Indice

Voci

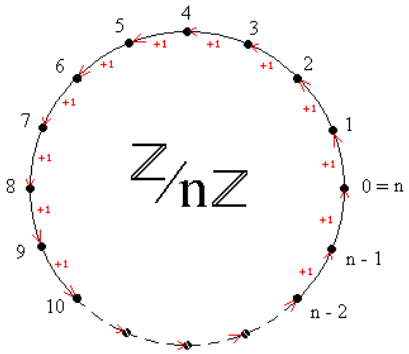
Note

Licenze della voce

Benvenuto nel wikibook:

Aritmetica modulare

Autore: Dr Zimbu



Vai ai contenuti >>

Fase di sviluppo:Aritmetica modulare

Aritmetica modulare

Questo libro intende trattare alcuni aspetti basilari dell'**aritmetica modulare**: dalla definizione di congruenza ai teoremi di Fermat e Wilson, fino alla legge di reciprocità quadratica.

Finalità

Non sono necessari particolari prerequisiti, a parte alcune conoscenze basilari di algebra, tra cui la nozione di divisibilità e di relazione di equivalenza.

Libri correlati

- Algebra
- Matematica per le superiori

Altri progetti

- **Wikipedia** contiene una voce riguardante la **aritmetica modulare**

Aritmetica modulare

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.

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:

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

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

$$a \equiv b \mod n$$

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

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

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 *b* - *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

$$a = qn + b$$

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

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

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

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

$$|a| \mod n = \begin{cases} a & \text{se } a \leq n/2 \\ n-a & \text{se } a > n/2 \end{cases}$$

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

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

Si ha allora

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

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

$$2 \cdot 4 \equiv 8 \mod 8 \equiv 0 \mod 8$$

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 $ab \equiv 0 \mod n$, 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*.

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

$$ax \equiv 1 \mod n$$

ovvero a trovare *x* e *b* tali che

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

Attraverso l'algoritmo euclideo è possibile dimostrare che questa congruenza è risolubile 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

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

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

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.

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

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10^1 + a_0$$

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

$$n \equiv 1 \cdot a_k + 1 \cdot a_{k-1} + \cdots + 1 \cdot a_1 + \cdot a_0 \mod 3 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \mod 3$$

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

$$10^k \equiv \begin{cases} 1 \mod 11 & \text{per k pari} \\ -1 \mod 11 & \text{per k dispari} \end{cases}$$

Di conseguenza

$$n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \mod 11$$

Questi risultati possono essere generalizzati se il numero *n* è scritto in una base *b* qualunque. In particolare, per i *d* tali che $b \equiv 1 \mod d$, *n* è divisibile per *d* se e solo se lo è la somma delle sue cifre quando è scritto in base *b*; invece, se $b \equiv -1 \mod d$ 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.

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

$$a^p \equiv a \mod p$$

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

$$a^{p-1} \equiv 1 \mod p$$

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 $a \equiv 0 \mod p$, 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

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a^1 + 1$$

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

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

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

$$(a+1)^p \equiv a + 0 + 0 + \cdots + 1 \mod p \equiv a + 1 \mod p$$

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

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

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

$$ia \equiv ja \mod p \Longrightarrow (i-j)a \equiv 0 \mod p$$

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

$$(1a)(2a)(3a)\cdots[(p-1)a] \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$$

ovvero $[1 \cdot 2 \cdot 3 \cdots (p-1)]a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$ A questo punto basta semplificare il prodotto $1 \cdot 2 \cdot 3 \cdots (p-1)$ per ottenere il teorema.

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

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

per ogni *a* coprimo con *n*. Questo si riduce al piccolo teorema notando che, se *p* è primo, $\phi(n) = n - 1$
La dimostrazione è essenzialmente quella del teorema di Fermat: detti $a_1, a_2, a_3, \cdots a_{\phi(n)}$ gli interi coprimi con *n*, i numeri

$$aa_1, aa_2, aa_3, \cdots aa_{\phi(n)}$$

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

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

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.

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

$$(n-1)! \equiv -1 \mod n$$

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 $(n-1)! \equiv 0 \mod n$. 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

$$x^2 \equiv 1 \mod n$$

cioè

$$(x^2 - 1) = (x+1)(x-1) = kn$$

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

$$(n-1)! \equiv 1 \cdot (n-1) \mod n \equiv -1 \mod n$$

come volevasi dimostrare.

