Congruenze

Alberto Abbondandolo

Forte dei Marmi, 17 Novembre 2006

1 Il resto nella divisione tra interi

Consideriamo i numeri naturali $0, 1, 2, 3, \ldots$ ed effettuiamone la divisione per 3, indicando il resto:

$$\begin{array}{lll} 0 = 0 \cdot 3 + 0, & 3 = 1 \cdot 3 + 0, & 6 = 2 \cdot 3 + 0, \quad \ldots \\ 1 = 0 \cdot 3 + 1, & 4 = 1 \cdot 3 + 1, & 7 = 2 \cdot 3 + 1, \quad \ldots \\ 2 = 0 \cdot 3 + 2, & 5 = 1 \cdot 3 + 2, & 8 = 2 \cdot 3 + 2, \quad \ldots \end{array}$$

I resti di questa divisione sono $0, 1, 2$ e si ripetono in modo periodico. Sulla stessa riga abbiamo indicato i numeri che, divisi per 3, danno lo stesso resto. Ad esempio, 7 e 4 danno entrambi resto 1. Per indicare il fatto che 7 e 4 danno lo steso resto quando divisi per 3, il matematico tedesco Carl Friedrich Gauss (1777-1855) ha introdotto la notazione

$$7 \equiv 4 \pmod 3$$

che si legge 7 *è congruo a* 4 *modulo 3*. In generale:

Definizione 1 *Siano a, b due interi e sia d un intero positivo. Diciamo che a è congruo a b modulo d, in formula*

$$a \equiv b \pmod d,$$

se a e b divisi per d danno lo stesso resto.

Equivalentemente, stiamo richiedendo che

$$a = nd + r, \quad b = md + r,$$

per opportuni interi m, n, con $0 \leq r \leq d-1$. Un'altra definizione equivalente è la seguente: $b - a$ è divisibile per d.

Ogni numero intero è congruo modulo d al suo resto nella divisione per d, ossia ad un numero compreso tra 0 e $d-1$: questi numeri si dicono *resti modulo d*. Vi sono quindi esattamente d resti modulo d.

Una rappresentazione grafica utile per studiare le congruenze modulo d è costituita da un cerchio con d tacche equidistanti. Marchiamo la prima tacca con 0, la seconda - ad esempio girando in senso orario - con 1, e così via fino all'ultima, che marchiamo con $d-1$. La successiva a questo punto è quella già marcata con 0, e infatti d è congruo a 0 modulo d. Proseguendo ritroviamo 1, e infatti $d+1$ è congruo ad 1 modulo d. In effetti, quando leggiamo l'ora su un normale orologio con 12 tacche abbiamo a che fare con delle congruenze modulo 12: se la lancetta delle ore è sul 4, sappiamo che sono le 4 oppure le 16, visto che 16 è congruo a 4 modulo 12.

Il simbolo $\equiv$ che si usa per indicare la relazione di congruenza è simile al simbolo $=$ dell'usuale relazione di uguaglianza: questa notazione è giustificata dal fatto che la relazione di congruenza soddisfa molte delle proprietà dell'uguaglianza. In particolare, valgono le seguneti proprietà, tutte di immediata verifica:

1. (riflessività) $a \equiv a \pmod d$;
2. (simmetria) se $a \equiv b \pmod d$, allora $b \equiv a \pmod d$;

3. (transitività) se $a \equiv b$ e $b \equiv c \pmod d$, allora $a \equiv c \pmod d$.

Inoltre la relazione di congruenza si comporta bene rispetto alle operazioni algebriche di addizione, sottrazione e moltiplicazione[1]. Supponiamo infatti che

$$a \equiv a' \quad \text{e} \quad b \equiv b' \pmod d.$$

Allora possiamo sommare, sottrarre, e moltiplicare queste due "equazioni", ottenendo:

4. $a + b \equiv a' + b' \pmod d$;
5. $a - b \equiv a' - b' \pmod d$;
6. $a \cdot b \equiv a' \cdot b' \pmod d$.

