 < x \in \mathbb{R}$. Per la proposizione 7.4, e l'osservazione che segue la definizione di $\psi(x)$, si ha

$$\frac{1}{4} x \log 2 \leq \psi(x) \leq \pi(x) \log x$$

da cui si ricava la limitazione inferiore

$$\frac{\log 2}{4} \frac{x}{\log x} \leq \pi(x) \ .$$

Sia ora $\delta \in \mathbb{R}$, con $0 < \delta < 1$. Allora $x^\delta < x$, e

$$\theta(x) \geq \sum_{x^\delta < p \leq x} \log p \geq \sum_{x^\delta < p \leq x} \log(x^\delta) \geq \log(x^\delta) \left[\pi(x) - \pi(x^\delta)\right]$$

e dunque

$$\pi(x) \log(x^\delta) \leq \theta(x) + \pi(x^\delta) \log(x^\delta) \leq \theta(x) + x^\delta \log(x^\delta) \ .$$

Applicando la Proposizione 7.3, si ottiene

$$\pi(x) \log(x^\delta) \leq 2x \log 2 + x^\delta \log(x^\delta)$$

e ancora

$$\pi(x) \leq 2x \frac{\log 2}{\log(x^\delta)} + x^\delta \ .$$

Ponendo $\delta = \frac{1}{2}$, si ricava

$$\pi(x) \leq \frac{4x \log 2}{\log x} + \sqrt{x} \ .$$

Ora, per $x \geq 2$,

$$\sqrt{x} < \frac{2x}{\log x} \ ,$$

quindi è possibile maggiorare la diseguaglianza precedente

$$\pi(x) \leq \frac{4x \log 2}{\log x} + \frac{2x}{\log x} = (4 \log 2 + 2) \frac{x}{\log x}$$

completando la dimostrazione. ∎

Con tecniche simili è possibile provare un interessante e talvolta utile risultato che, nonostante sia un teorema a tutti gli effetti, prende il nome di postulato di Bertrand, dato che per molto tempo è rimasto una congettura (formulata, appunto, da Bertrand)

Teorema 7.6 (Postulato di Bertrand). *Sia $n \in \mathbb{N}^*$. Allora esiste un numero primo p tale che $n < p \leq 2n$.*

Dimostrazione. Poiché i numeri

$$2,\ 3,\ 5,\ 7,\ 13,, 23,\ 43,\ 83,\ 163,\ 317,\ 631$$

sono numeri primi, ognuno dei quali è maggiore della metà del successivo, l'affermazione dell'enunciato è vera per $n \leq 630$; in particolare è vera per $n \leq 2^9 = 512$.
Sia ora $n \geq 512$, e poniamo $N = \binom{2n}{n}$. Supponiamo per assurdo che non esista alcun numero primo p con $n < p \leq 2n$, allora

$$N = \binom{2n}{n} = \sum_{p \leq 2n} p^{r_p(N)} = \sum_{p \leq n} p^{r_p(N)} \ .$$

dove (si veda la dimostrazione della Proposizione 7.4)

$$r_p(N) = \sum_{m \geq 1} \left(\left[\frac{2n}{p^m} \right] - 2 \left[\frac{n}{p^m} \right] \right) \ .$$

Sia p un numero primo con $\frac{2}{3}n < p \leq n$. Allora $2p \leq 2n < 3p$, e $2n < \frac{4}{9}n^2 < p^2$, e si ha

$$r_p(N) = \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] = 0 \ .$$

Dunque se p è un divisore primo di N, si ha $p \leq \frac{2}{3}n$; e quindi, per la Proposizione 7.3,

$$\sum_{p|N} \log p \leq \sum_{p \leq \frac{2}{3}n} \log p = \theta(\frac{2}{3}n) \leq \frac{4}{3} n \log 2 \ .$$

Ora, sia p un primo tale che $p^2|N$ (cioè $r_p(N) \geq 2$) ; allora (si veda ancora la dimostrazione della Proposizione 7.4),

$$2 \leq r_p(N) \leq \left[\frac{\log 2n}{\log p} \right] \leq \frac{\log 2n}{\log p}$$

e quindi $r_p(N) \log p \leq \log 2n$, e in particolare $p^2 \leq 2n$, cioè $p \leq \sqrt{2n}$. Pertanto

$$\sum_{p^2|N} r_p(N) \log p \leq \sqrt{2n} \log 2n \ ,$$

da cui si ricava

$$\log N = \sum_{p|N} r_p(N) \log p = \sum_{r_p(N)=1} \log p + \sum_{p^2|N} r_p(N) \log p \leq \frac{4}{3} n \log 2 + \sqrt{2n} \log 2n \ .$$

