OSSERVAZIONI DI ARITMETICA MODULARE E SUI TEOREMI DI FERMAT E DI WILSON

di Guido Carolla[1]

Sunto. Il presente articolo ha fine prevalentemente didattico. Spesso viene perseguito il metodo induttivo, dal concreto all'astratto, a cominciare dal primo paragrafo. Il percorso seguito ha lo scopo, speriamo condiviso dal lettore, di rendere più comprensibili alcune argomentazioni che trattano di aritmetica modulare con i numeri (primi e non), con riferimenti finali alla Teoria dei gruppi.

Introduzione sui moduli

Dato un numero intero n > 1 ci sono n resti possibili della divisione di un qualsiasi intero per n. L'insieme di questi resti viene indicato con $\mathbf{Z}_n$.

$$\mathbf{Z}_n = \{ 0, 1, 2, \ldots, n-1\}$$

Per esempio:

$$\mathbf{Z}_7 = \{ 0, 1, 2, 3, 4, 5, 6\}$$

Denotiamo inoltre con

$$\boldsymbol{x}\ \mathbf{mod\ n} \quad \text{oppure con} \quad \mathbf{res}_n(x)$$

il resto della divisione di ***x*** per **n**.
Quindi l'espressione **r** = 27 mod 14, assegna ad **r** il valore 13.

In generale, dato un numero intero positivo **n**, i numeri interi si distribuiscono in **n classi di resto modulo n**, a seconda del resto che danno quando vengono divisi per **n**.

Due interi a, b stanno nella stessa classe di resto se e solo se

$$\mathbf{a = b\ mod\ n} \qquad \mathbf{(1)}$$

La (1) è perfettamente equivalente alla

$$\mathbf{n\ divide\ a-b} \qquad \mathbf{(2)}$$

Si dice anche che **a** *è congruo o congruente a* ***b*** *modulo* ***n***, e si scrive:

$$\mathbf{a \equiv b\ (mod\ n).}$$

[1] Docente ordinario di matematica e dirigente scolastico in ogni ordine di scuola a r.

Nel prosieguo cercheremo di dare qualche ulteriore elementare spiegazione ed adotteremo una sintetica simbologia modulare per consentire la comprensione dell'argomento anche ai non addetti ai lavori.
$\forall m,n \in []_9 \Rightarrow m-n=k9$, possiamo avere le varie classi dei resti mod 9:
$[0]_9 = \{...,-27,-18,-9,0,9,18,27,36,...\}$,

$[1]_9 = \{...,-10,-1,1,10,19,28,37,...\}$, $[2]_9 = \{...,-11,-2,2,11,20,29,38,...\}$, …,
$[8]_9 = \{...,-35,-26,-17,8,17,26,35,...\}$.

Due teoremi sul mod 9

Lo scopo didattico dell'articolo ci suggerisce di ricorrere all'impostazione dei due teoremi che seguono.
Teorema 1
Il modulo 9 del cubo di ogni numero primo, con eccezione del 3, è 1 oppure 8.

Dimostrazione:
E` noto[2] che i possibili resti modulo 9 dei numeri primi, ad eccezione del 3
$[p \backslash 3]_9 = \{1,2,4,5,7,8\}$, sono $[1]_9\ [2]_9\ [4]_9\ [5]_9\ [7]_9\ [8]_9$, ciò vuol dire che dividendo ogni primo per 9 i resti sono esclusivamente 1, 2, 4, 5, 7, 8, ossia facendo la somma delle cifre dei numeri primi e sottraendo sempre 9 si hanno solo e sempre 1, 2, 4, 5, 7, 8.

Ora, adottando la proprietà delle potenze dei moduli, $\forall n \in N$ ed $m \in Z$, si ha in generale
$[m]_9^n = [m^n]_9$ ed in particolare, sottintendendo il pedice 9:
$[1]^3 = [1^3] = [1]$; $[2]^3 = [2^3] = [8]$; $[4]^3 = [4^3] = [64] = [1]$; $[5]^3 = [5^3] = [125] = [8]$;
$[7]^3 = [7^3] = [343] = [1]$; $[8]^3 = [8^3] = [512] = [8]$ c. v. d.

