

Aritmetica modulare

Dr Zimbu, da it.wikibooks.org

Questo testo proviene dal sito [it.wikibooks.org/wiki/Aritmetica modulare](http://it.wikibooks.org/wiki/Aritmetica_modulare) ed è stato scritto collettivamente dagli utenti di tale sito.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled GNU Free Documentation License.

Disclaimer

Wikibooks è un progetto online a contenuto aperto, ovvero, è un'associazione volontaria di individui e gruppi che sviluppano una risorsa comune di conoscenza umana. La sua struttura permette a chiunque sia connesso ad Internet e possieda un browser web di modificare il contenuto delle sue pagine. Pertanto, si prega di tener presente che nessuna delle informazioni presenti in queste pagine è stata necessariamente controllata da professionisti informati nei campi di specializzazione necessari per fornire un'informazione completa, accurata o certa su un qualsiasi argomento.

Qualsiasi marchio registrato, marchio di servizio, marchio collettivo, diritto di design, diritto di immagine o diritti simili che sono menzionati, usati o citati negli articoli di Wikibooks sono proprietà dei rispettivi proprietari. Il loro utilizzo in Wikibooks non implica che sia possibile un qualsiasi uso diverso da quello informativo, come contemplato dagli autori originali di questi articoli di Wikibooks, in base allo schema di licenza GFDL. Se non diversamente dichiarato i siti di Wikibooks e Wikimedia non sono né approvati, né affiliati ad alcuno dei detentori di tali diritti, e come tali non possono garantire alcun diritto per l'utilizzo di materiale altrimenti protetto. L'eventuale uso di una qualsiasi di tali proprietà incorporee è a vostro unico rischio.

Questo non significa che non troverete informazioni interessanti e accurate su Wikibooks, ciò nonostante siate coscienti che Wikibooks NON PUÒ garantire, in qualsiasi forma, la validità delle informazioni trovate al suo interno. Possono essere state cambiate, vandalizzate o alterate da qualcuno la cui opinione non corrisponde allo stato della conoscenza nella particolare area alla quale siete interessati a informarvi.

Nessuno degli autori, contributori, sponsor, amministratori, sistemisti, o chiunque altro sia in qualsiasi modo connesso a Wikibooks può essere responsabile per il comparire di una qualsiasi informazione inaccurata o diffamatoria o per l'uso che può venire fatto delle informazioni contenute su queste pagine web o su quelle raggiungibili da esse.

Per favore, assicuratevi di aver compreso che le informazioni qui presenti sono fornite in maniera libera e gratuita, e che nessun tipo di accordo o contratto viene creato tra voi e i proprietari o gli altri utenti del sito, i proprietari dei server su cui viene ospitato, i singoli contributori di Wikibooks, qualsiasi amministratore del progetto, gli amministratori di sistema o chiunque altro sia in qualsiasi modo collegato a questo progetto e a quelli collaterali. Vi viene garantita una licenza limitata di copia di qualsiasi parte del sito; ciò non crea o implica alcuna responsabilità contrattuale o extra-contrattuale da parte di Wikibooks o di uno qualsiasi dei suoi agenti, membri, organizzatori o altri utenti.

Per favore prendete nota che le informazioni trovate qui possono essere in violazione delle leggi della nazione dalla quale le state consultando. Wikibooks non incoraggia la violazione di alcuna legge, ma poiché queste informazioni sono conservate su dei server in California negli Stati Uniti d'America, vengono mantenute in riferimento alle protezioni garantite a tutti in base al Primo emendamento della Costituzione degli Stati Uniti d'America e alla Dichiarazione Universale dei Diritti dell'Uomo delle Nazioni Unite. Le leggi della vostra nazione potrebbero non riconoscere una protezione del diritto di parola così ampia come quella delle leggi degli Stati Uniti o dei principi sotto lo statuto dell'ONU, e come tali, Wikibooks non può essere responsabile per una qualsiasi violazione potenziale di tali leggi

nel caso vi colleghiate a questo dominio o utilizzate una qualsiasi informazione in esso contenuta in qualsiasi modo.

Se avete bisogno di consigli specifici (ad esempio, medici, legali, gestione dei rischi) per favore cercate un professionista che sia certificato e informato in quel campo.

Leggete Disclaimer sul rischio, Disclaimer Medico e Disclaimer Legale per disclaimer specifici. È possibile che brevi annotazioni che rimandano a questa pagina compaiano in apertura o in chiusura di alcuni articoli segnalati dagli autori per il loro presentare o descrivere situazioni a potenziale rischio; tali annotazioni sono da intendersi aggiuntive al contenuto di questa pagina, che si applica ad ogni articolo contenuto in Wikibooks.

Wikibooks non è uniformemente revisionata; mentre i lettori possono correggere errori o rimuovere suggerimenti errati, non hanno nessun dovere legale di farlo e quindi tutte le informazioni qui presenti sono fornite senza qualsiasi garanzia implicita di idoneità per qualsiasi scopo o utilizzo.

Nessun danno consequenziale può essere richiesto contro Wikibooks, in quanto essa è un'associazione volontaria di individui, sviluppata liberamente per creare diverse risorse educative, culturali e informative, online e open source. Questa informazione viene data in maniera gratuita e non c'è nessun accordo o intendimento fra voi e Wikibooks circa il vostro utilizzo o modifica di queste informazioni oltre alla GNU Free Documentation License; tantomeno è chiunque in Wikibooks responsabile se qualcuno dovesse cambiare, editare, modificare o rimuovere qualsiasi informazione che voi potete aver inserito su Wikibooks o su uno qualsiasi dei suoi progetti associati.

Grazie per aver speso del tempo nel leggere questa pagina, ci auguriamo che possiate godervi la vostra esperienza su Wikibooks.

Indice

1	La relazione di congruenza	7
1.1	La relazione	7
1.2	Le operazioni	8
1.3	La divisione	9
2	Prime proprietà e applicazioni	11
2.1	Criteri di divisibilità	11
2.2	Il teorema di Fermat	12
2.3	Il teorema di Eulero	13
2.4	Fattoriali	13
3	Congruenze lineari	15
3.1	Congruenze semplici	15
3.2	Sistemi di congruenze lineari	16
3.3	Isomorfismi	17
3.4	Un'applicazione: la funzione di Eulero	18
3.5	Il lemma di Thue	18
4	Polinomi in aritmetica modulare	20
4.1	Modulo primo contro modulo composto	20
4.2	Il teorema di Chevalley	21
4.3	Generalizzazioni	21
5	Radici primitive	23
5.1	Terminologia	23
5.2	Prime proprietà dell'ordine	23
5.3	Numeri primi	24
5.4	Potenze dei numeri primi	25
5.5	Numeri divisibili da più di un primo	26
5.6	Indici	27
6	Congruenze quadratiche	28
6.1	Introduzione	28
6.2	Il simbolo di Legendre e il criterio di Eulero	29
6.3	Il lemma di Gauss	30
6.3.1	Il caso $a = 2$	31
6.4	La legge di reciprocità	32

6.4.1	Esempi	33
7	Alune applicazioni	34
7.1	Numeri primi	34
7.2	Teorema di Fermat sulle somme di due quadrati	35
7.3	Un problema additivo	35
8	Esercizi	37
Capitolo 1	37
Capitolo 2	37
Capitolo 3	38
Capitolo 4	38
Capitolo 5	39
Capitolo 6	39
Capitolo 7	39
	Bibliografia	40
A	Soluzioni degli esercizi	41
Capitolo 1	41
Capitolo 2	41
Capitolo 3	41
Capitolo 4	41
Capitolo 5	42
Capitolo 6	42
Capitolo 7	42
B	Cronologie	43
B.1	La relazione di congruenza	43
B.2	Prime proprietà e applicazioni	43
B.3	Congruenze lineari	43
B.4	Polinomi in aritmtica modulare	44
B.5	Radici primitive	44
B.6	Congruenze quadratiche	45
B.7	Alcune applicazioni	45
B.8	Bibliografia	45
B.9	Esercizi	46
C	GNU Free Documentation License	47
1.	APPLICABILITY AND DEFINITIONS	47
2.	VERBATIM COPYING	48
3.	COPYING IN QUANTITY	48
4.	MODIFICATIONS	49
5.	COMBINING DOCUMENTS	50
6.	COLLECTIONS OF DOCUMENTS	51

7. AGGREGATION WITH INDEPENDENT WORKS	51
8. TRANSLATION	51
9. TERMINATION	51
10. FUTURE REVISIONS OF THIS LICENSE	51

1 La relazione di congruenza

Questo capitolo tratta le proprietà elementari delle congruenze: la definizione delle relazione di congruenza e del relativo insieme quoziente, più il suo rapporto con le operazioni.

1.1 La relazione

Sia \mathbb{Z} l'insieme dei numeri interi, e n un intero maggiore o uguale a 2. All'interno di \mathbb{Z} definiamo la **'relazione di congruenza** \equiv_n come:

$$a \equiv_n b \iff n|(a - b) \quad (1.1)$$

dove la notazione $k|h$ indica che k divide h , ossia esiste un numero intero m tale che $h = mk$. Il fatto che a è in relazione con b può anche essere scritto come

$$a \equiv b \pmod{n} \quad (1.2)$$

e può essere espresso dicendo che a è *congruo*, o *congruente* a b modulo n . Chiaramente, diverse scelte di n porteranno a diverse relazioni, ma molte proprietà (e tutte quelle di carattere elementare) sono indipendenti da questa scelta.

È di facile verifica che la relazione \equiv_n così definita è di equivalenza:

- è riflessiva: $a - a = 0$, e 0 è divisibile per n ;
- è simmetrica: se $a - b = kn$, allora $b - a = -(a - b) = -kn = (-k)n$, e $-k$ è ancora un intero;
- è transitiva: se $a - b = kn$ e $b - c = jn$, allora

$$a - c = a - b + b - c = kn - jn = (k - j)n \quad (1.3)$$

Inoltre, se b e c sono due numeri diversi tra loro ma entrambi compresi tra 0 e $n - 1$, allora non possono essere congruenti: uno dei due deve essere infatti maggiore (sia ad esempio b): a questo punto $-c$ è un numero minore di b (e quindi strettamente minore di n) ma diverso da 0 (essendo b e c diversi). Quindi $b - c$, essendo minore di n e maggiore di 0, non può essere divisibile per n , ovvero b e c non sono in relazione tra loro.

Ora, dato un qualsiasi intero a , lo si può scrivere come

$$a = qn + b \quad (1.4)$$

dove b è compreso tra 0 e $n - 1$. Di conseguenza, a e b sono congrui modulo n . Per quanto abbiamo dimostrato prima, a non può essere anche congruo ad un altro numero

c compreso tra 0 e $n - 1$, perché altrimenti b e c sarebbero in relazione tra loro (per la proprietà transitiva). Quindi, dato un intero a , esiste ed è unico un b compreso tra 0 e $n - 1$ a cui è congruo.

A questo punto è possibile passare all'insieme quoziente della relazione sull'insieme \mathbb{Z} , ovvero creare un nuovo insieme (che possiamo denotare con \mathbb{Z}_n) i cui elementi saranno le classi di equivalenza della relazione \equiv_n . In base ai risultati precedenti, possiamo considerare questo insieme come costituito dalle classi degli elementi 0, 1, 2, ..., $n - 1$, ovvero

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n - 1]_n\} \quad (1.5)$$

dove i pedici possono essere omessi quando è chiaro senza possibilità d'equivoco di quale modulo stiamo parlando.

A volte è conveniente usare, anziché i valori -1, -2, e così via, al posto di $n - 1$, $n - 2$, eccetera. In questo senso, è possibile anche parlare di modulo:

$$|a| \bmod n = \begin{cases} a & \text{se } a \leq n/2 \\ n - a & \text{se } a > n/2 \end{cases} \quad (1.6)$$

1.2 Le operazioni

È naturale a questo punto chiedersi che rapporto abbia la relazione di congruenza con le usuali operazioni tra interi, ovvero l'addizione (e quindi la sottrazione) e la moltiplicazione (non la divisione, perché questa non può generalmente essere compiuta tra due interi).

La relazione di congruenza è *compatibile* con l'addizione e la moltiplicazione nel senso seguente: dati due numeri a e b , si ha che la classe di equivalenza cui appartiene la somma (rispettivamente il prodotto) non cambia se si variano i rappresentanti delle classi di equivalenza.

Infatti, siano a' e b' due interi rispettivamente nelle classi di equivalenza di a e di b , ovvero tali che

$$a' = a + kn \quad \text{e} \quad b' = b + kn \quad (1.7)$$

Si ha allora

$$a' + b' = a + kn + b + jn = (a + b) + (k + j)n \quad (1.8)$$

ovvero $a' + b'$ è nella stessa classe di $a + b$.

