Aritmetica Modulare

Bruno Bucciotti

February 28, 2017

Abstract

Introduco l'aritmetica modulare per fini olimpici, cercando di abbondare con gli esempi

1 Introduzione

Guardate un orologio (per comodità consideriamo le 12h ignorando la differenza fra mattina e sera). Diciamo che sono le 10 e che ho un appuntamento fra 4 ore: su che numero sarà la lancetta delle ore? Sarà sul 2. Formalmente potremmo provare a scrivere $10+4=2$, ma dovremmo tenere conto del fatto che arrivati a contare fino a 12 dobbiamo ripartire da 0. Scriveremo allora $10+4 \equiv 2(mod 12)$. Si legge "dieci più quattro congruo/uguale/equivalente a due modulo dodici".

1.1 Esempi

$7+4 \equiv 1 \pmod 5$
$4+3 \equiv 0 \pmod 7$
$6+4 \equiv 0 \pmod 2$
$3+2 \equiv 2 \pmod 3$
Possiamo fare un passo indietro e parlare di a modulo b con a, b numeri interi. In questo caso la domanda equivale a: se prendo un orologio con b ore, parto da 0 e faccio passare a ore (se a è negativo mi muovo in senso antiorario), su quale ora cadrà la lancetta alla fine?

1.2 Esempi

$12 \equiv 2 \pmod 5$
$12 \equiv 5 \pmod 7$
$-5 \equiv 3 \pmod 8$
$8 \equiv 0 \pmod 4$

Morale: nelle congruenze modulo m possiamo impunemente aggiungere o sottrarre il modulo e otteniamo un insieme di valori che sono detti tutti "equivalenti modulo m".

1.3 Chiarimenti

$\forall a \in \mathbb{Z},\ m \in \mathbb{N},\ a \equiv a \pmod{m}$; $(a \equiv b \pmod{m}) \Rightarrow (b \equiv a \pmod{m})$; $(a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}) \Rightarrow (a \equiv c \pmod{m})$. Dunque $[2] \bmod 5 = \{2, 7, 12, -3, -8, ..\}$ dove i numeri sono ottenuti aggiungendo o sottraendo m. Si tratta quindi di una classe di equivalenza nel senso delle relazioni. Per ognuna di queste classi vi è un **rappresentante privilegiato**, cioè quello compreso fra 0 e $m-1$ (estremi esclusi): questo corrisponde nel gioco di prima dell'orologio al numero effettivamente segnato dalla lancetta (fine interludio astratto).
Più concretamente è importante notare la piccola ambiguità che si genera chiedendo di calcolare $a \pmod{m}$: si piò intendere infatti sia il rappresentante privilegiato compreso fra 0 e m-1, sia l'intera classe di equivalenza. Ai fini olimpici si intenderà usualmente il primo.

1.4 Moduli come resti della divisione per m

Calcoliamo 13 : 5: viene $2 resto 3$. Notiamo che $13 \equiv 2 \pm 5$ poichè mi basta sottrarre il modulo 2 volte per passare da 13 a 2. Più in generale ho che se $a \equiv b \pmod{m}$ e $a \geq m$ e $0 \leq b < m$, cioè b è il "rappresentante privilegiato", allora $a : m = roba + resto\, b$.

2 Aritmetica con i moduli

Notate che $a + b \equiv c \pmod{m}$ assomiglia a $a + b = c$, solo che dopo aver calcolato l'espressione a sinistra (o mentre la si calcola) si può aggiungere m a piacere. Questo ci suggerisce che dovremmo considerare espressioni più generali delle sole somme. Useremo questo fatto fondamentale per impostare qualche dimostrazione: $a \equiv b \pmod{m} \iff a = b + k * m$ per qualche k intero. Convincetevene pensando di aggiungere/sottrarre m a destra quanto basta per far sparire il termine $k * m$. Esempio: $26 \equiv 2 \pmod{3}$ e $26 = 2 + 3 * 8$ con $a = 26, b = 2, m = 3, k = 8$.