Detta tesi equivale a due congruenze $p^3 \equiv 1 (\mathrm{mod}\, 9)$ e $p^3 \equiv 8 (\mathrm{mod}\, 9)$ quando dividendo ogni *p* per 9 si hanno tre resti rispettivamente uguali a *1, 4,* 7 per la prima congruenza e 2, 5, 8 per la seconda.
Ess.: per $p = 13$ abbiamo $[13]_9 = [4]_9, 13^3 = 2197, [2197]_9 = [1]_9$;
per $p = 11$ abbiamo $[11]_9 = [2]_9, 11^3 = 1331, [1331]_9 = [8]_9$.

Teorema 2
Il modulo 9 della potenza di 6 di ogni numero primo, ad eccezione del 3, è sempre 1.

Dimostrazione:
Adottando la proprietà delle potenze mod 9, sottintendendo sempre il pedice 9, abbiamo

[2] "Alcune regolarità dai numeri primi" dello stesso autore

$[1]^6 = [1^6] = [1]$; $[2]^6 = [2^6] = [64] = [1]$; $[4]^6 = [4^6] = [4096] = [1]$; $[5]^6 = [5^6] = [15625] = [1]$;
$[7]^6 = [7^6] = [117649] = [1]$; $[8]^6 = [8^6] = [262144] = [1]$ c. v. d.

Detta tesi equivale alla congruenza $p^6 \equiv 1(\mathrm{mod}\,9)$.

Naturalmente non solo tutte le potenze di 6 dei primi, con esclusione di 3, danno $p^6 \equiv 1(\mathrm{mod}\,9)$ (p^6 e 1 sono nella stessa classe di resto se e solo se $p^6 = 1 \mathrm{mod}\,9$, per cui l'equivalenza è 9 divide ($p^6 - 1$)), ma anche tutte le restanti potenze di 6 dei numeri naturali ad esclusione di 3 e di tutti i suoi multipli: cioè a partire da 1, ogni gruppo di tre numeri ha, per i primi due, l come mod 9, per il terzo no.

Inoltre, prima di proseguire col mod 9, osserviamo che anche dalla potenza quarta di tutti i primi con i moduli 10 e 12 possiamo avere tutti 1, con eccezioni rispettivamente per le coppie di primi 2, 5 e 2, 3. Infatti abbiamo le due congruenze

$$p^4 \equiv 1(\mathrm{mod}10) \text{ e } p^4 \equiv 1(\mathrm{mod}12) ,$$

che sono verificate rispettivamente con le possibili classi dei resti dei moduli 10 e 12 dei numeri primi $[p \backslash 2,5]_{10} \in \{1,3,7,9\}$ e $[p \backslash 2,3]_{12} \in \{1,5,7,11\}$.

Con ciò, a nostro avviso, nulla viene tolto pero` alla "*Generalita` delle argomentazioni...*" che andremo ad esporre nel relativo paragrafo ed alle singolarita` di quelle esposte e che seguono sui moduli 7, 9, 5.

Dalla congruenza di Fermat $a^{m-1} \equiv 1(\mathrm{mod}\ m)$ con $m \in \{m : numeroprimo\}$ e a non divisibile per m, posti $a = p_2$ ed $m = p_1$ abbiamo $p_2^{p_1-1} \equiv 1(\mathrm{mod}\ p_1)$, per la quale non ci sono preclusioni, in quanto ad *a* ed *m* abbiamo sostituito due numeri primi; per la proprietà che dice "se due numeri sono congrui mod *m*, i loro rispettivi prodotti per $n \neq 0$ sono congrui mod *mn*", per $p_1 = 3$ e per $n = 3$ abbiamo $p_2^{3-1} \cdot 3 \equiv 1(\mathrm{mod}(3 \cdot 3))$ ed in generale per $p_2 = p$ abbiamo anche $3(p^2 - 1) \equiv 0(\mathrm{mod}\,9)$, dove $p \neq 3$.

Analoga dimostrazione abbiamo per $d^6 \equiv 1(\mathrm{mod}\,9)$ con $d \in \{d : numeridispari \neq 3k\}$ con *k=1,2,3,...*: posti $a = d_2$ ed $m = d_1$ abbiamo $d_2^{d_1-1} \equiv 1(\mathrm{mod}\,d_1)$, per la quale qui vi è la preclusione che d_2 non debba essere divisibile per d_1.

Per la proprietà` che dice "se due numeri sono congrui mod *m*, i loro rispettivi prodotti per $n \neq 0$ sono congrui mod *mn*", mutatis mutandis, per $d_1 = 3$ e per $n = 3$ abbiamo $d_2^{3-1} \cdot 3 \equiv 1(\mathrm{mod}(3 \cdot 3))$ ed in generale per $d_2 = d$: $3(d^2 - 1) \equiv 0(\mathrm{mod}\,9)$, dove $d \neq 3k$.