Ma, per il Lemma 7.2,

$$\log N \geq \log \left(\frac{2^{2n}}{2n} \right) = 2n \log 2 - \log 2n \ ,$$

che, dal confronto con la diseguaglianza precedente, dà

$$2n \log 2 \leq \log N + \log 2n \leq \frac{4}{3} n \log 2 + \sqrt{2n} \log 2n$$

da cui si ricava

$$2n \log 2 \leq 3(\sqrt{2n} + 1) \log 2n$$

ed ancora

$$2n \leq 3(\sqrt{2n} + 1)(\log_2 n + 1) \ .$$

La dimostrazione si conclude provando che tale diseguaglianza non vale per $n \geq 512$. In tal caso, infatti, $\sqrt{2n} \geq 15$, e quindi $3(\sqrt{2n}+1) \leq \frac{16}{5}\sqrt{2n}$, che, se vale la disuguaglianza di sopra, implica

$$2n \leq \frac{16}{5}\sqrt{2n}(\log_2 n + 1)$$

da cui

$$\sqrt{2n} \leq \frac{16}{5}(\log_2 n + 1) \ .$$

Siano $f(x) = \sqrt{2x}$, e $g(x) = \frac{16}{5}(\log_2 x + 1)$. Per $x = 512 = 2^9$, si ha

$$f(x) = 2^5 = 32 \qquad \text{e} \qquad g(x) = \frac{16}{5}(\log_2 2^9 + 1) = \frac{16}{5} 10 = 32 \ ,$$

mentre per $x > 512$, $f(x) > g(x)$. Quasta contraddizione completa la dimostrazione. ∎

7.2 La funzione di Mangoldt

In questa sezione cominciamo il lavoro preparatorio per la dimostrazione del Teorema di Dirichlet sull'esistenza di numeri primi in una successione aritmetica. Iniziamo con alcune tecniche elementari ma assai utili per la stima di sommatorie su numeri interi.

Lemma 7.7 *Sia $f(t)$ una funzione reale positiva e crescente in $t \geq 1$. Allora*

$$\left| \sum_{n \leq x} f(n) - \int_1^x f(t) \mathrm{d}t \right| \leq f(x).$$

Dimostrazione. Supponiamo che $f(t)$ sia positiva e crescente. Per ogni numero naturale i si ha allora

$$f(i) \leq \int_i^{i+1} f(t) \mathrm{d}t \leq f(i+1)$$

quindi, per ogni $a, b \in \mathbb{N}^*$, con $a < b$,

$$\sum_{n=a}^{b} f(n) - f(b) = \sum_{n=a}^{b-1} f(n) \leq \int_a^b f(t) \mathrm{d}t \leq \sum_{n=a+1}^{b} f(n) = \sum_{n=a}^{b} f(n) - f(a)$$

e dunque

$$f(a) \leq \sum_{n=a}^{b} f(n) - \int_a^b f(t)\mathrm{d}t \leq f(b).$$

Sia ora $1 < x \in \mathbb{R}$. Allora, per quanto visto sopra, essendo $f(t)$ positiva,

$$\sum_{n\leq x} f(n) - \int_1^x f(t)\mathrm{d}t \leq \sum_{n=1}^{[x]} f(n) - \int_1^{[x]} f(t)\mathrm{d}t \leq f(b) \leq f(x).$$

D'altra parte

$$\sum_{n\leq x} f(n) - \int_1^x f(t) = \sum_{n\leq x} f(n) - \int_1^{[x]} f(t) - \int_{[x]}^x f(t) \geq f(1) - f(x)\ .$$

Pertanto

$$\left|\sum_{n\leq x} f(n) - \int_1^x f(t)\right| \leq f(x)\ .$$

■

Esercizio 6. Sia $f(t)$ una funzione positiva e monotona in $t \geq 1$. Si provi che, per ogni $1 \leq y, x \in \mathbb{R}$, con $y < [x]$,

$$\left|\sum_{y<n\leq x} f(n) - \int_y^x f(t)\mathrm{d}t\right| \leq \max\{f(y), f(x)\}.$$

Teorema 7.8 (Somme per parti) *Siano f e g funzioni aritmetiche, e per $1 \leq x \in \mathbb{R}$, sia definita $F(x) = \sum_{n\leq x} f(n)$. Siano $a, b \in \mathbb{N}$ con $a < b$. Allora*

$$\sum_{n=a+1}^{b} f(n)g(n) = F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)).$$

Sia g definita su $[1, x]$ e ivi derivabile con continuità. Allora, per $x \geq 2$,

$$\sum_{n\leq x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)\mathrm{d}t\ .$$

Dimostrazione. La prima uguaglianza è un semplice calcolo, tenendo conto che, per ogni $2 \leq n \in \mathbb{N}$, $f(n) = F(n) - F(n-1)$:

$$\sum_{n=a+1}^{b} f(n)g(n) = \sum_{n=a+1}^{b} (F(n) - F(n-1))g(n) = \sum_{n=a+1}^{b} F(n)g(n) - \sum_{n=a}^{b-1} F(n)g(n+1)$$

$$= F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)).$$

Supponiamo ora che $g(t)$ sia derivabile con continuità in $[1, x]$. Allora, per ogni $n \leq x-1$,

$$g(n+1) - g(n) = \int_n^{n+1} g'(t)udt.$$

Poiché, per $n \leq t < n+1$, $F(t) = F(n)$, si ha

$$F(n)\left(g(n+1) - g(n)\right) = \int_n^{n+1} F(t)g'(t)\mathrm{d}t.$$

Sia ora $b = [x]$. Utilizzando la prima identità, tenendo conto che $F(x) = F(b)$,

$$\sum_{n\leq x} f(n)g(n) = f(1)g(1) + \sum_{n=2}^{b} f(n)g(n) =$$

$$f(1)g(1) + F(x)g(b) - F(1)g(2) - \sum_{n=2}^{b-1} F(n)\left(g(n+1) - g(n)\right).$$