Lo stesso può essere fatto con la sottrazione e la moltiplicazione, così come con l'elevamento a potenza: questo significa che è possibile indicare le classi di equivalenza come semplici numeri (alleggerendo la notazione), senza incorrere in errori pratici.

Queste operazioni conservano tutte le proprietà che avevano tra gli interi: in particolare l'addizione e la moltiplicazione sono commutative e associative, e la moltiplicazione è distributiva rispetto all'addizione. L'elemento neutro dell'addizione è la classe 0 (ovvero la classe dei multipli di n), mentre quello della moltiplicazione è la classe 1. Queste proprietà fanno sì che l'insieme \mathbb{Z}_n sia un *anello commutativo unitario* rispetto a queste operazioni.

Un'altra proprietà invece *non* si conserva passando a questo nuovo insieme: non vale la *legge di annullamento del prodotto*, ovvero non sempre il prodotto di due elementi non nulli è ancora diverso da 0. Ad esempio, se $n = 8$, 2 e 4 sono chiaramente diversi da 0, ma

$$2 \cdot 4 \equiv 8 \pmod{8} \equiv 0 \pmod{8} \quad (1.9)$$

È facile dimostrare che questo può avvenire se e solo se n non è un numero primo: se infatti $n = ab$, allora il prodotto di a e b è congruo a 0, ma entrambi i fattori non sono nulli. Se invece n è primo, e $ab \equiv 0 \pmod{n}$, allora $n|ab$. Per il lemma di Euclide, allora, n deve dividere o a o b , ovvero almeno uno dei due deve essere congruo a 0 modulo n . Detto in altri termini, poiché in \mathbb{Z} ogni numero ha una sola fattorizzazione, n deve essere presente o nella fattorizzazione di a o in quella di b , perché altrimenti non potrebbe essere presente nella fattorizzazione di ab .

1.3 La divisione

Eseguire la divisione tra a e b significa trovare un k tale che $a = kb$, oppure moltiplicare a per l'inverso di b , ovvero quel numero che moltiplicato per b dà l'elemento neutro della moltiplicazione. In \mathbb{Z}_n tale elemento è 1: trovare l'inverso x di un elemento a equivale dunque a risolvere la congruenza

$$ax \equiv 1 \pmod{n} \quad (1.10)$$

ovvero a trovare x e b tali che

$$ax = 1 + bn \quad \text{ovvero} \quad ax - bn = 1 \quad (1.11)$$

Attraverso l'algoritmo euclideo è possibile dimostrare che questa congruenza è risolvibile se e solo se il massimo comun divisore tra a e n è 1 (cioè se a e n sono *coprimi*). In tal caso, anche x sarà coprimo con n . Quindi a e x sono uno l'inverso dell'altro. x viene spesso denotato con a^{-1} .

Se indichiamo con \mathbb{Z}_n^* l'insieme degli elementi che possiedono un inverso (ovvero degli elementi *invertibili*) otteniamo che questi verificano senza sforzo gli assiomi di gruppo rispetto alla moltiplicazione: infatti essa è

- associativa: come in \mathbb{Z}_n ;
- possiede elemento neutro: 1 ha come inverso sé stesso, e quindi appartiene a \mathbb{Z}_n^* ;
- ogni elemento ha un inverso: ovvio per come abbiamo definito l'insieme.

In più la moltiplicazione è commutativa, e quindi l'insieme \mathbb{Z}_n^* è un gruppo abeliano.

0, ovviamente, non ha mai un inverso; se invece n è un numero primo, ogni elemento non nullo possiede un inverso, e quindi è invertibile. Di conseguenza, per n primo, l'insieme \mathbb{Z}_n^* coincide con $\mathbb{Z}_n \setminus \{0\}$ (cioè la divisione ha sempre senso, eccetto quella per 0). Poiché \mathbb{Z}_n era già un anello commutativo, in questo caso abbiamo una struttura molto più potente, e cioè quella di *campo*. Non solo: è possibile dimostrare, con strumenti molto

più sofisticati, che ogni campo con un numero finito di elementi è o un \mathbb{Z}_n , per n primo, o una sua estensione. Se invece n non è primo, in generale l'insieme degli invertibili sarà decisamente più piccolo di \mathbb{Z}_n .

La cardinalità dell'insieme \mathbb{Z}_n^* è generalmente denotata con $\phi(n)$: tale funzione è detta *funzione phi* o *funzione di Eulero*.

La moltiplicazione tra a e b^{-1} può anche essere denotata come frazione, cioè

$$ab^{-1} = \frac{a}{b} \tag{1.12}$$

Con questa notazione, possiamo dire che le frazioni hanno senso in aritmetica modulare, purché b sia coprimo con n .

2 Prime proprietà e applicazioni

In questo modulo saranno presentati i primi usi delle congruenze, e verrà dimostrato il teorema di Fermat e la sua generalizzazione.

2.1 Criteri di divisibilità

Attraverso l'uso delle congruenze è semplice dimostrare i noti criteri di divisibilità per 3 e per 11. Essi sono:

- un numero è divisibile per 3 (o per 9) se lo è la somma delle sue cifre;
- un numero è divisibile per 11 se lo è la differenza tra le sue cifre di posto pari e le sue cifre di posto dispari.

Sia infatti n un qualsiasi numero. Scriverlo in base 10 significa scriverlo come

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10^1 + a_0 \quad (2.1)$$

Ora, $10 \equiv 1 \pmod{3}$, e quindi $10^k \equiv 1^k \pmod{3} \equiv 1 \pmod{3}$. La congruenza può essere riscritta come

$$n \equiv 1 \cdot a_k + 1 \cdot a_{k-1} + \dots + 1 \cdot a_1 + a_0 \pmod{3} \equiv a_k + a_{k-1} + \dots + a_1 + a_0 \pmod{3} \quad (2.2)$$

Poiché inoltre essere divisibile per 3 equivale ad essere congruo a 0 modulo 3, n è quindi multiplo di 3 se e solo se lo è la somma delle sue cifre; non solo, ma questa caratteristica è un po' più forte, perché n è esattamente congruo alla somma delle sue cifre.

La stessa dimostrazione si applica nel caso della divisibilità per 9; nel caso di 11, invece, bisogna considerare i due casi

$$10^k \equiv \begin{cases} 1 \pmod{11} & \text{per } k \text{ pari} \\ -1 \pmod{11} & \text{per } k \text{ dispari} \end{cases} \quad (2.3)$$

Di conseguenza

$$n \equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k \pmod{11} \quad (2.4)$$

Questi risultati possono essere generalizzati se il numero n è scritto in una base b qualunque. In particolare, per i d tali che $b \equiv 1 \pmod{d}$, n è divisibile per d se e solo se lo è la somma delle sue cifre quando è scritto in base b ; invece, se $b \equiv -1 \pmod{d}$ allora la divisibilità di n è equivalente a quella della differenza tra le somme delle cifre di posto dispari e di posto pari, quando n è scritto in base d . Le dimostrazioni si possono ottenere esattamente con i metodi descritti sopra.

2.2 Il teorema di Fermat

Il teorema di Fermat (spesso chiamato piccolo per distinguerlo dall'Ultimo teorema di Fermat) è un risultato fondamentale dell'aritmetica modulare. Afferma che, dato un numero primo p , per ogni a si ha

$$a^p \equiv a \pmod{p} \quad (2.5)$$

oppure, equivalentemente, che se a non è divisibile per p allora

$$a^{p-1} \equiv 1 \pmod{p} \quad (2.6)$$

L'equivalenza tra le due formulazioni è ovvia, perché l'unico caso in cui la seconda forma non si applica è quando $p|a$, cioè quando $a \equiv 0 \pmod{p}$, che verifica banalmente la prima uguaglianza.

Esistono diverse dimostrazioni del teorema; la prima non fa uso di proprietà dell'aritmetica modulare, ma procede per induzione su a , dimostrando la prima delle due forme:

- se $a = 0$ il teorema è ovvio;
- sia vero il teorema per ogni numero naturale fino ad a . Allora per il teorema del binomio

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a^1 + 1 \quad (2.7)$$

Ogni coefficiente binomiale $\binom{p}{k}$ è divisibile per p : infatti

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad (2.8)$$

e il denominatore non può essere diviso da p , perché è un numero primo, mentre p divide il numeratore. Quindi, passando al modulo p , abbiamo

$$(a+1)^p \equiv a + 0 + 0 + \dots + 1 \pmod{p} \equiv a + 1 \pmod{p} \quad (2.9)$$

stabilendo il risultato per ogni a .

Un'argomentazione molto più trasparente e con molte più potenzialità è quella data da Eulero. Fissiamo a , e consideriamo i numeri

$$1a, 2a, 3a, \dots, (p-1)a \quad (2.10)$$

Se due di essi fossero uguali, ad esempio ia e ja , allora si avrebbe

$$ia \equiv ja \pmod{p} \implies (i-j)a \equiv 0 \pmod{p} \quad (2.11)$$

e poiché a , non essendo divisibile per p , è coprimo con p , si deve avere $i = j$. Quindi i valori $1a, 2a, 3a, \dots, (p-1)a$ sono tutti diversi e non nulli, e quindi corrispondono in qualche ordine ai valori $1, 2, 3, \dots, p-1$. Moltiplicandoli tutti tra loro abbiamo

$$(1a)(2a)(3a) \dots [(p-1)a] \equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p} \quad (2.12)$$

ovvero

$$[1 \cdot 2 \cdot 3 \dots (p-1)]a^{p-1} \equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p} \quad (2.13)$$

A questo punto basta semplificare il prodotto $1 \cdot 2 \cdot 3 \dots (p-1)$ per ottenere il teorema.

2.3 Il teorema di Eulero

Una generalizzazione del piccolo teorema è data dal teorema di Eulero, che coinvolge la funzione di Eulero $\phi(n)$ che ricordiamo essere, per ogni n , il numero di interi coprimi con n . Il teorema di Eulero afferma che

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad (2.14)$$

per ogni a coprimo con n . Questo si riduce al piccolo teorema notando che, se p è primo, $\phi(p) = p - 1$

La dimostrazione è essenzialmente quella del teorema di Fermat: detti $a_1, a_2, a_3, \dots, a_{\phi(n)}$ gli interi coprimi con n , i numeri

$$aa_1, aa_2, aa_3, \dots, aa_{\phi(n)} \quad (2.15)$$

sono tutti diversi tra loro e tutti coprimi con n , e quindi sono uguali, in qualche ordine, a $a_1, a_2, a_3, \dots, a_{\phi(n)}$. Moltiplicandoli tutti tra loro si ottiene

$$(aa_1)(aa_2)(aa_3) \cdots (aa_{\phi(n)}) \equiv a_1 a_2 a_3 \cdots a_{\phi(n)} \pmod{n}$$
$$a^{\phi(n)} \equiv 1 \pmod{n} \quad (2.16)$$

Questo teorema è in realtà un caso particolare di una proposizione molto più generale, che riguarda ogni gruppo: se a è un elemento di un gruppo G di ordine n (ovvero con n elementi) allora $a^n = e$, dove e è l'elemento neutro del gruppo. (Ricordiamo che l'insieme degli elementi invertibili di \mathbb{Z}_n è un gruppo di ordine $\phi(n)$ rispetto alla moltiplicazione.) La dimostrazione di questo teorema più generale può essere ottenuta ricalcando la prova qui presentata.

2.4 Fattoriali

Un altro teorema importante e di facile dimostrazione è il teorema di Wilson, che riguarda il rapporto tra i fattoriali e i numeri primi. (Il fattoriale di n , indicato come $n!$, è il prodotto $1 \cdot 2 \cdot 3 \cdots n$.) Afferma che

$$(n-1)! \equiv -1 \pmod{n} \quad (2.17)$$

se e solo se n è primo.

Se n non è primo, allora tutti i fattori di n sono minori di n , e quindi sono fattori di $(n-1)!$, ovvero $(n-1)! \equiv 0 \pmod{n}$. Di conseguenza n non può verificare la proprietà precedente.