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

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

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

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

Inoltre

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

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 $(p-1-a)! \equiv \frac{-1}{(-1)^a a!}$ e ritornando al coefficiente binomiale

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

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.

Congruenze semplici

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

$$ax \equiv b \mod n$$

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 $ax \equiv b \mod n$ equivale infatti a trovare *x* e *y* tali che

$$ax + ny = b$$

e questo è possibile se e solo se 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

$$1a, 2a, \ldots, (n-1)a$$

sono tutti distinti (altrimenti si avrebbe $(i-j)a \equiv 0 \mod n$, e poiché 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* =MCD(a,n), e poniamo a=Ad, n=Nd, b=Bd. Allora possiamo riscrivere $ax + ny = b$ come

$$Adx + Ndy = Bd$$

e semplificando *d*,

$$Ax + Ny = B$$

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

$$Ax \equiv B \mod N$$

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

$$x_k = \overline{x} + kN$$

sono ancora soluzioni delle congruenza per ogni valore intero di *k* (in particolare, $x_0 = \overline{x}$). 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 $\overline{x}$. 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*.

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

$$\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ \vdots \\ x \equiv a_k \mod n_k \end{cases}$$

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

$$a_i x \equiv b_i \mod n_i$$

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 $(a_1, a_2 \ldots, a_k)$, 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

$$\overline{x} = a_1 N_1 N_1^* + a_2 N_2 N_2^* + \cdots + a_k N_k N_k^*$$

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

$$\overline{x} \equiv a_i N_i N_i^* \mod n_i \equiv a_i \mod n_i$$

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

Abbiamo quindi *N* soluzioni diverse, una per ogni sequenza degli *a*. Consideriamo un'altra soluzione $\overline{y}$ del sistema. La differenza $\overline{x} - \overline{y}$ 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*.

Isomorfismi

Modulo 45 visto come modulo 9 per modulo 5

		mod 5				
		0	**1**	**2**	**3**	**4**
mod 9	**0**	0	36	27	18	9
	1	10	1	37	28	19
	2	20	11	2	38	29
	3	30	21	12	3	39
	4	40	31	22	13	4
	5	5	41	32	23	14
	6	15	6	42	33	24
	7	25	16	7	43	34
	8	35	26	17	8	44

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

$$2x^5 - 6x^4 + 3x^3 - 5x + 5 \equiv 0 \mod 15$$

è possibile risolvere invece le due congruenze

$$2x^5 - 6x^4 + 3x^3 - 5x + 5 \equiv 0 \mod 3 \Longrightarrow 2x^5 - 2x + 2 \equiv 0 \mod 3$$
$$2x^5 - 6x^4 + 3x^3 - 5x + 5 \equiv 0 \mod 5 \Longrightarrow 2x^5 - x^4 + 3x^3 \equiv 0 \mod 5$$

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

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

è spezzata in

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

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*.

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

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

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

$$x \equiv y \mod a, \qquad x \equiv z \mod b$$

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,

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

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

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

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

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

o, in forma più elegante,

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

Il lemma di Thue

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

$$ax \equiv y \mod p$$

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

$$0 \le x \le [\sqrt{p}], \quad 0 \le y \le [\sqrt{p}]$$

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 $ax_1 - y_1 \equiv ax_2 - y_2 \mod n$; inoltre $x_1 \neq x_2$, perché altrimenti si avrebbe

$$\begin{cases} ax_1 - y_1 \equiv c \mod p \\ ax_1 - y_2 \equiv c \mod p \end{cases}$$

e quindi

$$y_1 \equiv ax_1 - c \mod p$$

e

$$y_2 \equiv ax_1 - c \mod p$$

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

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

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

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

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 $p \equiv 1 \mod 4$. La dimostrazione è presentata nell'ultimo modulo.

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.

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, $P(3) = 2 \cdot 4 \equiv 0 \mod 8$.

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 comprimi rende particolarmente importante la soluzione di congruenze polinomiali quando il modulo è primo. Congruenze generiche in più incognite verranno trattare successivamente in questo capitolo, mentre uno studio approfondito delle congruenze quadratiche in un'unica incognita è l'argomento dell'ultimo capitolo.