Applicando ora quanto sopra osservato

$$\sum_{n\leq x} f(n)g(n) = f(1)g(1) + F(x)g(b) - F(1)g(2) - \sum_{n=2}^{b-1}\int_n^{n+1} F(t)g'(t)\mathrm{d}t =$$

$$= f(1)\left(g(1) - g(2)\right) + F(x)g(b) - \int_2^b F(t)g'(t)\mathrm{d}t.$$

Poiché inoltre

$$\int_1^2 F(t)g'(t)\mathrm{d}t = f(1)\left(g(2) - g(1)\right)$$

e

$$\int_b^x F(t)g'(t)\mathrm{d}t = F(b)\left(g(x) - g(b)\right) = F(x)(g(x) - g(b))$$

si conclude che

$$\sum_{n\leq x} f(n)g(n) = F(x)g(x) - \int_b^x F(t)g'(t)\mathrm{d}t - \int_1^2 F(t)g'(t)\mathrm{d}t - \int_2^b F(t)g'(t)\mathrm{d}t$$

ottenendo infine l'identità voluta. ∎

Lemma 7.9 *Per* $1 \leq x \in \mathbb{R}$,

$$\sum_{n\leq x} \log n = x\log x - x + O(\log x)\ .$$

Dimostrazione. Poiché per $x \geq 1$ la funzione $\log x$ è positiva e crescente, si ha, applicando il Lemma 7.7,

$$\sum_{n\leq x} \log n = \int_1^x \log t\,\mathrm{d}t + O(\log x) = x\log x - x + O(\log x)\ ,$$

e questo dimostra il Lemma. ∎

Lemma 7.10 *Esiste una costante C_2 tale che, per $1 \leq x \in \mathbb{R}$,*

$$\sum_{n \leq x} n^{-\frac{1}{2}} = 2\sqrt{x} + C_2 + O(x^{-\frac{1}{2}}) \ .$$

DIMOSTRAZIONE. Per ogni numero reale $t \geq 1$, denotiamo con $\epsilon(t)$ la differenza $t - [t]$; quindi $0 \leq \epsilon(t) < 1$. Osserviamo ora che l'integrale

$$\int_1^\infty \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t$$

esiste finito. Infatti

$$0 < \int_1^\infty \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t < \int_1^\infty t^{-\frac{3}{2}} \mathrm{d}t = 2.$$

Poniamo quindi

$$C_2 = -1 - \frac{1}{2} \int_1^\infty \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t.$$

Applichiamo il Teorema 7.8, con $f(n) = 1$ e $g(t) = t^{-\frac{1}{2}}$. Allora, per $1 \leq x \in \mathbb{R}$, $F(x) = [x]$. Per 7.8, si ha quindi

$$\sum_{n \leq x} n^{-\frac{1}{2}} = \frac{[x]}{\sqrt{x}} + \frac{1}{2} \int_1^x [t] t^{-\frac{3}{2}} \mathrm{d}t = \frac{[x]}{\sqrt{x}} + \frac{1}{2} \int_1^x (t - \epsilon(t)) t^{-\frac{3}{2}} \mathrm{d}t =$$

$$= \frac{[x]}{\sqrt{x}} + \frac{1}{2} \int_1^x t^{-\frac{1}{2}} \mathrm{d}t - \frac{1}{2} \int_1^x \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t = \sqrt{x} - \frac{\epsilon(x)}{\sqrt{x}} + \sqrt{x} - 1 - \frac{1}{2} \int_1^x \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t.$$

Dunque, con la notazione prima introdotta,

$$\sum_{n \leq x} n^{-\frac{1}{2}} = 2\sqrt{x} - \frac{\epsilon(x)}{\sqrt{x}} + C_2 + \frac{1}{2} \int_x^\infty \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t,$$

e poiché

$$0 < \frac{1}{2} \int_x^\infty \epsilon(t) t^{-\frac{3}{2}} \mathrm{d}t < \frac{1}{2} \int_x^\infty t^{-\frac{3}{2}} \mathrm{d}t = \frac{1}{\sqrt{x}}$$

si ottiene il risultato dell'enunciato. ∎

Definiamo ora la funzione Λ *di Mangoldt*, ponendo per ogni $n \in \mathbb{N}^*$,

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^k \text{ per qualche primo } p \text{ e } k \geq 1 \\ \\ 0 & \text{altrimenti} \end{cases}$$

Lemma 7.11 *Per ogni $n \in \mathbb{N}^*$,*

$$\sum_{d|n} \Lambda(d) = \log n \quad \text{e} \quad \Lambda(n) = -\sum_{d|n} \mu(d) \log d \ .$$

DIMOSTRAZIONE. Sia $n = \prod_{p|n} p^{r_p(n)}$. Per definizione di Λ,

$$\sum_{d|n} \Lambda(d) = \sum_{p^i|n} \log p = \sum_{p|n} r_p(n) \log p = \log n \ .$$

Applicando quindi la formula di inversione di Möbius si ottiene

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d \ ,$$

ricordando che, per $n > 1$, $\sum_{d|n} \mu(d) = 0$. ∎

Lemma 7.12 *Esiste una costante B tale che, per $1 \leq x \in \mathbb{R}$,*

$$\sum_{n \leq x} \Lambda(n) \leq Bx$$

(e quindi, $\sum_{n \leq x} \Lambda(n) = O(x)$).