Sia ora n primo, $n > 2$ ($n = 2$ verifica banalmente il teorema), e consideriamo le coppie di inversi. Se le moltiplichiamo tutte tra loro abbiamo 1; poiché n è primo, inoltre, tutti gli elementi di \mathbb{Z}_n , eccetto lo 0, hanno un inverso. Moltiplicandoli tutti tra loro, possiamo

dunque raggruppare tutti gli elementi il cui inverso è diverso da sé stesso e semplificare le coppie. Gli elementi che coincidono con il proprio inverso devono verificare

$$x^2 \equiv 1 \pmod{n} \quad (2.18)$$

cioè

$$(x^2 - 1) = (x + 1)(x - 1) = kn \quad (2.19)$$

per qualche k . Questo equivale a dire che $x + 1$ o $x - 1$ dividono n , cioè x è congruo a 1 o $n - 1$ modulo n . Quindi

$$(n - 1)! \equiv 1 \cdot (n - 1) \pmod{n} \equiv -1 \pmod{n} \quad (2.20)$$

come volevasi dimostrare.

Usando il teorema di Wilson è facile dimostrare la seguente proprietà dei coefficienti binomiali:

$$\binom{p-1}{a} \equiv (-1)^a \pmod{p} \quad (2.21)$$

per ogni p primo. Infatti, osserviamo innanzitutto che, per definizione,

$$\binom{p-1}{a} = \frac{(p-1)!}{a!(p-1-a)!} \quad (2.22)$$

Inoltre

$$(p-1-a)! = \frac{(p-1)!}{(p-a)(p-a+1)\cdots(p-1)} \equiv \frac{-1}{(-a)(-a+1)\cdots(-2)(-1)} \pmod{n} \quad (2.23)$$

dove si è usata la frazione per denotare la divisione, ovvero la moltiplicazione per l'inverso, possibile in quanto nessuna delle quantità coinvolte è divisibile per p . Raccogliendo -1 da ogni fattore del prodotto $(-a)(-a+1)\cdots(-2)(-1)$ otteniamo

$$(p-1-a)! \equiv \frac{-1}{(-1)^a a!} \pmod{n} \quad (2.24)$$

e ritornando al coefficiente binomiale

$$\binom{p-1}{a} = \frac{(p-1)!}{a!(p-1-a)!} \equiv \frac{-1}{a! \frac{-1}{(-1)^a a!}} \pmod{n} \equiv (-1)^a \pmod{n} \quad (2.25)$$

3 Congruenze lineari

Questo modulo tratta delle cosiddette *congruenze lineari*, ovvero le congruenze che coinvolgono polinomi di primo grado. In particolare sarà dimostrato il cosiddetto teorema cinese del resto, che riguarda la risolubilità di un sistema di congruenze lineari.

3.1 Congruenze semplici

Abbiamo già incontrato la congruenza lineare $ax \equiv 1 \pmod{n}$, stabilendo che è risolubile se e solo se a è coprimo con n . Una congruenza più generale è

$$ax \equiv b \pmod{n} \quad (3.1)$$

che rappresenta la congruenza lineare base. Una caratteristica importante di questa congruenza è che può avere un qualunque numero di soluzioni, eccetto infinito; tuttavia, se esistono soluzioni, è sempre possibile ridursi ad un'unica soluzione variando opportunamente il modulo n .

Una condizione necessaria e sufficiente perché la congruenza sia risolubile è che b sia un multiplo del massimo comun divisore tra a e n . La dimostrazione segue immediatamente dalle proprietà dell'identità di Bézout: risolvere $ax \equiv b \pmod{n}$ equivale infatti a trovare x e y tali che

$$ax + ny = b \quad (3.2)$$

e questo è possibile se e solo se $\text{MCD}(a, n) | b$. Un altro modo di vedere la cosa, nel caso che a ed n siano coprimi, è osservare (in modo simile a quanto fatto nella dimostrazione del piccolo teorema di Fermat e del teorema di Eulero) che i numeri

$$1a, +2a, \dots, (n-1)a \quad (3.3)$$

sono tutti distinti (altrimenti si avrebbe $(i-j)a \equiv 0 \pmod{n}$, e poiché $\text{MCD}(a, n) = 1$, $i = j$) e diversi da 0. Quindi ogni elemento di \mathbb{Z}_n appare tra quei numeri, ed esattamente uno è uguale a b .

Supponiamo ora che la congruenza sia risolubile, sia $d = \text{MCD}(a, n)$, e poniamo $a = Ad$, $n = Nd$, $b = Bd$. Allora possiamo riscrivere $ax + ny = b$ come

$$Adx + Ndy = Bd \quad (3.4)$$

e semplificando d ,

$$Ax + Ny = B \quad (3.5)$$

Poiché abbiamo tolto tutti i fattori comuni tra a ed n , abbiamo che A ed N sono coprimi, inoltre, portandoci nelle congruenza modulo N , abbiamo

$$Ax \equiv B \pmod{N} \quad (3.6)$$

che ammette esattamente una soluzione, come dimostrato prima: sia \bar{x} . I valori

$$x_k = \bar{x} + kN \quad (3.7)$$

sono ancora soluzioni delle congruenza per ogni valore intero di k (in particolare, $x_0 = \bar{x}$). Per $k < d$, inoltre, questi valori sono minori di n , e quindi sono incongruenti modulo n . Questi sono tutti e soli i valori minori di n che, modulo N , sono congrui a \bar{x} . Se y , modulo n , è diverso da tutti gli x_i , allora non è una soluzione della congruenza perché non vi sono altre soluzioni modulo N : quindi la congruenza originale ammette esattamente d soluzioni modulo n .

3.2 Sistemi di congruenze lineari

Una volta risolte congruenze in un unico modulo, è possibile passare a risolvere *sistemi* di congruenze lineari: la situazione di partenza è un sistema del tipo

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \quad (3.8)$$

dove $MCD(n_i, n_j) = 1$ per ogni $i \neq j$.

Ci si può sempre ridurre a questo caso a partire da un sistema in cui ogni equazione è del tipo

$$a_i x \equiv b_i \pmod{n_i} \quad (3.9)$$

nel caso in cui in quest'ultima esistono soluzioni, risolvendo la congruenza lineare come nel paragrafo precedente, eventualmente modificando il modulo.

Poiché esistono $N = n_1 n_2 \cdots n_k$ diverse scelte di sequenze (a_1, a_2, \dots, a_k) , è naturale cercare le soluzioni del sistema nel modulo N : dimostreremo che, in questo modulo, la soluzione esiste ed è unica.

Definiamo infatti $N_i = \frac{\prod_{j=1}^k n_j}{n_i}$, ovvero il prodotto di tutti gli n_j eccetto n_i : questo è ovviamente divisibile per tutti gli n_j , eccetto n_i , con cui è coprimo perché è il prodotto di fattori coprimi con n_i . Di conseguenza ogni N_i ha un inverso modulo n_i ; sia N_i^* . Consideriamo il numero

$$\bar{x} = a_1 N_1^* + a_2 N_2^* + \cdots + a_k N_k^* \quad (3.10)$$

Modulo n_i (per ogni i), si cancellano tutti i termini meno $a_i N_i N_i^*$. Quindi

$$\bar{x} \equiv a_i N_i N_i^* \pmod{n_i} \equiv a_i \pmod{n_i} \quad (3.11)$$

perché il prodotto $N_i N_i^*$ è per definizione, congruo a 1 modulo n_i . Quindi il numero \bar{x} è una soluzione del sistema.

Abbiamo quindi N soluzioni diverse, una per ogni sequenza degli a . Consideriamo un'altra soluzione \bar{y} del sistema. La differenza $\bar{x} - \bar{y}$ è congrua a 0 per ogni n_i , cioè è divisibile per ogni n_i , e quindi è divisibile per il loro prodotto N . Quindi la soluzione è unica modulo N .

3.3 Isomorfismi

L'esistenza e l'unicità modulo N delle soluzioni dei sistemi di congruenze lineari permette di stabilire una corrispondenza biunivoca dal prodotto cartesiano $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ a \mathbb{Z}_N che, come si può vedere facilmente, rispetta le operazioni. In linguaggio algebrico, questo equivale a dire che c'è un *isomorfismo* tra il prodotto cartesiano e l'insieme \mathbb{Z}_N .

Questo può essere sfruttato per risolvere delle congruenze, ad esempio di un polinomio di grado elevato, da un modulo n qualsiasi a diversi moduli più piccoli. Ad esempio, volendo trovare le soluzioni di

$$x^5 - 6x^4 + 3x^3 - 5x + 4 \equiv 0 \pmod{15} \quad (3.12)$$

è possibile risolvere invece le due congruenze

$$2x^5 - 6x^4 + 3x^3 - 5x + 5 \equiv 0 \pmod{3} \implies 2x^5 - 2x + 2 \equiv 0 \pmod{3}$$

$$2x^5 - 6x^4 + 3x^3 - 5x + 5 \equiv 0 \pmod{5} \implies 2x^5 - x^4 + 3x^3 \equiv 0 \pmod{5} \quad (3.13)$$

Ora x^5 assume, per il piccolo teorema di Fermat, gli stessi valori di x ; quindi la congruenza modulo 3 è impossibile, e così è quella originaria.

Questo sistema è utile per trovare il numero di soluzioni di un'equazione a partire dal numero di soluzioni della stessa equazione in moduli più piccoli: se ad esempio

$$f(x) \equiv 0 \pmod{n} \quad (3.14)$$

è spezzata in

$$\begin{cases} f(x) \equiv 0 \pmod{n_1} \\ f(x) \equiv 0 \pmod{n_2} \\ \vdots \\ f(x) \equiv 0 \pmod{n_k} \end{cases} \quad (3.15)$$

dove i vari moduli sono a due a due coprimi, e $\rho(n_i)$ indica il numero di soluzioni della congruenza modulo n_i , allora $\rho(n) = \rho(n_1)\rho(n_2) \cdots \rho(n_k)$ perché ogni possibile gruppo di soluzioni nei diversi moduli genera una diversa soluzione modulo n .

3.4 Un'applicazione: la funzione di Eulero

A partire da queste considerazioni si può provare che la funzione di Eulero è *moltiplicativa*, cioè per ogni a e b coprimi si ha

$$\phi(ab) = \phi(a)\phi(b) \quad (3.16)$$

Il punto di partenza è la considerazione che un numero n è coprimo con un prodotto ab se e solo se è coprimo sia con a che con b . Infatti, se i fattori di n sono distinti da quelli di ab , saranno a maggior ragione diversi sia da quelli di a che da quelli di b , viceversa, se i fattori di n non compaiono né nella fattorizzazione di a né in quella di b , non potranno essere in quella di ab .

Consideriamo ora un $x \in \mathbb{Z}_{ab}$: per quanto abbiamo detto prima, lo possiamo identificare come una coppia $y \in \mathbb{Z}_a$, $z \in \mathbb{Z}_b$ (dove a e b sono tra loro coprimi), e si ha che

$$x \equiv y \pmod{a}, \quad x \equiv z \pmod{b} \quad (3.17)$$

Quindi, poiché ridurre modulo n non cambia l'essere coprimo con n , x è coprimo con ab se e solo se y è coprimo con a e z con b . Per quanto abbiamo dimostrato precedentemente, ogni coppia (y, z) di elementi coprimi (rispettivamente con a e b) corrisponde ad un unico x coprimo con ab e, viceversa, ogni x coprimo con ab corrispondente ad una coppia (y, z) . Ora questo tipo di coppie sono $\phi(a)\phi(b)$ (essendo $\phi(n)$ la quantità di numeri minori di n coprimi con n), mentre il numero di x coprimi con ab è $\phi(ab)$; poiché questi due numeri sono uguali,

$$\phi(ab) = \phi(a)\phi(b) \quad (3.18)$$

per ogni coppia di a e b coprimi.

A partire da questo è facile calcolare il valore di $\phi(n)$ per ogni n : infatti questo può essere scomposto nel prodotto

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad (3.19)$$

dove i p_k sono primi e diversi tra loro. A questo punto resta da calcolare solamente $\phi(p^a)$: ma questo è facile, perché gli unici numeri minori di p^a e non coprimi con esso sono i multipli di p , e questi sono in numero di p^{a-1} ; quindi $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.

A questo punto si ottiene

$$\phi(n) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1) \cdots p_k^{a_k-1}(p_k-1) \quad (3.20)$$

o, in forma più elegante,

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \quad (3.21)$$

3.5 Il lemma di Thue

Un'altra congruenza lineare interessante, questa volta nella due incognite x e y , è

$$ax \equiv y \pmod{p} \quad (3.22)$$

dove p è un numero primo.

È ovvio che questa congruenza ha p soluzioni, una per ogni scelta di x : il lemma di Thue afferma che esiste una coppia (x_0, y_0) che la verifica tale che $|x_0|, |y_0| < \sqrt{p}$ ed entrambi sono diversi da 0.