Il teorema di Chevalley

Supponiamo di avere un polinomio in *n* incognite $P(x_1, x_2, \ldots, x_n)$ 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 $P(0, 0, \ldots, 0) \equiv 0 \mod p$, 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 $(x_1, x_2, \ldots, x_n)$)

$$f(X) = 1 - [P(X)]^{p-1}$$
$$g(X) = (1 - x_1^{p-1})(1 - x_2^{p-1}) \ldots (1 - x_n^{p-1})$$

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.

Generalizzazioni

Il teorema di Chevalley può essere generalizzato.

Infatti, supponiamo che l'unica soluzione conosciuta non sia quella nulla (0,0,...,0), ma una generica $(a_1, a_2, \ldots, a_n)$, 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*):
$g(X) = [1 - (x_1 - a_1)^{p-1}][1 - (x_2 - a_2)^{p-1}] \ldots [1 - (x_n - a_n)^{p-1}]$
La situazione è esattamente quella precedente: *g*(*X*)=1 se e solo se $X = (a_1, a_2, \ldots, a_n)$, 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 $X_1, X_2, \ldots, X_m$, e costruiamo i polinomi

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

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

$$g(X) = g(X_1) + g(X_2) + \ldots + g(X_m)$$

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

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

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

$$mx_1^{p-1}x_2^{p-1}\dots x_n^{p-1} \equiv 0 \mod p$$

per ogni scelta degli x_i . perché sia possibile, si deve avere $m \equiv 0 \mod p$, 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 ultima sono in numero divisibile per *p*, come volevasi dimostrare.

Radici primitive

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

Terminologia

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

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

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

$$x^h \equiv 1 \mod n$$

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

$$2^1 \equiv 2 \mod 5,\quad 2^2 \equiv 4 \mod 5,\quad 2^3 \equiv 3 \mod 5,\quad 2^4 \equiv 1 \mod 5$$

mentre 8 non ne ha una, in quanto

$$1^2 \equiv 1 \mod 8,\quad 3^2 \equiv 1 \mod 8,\quad 5^2 \equiv 1 \mod 8,\quad 7^2 \equiv 1 \mod 8$$

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

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*. Suppooniamo infatti che MCD(*h*,*N*)= *k* < *h*. Allora la congruenza

$$hy \equiv k \mod N$$

è risolubile per un *y* >1. Quindi

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

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* abbiamo 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

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

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

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

e anche $(xy)^{HjK} = [(xy)^{HK}]^j \equiv 1 \mod n$

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

$$x^l \equiv 1 \mod nm$$

equivale a dire

$$\begin{cases} x^l \equiv 1 \mod n \\ x^l \equiv 1 \mod m \end{cases}$$

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*.

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

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

Se riuscissimo a trovare un gruppo di elementi $x_1, x_2, \ldots, x_s$ 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

$$x^{q^{a_i}} \equiv 1 \mod p$$

ma non

$$x^{q^{a_i - 1}} \equiv 1 \mod p$$

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

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

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

$$x^{q^{a-1}} \equiv 1 \mod p$$

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 $q_1^{a_1} q_2^{a_2} \cdots q_s^{a_s} = p - 1$, cioè una radice primitiva.

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 $a^2 \equiv 1 \mod 8$ 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

$$a^k \equiv 1 \mod p^2$$

si deve avere

$$a^k \equiv 1 \mod p$$

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

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

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

$$(p-a)^{p-1} \equiv \binom{p-1}{p-2}(-1)^{p-2}a^{p-2}p + \binom{p-1}{p-1}(-1)^{p-1}a^{p-1} \mod p^2 \equiv (p-1)(-1)a^{-1}p+1 \mod p^2 \equiv pa^{-1}+1 \mod p^2$$

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

$$pa^{-1} \equiv 0 \mod p^2 \iff a^{-1} \equiv 0 \mod p$$

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.

Dimostreremo 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

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

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

$$a^{\phi(p^{K-1})} = a^{p^{K-2}(p-1)} = (a^{p^{K-3}(p-1)})^p = (a^{\phi(p^{K-2})})^p = (1+lp^{K-2})^p = \binom{p}{0}p^0 + \binom{p}{1}lp^{K-2} + \binom{p}{2}l^2p^{2(K-2)} + \cdots$$

e calcolando modulo p^K

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

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

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

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.