Verifichiamo ad esempio la proprietà (6). L'ipotesi equivale a dire che esistono interi n, m tali che $a - a' = nd$ e $b - b' = md$. Allora

$$ab - a'b' = ab - a'b + a'b - a'b' = b(a - a') + a'(b - b') = bnd + a'md = (bn + a'm)d,$$

quindi $ab - a'b'$ è divisibile per d, ossia $ab \equiv a'b' \pmod d$.

2 Criteri di divisibilità

Divisibilità per 3 C'è un modo rapido per decidere se il numero 17112006 è divisibile per 3? Si può usare il criterio di divisibilità per 3 imparato alla Scuola Media: sommiamo le cifre di questo numero, ottenendo

$$1 + 7 + 1 + 1 + 2 + 0 + 0 + 6 = 18;$$

dato che il risultato, 18, è divisibile per 3, anche il numero iniziale 17112006 lo è. Grazie alle congruenze possiamo spiegare come mai il criterio imparato alla Scuola Media funziona.

Quando scriviamo 17112006 stiamo usando la notazione decimale: l'ultima cifra, 6, indica le unità, la penultima, 0, indica le decine, e così via. In altre parole, stiamo considerando il numero

$$6 \cdot 10^0 + 0 \cdot 10^1 + 0 \cdot 10^2 + 2 \cdot 10^3 + 1 \cdot 10^4 + 1 \cdot 10^5 + 7 \cdot 10^6 + 1 \cdot 10^7.$$

Per decidere a cosa è congruo questo numero modulo 3, ci serve capire a cosa sono congrue modulo 3 le potenze di 10. La potenza $10^0 = 1$ è ovviamente congrua a 1 qualunque sia il modulo. La potenza $10^1 = 10$ è congrua a 1 modulo 3. Grazie alla proprietà (6), ciò implica che anche

$$10^2 = 10 \cdot 10 \equiv 1 \cdot 1 = 1 \pmod 3,$$

come del resto si vede direttamente dall'uguaglianza $10^2 = 100 = 99 + 1 = 3 \cdot 33 + 1$. Analogamente,

$$10^3 = 10^2 \cdot 10 \equiv 1 \cdot 1 = 1 \pmod 3,$$

e in generale

$$10^n = 10^{n-1} \cdot 10 \equiv 1 \cdot 1 = 1 \pmod 3,$$

per ogni intero positivo n. Quindi *tutte le potenze di 10 sono congrue ad* 1 *modulo* 3. È questo il fatto che sta alla base del criterio di divisibilità per 3. Infatti, usando le proprietà (4) e (6) delle congruenza troviamo che

$$\begin{aligned} 17112006 &= 6 \cdot 10^0 + 0 \cdot 10^1 + 0 \cdot 10^2 + 2 \cdot 10^3 + 1 \cdot 10^4 + 1 \cdot 10^5 + 7 \cdot 10^6 + 1 \cdot 10^7 \\ &\equiv 6 \cdot 1 + 0 \cdot 1 + 0 \cdot 1 + 2 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 7 \cdot 1 + 1 \cdot 1 = 18 \pmod 3, \end{aligned}$$

quindi il numero 17112006 è congruo modulo 3 alla somma delle sue cifre, cioè 18. Perciò 17112006 è divisibile per 3, in quanto 18 lo è. Quel che abbiamo verificato per questo numero particolare ha validità del tutto generale: *ogni numero è congruo modulo 3 alla somma delle sue cifre.* Da questo fatto deduciamo una piccola generalizzazione del criterio della Scuola Media: *il resto della divisione per 3 di un numero è uguale al resto della divisione per 3 della somma delle sue cifre.*

[1] La divisione è più problematica, dato che il quoziente di due interi non è necessariamente un intero. Ma vedi più avanti la sezione "Inverso modulo d".