Consideriamo infatti i numeri $ax - y$ (modulo p) tali che

$$0 \leq x \leq [\sqrt{p}], \quad 0 \leq y \leq [\sqrt{p}] \quad (3.23)$$

dove $[a]$ indica la parte intera di a , ovvero il più piccolo intero non maggiore di a . Questi valori sono in numero di $([\sqrt{p}] + 1)^2 > (\sqrt{p} - 1 + 1)^2 = p$. Quindi esistono due coppie (x_1, y_1) e (x_2, y_2) tali che $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$; inoltre $x_1 \neq x_2$, perché altrimenti si avrebbe

$$\begin{cases} ax_1 - y_1 \equiv c \pmod{p} \\ ax_1 - y_2 \equiv c \pmod{p} \end{cases} \quad (3.24)$$

e quindi

$$y_1 \equiv ax_1 - c \pmod{p} \quad (3.25)$$

e

$$y_2 \equiv ax_1 - c \pmod{p} \quad (3.26)$$

ovvero $y_1 = y_2$ e le coppie non sarebbero distinte. Consideriamo l'espressione

$$a(x_1 - x_2) - (y_1 - y_2) = (ax_1 - y_1) - (ax_2 - y_2) \quad (3.27)$$

Questa è palesemente congrua a 0 modulo n . $x_1 - x_2$ è la differenza tra due quantità minori di $[\sqrt{p}]$, e quindi è essa stessa minore di $[\sqrt{p}]$. Allo stesso modo $y_1 - y_2 < \sqrt{p}$. Quindi ponendo

$$x_0 = x_1 - x_2, \quad y_0 = y_1 - y_2 \quad (3.28)$$

si ha la coppia desiderata.

Questo lemma può essere usato per dimostrare il teorema di Fermat sulle somme di due quadrati, che afferma che un primo p è rappresentabile come somma di due quadrati se e solo se $p \equiv 1 \pmod{4}$. La dimostrazione è presentata nell'ultimo modulo.

4 Polinomi in aritmetica modulare

Questo modulo tratta delle proprietà dei polinomi in aritmetica modulare. In particolare, verrà dimostrato il teorema di Waring sul numero di soluzioni di una congruenza polinomiale in più incognite.

4.1 Modulo primo contro modulo composto

Quando considerati in aritmetica modulare, i polinomi possono presentare proprietà inusuali e controintuitive. Lo stesso piccolo teorema di Fermat ne è un esempio: può essere infatti interpretato dicendo che, dato un primo p , i polinomi x^p e x (che sono, formalmente, distinti) assumono sempre lo stesso valore quando considerati modulo p . Questo non può avvenire quando sono considerati polinomi a coefficienti reali o razionali, ma permette invece di ridurre il grado di un polinomio, se questo è maggiore di p , senza cambiare i valori che questo assume e, di conseguenza, i valori per cui il polinomio si annulla.

Altri fenomeni riguardo il rapporto tra il numero di zeri di un polinomio e il suo grado: se infatti in ambienti usuali come i polinomi reali o razionali il numero di soluzioni non può superare il grado del polinomio, questo non sempre avviene in aritmetica modulare: un esempio semplice è $P(x) = x^2 - 1$ che, se considerato modulo 8, ha quattro soluzioni distinte, e cioè 1, 3, 5 e 7. Questo deriva dal fatto che \mathbb{Z}_8 non è un dominio d'integrità: infatti normalmente, fattorizzando $P(x)$ come $(x - 1)(x + 1)$, gli unici zeri del polinomio sarebbero in 1 e -1, cioè (in questo caso) in 1 e 7. Tuttavia, non è necessario che uno dei due fattori sia zero perché sia zero il prodotto: in questo caso, $P(3) = 2 \cdot 4 \equiv 0 \pmod{8}$.

Da quanto detto appare chiaro che, trasferendosi in \mathbb{Z}_p , dove p è un numero primo, si ottiene la stessa situazione dei razionali o dei reali. La dimostrazione è la stessa che in questi ultimi casi: dato $P(x)$ di grado n , se $P(a) = 0$, allora $(x - a)$ divide $P(x)$; se ora ci fossero $n + 1$ (o più) radici, il polinomio formato dal prodotto dei vari $(x - a)$ sarebbe di grado $n + 1$ e dovrebbe dividere $P(x)$, il che è impossibile. Quindi possono esistere al massimo n zeri.

Questo permette di dimostrare che, dati due polinomi $P(x)$ e $Q(x)$ di grado minore di p , se sono distinti, non possono avere lo stesso valore ovunque (modulo p): infatti il polinomio differenza $R(x) = P(x) - Q(x)$ avrebbe un grado compreso tra 0 e $p - 1$, ma p soluzioni, il che è impossibile.

Questa proprietà, unita alla scomposizione di una congruenza in altri moduli tra loro comprimibili rende particolarmente importante la soluzione di congruenze polinomiali quando il modulo è primo. Congruenze generiche in più incognite verranno trattate

successivamente in questo capitolo, mentre uno studio approfondito delle congruenze quadratiche in un'unica incognita è l'argomento dell'ultimo capitolo.

4.2 Il teorema di Chevalley

Supponiamo di avere un polinomio in n incognite $P(x_1, x_2, \dots, x_n)$ di grado g (cioè tale che g è il massimo grado tra quelli dei monomi, dopo che il grado di ogni incognita è già stato ridotto ad essere minore di p), tale che $n > g$, e supponiamo che $P(0, 0, \dots, 0) \equiv 0 \pmod{p}$, ovvero che non ci sia un termine noto. Il teorema di Chevalley afferma che esiste almeno un'altra soluzione della congruenza.

Per dimostrarlo, ragioniamo per assurdo, e supponiamo che esista un'unica soluzione. Costruiamo i due nuovi polinomi (dove X denota la n -upla (x_1, x_2, \dots, x_n))

$$f(X) = 1 - [P(X)]^{p-1}$$

$$g(X) = (1 - x_1^{p-1})(1 - x_2^{p-1}) \dots (1 - x_n^{p-1}) \quad (4.1)$$

Se X è la n -upla nulla, allora $f(X) = 1$, e così $g(X)$, perché tutti i fattori sono uguali a 1. Se invece almeno uno tra gli x_i è diverso da 0, allora $g(X) = 0$ perché il fattore $(1 - x_i^{p-1})$ è uguale a 0; d'altra parte, si ha anche $P(X) \equiv 1$, perché $P(x)$ è diverso da 0 (l'unica soluzione è quella nulla) e si può applicare il piccolo teorema di Fermat. Quindi i due polinomi assumono sempre lo stesso valore modulo p .

Consideriamo ora i loro gradi. $g(X)$ ha grado $n(p-1)$, perché esiste un monomio in cui tutte le incognite hanno grado $p-1$, e non possono quindi essere ridotte. Il grado di $f(X)$, d'altra parte, non può essere più di $g(p-1)$ (potrebbe essere strettamente minore, in quanto ci si può trovare a dover ridurre il grado di un'incognita per farlo diventare minore di p); quindi $f(X)$ ha grado strettamente minore di $g(X)$: poiché il grado in ogni incognita è minore di p , $f(X)$ e $g(X)$ non possono però assumere sempre lo stesso valore, perché i loro gradi sono diversi.

Abbiamo quindi una contraddizione, che è dovuta all'aver supposto che esiste un'unica soluzione. Di conseguenza, esiste almeno un'altra n -upla che risolve la congruenza.

4.3 Generalizzazioni

Il teorema di Chevalley può essere generalizzato.

Infatti, supponiamo che l'unica soluzione conosciuta non sia quella nulla $(0, 0, \dots, 0)$, ma una generica (a_1, a_2, \dots, a_n) , e che $P(x)$ abbia comunque grado minore del numero di incognite. In questo caso, per dimostrare che esiste un'altra soluzione, è sufficiente variare la definizione di $g(X)$:

$$g(X) = [1 - (x_1 - a_1)^{p-1}][1 - (x_2 - a_2)^{p-1}] \dots [1 - (x_n - a_n)^{p-1}] \quad (4.2)$$

La situazione è esattamente quella precedente: $g(X) = 1$ se e solo se $X = (a_1, a_2, \dots, a_n)$, mentre altrimenti è uguale a 0, così come $f(X)$. Inoltre il loro grado è rispettivamente

$n(p-1)$ e un numero minore o uguale di $g(p-1)$: quindi non possono essere uguali, e i due polinomi non possono coincidere, il che è assurdo perché hanno sempre lo stesso valore. Quindi esiste almeno un'altra soluzione.

Un teorema molto più forte è invece il teorema di Waring. Esso afferma che, nelle stesse condizioni di questa prima generalizzazione (grado minore del numero di incognite, esistenza di almeno una soluzione) il numero di soluzioni è divisibile per p . Supponiamo infatti che ci siano m soluzioni X_1, X_2, \dots, X_m , e costruiamo i polinomi

$$g(X_i) = [1 - (x_1 - a_1^i)^{p-1}][1 - (x_2 - a_2^i)^{p-1}] \dots [1 - (x_n - a_n^i)^{p-1}] \quad (4.3)$$

dove a_j^i indica la j -esima componente di X_i , e li sommiamo insieme, costruendo

$$g(X) = g(X_1) + g(X_2) + \dots + g(X_m) \quad (4.4)$$

Quando X è una delle soluzioni, $g(X)$ è uguale a 1, perché il corrispondente $g(X_i)$ è uguale a 1, mentre gli altri sono uguali a 0; se invece X non è una delle soluzioni, tutti gli addendi sono uguali a 0, e quindi anche $g(X)$.

Come prima, costruiamo anche

$$f(X) = 1 - [P(X)]^{p-1} \quad (4.5)$$

che ha grado minore o uguale di $g(p-1)$, e assume sempre lo stesso valore di $g(X)$. Ora in $g(X)$ vi sono m fattori del tipo $x_1^{p-1} x_2^{p-1} \dots x_n^{p-1}$ che sono di grado $n(p-1)$. Ma i due gradi devono essere uguali, quindi il monomio di grado $n(p-1)$ di $g(X)$ deve annullarsi, cioè si deve avere

$$m x_1^{p-1} x_2^{p-1} \dots x_n^{p-1} \equiv 0 \pmod{p} \quad (4.6)$$

per ogni scelta degli x_i . perché sia possibile, si deve avere $m \equiv 0 \pmod{p}$, cioè m deve essere divisibile per p . Ma siccome m era stato definito come il numero di soluzioni di $P(x)$, si ha che queste ultime sono in numero divisibile per p , come volevasi dimostrare.

5 Radici primitive

In questo modulo ci si concentrerà sul gruppo moltiplicativo dell'anello \mathbb{Z}_n .

5.1 Terminologia

Dal piccolo teorema di Fermat sappiamo che per ogni x ed n (con x ed n coprimi) si ha

$$x^{\phi(n)} \equiv 1 \pmod{n} \quad (5.1)$$

Può tuttavia esistere un numero $h < \phi(n)$ tale che

$$x^h \equiv 1 \pmod{n} \quad (5.2)$$

Se h è il minore intero possibile con questa caratteristica, si dice che h è l'**ordine** di x modulo n ; se in particolare $h = \phi(n)$, allora si dice che x è una **radice primitiva** modulo n . Ad esempio 5 ha la radice primitiva 2, perché

$$2^1 \equiv 2 \pmod{5}, \quad 2^2 \equiv 4 \pmod{5}, \quad 2^3 \equiv 3 \pmod{5}, \quad 2^4 \equiv 1 \pmod{5} \quad (5.3)$$

mentre 8 non ne ha una, in quanto

$$1^2 \equiv 1 \pmod{8}, \quad 3^2 \equiv 1 \pmod{8}, \quad 5^2 \equiv 1 \pmod{8}, \quad 7^2 \equiv 1 \pmod{8} \quad (5.4)$$

mentre $\phi(8) = 4$. Sorge quindi il problema di stabilire quali n possiedono una radice primitiva e quali no.

5.2 Prime proprietà dell'ordine

Da ora in poi supporremo sempre n fissato e x coprimo con n , e porremo $N = \phi(n)$.

Supponiamo che x abbia ordine h . Una prima proprietà, banale, è che h è un divisore di N . Supponiamo infatti che $\text{MCD}(h, N) = k < h$. Allora la congruenza

$$hy \equiv k \pmod{N} \quad (5.5)$$

è risolubile per un $y > 1$. Quindi

$$x^k \equiv x^{aN+hy} \pmod{n} \equiv (x^N)^a (x^h)^y \pmod{n} \equiv 1^a 1^y \pmod{n} \equiv 1 \pmod{n} \quad (5.6)$$

e quindi k dovrebbe essere l'ordine di x , essendo minore di h . Questo è assurdo, e h divide N .