DIMOSTRAZIONE. Applicando il teorema di Čebichev 7.5,

$$\sum_{n \leq x} \Lambda(n) = \sum_{p^i \leq x} \log p = \sum_{p \leq x} \left[\frac{\log x}{\log p}\right] \log p \leq \sum_{p \leq x} \log x = \pi(x) \log x \leq B \frac{x}{\log x} \log x = Bx$$

con $B = 2 + 4 \log 2$. ∎

Lemma 7.13 *Per $1 \leq x \in \mathbb{R}$,*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1) \ .$$

DIMOSTRAZIONE. Per il Lemma 7.11, $\sum_{d|n} \Lambda(d) = \log n$. Quindi, applicando il Lemma 2.6,

$$\sum_{n \leq x} \log n = \sum_{d \leq x} \left[\frac{x}{d}\right] \Lambda(d) \ .$$

Scrivendo $\frac{x}{n} = \left[\frac{x}{n}\right] + \epsilon(\frac{x}{n})$, si ottiene quindi

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \frac{1}{x} \sum_{n \leq x} \frac{\Lambda(n)x}{n} = \frac{1}{x} \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] + \frac{1}{x} \sum_{n \leq x} \Lambda(n) \epsilon(x/n).$$

Per il lemma 7.12

$$0 \leq \frac{1}{x} \sum_{n \leq x} \Lambda(n) \epsilon(x/n) \leq \frac{1}{x} \sum_{n \leq x} \Lambda(n) \leq B = O(1);$$

quindi, per l'osservazione iniziale, ed applicando il Lemma 7.9,

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \frac{1}{x} \sum_{n \leq x} \log n + O(1) = \frac{1}{x}(x \log x - x + O(\log x)) + O(1) = \log x + O(1)$$

come si voleva. ∎

7.3 Caratteri di Dirichlet

Sia $1 \leq c \in \mathbb{N}$. Una applicazione $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$, si dice *carattere di Dirichlet modulo c* se soddisfa alle seguenti condizioni:

per ogni $a, b \in \mathbb{Z}$

1) $\chi(a) = \chi(b)$ se $a \equiv b \,(mod\, c)$;

2) $\chi(a) \neq 0$ se e solo se $(a, c) = 1$;

3) $\chi(ab) = \chi(a)\chi(b)$.

Ad esempio, se p è un numero primo dispari, allora il simbolo di Legendre

$$\left(\frac{\cdot}{p}\right) \; : \; a \mapsto \; \left(\frac{a}{p}\right)$$

è un carattere di Dirichlet modulo p.

Dato $c \geq 1$, indichiamo con $\mathbb{Z}_c$ l'insieme (l'anello) $\mathbb{Z}/c\mathbb{Z}$ delle classi di resto modulo c, e con $\mathbb{Z}_c^*$ il gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_p$. Come nel capitolo precedente, denotiamo con $\widehat{\mathbb{Z}_c^*}$ il gruppo dei caratteri di $\mathbb{Z}_c^*$.
Si verifica facilmente che se χ è un carattere di Dirichlet modulo c, allora l'applicazione $\hat{\chi}$, definita da, per ogni $a + c\mathbb{Z} \in \mathbb{Z}_c^*$,

$$\hat{\chi}(a + c\mathbb{Z}) = \chi(a)$$

è un carattere di $\mathbb{Z}_c^*$ [la condizione 1) per i caratteri di Dirichlet assicura che è ben definita, la 2) che la sua immagine è contenuta in $\mathbb{C}^*$, e la 3) che è un omomorfismo di gruppi moltiplicativi].
Viceversa, ad ogni carattere ψ di $\mathbb{Z}_c^*$, si associa ψ' un carattere di Dirichlet modulo c ponendo, per ogni $a \in \mathbb{Z}$,

$$\psi'(a) = \begin{cases} 0 & \text{se } (a, c) \neq 1 \\ \psi(a + c\mathbb{Z}) & \text{se } (a, c) = 1 \end{cases}$$

È immediato verificare che queste corrispondenze sono l'una l'inversa dell'altra, e quindi stabiliscono una biezione tra l'insieme dei caratteri di Dirichlet modulo c ed il gruppo dei caratteri di $\mathbb{Z}_c^*$. In particolare il numero di caratteri di Dirichlet modulo c è uguale all'ordine di $\mathbb{Z}_c^*$, che, come sappiamo è uguale a $\phi(c)$. Inoltre, se χ è un carattere di Dirichlet modulo c, allora $\chi(1) = 1$ e per ogni a con $(a, c) = 1$, $\chi(a)$ è una radice $\phi(c)$-esima dell'unità.
Dato un carattere di Dirichlet χ, si definisce in modo naturale il carattere coniugato $\overline{\chi}$ (e si ha $\overline{\chi}' = \overline{\chi'}$), e si dice che un carattere di Dirichlet è *reale* se coincide con il suo coniugato (ovvero se la sua immagine è contenuta in $\mathbb{R}$). Continueremo poi a denotare con χ_o il carattere di Dirichlet *principale*, ovvero quello definito da

$$\chi_o(a) = \begin{cases} 1 & \text{se } (a, c) = 1 \\ 0 & \text{se } (a, c) \neq 1 \end{cases}$$

Infine, l'operazione di prodotto per caratteri si estende in modo naturale ai caratteri di Dirichlet. A questo punto le relazioni di ortogonalità si ottengono immediatamente da quelle per i caratteri (Teoremi 6.7 e 6.8).