2.1 Somme

Le abbiamo già introdotte all'inizio, ma rivediamo brevemente. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ allora $a + c \equiv b + d \pmod{m}$. Esempio $4 \equiv 7 \pmod{3}$ e $10 \equiv 4 \pmod{3}$ allora $4 + 10 \equiv 7 + 4 \pmod{3}$, difatti $14 \equiv 11 \pmod{3}$. Faccio solo questa dimostrazione, poi potete provare da soli/cercare su Wikipedia. In generale se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ ci devono essere k_1, k_2 per cui $a = b + m * k_1$ e $c = d + m * k_2$. Faccio la solita somma membro-a-membro e ho $a + c = b + d + (k_1 + k_2) * m$. Sottraendo m $k_1 + k_2$ volte ho la tesi. Notare che poichè la relazione è simmetrica ho anche che $a + d \equiv b + c \pmod{m}$.
Nota: D'ora innanzi se non scrivo il modulo intendete modulo generico m (lo

stesso numero per tutto il paragrafo). Se voglio parlare di moduli diversi (es mod 5 e mod 7) allora tornerò a indicarli.

2.2 Sottrazioni

Sono come le somme, vi faccio solo due esempi:
$-2 \equiv 5 \pmod 7$
$4 - 3 * 4 \equiv -8 \equiv 1 \pmod 9$

2.3 Prodotti

Questo è importante: oltre alle usuali regole dell'aritmetica vale la proprietà che se se avete una somma di termini e un termine è multiplo del modulo potete ucciderlo. Esempi a gogò:
$35 + 3 \equiv 7 * 5 + 3 \equiv 3 \pmod 5$
$20 + 4 \equiv 24 \equiv 4 \pmod{10}$
$31 \equiv 3 * 10 + 1 \equiv 1 \pmod{10}$
$132 \equiv 11 * 12 \equiv 0 \pmod{11}$
Più difficile:
$114 * 341 \equiv (44 + 70) * (350 - 9) \equiv 44 * (14 - 9) \equiv 2 * 5 \equiv 3 \pmod 7$
$683*3093*382 \equiv 11*12 \equiv (680+3)*(3080+13)*(380+2) \equiv 3*1*2 \equiv 2 \pmod 4$

2.4 Interludio: Criteri di divisibilità

Fatto fondamentale: se scriviamo in base 10 il numero abcd è, formalmente, $d + 10c + 100b + 1000a$. Secondo fatto fondamentale: ricordando il discorso a (1.4) un numero è divisibile per m quando è congruo a 0 modulo m.

Divisibilità per 2 e per 5 Poichè tutti i multipli di 10 sono divisibili per 2 e per 5 allora dato abcd=$1000a + 100b + 10c + d$ posso uccidere tutti i termini trannte d. Dunque un numero è divisibile per 2 o 5 solo se lo è la sua cifra delle unità, difatti se questa lo è allora $d \equiv 0 \pmod{2o5}$ da cui il numero iniziale è $\equiv 0 \pmod{2o5}$ e quindi è divisibile per 2 o 5.

Divisibilità per 3 $10 \equiv 1 \pmod 3$ $100 \equiv 1 \pmod 3$ ecc dunque abcd è divisibile per 3 se $1000a + 100b + 10c + d \equiv a + b + c + d \pmod 3$ cioè basta sommare le cifre: se la somma è divisibile per 3 allora anche il numero iniziale è divisibile per 3.

Divisibilità per 11 10^k è equivalente a 1 mod11 se k è pari (es:$10^k = 1, 100$, ecc). Vale -1 se k è dispari. Allora abcd=$10^3a+10^2b+10c+d \equiv d-c+b-a \pmod{11}$. Attenzione: l'ho fatto con un numero di 4 cifre, ma in generale si somma a segni alterni (il primo positivo) dalla cifra delle unità verso sinistra, cioè unità-decine+centinaia.. Di nuovo se questa cosa è divisibile per 11 allora lo è anche il numero iniziale.