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 $x_1, x_2, \ldots, x_s$, e a questa *s*-upla è possibile assegnare un elemento di $\mathbb{Z}_n$ (vedi il capitolo sulle 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 $\phi\left(2^k\right)$, 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.

Indici

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

$$g,\ g^2,\ g^3, \ldots, g^{p-1}$$

corrispondono, in qualche ordine, ai numeri 1,2,...,*p* -1. Se $x = g^k$, *k* è dello l'**indice** di *x* rispetto alla radice primitiva *g*.
Sia ora $x = g^a$. Le potenze di *x* saranno i numeri

$$g^a,\ g^{2a},\ g^{3a}, \ldots, g^{(p-1)a}$$

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

$$x^k \equiv y \mod p$$

(dove l'incognita è *k*) è equivalente a

$$g^{ak} \equiv g^b \mod p$$

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

$$ak \equiv b \mod (p-1)$$

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 $\phi(\phi(n))$.

Congruenze quadratiche

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

Introduzione

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

$$ax^2 + bx + c \equiv 0 \mod p \iff 4a^2x^2 + 4abx + 4ac \equiv 0 \mod p$$
$$4a^2x^2 + 4abx + b^2 \equiv b^2 - 4ac \mod p \iff (4ax + b)^2 \equiv b^2 - 4ac \mod p$$

A questo punto abbiamo bisogno di risolvere due congruenze diverse:

$$y^2 \equiv d \mod p$$
$$4ax + b \equiv \overline{y} \mod p$$

dove $\overline{y}$ 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 $y^2 \equiv d \mod p$.

È evidente che questa non sempre è risolubile, in quanto $a^2 \equiv (-a)^2 \mod p$ per ogni *a*; quindi per almeno metà dei *d* non abbiamo soluzioni. Tuttavia, poiché l'equazione $y^2 - d \equiv 0 \mod p$ 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

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

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

$$g^2,\ g^4,\ g^6, \ldots, g^{2(p-1)}$$

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

$$x^n \equiv a \mod p$$

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* = MCD(*n*,*p* -1), allora i residui *n* -esimi coincidono con i residui *k* -esimi.

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

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

Attraverso l'uso degli indici è facile dimostrare che

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

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

$$a^P \mod p = \left(\frac{a}{p}\right)$$

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

$$a^P \equiv k^{2P} \mod p \equiv a^{p-1} \mod p \equiv 1 \mod p$$

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

$$a^P \equiv g^{nP} \mod p$$

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

$$a^P \equiv g^P \mod p \equiv -1 \mod p$$

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 $p \equiv 1 \mod 4$, ovvero $p = 4k + 1$, allora $P = 2k$, e

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

Se invece $p \equiv 3 \mod 4$, 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.

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 $1a,\ 2a, \ldots, Pa$ 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

$$ia \equiv ja \mod p$$

allora $i \equiv j \mod p$, e quindi i vari numeri considerati non sono tra loro congrui modulo *p*. Allo stesso modo, se

$$ia \equiv -ja \mod p$$

allora $i \equiv -j \mod p$ e quindi *i* e *j* non possono essere entrambi minori o uguali di *P*. Da questo segue che i numeri $1a,\ 2a, \ldots, Pa$ sono congrui, in qualche ordine, all'insieme

$$\pm 1,\ \pm 2, \ldots, \pm P$$

dove si prende o il più o il meno. Sia *k* il numero di segni meno. Allora, moltiplicandoli tutti insieme abbiamo

$$(1a)(2a)\cdots(Pa) \equiv (-1)^k 1 \cdot 2 \cdots P \mod p$$

e semplificando

$$a^P \equiv (-1)^k \mod p$$

come volevasi dimostrare.