Teorema 7.14 *Sia $1 \leq c \in \mathbb{N}$. Denotiamo con $\mathfrak{D}_c$ l'insieme dei caratteri di Dirichlet modulo c. Per ogni $a \in \mathbb{Z}$,*

$$\sum_{\chi \in \mathfrak{D}_c} \chi(a) = \begin{cases} \phi(c) & se \;\; a \equiv 1 \,(mod\, c) \\ 0 & se \;\; a \not\equiv 1 \,(mod\, c) \end{cases}$$

Sia U un insieme di rappresentati delle classi di congruenza nodulo c. Per ogni $\chi \in \mathfrak{D}_c$,

$$\sum_{a \in U} \chi(a) = \begin{cases} \phi(c) & se \;\; \chi = \chi_o \\ 0 & se \;\; \chi \neq \chi_o \end{cases}$$

Teorema 7.15 *Con le stesse notazioni del Teorema precedente.*

Per ogni $a, b \in \mathbb{Z}$,

$$\sum_{\chi \in \mathfrak{D}_c} \chi(a)\overline{\chi}(b) = \begin{cases} \phi(c) & se \;\; (a,c) = 1 \;\; e \;\; a \equiv b \,(mod\, c) \\ 0 & altrimenti \end{cases}$$

Per ogni χ_1, $\chi_2 \in \mathfrak{D}_c$,

$$\sum_{a \in U} \chi_1(a)\overline{\chi_2}(a) = \begin{cases} \phi(c) & se \;\; \chi_1 = \chi_2 \\ 0 & se \;\; \chi_1 \neq \chi_2 \end{cases}$$

Esercizio 7. Si provi che se p è un numero primo dispari allora il carattere principale χ_0 ed il simbolo di Legendre sono i soli caratteri di Dirichlet reali modulo p.

Lemma 7.16 *Sia $2 \leq c \in \mathbb{N}^*$, e sia χ un carattere di Dirichlet modulo c, con $\chi \neq \chi_0$. Sia $\{a_n\}_{n \in \mathbb{N}^*}$ una successione decrescente di numeri reali positivi.*

(i) Se $m, n \in \mathbb{N}^*$, con $n < m$, allora

$$\left| \sum_{k=n}^{m} \chi(k) a_k \right| < 2\phi(c) a_n.$$

(ii) Se inoltre $\lim_{n \to \infty} a_n = 0$, allora è convergente la serie

$$\sum_{k=1}^{\infty} \chi(k) a_k.$$

DIMOSTRAZIONE. Siano $n, m \in \mathbb{Z}$, con $n < m$. Per la divisione euclidea, scriviamo $m - n = qc + r$, con $0 \leq r < c$. Allora, l'intervallo (di numeri interi) $n \leq i \leq n + qc - 1$ è l'unione di q sistemi di rappresentanti di classi di congruenza modulo c. Pertanto per il Teorema 7.14,

$$\sum_{i=n}^{n+qc-1} \chi(i) = 0$$

e quindi

$$\left|\sum_{i=n}^{m} \chi(i)\right| = \left|\sum_{i=0}^{r} \chi(i+n+qc)\right| = \left|\sum_{i=0}^{r} \chi(i+n)\right| \leq \sum_{i=0}^{r} |\chi(i+n)| \leq \phi(c).$$

Per ogni $0 \leq x \in \mathbb{R}$, definiamo $F(x) = \sum_{n \leq x} \chi(n)$. Sia $\{a_n\}_{n \in \mathbb{N}^*}$ una successione decrescente di numeri reali positivi. Allora, per la prima parte del Teorema 7.8,

$$\sum_{k=n}^{m} \chi(k)a_k = F(m)a_m - F(n-1)a_n - \sum_{k=n}^{m-1} F(k)(a_{k+1} - a_k).$$

Ma, per quanto osservato sopra, $|F(x)| \leq \phi(c)$; pertanto

$$\left|\sum_{k=n}^{m} \chi(k)a_k\right| < \phi(c)a_n + \phi(c)a_m + \phi(c) \sum_{k=n}^{m-1} (a_k - a_{k+1}) = 2\phi(c)a_n$$

provando così la prima parte.

Supponiamo ora che $\lim_{n \to \infty} a_n = 0$. Allora, per ogni $0 < \epsilon \in \mathbb{R}$, esiste un intero $n = n(\epsilon)$ tale che

$$a_n < \frac{\epsilon}{2\phi(c)}.$$

Allora, per ogni $m \geq n$, e $s \geq 1$, per la parte precedente, si ha

$$\left|\sum_{k=m}^{m+s} \chi(k)a_k\right| < 2\phi(c)a_m \leq 2\phi(c)a_n < \epsilon.$$

Dunque la serie $\sum_{k=1}^{\infty} \chi(k)a_k$ soddisfa il criterio di Cauchy ed è quindi convergente. ∎

7.4 Il Teorema di Dirichlet

Sia $2 \leq c \in \mathbb{N}$. Se χ è un carattere non-principale modulo c, si pone

$$L(\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} \ .$$

Per il Lemma 7.16, $L(\chi)$ è un numero complesso.