2.5 Teoremino sulla potenza

$(k*m+a)^b$ = tanta roba multipla di m $+a^b$, da cui $(k*m+a)^b \equiv a^b$.
Questo si può anche scrivere $a^u \pmod m = (a \pmod m))^u$.

Esempi Calcolo a mano $7^2 \pmod{20}$: è 9. Allora posso più facilmente calcolare $7^6 \equiv (7^2)^3 \equiv 9^3 \equiv 81*9 \equiv 1*9 \equiv 9 \pmod{20}$. Posso infine calcolare $7^{14} \equiv (7^6)^2 * 7^2 \equiv 9^2 * 9 \equiv 9^3 \equiv 9 \pmod{20}$

Primo vero esempio olimpico Calcolare la cifra delle unità di 66^{66}
Traduzione: quanto vale 66^{66} mod 10? E' come chiedersi quanto sia $(60+6)^{66} \equiv 6^{66} \pmod{10}$. Notiamo ora che $6*6 = 36 \equiv 6 \pmod{10}$, perciò se devo fare $6*6*6..*6$ 66 volte ho che il prodotto dei primi 2 termini mi dà 36, che è 6 per noi. Moltiplico ancora per 6 e ancora ottengo 6, e così via riottenendo sempre 6; perciò alla fine la cifra è 6.

Esempio più difficile Cifra delle unità di 44^{66}
Di nuovo uccido tutto dalle decine in su: 4^{66}. Ora faccio i primi termini (sempre mod 10): $4^2 = 4*4 \equiv 6$, $4^3 = 4^2*4 \equiv 6*4 \equiv 4$, $4^4 = 4*4 \equiv 6$. Potremmo fare una dimostrazione per induzione (chi sa cos'è ci provi), ma per ora limitiamoci a osservare che se l'esponente è pari allora viene 6, se è dispari viene 4. 66 è pari, quindi viene 6.

2.6 Semplificazione

Anche questo può tornare comodo. Guardo $4 \equiv 10 \pmod 6$ e noto che tutti i termini sono pari: in qualche modo vorrei semplificare (attenzione: non è detto che convenga!). L'espressione equivale a dire che, per qualche k intero, vale $4 = 10 + 6k$. Questa la posso semplificare al volo e ottengo $2 = 5 + 3k$. Allora è vero che $2 \equiv 5 \pmod 3$. Il ragionamento è generale e vale in qualunque caso i tre termini abbiano un divisore comune. Attenzione: se i primi due termini sono multipli di uno stesso divisore ma il modulo non lo è ho comunque una strada. Guardo $12 \equiv 2 \pmod 5$. Equivale a $12 = 2 + 5k$ che per essere vera esige che k sia pari, poichè $5k = 12 - 2 = 2(6-1)$ in cui evidenzio il 2 in comune. Ma allora posso dividere per 2 il 12, il 2 e il k stesso! Allora ho che $6 = 1 + 5k$. Il modulo quindi non cambia!! Ho che $6 \equiv 1 \pmod 5$

3 Ciclicità nelle operazioni

Partiamo da 3 e lavoriamo in aritmetica modulo 14. Moltiplichiamo 3 per 2 tante volte: 3, 6, 12, 24=10, 20=6, 12, 24=10, ecc.. . Concretamente visto che ci sono solo 14 numeri fra 0 e 13 al massimo dopo 14 passi si ritornerà a un numero precedente e da lì si entrerà in un loop. Una cosa analoga succede anche con l'elevamento a potenza: proviamo con 3 modulo 4 e lo eleviamolo alla n con $n \in \mathbb{N}$: $3^0 = 1, 3, 3^2 = 9 = 1, 3^3 = 1*3 = 3$. (NB: il primo esempio in realtà è

come il secondo, solo che davanti alla potenza con esponente variabile n ho un ulteriore fattore 2). Questo ha vaste applicazioni pratiche.