Supponiamo ora che x e y abbiano ordine rispettivamente h e k , e che h e k siano coprimi. Allora xy ha ordine hk . È infatti ovvio, da quanto detto prima, che ne è un divisore, perché

$$(xy)^{hk} = (x^h)^k (y^k)^h \equiv 1^k 1^h \pmod{n} \equiv 1 \pmod{n} \quad (5.7)$$

Supponiamo ora che l'ordine di xy sia HK , dove H divide h e K divide k ; H e K sono coprimi, essendo i loro multipli. Supponiamo $h = Hj$; elevando xy alla HjK , si ha

$$(xy)^{HjK} = (x^h)^k y^{hK} \equiv y^{hK} \pmod{n} \quad (5.8)$$

e anche

$$(xy)^{HjK} = [(xy)^{HK}]^j \equiv 1 \pmod{n} \quad (5.9)$$

e quindi hK è un multiplo di k ; essendo h coprimo con k , si deve avere che K è un multiplo di k , e quindi, essendone anche un divisore, $k = K$. Allo stesso modo $h = H$, e l'ordine di xy è hk .

Consideriamo ora il caso dell'ordine di un numero x rispetto a due moduli coprimi n ed m . Sia h l'ordine di x rispetto ad n e k l'ordine di x rispetto a m . Allora l'ordine di x rispetto a nm è il minimo comune multiplo tra h e k . Infatti, dire che

$$x^l \equiv 1 \pmod{nm} \quad (5.10)$$

equivale a dire

$$\begin{cases} x^l \equiv 1 \pmod{n} \\ x^l \equiv 1 \pmod{m} \end{cases} \quad (5.11)$$

e questo è possibile solo se l è multiplo sia di h che di k , e in particolare vale per ogni multiplo comune di h e di k : quindi il loro multiplo comune più piccolo, cioè il loro m.c.m., è l'ordine di x rispetto a nm .

5.3 Numeri primi

Supponiamo ora che n è un numero primo, e denotiamolo quindi con p . Dimostreremo che per ogni p esiste una radice primitiva.

$\phi(p) = p - 1$, quindi gli ordini dei vari elementi sono divisori di $p - 1$. Possiamo fattorizzare quest'ultimo numero, ottenendo

$$p - 1 = q_1^{a_1} q_2^{a_2} \cdots q_s^{a_s} \quad (5.12)$$

Se riuscissimo a trovare un gruppo di elementi x_1, x_2, \dots, x_s tali che x_i ha ordine a_i per ogni i , allora il prodotto $x_1 x_2 x_3 \cdots x_s$ avrebbe, per le proprietà dimostrate precedentemente, ordine esattamente $p - 1$.

Un x_i di ordine precisamente a_i soddisfa la congruenza

$$x^{a_i} \equiv 1 \pmod{p} \quad (5.13)$$

ma non

$$x^{q^{a_i-1}} \equiv 1 \pmod{p} \quad (5.14)$$

Consideriamo il polinomio $P(x) = x^{p-1} - 1$: per il piccolo teorema, ha esattamente $p-1$ zeri distinti (cioè tutti gli elementi di \mathbb{Z}_p eccetto lo zero), e poniamo $q_i = q$, $a_i = a$. Si ha $p-1 = q^a w$ per un m ; ponendo $x^{q^a} = y$, risulta evidente che

$$x^{p-1} - 1 = y^w - 1 = (y-1)(y^{w-1} + y^{w-2} + \dots + y^1 + 1) \quad (5.15)$$

In x , i due polinomi a destra hanno grado rispettivamente q^a e $p-1-q^a$, e quindi, poiché p è primo, hanno al massimo rispettivamente q^a e $p-1-q^a$ soluzioni. Ma la somma del loro numero di soluzioni deve dare $p-1$, quindi ne hanno esattamente tante. Ma ora la congruenza

$$x^{q^{a-1}} \equiv 1 \pmod{p} \quad (5.16)$$

ha al massimo q^{a-1} soluzioni, che sono di meno di q^a ; quindi esattamente $q^a - q^{a-1}$ elementi di \mathbb{Z}_p hanno ordine q^a . Poiché questo avviene per ogni i , per quanto detto prima, esiste un elemento che ha ordine $q_1^{a_1} q_2^{a_2} \dots q_s^{a_s} = p-1$, cioè una radice primitiva.

5.4 Potenze dei numeri primi

Esaminiamo ora il caso delle potenze dei numeri primi, e consideriamo il caso $p=2$. Per $n=4$, 3 è una radice primitiva. L'esempio all'inizio del capitolo mostra invece che 8 non ha una radice primitiva, perché $a^2 \equiv 1 \pmod{8}$ per ogni a dispari; questo implica che per ogni altra potenza di due non può esserci una radice primitiva: infatti supponiamo che questo avvenga per un 2^k , e che a sia la radice primitiva, tale che a è congruo a b modulo 8 (questa congruenza su una congruenza ha senso, perché 2^k è, per ipotesi, multiplo di 8). Allora le potenze di a sono congrue, modulo 8, alternativamente a b e ad 1, mentre dovrebbero essere congrue anche alle altre due (se $b=3$, ad esempio, dovrebbero essere congrue anche a 5 e a 7); quindi una radice primitiva non può esistere.

Sia ora p un primo maggiore di 2, e a una sua radice primitiva. $\phi(p^2) = p(p-1)$; inoltre, l'ordine di a modulo p^2 è un multiplo di $p-1$, perché per avere

$$a^k \equiv 1 \pmod{p^2} \quad (5.17)$$

si deve avere

$$a^k \equiv 1 \pmod{p} \quad (5.18)$$

Gli unici multipli di $p-1$ che dividono $p(p-1)$ sono i due estremi, cioè gli stessi $p-1$ e $p(p-1)$: se è quest'ultimo, allora a è una radice primitiva modulo p^2 ; supponiamo invece che non lo sia, e consideriamo il numero (coprimo con p) $p-a$. Attraverso lo sviluppo del binomio di Newton si ha

$$(p-a)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^i a^i p^{p-1-i} \quad (5.19)$$

Modulo p^2 , gli unici elementi che restano sono quelli con $i = p - 2$ e $i = p - 1$:

$$\begin{aligned} (p - a)^{p-1} &\equiv \binom{p-1}{p-2} (-1)^{p-2} a^{p-2} p + \binom{p-1}{p-1} (-1)^{p-1} a^{p-1} \pmod{p^2} \equiv \\ &\equiv (p-1)(-1)a^{-1}p + 1 \pmod{p^2} \equiv pa^{-1} + 1 \pmod{p^2} \end{aligned} \quad (5.20)$$

che è congruo a 1 modulo p^2 se e solo se

$$pa^{-1} \equiv 0 \pmod{p^2} \iff a^{-1} \equiv 0 \pmod{p} \quad (5.21)$$

che è impossibile perché a è coprimo con p , essendone una radice primitiva. Quindi o a o $p - a$ è una radice primitiva per p^2 , o, detto in altri termini, questa esiste sempre.

Dimostriamo ora che, se a è una radice primitiva per p^2 , allora è una radice primitiva anche per p^k per ogni $k > 2$. Procediamo per induzione: se $k = 2$ questo è vero per ipotesi (abbiamo dimostrato prima che a esiste) e inoltre a è una radice primitiva modulo p . Supponiamo che il teorema sia valido per ogni k fino a K escluso. In questo caso l'ordine di a può essere solamente $\phi(p^{K-1}) = p^{K-2}(p-1)$ oppure $\phi(p^K) = p^{K-1}(p-1)$. Inoltre abbiamo

$$a^{\phi(p^{K-2})} = 1 + lp^{K-2} \quad (5.22)$$

Elevando a alla $\phi(p^{K-1})$ si ha

$$\begin{aligned} a^{\phi(p^{K-1})} &= a^{p^{K-2}(p-1)} = (a^{p^{K-3}(p-1)})^p = (a^{\phi(p^{K-2})})^p = (1 + lp^{K-2})^p = \\ &= \binom{p}{0} p^0 + \binom{p}{1} lp^{K-2} + \binom{p}{2} l^2 p^{2(K-2)} + \dots \end{aligned} \quad (5.23)$$

e calcolando modulo p^K

$$a^{\phi(p^{K-1})} \equiv 1 + lpp^{K-2} \pmod{p^K} \equiv 1 + lp^{K-1} \pmod{p^K} \quad (5.24)$$

Se ora l non è divisibile per p , abbiamo dimostrato che a è una radice primitiva modulo p^K ; se invece a è divisibile per p si ha

$$a^{\phi(p^{K-2})} = 1 + l_1 pp^{K-2} \equiv 1 \pmod{p^{K-1}} \quad (5.25)$$

e quindi a ha ordine $\phi(p^{K-2})$ modulo p^{K-1} , contro l'ipotesi che a sia una radice primitiva, questo è assurdo, e quindi a è una radice primitiva modulo p^K . Per induzione, segue che a è una radice primitiva per ogni p^k , $k > 2$.

5.5 Numeri divisibili da più di un primo

Consideriamo ora un numero n che non è potenza di un numero primo, fattorizzandolo come $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. La funzione di Eulero è moltiplicativa, quindi l'ordine necessario per essere una radice primitiva è $\phi(p_1^{a_1}) \phi(p_2^{a_2}) \cdots \phi(p_k^{a_k})$; se x non è una radice primitiva modulo p^a (qualunque p), a maggior ragione non lo potrà essere modulo n , perché vi

sono degli elementi modulo p^a che non genera (sia b uno di questi): se x^k non è mai congruo a b modulo p^a , non lo potrà mai essere modulo n , e quindi x non è una radice primitiva.

Consideriamo ora un x che è una radice primitiva modulo $p_i^{a_i}$ per ogni i . Questa esiste, perché di ognuna esistono le radici primitive x_1, x_2, \dots, x_s , e a questa s -upla è possibile assegnare un elemento di \mathbb{Z}_n (vedi il capitolo sulle [[Aritmetica modulare/Congruenze lineari|congruenze lineari]]). Affinché il suo ordine modulo n sia il prodotto degli ordini, questi devono essere tutti coprimi tra loro. Tuttavia, se p è un primo dispari, $\phi(p) = p-1$ è pari, e così la funzione di Eulero delle sue potenze. Anche $\phi(2^k)$, per $k > 1$, è pari: quindi, per avere una radice primitiva, n può contenere nella sua fattorizzazione al massimo un primo dispari (eventualmente elevato a qualche potenza) e 2.

Ricapitolando, gli unici n che hanno una radice primitiva sono:

- 2 e 4;
- p^k per p primo dispari e k qualsiasi;
- $2p^k$ per p primo dispari e k qualsiasi.

5.6 Indici

Consideriamo ora una radice primitiva g per un numero primo p : per definizione, i numeri

$$g, g^2, g^3, \dots, g^{p-1} \tag{5.26}$$

corrispondono, in qualche ordine, ai numeri $1, 2, \dots, p-1$. Se $x = g^k$, k è dello **indice** di x rispetto alla radice primitiva g .

Sia ora $x = g^a$. Le potenze di x saranno i numeri

$$g^a, g^{2a}, g^{3a}, \dots, g^{(p-1)a} \tag{5.27}$$

dove gli esponenti possono essere ridotti modulo $p-1$. Fissato un altro numero y , la congruenza

$$x^k \equiv y \pmod{p} \tag{5.28}$$

(dove l'incognita è k) è equivalente a

$$g^{ak} \equiv g^b \pmod{p} \tag{5.29}$$

ovvero, poiché possiamo ridurre modulo $p-1$ gli esponenti,

$$ak \equiv b \pmod{p-1} \tag{5.30}$$

che è risolubile, come sappiamo, se e solo se l'MCD($a, p-1$) divide b . In particolare, se a è coprimo con $p-1$, allora è risolubile per ogni b , e viceversa. In questo caso, le potenze di x corrispondono a tutte le potenze di g , ovvero a tutto $\mathbb{Z}_p \setminus \{0\}$, e quindi x è un'altra radice primitiva per p . Quindi esistono esattamente $\phi(p-1)$ radici primitive.

Lo stesso ragionamento si può applicare agli altri numeri n per i quali esiste una radice primitiva: in questo caso esse sono in numero di $\phi(\phi(n))$.

6 Congruenze quadratiche

In questo modulo verranno studiate le congruenze quadratiche, ossia di secondo grado, e in particolare verrà dimostrata la legge di reciprocità quadratica.