Esempio. Ci sono solo due caratteri di Dirichlet modulo 3: il carattere principale ed il simbolo di Legendre (chiamiamolo, per questa volta, λ). Per ogni $a \in \mathbb{Z}$ si ha

$$\lambda(a) = \begin{cases} 0 & \text{se } a \equiv 0 \,(mod\, 3) \\ 1 & \text{se } a \equiv 1 \,(mod\, 3) \\ -1 & \text{se } a \equiv 2 \,(mod\, 3). \end{cases}$$

Quindi

$$L(\lambda) = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \cdots = \frac{2}{3}.$$

Uno dei passi principali della dimostrazione di Dirichlet è provare che, per ogni carattere non-principale, $L(\chi) \neq 0$. Vediamo subito il caso dei caratteri reali.

Lemma 7.17 *Sia χ un carattere di Dirichlet modulo c, reale e tale che $\chi \neq \chi_0$. Allora $L(\chi) \neq 0$.*

Dimostrazione. Per ogni $n \in \mathbb{N}^*$, poniamo

$$f(n) = \sum_{d|n} \chi(d).$$

Per il Teorema 2.1, f è una funzione moltiplicativa. Sia p un primo e $m \geq 1$; poiché χ è un carattere reale, $\chi(p) \in \{0, 1, -1\}$.

- se $\chi(p) = 1$, allora $f(p^m) = m + 1 \geq 1$;
- se $\chi(p) = 0$, allora $f(p^m) = \chi(1) = 1$;
- se $\chi(p) = -1$, allora $f(p^m) = 1, 0$ a seconda se m è pari o dispari.

Poiché f è moltiplicativa si conclude che, per ogni $n \in \mathbb{N}^*$, $f(n) \geq 0$, e che $f(n) \geq 1$ se n è un quadrato.

Per $1 \leq x \in \mathbb{R}$, sia

$$F(x) = \sum_{n \leq x} \frac{f(n)}{\sqrt{n}} \ .$$

Per quanto osservato sopra, i termini della somma in $F(x)$ sono tutti positivi, e inoltre

$$F(x) \geq \sum_{n^2 \leq x} \frac{1}{n}$$

e dunque

$$\lim_{x \to \infty} F(x) = \infty \ .$$

D'altra parte, utilizzando il Lemma 2.5,

$$F(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{dj \leq x} \frac{\chi(d)}{\sqrt{dj}}.$$

Sia D l'insieme delle coppie ordinate (d, j) di interi positivi e non nulli tali che $dj \leq x$. Poniamo

$$D_1 = \{(d,j) \in D \mid d \leq \sqrt{x}\}, \qquad D_2 = \{(d,j) \in D \mid d > \sqrt{x}\} \ .$$

Allora, usando il Lemma 7.10,

$$F_1(x) = \sum_{(d,j)\in D_1} \frac{\chi(d)}{\sqrt{dj}} = \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{j\leq x/d} \frac{1}{\sqrt{j}} = \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(2\sqrt{x/d} + C_2 + O(\sqrt{d/x})\right)$$

da cui segue

$$F_1(x) = 2\sqrt{x} \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + C_2 \cdot O(1) + \frac{1}{\sqrt{x}} \cdot O(1)$$

e dunque

$$F_1(x) = 2\sqrt{x} \left(L(\chi) - \sum_{d>\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \right) + O(1) = 2L(\chi)\sqrt{x} + O(1).$$

Per quanto riguarda le rimanenti coppie (d, j),

$$F_2(x) = \sum_{(d,j)\in D_1} \frac{\chi(d)}{\sqrt{dj}} = \sum_{j\leq\sqrt{x}} \frac{1}{\sqrt{j}} \sum_{\sqrt{x}<d\leq x/j} \frac{\chi(d)}{\sqrt{d}} \ ;$$

quindi, applicando l'osservazione all'inizio del paragrafo,

$$|F_2(x)| \leq 2\phi(c) \frac{1}{x^{1/4}} \sum_{j\leq\sqrt{x}} \frac{1}{\sqrt{j}} \leq 2\phi(c) \frac{1}{x^{1/4}} \cdot O(x^{1/4}) = O(1).$$

Pertanto, si ottiene

$$F(x) = F_1(x) + F_2(x) = 2L(\chi)\sqrt{x} + O(1) \ ,$$

che è compatibile con $\lim_{x\to\infty} F(x) = \infty$ soltanto se $L(\chi) \neq 0$. ∎