Divisibilità per 9. Dato che 10 è congruo a 1 modulo 9, come prima ricaviamo che *tutte le potenze di 10 sono congrue ad 1 modulo 9.* Quindi *il resto della divisione per 9 di un numero è uguale al resto della divisione per 9 della somma delle sue cifre.* In particolare, un numero è divisibile per 9 se e solamente se la somma delle sue cifre lo è.

Divisibilità per 11. Vediamo di trovare un criterio di divisibilità per 11. Dobbiamo capire a cosa sono congrue modulo 11 le varie potenze di 10. Ovviamente $10^0 = 1$ è congruo a 1 modulo 11. La potenza $10^1 = 10$ è invece congrua a -1 modulo 11. Ne segue che

$$10^2 = 10 \cdot 10 \equiv (-1) \cdot (-1) = 1 \pmod{11},$$

e quindi

$$10^3 = 10 \cdot 10^2 \equiv (-1) \cdot 1 = -1 \pmod{11}.$$

Procedendo allo stesso modo, vediamo che *le potenze pari di 10 sono congrue a 1 mentre quelle dispari sono congrue a -1 modulo 11.* Per decidere se il numero 6131829 è divisibile per 11 possiamo ragionare come prima e scrivere

$$6131829 = 9 \cdot 10^0 + 2 \cdot 10^1 + 8 \cdot 10^2 + 1 \cdot 10^3 + 3 \cdot 10^4 + 1 \cdot 10^5 + 6 \cdot 10^6 \equiv 9 - 2 + 8 - 1 + 3 - 1 + 6 = 22 \equiv 0 \pmod{11}.$$

Quindi 6131829 è divisibile per 11. In generale: *un numero è divisibile per 11 se e solamente se la somma delle sue cifre a segni alterni è divisibile per 11.*

Divisibilità per 2,5,10,4,25 Per decidere se un numero è divisibile per 2,5, o 10, basta guardare la sua ultima cifra. Per decidere se un numero è divisibile per 4 o 25, basta guardare il numero composto dalle ultime due cifre. Questi fatti elementari sono conseguenza del fatto che 10 è divisibile per 2, 5, e 10 (e quindi anche tutte le potenze lo sono), mentre 10^2 è divisibile per 4 e 25 (quindi tutte le potenze di 10 superiori alla prima lo sono).

Esercizio 1 *Trovare i criteri di divisibilità per 7 e per 13.*

3 Inverso modulo d

L'inverso di un numero $a \neq 0$ è un numero che moltiplicato per a dà 1, ossia $1/a$. Se a è un intero diverso da 1 e -1, il suo inverso non sarà un intero, quindi *gli interi diversi da 1 e -1 non hanno inverso nell'insieme dei numeri interi.* Le cose cambiano se guardiamo gli interi modulo d, dove d è un intero positivo fissato. La domanda che ci stiamo chiedendo in questo caso è diversa: dato un intero a, esiste un intero b tale che $a \cdot b$ è congruo ad 1 modulo d?

Ad esempio, *3 è un inverso di 2 modulo 5*, in quanto

$$3 \cdot 2 = 6 \equiv 1 \pmod{5}.$$

Esiste un inverso di 4 modulo 6? I resti modulo 6 sono 0,1,2,3,4,5. Vediamo se tra di loro c'è un inverso di 4 modulo 6:

$$0 \cdot 4 \equiv 0, \quad 1 \cdot 4 \equiv 4, \quad 2 \cdot 4 \equiv 2, \quad 3 \cdot 4 \equiv 0, \quad 4 \cdot 4 \equiv 4, \quad 5 \cdot 4 \equiv 2 \pmod{6}.$$

Non è mai saltato fuori 1 come risultato, quindi *4 non ha un inverso modulo 6.* Il problema qua è che i numeri 4 e 6 non sono primi tra loro:

Esercizio 2 *Se a e d non sono primi tra loro, allora a non ha un inverso modulo d.*