6.1 Introduzione

Partiamo da un'equazione qualsiasi di secondo grado in un'incognita con un modulo primo (maggiore di 2), ovvero $ax^2 + bx + c \equiv 0 \pmod{p}$. Possiamo applicare ad essa gli stessi passaggi di un'equazione nei reali:

$$\begin{aligned} ax^2 + bx + c \equiv 0 \pmod{p} &\iff 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p} \\ 4a^2x^2 + 4abx + b^2 &\equiv b^2 - 4ac \pmod{p} \iff (4ax + b)^2 \equiv b^2 - 4ac \pmod{p} \end{aligned} \quad (6.1)$$

A questo punto abbiamo bisogno di risolvere due congruenze diverse:

$$\begin{aligned} y^2 &\equiv d \pmod{p} \\ ax + b &\equiv \bar{y} \pmod{p} \end{aligned} \quad (6.2)$$

dove \bar{y} è una soluzione della prima congruenza. Poiché quest'ultima è sempre risolubile (se a non è divisibile per p), per risolvere la congruenza originaria basta concentrarsi su quelle del tipo $y^2 \equiv d \pmod{p}$.

È evidente che questa non sempre è risolubile, in quanto $a^2 \equiv (-a)^2 \pmod{p}$ per ogni a ; quindi per almeno metà dei d non abbiamo soluzioni. Tuttavia, poiché l'equazione $y^2 - d \equiv 0 \pmod{p}$ non può avere più di due soluzioni, e visto che una soluzione a ne chiama un'altra $-a$, esattamente metà dei d hanno delle soluzioni. Chiameremo quelli la cui congruenza è risolubile **residui quadratici**.

C'è un altro modo, più generale, per vedere le cose. Consideriamo un generatore g modulo p . L'insieme dei numeri

$$1^2, 2^2, 3^2, \dots, (p-1)^2 \quad (6.3)$$

coincide, a parte l'ordine, con quello dei numeri

$$g^2, g^4, g^6, \dots, g^{2(p-1)} \quad (6.4)$$

Riducendo modulo $p-1$ gli esponenti, questi rimarranno pari (perché anche $p-1$ è pari); quindi i residui quadratici sono esattamente quegli elementi il cui indice è pari.

Questo metodo può essere esteso per individuare i *residui n -esimi*, cioè gli a per cui ha soluzioni una congruenza del tipo

$$x^n \equiv a \pmod{p} \quad (6.5)$$

Se n divide $p - 1$, allora i residui n -esimi sono esattamente gli elementi i cui indici sono divisibile per n ; viceversa, se n e $p - 1$ sono coprimi, tutti i numeri sono residui n -esimi. Nei casi intermedi è facile dimostrare che, se $k = 1 \text{ MCD}(n, p - 1)$, allora i residui n -esimi coincidono con i residui k -esimi.

6.2 Il simbolo di Legendre e il criterio di Eulero

Per indicare se un numero è residuo quadratico o meno, si può usare il cosiddetto *simbolo di Legendre*: questo è

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ residuo quadratico modulo } p \\ 0 & a \text{ divisibile per } p \\ -1 & a \text{ non residuo quadratico modulo } p \end{cases} \quad (6.6)$$

Attraverso l'uso degli indici è facile dimostrare che

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \quad (6.7)$$

cioè il simbolo di Legendre è una funzione *completamente moltiplicativa* nel suo primo argomento. Questo avviene perché, se a e b sono entrambi residui o non residui, sommando i loro indici si avrà un indice pari, ovvero moltiplicandoli si avrà un residuo quadratico; viceversa, se uno è un residuo e l'altro no, l'indice del loro prodotto sarà dispari, e ab non è un residuo.

Un test generale ma di non molta utilità pratica è il *criterio di Eulero*. Posto $P = \frac{p-1}{2}$, questo afferma che

$$a^P \pmod{p} = \left(\frac{a}{p}\right) \quad (6.8)$$

Anche questo è banale se considerato con gli indici: se a è un residuo, allora esiste k tale che $k^2 \equiv a \pmod{p}$; quindi

$$a^P \equiv k^{2P} \pmod{p} \equiv a^{p-1} \pmod{p} \equiv 1 \pmod{p} \quad (6.9)$$

Se viceversa a non è un residuo quadratico, allora $a \equiv g^n \pmod{p}$, dove g è una radice primitiva e n è dispari, e

$$a^P \equiv g^{nP} \pmod{p} \quad (6.10)$$

Poiché n è dispari, nP è congruo a P modulo $p - 1$, ovvero

$$a^P \equiv g^P \pmod{p} \equiv -1 \pmod{p} \quad (6.11)$$

perché l'ordine di g è esattamente $p - 1$.

Attraverso questo criterio si determina immediatamente la caratteristica quadratica di -1 modulo un qualsiasi primo p . Se infatti $p \equiv 1 \pmod{4}$, ovvero $p = 4k + 1$, allora $P = 2k$, e $\left(\frac{-1}{p}\right) = (-1)^{2k} = 1$. Se invece $p \equiv 3 \pmod{4}$, cioè $p = 4k + 3$, $P = 2k + 1$ e $\left(\frac{-1}{p}\right) = (-1)^{2k+1} = -1$. L'unico caso rimanente è $p = 2$, per cui $-1 = 1$ è (ovviamente) residuo quadratico.

6.3 Il lemma di Gauss

Avanzando nello studio dei residui quadratici, il prossimo passo è il lemma di Gauss. Sia p un primo e a un numero compreso tra 0 e p (esclusi). Consideriamo i numeri $1a, 2a, \dots, Pa$ e sottraiamo p finché non rimane un numero compreso tra $-\frac{1}{2}p$ e $\frac{1}{2}p$ (o, detto in un'altra maniera, prendiamo il valore assoluto modulo p di questi numeri). Sia k il numero di elementi negativi in questo insieme. Il lemma di Gauss afferma che $\left(\frac{a}{p}\right) = (-1)^k$.

La dimostrazione di questo lemma è simile, per certi versi, alla dimostrazione del piccolo teorema di Fermat. È infatti ovvio che, se $ia \equiv ja \pmod{p}$ allora $i \equiv j \pmod{p}$, e quindi i vari numeri considerati non sono tra loro congrui modulo p . Allo stesso modo, se $ia \equiv -ja \pmod{p}$ allora $i \equiv -j \pmod{p}$ e quindi i e j non possono essere entrambi minori o uguali di P . Da questo segue che i numeri $1a, 2a, \dots, Pa$ sono congrui, in qualche ordine, all'insieme $\pm 1, \pm 2, \dots, \pm P$ dove si prende o il più o il meno. Sia k il numero di segni meno. Allora, moltiplicandoli tutti insieme abbiamo $(1a)(2a) \cdots (Pa) \equiv (-1)^k 1 \cdot 2 \cdots P \pmod{p}$ e semplificando $a^P \equiv (-1)^k \pmod{p}$ come volevasi dimostrare.

Come conseguenza di questo lemma si può dimostrare un importante teorema: se p e q sono primi tali che $p \equiv q \pmod{4a}$ oppure $p \equiv -q \pmod{4a}$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) \quad (6.12)$$

Per il lemma di Gauss, infatti, il primo dei due simboli di Legendre dipende dal numero di interi dell'insieme $a, 2a, 3a, \dots, Pa$ che sono negli intervalli

$$\left(\frac{1}{2}p, p\right), \left(\frac{3}{2}p, 2p\right), \left(\frac{5}{2}p, 3p\right), \dots, \left(\left(b - \frac{1}{2}p\right), bp\right) \quad (6.13)$$

dove $b = \frac{1}{2}(a - 1)$ o $b = \frac{1}{2}a$, a seconda di quale dei due sia un intero. ($Pa = \frac{1}{2}a(p - 1) = \frac{1}{2}ap - \frac{1}{2}a \leq \frac{1}{2}ap$)

Questo può essere interpretato come il numero di multipli di a nei vari intervalli; ovvero, dividendo tutto per a , il numero di interi negli intervalli

$$\left(\frac{1}{2}\frac{p}{a}, \frac{p}{a}\right), \left(\frac{3}{2}\frac{p}{a}, 2\frac{p}{a}\right), \dots, \left(\left(b - \frac{1}{2}\frac{p}{a}\right), b\frac{p}{a}\right) \quad (6.14)$$

e ponendo $p = 4ak + r$,

$$\left(\frac{1}{2}\frac{4ak+r}{a}, \frac{4ak+r}{a}\right), \left(\frac{3}{2}\frac{4ak+r}{a}, 2\frac{4ak+r}{a}\right), \dots, \left(\left(b - \frac{1}{2}\frac{4ak+r}{a}\right), b\frac{4ak+r}{a}\right) \quad (6.15)$$

cioè

$$\left(2k + \frac{1}{2}\frac{r}{a}, 4k + \frac{r}{a}\right), \left(6k + \frac{3}{2}\frac{r}{a}, 8k + 2\frac{r}{a}\right), \dots, \left(\left(2kb + \frac{(2b-1)r}{a}\right), 4kb + \frac{br}{a}\right) \quad (6.16)$$

Poiché a noi interessa solamente la *parità* del numero degli interi, e nessuno degli estremi degli intervalli è un intero, possiamo eliminare i vari multipli di k ; quindi $\left(\frac{a}{p}\right)$ dipende soltanto da r . Ma questo vuol dire che per ogni q congruo a r (cioè a p) modulo $4a$ la caratteristica quadratica è la stessa. Questo dimostra la prima parte del teorema. Se invece $q \equiv -p \equiv 4a - r \pmod{4a}$, allora, sostituendo r con $4a - r$ negli intervalli, si ha

$$\begin{aligned} &\left(2k + \frac{1}{2}\frac{4a-r}{a}, 4k + \frac{4a-r}{a}\right), \left(6k + \frac{3}{2}\frac{4a-r}{a}, 8k + 2\frac{4a-r}{a}\right), \\ &\dots, \left(\left(2kb + \frac{(2b-1)(4a-r)}{a}\right), 4kb + \frac{b(4a-r)}{a}\right) \end{aligned} \quad (6.17)$$

e quindi

$$\begin{aligned} &\left(2k + 2 - \frac{1}{2}\frac{r}{a}, 4k + 4 - \frac{r}{a}\right), \left(6k + 6 - \frac{3}{2}\frac{r}{a}, 8k + 8 - \frac{2r}{a}\right), \\ &\dots, \left(\left(2kb + 4(2b-1) - \frac{(2b-1)r}{a}\right), 4kb + 4b - \frac{b(4a-r)}{a}\right) \end{aligned} \quad (6.18)$$

che, come numero di interi, coincide col numero precedente.

6.3.1 Il caso $a = 2$

Consideriamo in particolare il caso $a=2$. Questo può essere trattato con lo stesso metodo visto precedentemente: sia $p = 8k + r$ un primo; i numeri $2, 4, 6, \dots, 2P$ sono tutti minori di p , e quindi per il lemma di Gauss la caratteristica quadratica di 2 corrisponde a $(-1)^n$, dove n è la parità del numero di quegli elementi maggiori di $p/2$. Sia x un numero minore di P .

$$\frac{1}{2}p < 2x < p \quad (6.19)$$

equivale a

$$2k + \frac{1}{4}r < x < 4k + \frac{1}{2}r \quad (6.20)$$

e ignorando $2k$ e $4k$, che non variano la parità, si ottengono, come soluzioni di x in interi:

- 0 soluzioni se $r = 1$;
- 1 soluzione se $r=3$ o $r=5$;

- 2 soluzioni se $r = 7$

e quindi 2 è residuo quadratico se $p = 8k \pm 1$ e non lo è altrimenti.

Naturalmente si poteva anche applicare il teorema generale dimostrato precedentemente, trovando un primo congruo a 1 modulo 8 e uno congruo a 3, e dedurne il comportamento per ogni p .

6.4 La legge di reciprocità

La legge di reciprocità quadratica, infine, afferma che

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad (6.21)$$

o, detto a parole, che la caratteristica quadratica di p modulo q e di q modulo p è la stessa a meno che non siano entrambi congrui a 3 modulo 4.

Supponiamo innanzitutto che $p \equiv q \pmod{4}$, ovvero che $p - q = 4a$ (possiamo supporre $p > q$) per un qualche intero a . Allora

$$\left(\frac{p}{q}\right) = \left(\frac{4a + q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) \quad (6.22)$$

e similmente

$$\left(\frac{q}{p}\right) = \left(\frac{p - 4a}{p}\right) = \left(\frac{-4a}{p}\right) \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right) \quad (6.23)$$

e quindi

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \left(\frac{a}{q}\right) \left(\frac{a}{p}\right) \left(\frac{-1}{p}\right) \quad (6.24)$$

Ora p e q hanno lo stesso resto nella divisione per $4a$ ($p = 4a + q$) e quindi due dei coefficienti di Legendre sono uguali, e quindi il loro prodotto è 1. Cioè

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) \quad (6.25)$$

che, per quanto abbiamo detto prima, è 1 se p è congruo a 1 modulo 4 e -1 altrimenti.