Per ogni carattere di Dirichlet χ (modulo c), definamo ora, per $1 \leq x \in \mathbb{R}$, la funzione

$$T_\chi(x) = \sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} \ .$$

Lemma 7.18 *Sia χ_o il carattere principale modulo c. Allora*

$$T_{\chi_o}(x) = \log x + O(1).$$

DIMOSTRAZIONE. Osserviamo che l'insieme Δ dei primi che dividono c è finito, e che $\Lambda(n)\chi_o(n) \neq 0$ se e solo se n è potenza di un primo che non appartiene a Δ, ed in tal caso $\chi_o(n) = 1$. Dunque

$$T_{\chi_o}(x) = \sum_{p^i \leq x} \frac{\Lambda(p^i)}{p^i} - \sum_{p\in\Delta} \sum_{p^i \leq x} \frac{\Lambda(p^i)}{p^i} = \sum_{n\leq x} \frac{\Lambda(n)}{n} - \sum_{p\in\Delta} \left(\log p \sum_{p^i \leq x} \frac{1}{p^i} \right).$$

Ora

$$\sum_{p\in\Delta} \log p \sum_{p^i \leq x} \frac{1}{p^i} < \sum_{p\in\Delta} \log p \sum_{i=1}^{\infty} \frac{1}{p^i} = \sum_{p\in\Delta} \frac{\log p}{p-1} = O(1),$$

essendo Δ finito. In conclusione, applicando il Lemma 7.13,

$$T_{\chi_o}(x) = \sum_{n\leq x} \frac{\Lambda(n)}{n} + O(1) = \log x + O(1),$$

come si voleva. ∎

Lemma 7.19 *Sia χ un carattere di Dirichlet, tale che $\chi \neq \chi_o$. Allora*

(i) $L(\chi)T_\chi(x) = O(1)$;

(ii) $T_\chi(x) = -\log x + L(\chi)R(x) + O(1)$, *(dove* $R(x) = \sum_{n\leq x} \frac{\chi(n)\mu(n)}{n} \log \frac{x}{n}$*).*

DIMOSTRAZIONE. (i) Consideriamo la funzione

$$A(x) = \sum_{n\leq x} \frac{\chi(n)\log n}{n}.$$

Allora, dato che χ è moltiplicativa, e $\log n = \sum_{d|n} \Lambda(d)$,

$$A(x) = \sum_{n\leq x} \frac{\chi(n)}{n} \sum_{d|n} \Lambda(d) = \sum_{m\leq x} \frac{\chi(m)\Lambda(m)}{m} \sum_{d\leq x/m} \frac{\chi(d)}{d} = L(\chi)T_\chi(x) - R_1(x)$$

dove

$$R_1(x) = \sum_{m\leq x} \frac{\chi(m)\Lambda(m)}{m} \sum_{k>x/m} \frac{\chi(k)}{k}.$$

Ora, poiché $|\chi(m)| \leq 1$, applicando il lemma 7.16,

$$|R_1(x)| \leq \sum_{m\leq x} \frac{\Lambda(m)}{m} \left| \sum_{k>x/m} \frac{\chi(k)}{k} \right| < \sum_{m\leq x} \left(\frac{\Lambda(m)}{m} 2\phi(c) \frac{m}{x} \right)$$

e per il Lemma 7.12,

$$|R_1(x)| < \frac{2\phi(c)}{x} \sum_{m\leq x} \Lambda(m) \leq \frac{2\phi(c)}{x} Bx = O(1).$$

D'altra parte, per il lemma 7.16, $A(x)$ è limitata (cioè $A(x) = O(1)$), e quindi

$$L(\chi)T_\chi(x) = A(x) + R_1(x) = O(1).$$

(ii) Consideriamo la funzione

$$B(x) = \sum_{n\le x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log \frac{x}{d}.$$

Per il Lemma 2.7, abbiamo

$$B(x) = \sum_{n\le x} \frac{\chi(n)}{n} \left(\log x \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \right) = \log x - \sum_{n\le x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log d$$

e quindi per il Lemma 7.11,

$$B(x) = \log x + \sum_{n\le x} \frac{\chi(n)}{n} \Lambda(n) = \log x + T_\chi(x).$$

D'altra parte, riscrivendo la somma in $B(x)$ usando il Lemma 2.5 e tenendo conto che χ è moltiplicativa,

$$B(x) = \sum_{m\le x} \left(\frac{\chi(m)\mu(m)}{m} \log \frac{x}{m} \sum_{k\le x/m} \frac{\chi(k)}{k} \right) = L(\chi) \sum_{m\le x} \frac{\chi(m)\mu(m)}{m} \log \frac{x}{m} - R_2(x),$$

dove abbiamo posto

$$R_2(x) = \sum_{m\le x} \left(\frac{\chi(m)\mu(m)}{m} \log \frac{x}{m} \sum_{k>x/m} \frac{\chi(k)}{k} \right).$$

Valutiamo ora tale termmine residuo. Siccome per ogni naturale m, $|\chi(m)\mu(m)| \le 1$,

$$|R_2(x)| \le \sum_{m\le x} \left(\frac{1}{m} \log \frac{x}{m} \left| \sum_{k>x/m} \frac{\chi(k)}{k} \right| \right)$$

e dunque, per il Lemma 7.16,

$$|R_2(x)| \le \sum_{m\le x} \frac{1}{m} \log \frac{x}{m} \left(2\phi(c) \frac{m}{x} \right) = \frac{2\phi(c)}{x} \sum_{m\le x} \log \frac{x}{m}$$

e, infine, per il Lemma 7.9,

$$|R_2(x)| \le \frac{2\phi(c)}{x} \sum_{m\le x} (\log x - \log m) \le \frac{2\phi(c)}{x} (x \log x - x \log x + x + O(\log x)) = O(1).$$

In conclusione, ricordando quanto osservato all'inizio su $B(x)$, e con le notazione per $R(x)$ data nell'enunciato, si ricava

$$\log x + T_\chi(x) = B(x) = L(\chi)R(x) - R_2(x),$$

concludendo la dimostrazione del punto (ii). ∎

Proposizione 7.20 *Sia χ un carattere di Dirichlet, tale che $\chi \neq \chi_o$. Allora*

(i) $L(\chi) \neq 0$;

(ii) $T_\chi(x) = O(1)$.