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

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

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

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

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

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

e ponendo *p*=4*ak*+*r*,

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

cioè

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

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 4*a* la caratteristica quadratica è la stessa. Questo dimostra la prima parte del teorema. Se invece $q \equiv -p \equiv 4a - r \mod 4a$, allora, sostituendo *r* con 4*a*-*r* negli intervalli, si ha

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

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

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

Il caso a=2

Consideriamo in particolare il caso *a*=2. Questo può essere trattato con lo stesso metodo visto precedentemente: sia *p*=8*k*+*r* un primo; i numeri 2, 4, 6, ... , 2*P* 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*.

$$\frac{1}{2}p < 2x < p$$

equivale a

$$2k + \frac{1}{4}r < x < 4k + \frac{1}{2}r$$

e ignorando 2*k* e 4*k*, 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*.

La legge di reciprocità

La legge di reciprocità quadratica, infine, afferma che

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

o, detto a parole, che pa 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 $p \equiv q \mod 4$, ovvero che $p - q = 4a$ (possiamo supporre *p*>*q*) per un qualche intero *a*. Allora

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

e similmente

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

e quindi

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

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

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

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

Se invece $p \equiv -q \mod 4$ si ha *p*+*q*=4*a*, e

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

così come

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

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.

Esempi

Per mostrare la potenza di questo teorema, calcoliamo ad esempio

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

Fattorizzando 520, abbiamo

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

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

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

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

(considerando che $91 \equiv 3 \mod 8$), e infine

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

e 637 è un residuo quadratico modulo 719.

Alcune applicazioni

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

Numeri primi

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

$$p_1 p_2 p_3 \cdots p_n - 1$$

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 $p_1,\ p_2, \ldots, p_n$, 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 $p_1,\ p_2, \ldots, p_n$ ci sarebbe sempre almeno uno zero. Ma questo è palesemente falso, in quanto basta scegliere la *n*-upla (1,1,...,-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 $p_1,\ p_2, \ldots, p_n$: 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 4*k*+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 $p_1,\ p_2, \ldots, p_n$. 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

$$x^2 + 1 \equiv 0 \mod q$$

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

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 $a^2 + 1 \equiv 0 \mod p$. Per il lemma di Thue esiste una soluzione alla congruenza

$$ax \equiv y \mod p$$

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

$$a^2x^2 \equiv y^2 \mod p \Longrightarrow -x^2 \equiv y^2 \mod p \Longrightarrow x^2+y^2 \equiv 0 \mod p \Longrightarrow x^2+y^2 = kp$$

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

$$x^2 + y^2 < p + p = 2p$$

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

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 $x^2 + y^2 \equiv 0 \mod p$ 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 $ax_1,\ ax_2, \ldots, ax_k$ (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

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

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 tenda conto di questo fatto, e dimostrare che gli elementi di ogni classe sono somma di un certo numero di residui *n*-esimi.

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.

Esercizi

Di seguito sono presentati degli esercizi, con le rispettive soluzioni, divisi per capitoli.

Capitolo 1

<quiz display=simple> {Trovare: |type="{}"} 20 mod 3 = { 2_3 } 31 mod 4 = { 3_3 } 1895 mod 7 = { 5_3 } 43245 mod 13 = { 7_3 }

{Dire quali dei seguenti elementi sono invertibili: |type="[]"} - 4 (modulo 8) - 10 (modulo 14) + 12 (modulo 31) - 15 (modulo 35) + 8 (modulo 9) - 438 (modulo 15) </quiz>

Capitolo 2

- Dimostrare che se $b \equiv 1 \mod d$ allora *n* è divisibile per *d* se e solo se lo è la somma delle sue cifre, quando *n* è scritto in base *b*.

<quiz display=simple> {Calcolare usando il piccolo teorema di Fermat o il teorema di Eulero: |type="{}"} $2^{75} \mod 5$= { 3 _3 } $5^{89} \mod 7$= { 3 _3 } $4^{90} \mod 11$= { 1 _3 } $16^{96} \mod 13$= { 1 _3 } $56681^{123432} \mod 13$= { 1 _3 } $14^{54} \mod 10$= { 6 _3 } $26^{32} \mod 12$= { 1 _3 } $7^{19} \mod 15$= { 13 _3 } $9^{9} \mod 6$= { 3 _3 } </quiz>

Capitolo 3

<quiz display=simple> {Risolvere: |type="{}"} $2x \equiv 3 \mod 5$= { 4 } $3x \equiv 7 \mod 8$= { 5 } $6x \equiv 8 \mod 9$= { insolubile|impossibile|no } $21x \equiv 7 \mod 28$= { 3 mod 4 (3, 7, 11, 15, 19, 23, 27 mod 28) } $8x \equiv 7 \mod 9$= { 2 } $91x \equiv 991 \mod 3$= { 1 }