Se invece $p \equiv -q \pmod{4}$ si ha $p + q = 4a$, e

$$\left(\frac{p}{q}\right) = \left(\frac{4a - q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) \quad (6.26)$$

così come

$$\left(\frac{q}{p}\right) = \left(\frac{4a - p}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right) \quad (6.27)$$

Questi due risultati sono di nuovo uguali per il teorema precedente, in quanto p e q hanno resti opposti nella divisione per $4a$, e quindi sono uguali, e il loro prodotto è 1.

6.4.1 Esempi

Per mostrare la potenza di questo teorema, calcoliamo ad esempio

$$\left(\frac{637}{719}\right) \tag{6.28}$$

Fattorizzando 520, abbiamo

$$\left(\frac{637}{719}\right) = \left(\frac{7}{719}\right) \left(\frac{91}{719}\right) \tag{6.29}$$

719 è congruo a 3 modulo 4, così come 7 e 91; quindi

$$\left(\frac{7}{719}\right) = -\left(\frac{719}{7}\right) = -\left(\frac{5}{7}\right) = (-1)(-1) = 1$$

$$\left(\frac{91}{719}\right) = -\left(\frac{719}{91}\right) = -\left(\frac{82}{91}\right) = -\left(\frac{2}{91}\right) \left(\frac{41}{91}\right) = (-1) \left(\frac{2}{3}\right) \left(\frac{91}{41}\right) = (-1)(-1) \left(\frac{9}{41}\right) = 1 \tag{6.30}$$

(considerando che $91 \equiv 3 \pmod{8}$), e infine

$$\left(\frac{637}{719}\right) = 1 \cdot 1 = 1 \tag{6.31}$$

e 637 è un residuo quadratico modulo 719.

7 Alcune applicazioni

In questo capitolo vedremo tre applicazioni dell'aritmetica modulare alla teoria dei numeri.

7.1 Numeri primi

I numeri primi sono infiniti. La prima e più semplice dimostrazione è quella di Euclide: se fossero in numero finito (ad esempio p_1, p_2, \dots, p_n), allora il numero

$$p_1 p_2 p_3 \cdots p_n - 1 \tag{7.1}$$

non è uno dei primi, ma non è diviso da nessuno di essi, e quindi è primo, contro l'assunzione che tutti i primi siano contenuti nell'elenco precedente.

Questa dimostrazione ammette un'interpretazione in aritmetica modulare: se infatti i primi fossero soltanto quelli nella lista p_1, p_2, \dots, p_n , allora quando \mathbb{Z}_n (dove n è il prodotto di tutti i primi) viene scomposto attraverso il teorema cinese del resto, ogni suo elemento x sarebbe divisibile per qualche p_i , e quindi rappresentando x secondo i moduli p_1, p_2, \dots, p_n ci sarebbe sempre almeno uno zero. Ma questo è palesemente falso, in quanto basta scegliere la n -upla $(1, 1, \dots, -1)$ per ottenere un elemento che non verifica le ipotesi.

L'aritmetica modulare permette anche di spingersi oltre, e di dimostrare che esistono infiniti numeri primi congrui a 3 modulo 4. Supponiamo infatti tutti i primi di questo tipo p_1, p_2, \dots, p_n : allora $n = 4p_1 p_2 p_3 \cdots p_n - 1$ è ancora congruo a 3 modulo 4 e non è diviso da nessuno dei p_i . Ma se tutti i suoi fattori sono congrui a 1 modulo 4, allora anche n lo sarebbe, il che è impossibile. Quindi esistono infiniti numeri primi nella forma $4k + 3$. Una simile dimostrazione si applica ai primi congrui a 2 modulo 3 e congrui a 5 modulo 6.

Fin qui l'uso che è stato fatto dell'aritmetica modulare è puramente linguistico, cioè è semplicemente una conveniente notazione per spiegare le dimostrazioni. Per dimostrare che esistono infiniti primi congrui a 1 modulo 4 la situazione cambia, in quanto è necessario usare alcune nozioni della teoria dei residui quadratici.

Supponiamo, ancora una volta, che i primi di questo tipo siano finiti, e che siano p_1, p_2, \dots, p_n . Costruiamo il numero $n = 4(p_1 p_2 p_3 \cdots p_n)^2 + 1$: questo è ancora una volta congruo a 1 modulo 4, e non è divisibile per nessuno dei p_i . Questo ancora non dimostra il teorema (potrebbero esserci due fattori primi congrui a 3, che moltiplicati danno 1): supponiamo ora che q sia congruo a 3 modulo 4 e che divida n . Questo è nella forma $x^2 + 1$, e quindi dovrebbe essere risolubile la congruenza

$$x^2 + 1 \equiv 0 \pmod{q} \tag{7.2}$$

ovvero -1 dovrebbe essere un residuo quadratico modulo q , il che è impossibile perché $q \equiv 3 \pmod{4}$. Quindi n dovrebbe essere primo e congruo a 1 modulo 4, il che è assurdo. Quindi esistono infiniti primi nella forma $4k+1$.

In realtà questi sono corollari di un teorema molto più generale, che dice che in ogni progressione aritmetica $ak + b$, dove a e b sono coprimi, esistono infiniti numeri primi; tuttavia i metodi necessari sono molto più complessi di quelli qui applicati.

7.2 Teorema di Fermat sulle somme di due quadrati

Questo teorema afferma che un numero primo p può essere scritto come somma di due quadrati se e solo se $p = 2$ oppure p è congruo a 1 modulo 4.

Una delle implicazioni è facile da dimostrare: tutti i quadrati sono congrui a 0 o a 1 modulo 4, e quindi la somma di due di essi può essere congrua solamente a 0, 1 o 2.

Per l'altra implicazione una dimostrazione molto diretta si ottiene attraverso il lemma di Thue: sia a tale che $a^2 + 1 \equiv 0 \pmod{4}$. Per il lemma di Thue esiste una soluzione alla congruenza

$$ax \equiv y \pmod{p} \quad (7.3)$$

dove x e y sono minori in modulo di \sqrt{p} . Elevando al quadrato entrambi i lati si ha

$$a^2x^2 \equiv y^2 \pmod{p} \implies -x^2 \equiv y^2 \pmod{p} \implies x^2 + y^2 \equiv 0 \pmod{p} \implies x^2 + y^2 = kp \quad (7.4)$$

(dove k è intero). Ma poiché $|x|, |y| < \sqrt{p}$, si ha $x^2, y^2 < p$ e quindi

$$x^2 + y^2 < p + p = 2p \quad (7.5)$$

Di conseguenza si deve avere $k = 1$, cioè $x^2 + y^2 = p$.

7.3 Un problema additivo

Abbiamo visto che in \mathbb{Z}_p vi sono $\frac{p-1}{2}$ residui quadratici. È possibile chiedersi se ogni altro non residuo può essere scritto come somma di due residui. La risposta è positiva, e la dimostrazione è sorprendentemente semplice.

Naturalmente dobbiamo escludere 0 dal teorema, oppure considerarlo come la somma di zero residui quadratici, in quanto non sempre la congruenza $x^2 + y^2 \equiv 0 \pmod{p}$ ha soluzioni diverse da $(0,0)$.

Sia a un non residuo. Poiché ax non è congruo a ay se x non è congruo a y , gli elementi ax_1, ax_2, \dots, ax_k (dove gli x_i sono tutti i residui) sono tutti diversi e sono tutti non residui. Inoltre, se $a \equiv x^2 + y^2$, allora

$$az^2 \equiv (xz)^2 + (yz)^2 \quad (7.6)$$

e quindi se un non residuo è somma di due residui lo sono anche tutti gli altri.

A questo punto, basta osservare che esiste almeno un residuo x tale che $x+1$ non è un residuo, perché altrimenti tutti gli elementi sarebbero dei residui quadratici, e quindi tutti i non residui sono somma di due residui.

Argomenti del genere possono essere estesi anche a residui di ordine superiore, sebbene con considerazioni molto più lunghe: il maggior ostacolo è il fatto che, moltiplicando un a per i residui n -esimi, si ottengono soltanto $\frac{p-1}{n}$ altri elementi, e quindi non tutti sono ottenuti in questo modo; diventa quindi necessario introdurre una relazione di equivalenza che tenga conto di questo fatto, e dimostrare che gli elementi di ogni classe sono somma di un certo numero di residui n -esimi.

8 Esercizi

Di seguito sono presentati degli esercizi, divisi per capitoli. Le soluzioni sono in appendice.

Capitolo 1

1. Trovare:
 - a) $20 \pmod{3}$
 - b) $31 \pmod{4}$
 - c) $1895 \pmod{7}$
 - d) $43245 \pmod{13}$
2. Dire se i seguenti elementi sono invertibili:
 - a) 4 (modulo 8)
 - b) 10 (modulo 14)
 - c) 12 (modulo 31)
 - d) 15 (modulo 35)
 - e) 8 (modulo 9)
 - f) 438 (modulo 15)

Capitolo 2

1. Dimostrare che se $b \equiv 1 \pmod{d}$ allora n è divisibile per d se e solo se lo è la somma delle sue cifre, quando n è scritto in base b .
2. Calcolare usando il piccolo teorema di Fermat o il teorema di Eulero
 - a) $2^{75} \pmod{5}$
 - b) $5^{89} \pmod{7}$
 - c) $4^{90} \pmod{11}$
 - d) $16^{96} \pmod{13}$
 - e) $56681^{123432} \pmod{13}$
 - f) $14^{54} \pmod{10}$
 - g) $26^{32} \pmod{12}$
 - h) $7^{19} \pmod{15}$

i) $9^9 \pmod{6}$

Capitolo 3

1. Risolvere:

a) $2x \equiv 3 \pmod{5}$

b) $3x \equiv 7 \pmod{8}$

c) $6x \equiv 8 \pmod{9}$

d) $21x \equiv 7 \pmod{28}$

e) $8x \equiv 7 \pmod{9}$

f) $91x \equiv 991 \pmod{3}$

2. Risolvere:

a)

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 3 \pmod{5} \end{cases} \quad (8.1)$$

b)

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \end{cases} \quad (8.2)$$

3. Trovare tutte le soluzioni di $x^4 + 3x^2 + 7x + 3 \pmod{21}$.

4. Determinare tutti gli x tali che $\phi(x)$ è dispari.

Capitolo 4

1. Dimostrare, usando il solo teorema di Chevalley, che la congruenza

$$x^2 + y^2 \equiv -1 \pmod{p} \quad (8.3)$$

ha soluzione per ogni primo p .

2. Trovare tutte le soluzioni della congruenza $x^2 + 2y^2 - z^2 \equiv 0 \pmod{3}$

Capitolo 5

1. Trovare l'ordine moltiplicativo di
 - a) $6 \pmod{11}$
 - b) $14 \pmod{25}$
 - c) $13 \pmod{43}$
 - d) $2 \pmod{15}$
 - e) $3 \pmod{63}$
2. Sapendo che $2^9 \equiv 1 \pmod{73}$ e $10^8 \equiv 1 \pmod{73}$, trovare una radice primitiva modulo 73.
3. Trovare le radici primitive modulo 23.
4. Sapendo che 2 è una radice primitiva modulo 13, trovare una radice primitiva modulo 169.
5. Costruire una tavola di indici modulo 11 a partire dalla radice primitiva 2.

Capitolo 6

1. Dimostrare che se a è una radice primitiva modulo un primo p congruo a 1 modulo 4 allora anche $p - a$ è una radice primitiva modulo p .
2. Elencare i residui quadratici modulo 13
3. Calcolare:
 - a) $\left(\frac{-26}{73}\right)$
 - b) $\left(\frac{34}{97}\right)$
 - c) $\left(\frac{57}{113}\right)$

Capitolo 7

Dimostrare che in \mathbb{Z}_p ogni elemento è somma di al più due residui quadratici usando il teorema sull'esistenza di infiniti primi in ogni progressione aritmetica.

Bibliografia

Per la scrittura del libro sono stati usati i seguenti libri:

David M. Burton, *Elementary Number Theory*, McGraw-Hill, 2007, ISBN 9780073051888
per il lemma di Thue e il capitolo 5.