DIMOSTRAZIONE. (i) Per ogni carattere χ poniamo

$$t(\chi) = \begin{cases} -1 & \text{se } L(\chi) = 0 \\ 0 & \text{se } L(\chi) \neq 0 \end{cases}$$

Per il Lemma precedente, se $\chi \neq \chi_0$, si ha quindi

$$T_\chi(x) = t(\chi) \log x + O(1).$$

Tenendo conto del Lemma 7.18, si ottiene la seguente diseguaglianza

$$\log x + \sum_{\chi \neq \chi_0} t(\chi) \log x + O(1) = \sum_{\chi} T_\chi(x) = \sum_{n \leq x} \frac{\Lambda(n)}{n} \sum_{\chi} \chi(n) \geq 0.$$

Ciò implica in particolare (basta considerare un x sufficientemente grande),

$$\sum_{\chi \neq \chi_0} t(\chi) \geq -1.$$

Dunque, esiste al più un carattere non principale χ tale che $t(\chi) = -1$, cioè $L(\chi) = 0$. Supponiamo che χ sia un tale carattere; allora, χ non è reale per il Lemma 7.17, e chiaramente, $L(\overline{\chi}) = 0$. Poiché $\chi \neq \overline{\chi}$, questo darebbe una contraddizione. Quindi $L(\chi) \neq 0$ per ogni carattere non principale χ.

(ii) Segue immediatamente dal punto (i) e dal. Lemma 7.19. ∎

Teorema 7.21 (Dirichlet). *Siano a e c due numeri naturali, con $c \geq 2$, e $(a, c) = 1$. Allora*

$$\sum_{x \geq p \equiv a (mod c)} \frac{\log p}{p} = \frac{\log x}{\phi(c)} + O(1).$$

DIMOSTRAZIONE. Fissati a e c come nell'ipotesi, denotiamo con $\overline{a}$ l'insieme di tutti i numeri naturali congrui ad a modulo c; consideriamo quindi la funzione, definita per $1 \leq x \in \mathbb{R}$,

$$F(x) = \sum_{x \geq n \in \overline{a}} \frac{\Lambda(n)}{n}.$$

Per definizione di Λ,

$$F(x) \leq \sum_{i=1}^{[log_2 x]} \sum_{x \geq p^i \in \overline{a}} \frac{\log p}{p^i} < \sum_{x \geq p \in \overline{a}} \frac{\log p}{p} + \sum_{x \geq p} \frac{\log p}{p^2} \left(\sum_{i=0}^{[log_2 x]} \frac{1}{p^i} \right);$$

poiché la serie

$$\sum_{n \leq 1}^{\infty} \frac{\log n}{n(n-1)}$$

è convergente, si ottiene quindi

$$F(x) < \sum_{x \geq p \in \overline{a}} \frac{\log p}{p} + \sum_{x \geq p} \frac{\log p}{p(p-1)} = \sum_{x \geq p \in \overline{a}} \frac{\log p}{p} + O(1).$$

Ora, poiché $(a, c) = 1$, esiste $b \in \mathbb{N}$, tale che

$$ab \equiv 1 \, (mod \, c).$$

Per la Proposizione 7.20, ed il Lemma 7.18,

$$\sum_{\chi} \chi(b) T_{\chi}(x) = T_{\chi_o}(x) + O(1) = \log x + O(1).$$

Ma, per ogni χ, carattere di Dirichlet modulo c, $\chi(b) = \overline{\chi}(a)$; quindi, per la legge di ortogonalità per caratteri di Dirichlet,

$$\sum_{\chi} \chi(b) T_{\chi}(x) = \sum_{\chi} \chi(b) \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n \leq x} \frac{\Lambda(n)}{n} \sum_{\chi} \chi(b)\chi(n) =$$

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} \sum_{\chi} \overline{\chi}(a)\chi(n) = \phi(c) \sum_{x \geq n \in \overline{a}} \frac{\Lambda(n)}{n} = \phi(c) F(x).$$

Dunque, per quanto provato sopra,

$$\log x + O(1) = \sum_{\chi} \chi(b) T_{\chi}(x) = \phi(c) \sum_{x \geq p \in \overline{a}} \frac{\log p}{p} + O(1),$$

da cui segeue l'enunciato. ∎

Il teorema di Dirichlet ora segue immediatamente:

Teorema 7.22 (Dirichlet). *Siano a e c due numeri interi tali che $c \geq 1$ e $(a, c) = 1$. Allora esistono infiniti numeri primi della forma $a + cn$ con $n \in \mathbb{Z}$.*