Supponiamo invece che a e d siano primi tra loro, ossia che il loro massimo comun divisore sia 1. Per il *Teorema di Bézout* (vedi la lezione "Equazioni diofantee") esistono interi h e k tali che

$$ha + kd = 1.$$

Quindi

$$ha = 1 - kd \equiv 1 \pmod{d},$$

da cui h è un inverso di a modulo d. Per trovare l'inverso di a modulo d è quindi sufficiente trovare gli interi h, k del Teorema di Bezout, e come abbiamo visto nella lezione "Equazioni diofantee" questi interi si ricavano dall'*Algoritmo di Euclide.*

Esercizio 3 *Trovare l'inverso di 13 modulo 64. Trovare l'inverso di 64 modulo 13. Trovare l'inverso di 17 modulo 44.*

Esercizio 4 *Supponiamo che a e d siano primi tra loro. Quanti sono gli inversi di a modulo d compresi tra 0 e $d-1$?*

4 Irrisolubilità di certe equazioni diofantee

Ricordiamo che le equazioni diofantee sono equazioni algebriche a coefficienti interi di cui si cercano soluzioni intere. Le congruenze possono essere usate per mostrare che certe equazioni diofantee non hanno soluzione. Mostriamo ad esempio che l'equazione

$$x^2 + y^2 = 39723$$

non ha soluzioni x, y intere. Possiamo ridurre questa equazione modulo 4: a destra troviamo 39723, e

$$39723 \equiv 23 \equiv 3 \pmod{4}.$$

È possibile che la somma a sinistra sia congrua a 3 modulo 4? Da questo lato compaiono dei quadrati, quindi dobbiamo vedere chi sono i quadrati modulo 4. Troviamo

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 0, \quad 3^2 \equiv 1 \pmod{4}.$$

Quindi *soltanto i resti* 0 *e* 1 *sono quadrati modulo 4*, mentre i resti 2 e 3 non sono mai quadrati modulo 4. Perciò x^2+y^2 è congruo modulo 4 alla somma $0+0=0$, oppure $0+1=1$, oppure $1+1=2$. Sommando due quadrati modulo 4 non troviamo mai il resto 3, quindi il lato di sinistra dell'equazione non è mai congruo a 3 modulo 4. Pertanto questa equazione diofantea non ha soluzioni.

Tutti i possibili quadrati modulo 4 si dicono *residui quadratici modulo 4*. In generale i *residui quadratici modulo d* sono quei resti modulo d che si realizzano come quadrati modulo d. Per alcuni valori di d vi sono pochi residui quadratici modulo d: tali valori d costituiscono dei validi test per mostrare che certe equazioni diofantee non hanno soluzione.

Esercizio 5 *Mostrare che:*

1. *i residui quadratici modulo 3 sono 0 e 1.*
2. *i residui quadratici modulo 5 sono 0,1,-1.*
3. *i residui quadratici modulo 8 sono 0,1,4.*

Esercizio 6 *Mostrare che le equazioni diofantee*

$$x^2 + y^2 = 2006200627 \quad e \quad x^2 - y^2 = 2006200626$$

non hanno soluzione.

Esercizio 7 *Mostrare che se a è un intero compreso tra 3 e 14 l'equazione diofantea*

$$x^4 + y^4 = z^4 + a$$

non ha soluzione.

5 Per saperne di più

Un'eccellente libro per approfondire la consoscenza della matematica elementare, ma non solo, è il classico

Richard Courant, Herbert Robbins, *Che cos'è la matematica?*, Bollati Boringhieri, 2000.

Per prepararsi alle gare di matematica a qualsiasi livello, uno strumento molto utile è il volumetto

Massimo Gobbino, *Schede olimpiche*, Edizioni Cremonese, 2005.

Nelle *Schede olimpiche* si trova anche un ricco elenco di siti internet dove trovare problemi ed altro materiale.

Questi appunti si basano sulle *Schede olimpiche* N04, N05, e sul supplemeneto al capitolo I, sezione 2, di *Che cos'è la matematica?*.