Harold Davenport, *Aritmetica superiore*. Zanichelli, Bologna, 1994. ISBN 8808091546
per i capitoli 2, 4, 5 (solo in parte), 6 e 7.

Giulia Maria Piacentini Cattaneo, *Algebra - un approccio algoritmico*. Decibel-Zanichelli,
Padova 1996, ISBN 9788808162700
per i capitoli 1 e 3, specialmente il teorema cinese del resto.

A Soluzioni degli esercizi

Capitolo 1

1. 2, 3, 5, 7
2. no, no, sì, no, sì, no

Capitolo 2

1. Chiaramente $b^x \equiv 1 \pmod{d}$ per ogni x naturale; scrivendo n in base b come

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b^1 + a_0 \quad (\text{A.1})$$

e riducendo modulo d si ha

$$n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \quad (\text{A.2})$$

e quindi n è divisibile da d se e solo se lo è la somma delle sue cifre in base b .

2. 3, 3, 5, 1, 1, 6, 1, 13, 3

Capitolo 3

1. 4, 5, insolubile, 3 mod 4, 2, 1
2. 43 mod 45, 59 mod 60
3. 6, 8, 15, 20
4. 1 e 2

Capitolo 4

1. Moltiplichiamo tutto per z^2 , ottenendo la congruenza $X^2 + Y^2 + z^2 \equiv 0 \pmod{p}$. Questa ha una soluzione in cui non tutte le incognite sono pari a zero, e quindi per simmetria una in cui z è diversa da 0. Sia (X_0, Y_0, z_0) questa soluzione. Allora

$$(X_0 z_0^{-1}, Y_0 z_0^{-1}) \quad (\text{A.3})$$

è una soluzione della congruenza originaria.

2. (0,0,0), (1,0,1), (1,0,2), (1,1,0), (1,2,0), (2,0,1), (2,0,2), (2,1,0), (2,2,0)

Capitolo 5

1. 10, 10, 21, 4, non esiste
2. L'ordine di $2 \cdot 10$ è $\text{mcm}(9, 2) = 72 = \phi(73)$, e quindi 20 è radice primitiva.
3. 5, 7, 10, 11, 14, 15, 17, 19, 20, 21
4. 2
5. 1- \rightarrow 0, 2- \rightarrow 1, 3- \rightarrow 8, 4- \rightarrow 2, 5- \rightarrow 4, 6- \rightarrow 9, 7- \rightarrow 7, 8- \rightarrow 3, 9- \rightarrow 6, 10- \rightarrow 5 (elemento- \rightarrow indice)

Capitolo 6

1. Le potenze di $-a$ sono le stesse di a , eccettuato il segno: quindi se $(-a)^k \equiv 1 \pmod{p}$ allora $a^k \equiv \pm 1 \pmod{p}$. k può essere uguale solo a $p-1$ o $\frac{p-1}{2}$: in quest'ultimo caso, tuttavia, essendo p è congruo a 1 modulo 4, $(p-1)/2$ è pari, e quindi si avrebbe anche $a^k \equiv 1 \pmod{p}$, impossibile perché a ha ordine $p-1$.
2. 1, 3, 4, 9, 10, 12
3. -1, -1, 1

Capitolo 7

Sia p un primo dispari, e $a \in \mathbb{Z}_p$. Uno tra $a, a+p, a+2p, a+3p$ è congruo a 1 modulo 4; sia b . La progressione aritmetica $b+4pk$ è congrua ad a modulo p ; in essa esistono infiniti numeri primi e quindi, in articolare, ne esiste uno: questo, essendo congruo a 1 modulo 4, è somma di due quadrati; sia $P = x^2 + y^2$. Ma allora questo vale anche riducendo modulo p ; di conseguenza a è somma di due residui quadratici.

B Cronologie

B.1 La relazione di congruenza

- (corr) (prec) 16:49, 7 set 2008 Dr Zimbu (discussione | contributi) m (8.761 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 19:47, 29 giu 2008 Ramac (discussione | contributi) m (8.723 bytes) (cambio avanzamento a 100%) (annulla singola modifica)
- (corr) (prec) 20:09, 23 giu 2008 Dr Zimbu (discussione | contributi) (8.663 bytes) (modulo) (annulla singola modifica)
- (corr) (prec) 17:08, 22 giu 2008 Dr Zimbu (discussione | contributi) (8.403 bytes) (?La divisione: frazioni) (annulla singola modifica)
- (corr) (prec) 17:31, 20 giu 2008 Dr Zimbu (discussione | contributi) (8.030 bytes) (Nuova pagina: Questo capitolo tratta le proprietà elementari delle congruenze: la definizione delle relazione di congruenza e del relativo insieme quoziente, più il suo rapporto con le operazioni....)

B.2 Prime proprietà e applicazioni

- (corr) (prec) 19:47, 29 giu 2008 Ramac (discussione | contributi) m (8.177 bytes) (cambio avanzamento a 100%) (annulla singola modifica)
- (corr) (prec) 15:37, 21 giu 2008 Dr Zimbu (discussione | contributi) (8.117 bytes) (fattoriali) (annulla singola modifica)
- (corr) (prec) 14:18, 21 giu 2008 Dr Zimbu (discussione | contributi) (5.891 bytes) (fermat+eulero) (annulla singola modifica)
- (corr) (prec) 13:02, 21 giu 2008 Dr Zimbu (discussione | contributi) (1.560 bytes) (Nuova pagina: In questo modulo saranno presentati i primi usi delle congruenze, e verrà dimostrato il teorema di Fermat e la sua generalizzazione. == Criteri di divisibilità == Attraverso l'uso ...)

B.3 Congruenze lineari

- (corr) (prec) 17:12, 5 set 2008 Dr Zimbu (discussione | contributi) m (11.854 bytes) (+link) (annulla singola modifica)
- (corr) (prec) 14:48, 30 giu 2008 Dr Zimbu (discussione | contributi) (11.759 bytes) (calcola funzione eulero) (annulla singola modifica)

- (corr) (prec) 19:48, 29 giu 2008 Ramac (discussione | contributi) m (10.932 bytes) (cambio avanzamento a 100%) (annulla singola modifica)
- (corr) (prec) 18:07, 26 giu 2008 Dr Zimbu (discussione | contributi) (10.872 bytes) (?Un'applicazione: la funzione di Eulero: precisazione) (annulla singola modifica)
- (corr) (prec) 18:05, 26 giu 2008 Dr Zimbu (discussione | contributi) (10.787 bytes) (applicazione alla funzione di eulero) (annulla singola modifica)
- (corr) (prec) 20:44, 23 giu 2008 Dr Zimbu (discussione | contributi) m (9.096 bytes) (?Il lemma di Thue: typo) (annulla singola modifica)
- (corr) (prec) 19:55, 23 giu 2008 Dr Zimbu (discussione | contributi) (9.050 bytes) (finito capitolo) (annulla singola modifica)
- (corr) (prec) 17:13, 23 giu 2008 Dr Zimbu (discussione | contributi) (7.305 bytes) (annulla singola modifica)
- (corr) (prec) 17:30, 22 giu 2008 Dr Zimbu (discussione | contributi) (2.838 bytes) (congruenze semplici)

B.4 Polinomi in aritmtica modulare

- (corr) (prec) 17:16, 12 set 2008 Dr Zimbu (discussione | contributi) m (7.905 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 19:48, 29 giu 2008 Ramac (discussione | contributi) m (7.904 bytes) (cambio avanzamento a 100%) (annulla singola modifica)
- (corr) (prec) 14:23, 25 giu 2008 Dr Zimbu (discussione | contributi) m (7.844 bytes) (fix) (annulla singola modifica)
- (corr) (prec) 14:21, 25 giu 2008 Dr Zimbu (discussione | contributi) (7.844 bytes) (annulla singola modifica)
- (corr) (prec) 18:31, 24 giu 2008 Dr Zimbu (discussione | contributi) m (5.057 bytes) (+cat) (annulla singola modifica)
- (corr) (prec) 18:30, 24 giu 2008 Dr Zimbu (discussione | contributi) (5.022 bytes) (Nuova pagina: Questo modulo tratta delle proprietà dei polinomi in aritmetica modulare. In particolare, verrà dimostrato il teorema di Waring sul numero di soluzioni di una congruenza polinomiale ...)

B.5 Radici primitive

- (corr) (prec) 17:33, 12 set 2008 Dr Zimbu (discussione | contributi) m (12.077 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 15:50, 2 lug 2008 Dr Zimbu (discussione | contributi) (12.071 bytes) (?Indici: correzione) (annulla singola modifica)
- (corr) (prec) 16:05, 1 lug 2008 Dr Zimbu (discussione | contributi) m (12.071 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 16:04, 1 lug 2008 Dr Zimbu (discussione | contributi) (12.071 bytes) (indici) (annulla singola modifica)

- (corr) (prec) 16:11, 30 giu 2008 Dr Zimbu (discussione | contributi) (10.685 bytes) (finito...) (annulla singola modifica)
- (corr) (prec) 19:48, 29 giu 2008 Ramac (discussione | contributi) m (4.512 bytes) (cambio avanzamento a 100%) (annulla singola modifica)
- (corr) (prec) 19:24, 29 giu 2008 Dr Zimbu (discussione | contributi) (4.452 bytes) (primi tre paragrafi)

B.6 Congruenze quadratiche

- (corr) (prec) 17:43, 12 set 2008 Dr Zimbu (discussione | contributi) m (12.319 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 17:09, 5 set 2008 Dr Zimbu (discussione | contributi) (12.316 bytes) (+caso a=2) (annulla singola modifica)
- (corr) (prec) 14:46, 15 lug 2008 Dr Zimbu (discussione | contributi) (11.315 bytes) (cambio avanzamento a 100%) (annulla singola modifica)
- (corr) (prec) 14:44, 15 lug 2008 Dr Zimbu (discussione | contributi) (11.279 bytes) (concludo) (annulla singola modifica)
- (corr) (prec) 20:58, 6 lug 2008 Dr Zimbu (discussione | contributi) (6.091 bytes) (+lemma di gauss) (annulla singola modifica)
- (corr) (prec) 19:54, 2 lug 2008 Diablo (discussione | contributi) m (4.652 bytes) (+cat) (annulla singola modifica)
- (corr) (prec) 16:34, 2 lug 2008 Dr Zimbu (discussione | contributi) (4.594 bytes) (prime due sezioni)

B.7 Alcune applicazioni

- (corr) (prec) 17:51, 12 set 2008 Dr Zimbu (discussione | contributi) m (6.041 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 20:28, 6 set 2008 Dr Zimbu (discussione | contributi) (6.040 bytes) (terzo paragrafo) (annulla singola modifica)
- (corr) (prec) 17:42, 5 set 2008 Dr Zimbu (discussione | contributi) (4.353 bytes) (primi due paragrafi)

B.8 Bibliografia

- (corr) (prec) 17:58, 12 set 2008 Dr Zimbu (discussione | contributi) m (629 bytes) (typo) (annulla singola modifica)
- (corr) (prec) 20:15, 6 set 2008 Dr Zimbu (discussione | contributi) (631 bytes) (Nuova pagina: $\{\{Aritmetica\ modular\}\}$) Per la scrittura del libro sono stati usati i seguenti libri: **David M. Burton, "Elementary Number Theory", McGraw-Hill, 2007, ISBN 9780073051888** **per il le...**

B.9 Esercizi

- (corr) (prec) 14:57, 12 set 2008 Dr Zimbu (discussione | contributi) (5.465 bytes) (finisco esercizi) (annulla singola modifica)
- (corr) (prec) 11:25, 8 set 2008 Dr Zimbu (discussione | contributi) (2.995 bytes) (+cap.3 e 4) (annulla singola modifica)
- (corr) (prec) 17:23, 7 set 2008 Dr Zimbu (discussione | contributi) (1.441 bytes) (cap.2) (annulla singola modifica)
- (corr) (prec) 16:56, 7 set 2008 Dr Zimbu (discussione | contributi) (406 bytes) (cap.1)

C GNU Free Documentation License

Version 1.2, November 2002

Copyright © 2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “**Document**”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “**you**”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “**Modified Version**” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “**Secondary Section**” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “**Invariant Sections**” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as

Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “**Cover Texts**” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “**Transparent**” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “**Opaque**”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “**Title Page**” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section “**Entitled XYZ**” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “**Acknowledgements**”, “**Dedications**”, “**Endorsements**”, or “**History**”.) To “**Preserve the Title**” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify

you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled “Acknowledgements” or “Dedications”, Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled “Endorsements”. Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled “Endorsements” or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version’s license notice. These titles must be distinct from any other section titles.

You may add a section Entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.