{Risolvere: |type="{}"} $\begin{cases} x \equiv 7 \mod 9 \\ x \equiv 3 \mod 5 \end{cases}$= { 43 mod 45 } $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 4 \\ x \equiv 4 \mod 5 \\ x \equiv 5 \mod 6 \end{cases}$= { 59 mod 60 }

{Risolvere: |type="{}"} $x^4 + 3x^2 + 7x + 3 \mod 21$= { 6, 8, 15, 20 }

{Determinare tutti gli *x* tali che $\phi(x)$è dispari. |type="{}"} { 1, 2|1 e 2 } </quiz>

Capitolo 4

- Dimostrare, usando il solo teorema di Chevalley, che la congruenza

$$x^2 + y^2 \equiv -1 \mod p$$

ha soluzione per ogni primo *p*.

- Trovare tutte le soluzioni della congruenza

$$x^2 + 2y^2 - z^2 \equiv 0 \mod 3$$

Capitolo 5

<quiz display=simple> {Trovare l'ordine moltiplicativo di: |type="{}"} 6 mod 11 = { 10 } 14 mod 25 = { 10 } 13 mod 43 = { 21 } 2 mod 15 = { 4 } 3 mod 63 = { no|non esiste|nessuno|impossibile } </quiz>

- Sapendo che $2^9 \equiv 1 \mod 73$ e $10^8 \equiv 1 \mod 73$, trovare una radice primitiva modulo 73.

<quiz display=simple> {Trovare le radici primitive modulo 23. |type="{}"} { 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 }

{Sapendo che 2 è una radice primitiva modulo 13, trovare una radice primitiva modulo 169. |type="{}"} { 2 } </quiz>

- Costruire una tavola di indici modulo 11 a partire dalla radice primitiva 2.

Capitolo 6

- 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*.

<quiz display=simple> {Elencare i residui quadratici modulo 13. |type="{}"} { 1, 3, 4, 9, 10, 12 }

{Calcolare: |type="{}" $\left(\frac{-26}{73}\right)$ = { -1 } $\left(\frac{34}{97}\right)$ = { -1 } $\left(\frac{57}{113}\right)$ = { 1 } </quiz>

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.

Fonti e autori delle voci

Fonte:: http://it.wikibooks.org/w/index.php?oldid=129191 *Autori:*: Dr Zimbu, Ramac

Aritmetica modulare *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=143858 *Autori:*: Diablo, Dr Zimbu, Ramac

La relazione di congruenza *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=219724 *Autori:*: Dr Zimbu, Ramac, 3 Modifiche anonime

Prime proprietà e applicazioni *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=129126 *Autori:*: Dr Zimbu, Ramac

Congruenze lineari *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=219720 *Autori:*: Dr Zimbu, Ramac, 2 Modifiche anonime

Polinomi in aritmetica modulare *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=215261 *Autori:*: Dr Zimbu, IESteve, LoStrangolatore, Ramac

Radici primitive *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=141490 *Autori:*: Dr Zimbu, Ramac

Congruenze quadratiche *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=141492 *Autori:*: Diablo, Dr Zimbu

Alcune applicazioni *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=197762 *Autori:*: Dr Zimbu, 1 Modifiche anonime

Bibliografia *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=141494 *Autori:*: Dr Zimbu

Esercizi *Fonte:*: http://it.wikibooks.org/w/index.php?oldid=201359 *Autori:*: Dr Zimbu, Pietrodn, 1 Modifiche anonime

Fonti, licenze e autori delle immagini

File:Anillo cíclico.png *Fonte:*: http://it.wikibooks.org/w/index.php?title=File:Anillo_cíclico.png *Licenza*: GNU Free Documentation License *Autori:*: Original uploader was Romero Schmidtke at es.wikipedia

Immagine:Wikipedia-logo.png *Fonte:*: http://it.wikibooks.org/w/index.php?title=File:Wikipedia-logo.png *Licenza*: logo *Autori:*: version 1 by Nohat (concept by Paullusmagnus);

Licenza