3.1 Esercizi

I primi 2 problemi tratti da Archimede 2015, l'ultimo da Febbraio 2014 (disclaimer: non possiedo nulla di questi esercizi)

1. Qual è la 2015_{esima} cifra dopo la virgola della scrittura decimale di 4/7?
2. Qual è la cifra delle unità di $7^{(8^9)}$?
3. Qual è l'esponente del fattore "2" nella fattorizzazione del numero $(5-1)(5^5-1)...(5^{5^{\cdot^{\cdot^{\cdot^5}}}}-1)$ dove in ogni fattore compare ad esponente un "5" in più che nel precedente e nell'ultimo ne compaiono, come esponenti, 2014?
4. (Questo non stava in quelle 2 gare) Determinare tutti i numeri il cui quadrato finisce per "3"

Se non sapete che pesci pigliare, controllate le soluzioni sul sito delle olimpiadi!

4 Residui quadratici

Studiamo i quadrati perfetti (cioè quadrati di numeri naturali) modulo 4. Denotiamo con n un generico naturale, che sarà congruo a 0, 1, 2 *o* 3 $\pmod 4$. Allora n^2 potrà essere congruo a $0^2,\ 1^2,\ 2^2,\ 3^2 \pmod 4 = 0,\ 1,\ 4,\ 9 \equiv 0,\ 1,\ 0,\ 1$. In conclusione se prendete un qualunque quadrato perfetto (ricordiamo che 0, 1, 2, 3 è la casistica completa per n modulo 4, sto guardando a qualunque possibilità) allora questo sarà congruo a 0 o a 1 $\pmod 4$. Non troverete mai quadrati perfetti congrui a 2 o 3 $\pmod 4$. 0 e 1 sono detti *residui quadratici* modulo 4. Naturalmente la tecnica è utile per escludere che un certo numero sia un quadrato perfetto: calcolo il numero in modulo 4 (o altro modulo, vedi sotto) e, se non è congruo a uno dei residui quadratici modulo 4, allora non è quadrato perfetto. Tuttavia non posso dire nulla se il numero passa il test! Certamente non tutti i numeri congrui a 0 o 1 modulo 4 sono quadrati perfetti, no? Altra domanda: come scelgo il modulo con cui testare il numero? Fortunatamente ci sono pochi moduli che danno risultati interessanti, quindi di solito sarà sufficiente guardare a questi:

- $n^2 \equiv 0,\ 1 \pmod 3$. Se è congruo a 0 $\pmod 3$ allora è divisibile per 3, ma poiché è un quadrato perfetto, in realtà è divisibile anche per 9
- $n^2 \equiv 0,\ 1 \pmod 4$. 0 se il quadrato è pari, 1 se è dispari
- $n^2 \equiv 0,\ 1,\ -1 \pmod 5$

Esempio: Esistono quadrati perfetti la cui somma delle cifre è 14? Scriviamo il quadrato perfetto usando cifre incognite: ..dcba (si intende quindi il numero $a+10b*100c+1000d+..$). Lo studio modulo 3 e, per lo stesso ragionamento che appare nel criterio di divisibilità per 3 (cioé che $10,\ 100,\ 1000,\ .. \equiv 1 \pmod 3$) ho che il quadrato perfetto è congruo a $a+b+c+d+.. \pmod 3$. Ma questa non è altro che la somma delle cifre del quadrato perfetto, che è 14 per ipotesi; dunque il quadrato perfetto è congruo a $14 \equiv 2 \pmod 3$. Ma ora sappiamo che nessun quadrato perfetto può essere congruo a $2 \pmod 3$, dunque un tale quadrato perfetto non esiste. Per completezza, calcolando a computer, 1444 (somma cifre è 13) è congruo a $1 \pmod 3$.
Esercizio sfida: Esistono esempi di quadrati perfetti la cui somma delle cifre è 12 o 15? (Hint: aiuta ragionare sulla divisibilità per 9..)