In particolare dall'asserto di Fermat, operando le sostituzioni *a=p* ed *m=7*, abbiamo, per $p \neq 7$, $p^{7-1} \equiv 1(\mathrm{mod}\,7)$ e quindi $p^6 \equiv 1(\mathrm{mod}\,7)$, che rispetto alla tesi del teorema 2, cioe`, per $p \neq 3$, $p^6 \equiv 1(\mathrm{mod}\,9)$, varia solo per il modulo; per *a=p* ed *m=5*, abbiamo per $p \neq 5$, $p^4 - 1 = 0(\mathrm{mod}5)$.

Es.: per *p=11* abbiamo $11^6 = 1771561$, $[1771561]_7 = [1]_7$, ossia $11^6 \equiv 1 (\mathrm{mod}\, 7)$, perché 7 divide $(11^6 - 1)$ ed anche $[1771561]_9 = [1]_9$, ossia $11^6 \equiv 1 (\mathrm{mod}\, 9)$, perché 9 divide $(11^6 - 1)$, infatti da 1771561-1=1771560 verifichiamo 1771560:7=253080 e 1771560:9=196840.

Ora, da quanto ottenuto sopra per il teorema di Fermat, per la proprietà del trasporto del termine 1, cioe` $p_2^{p_1-1} \equiv 1 (\mathrm{mod}\, p_1)$, $p_2^{p_1-1} - 1 \equiv 0 (\mathrm{mod}\, p_1)$ e per il teorema di Wilson, per il quale sussiste la congruenza reciproca $(p_1 - 1)! + 1 \equiv 0 (\mathrm{mod}\, p_1)$, considerata l'uguaglianza dei secondi membri deduciamo che p_1 divide con resto zero tanto $p_2^{p_1-1} - 1$ che $(p_1 - 1)! + 1$, per cui possiamo affermare: **da due primi, comunque presi** p_1 e p_2 **e` immediata la possibilità di trovare due numeri entrambi multipli di** p_1**, secondo le funzioni di numeri interi** $h(p_1, p_2) = \left(p_2^{p_1-1} - 1\right) / p_1$ e $k(p_1) = \left((p_1 - 1)! + 1\right) / p_1$ **dei quali numeratori del secondo membro, il numero primo** p_1 **è, a parte 1, il minore divisore comune.**

Per concludere il paragrafo riportiamo un esempio:
per $p_1 = 7$ e per $p_2 = 5$ da $5^{7-1} - 1 = 15624$, abbiamo $h = 15624 : 7 = 2232$ e da $(7-1)! + 1 = 721$ abbiamo $k = 721 : 7 = 103$. I due numeri 15624 e 721 sono entrambi multipli di 7 ed hanno chiaramente lo stesso 7, a parte 1, come minimo divisore comune. Ora scambiando i valori, cioè per p_1=5 e p_2=7 abbiamo i due numeri multipli 2400 e 25, il cui minimo comune divisore e' 5.

Test di primeità e test parziali di primeità

I primi due test che riportiamo, come noto, sono tratti il primo dal teorema di Wilson, il secondo dal piccolo teorema di Fermat relativi rispettivamente alle congruenze $(p-1)! + 1 \equiv 0 (\mathrm{mod}\, p)$ e $a^{p-1} - 1 \equiv 0 \,(\mathrm{mod}\, p)$ e il terzo dagli sviluppi che abbiamo ottenuto dal teorema di Fermat, in particolare con $p^6 - 1$:

1) per il primo test, il numero *p* è primo se divide senza resto $(p-1)! + 1$;
riportiamo di seguito alcune primeità parziali, pur consapevoli che esse lasciano il tempo che trovano;

2) per il secondo, il numero *p* è primo se divide senza resto $a^{p-1} - 1$, $\forall a \in N$ non divisibile per *p*, però non è sempre vero il contrario;.

3) *p* è primo se ($p^6 - 1$) è divisibile per 7, per 9, per 63, in particolare se *p*=7 allora ($p^6 - 1$) è solo divisibile per 9, se *p*=3 allora ($p^6 - 1$) è solo divisibile per 7. Però se il numero dispari da provare non ha fattori comuni con 7 e/o con 3, allora $d^6 - 1$ risulta divisibile per 7 e/o per 9, pur non essendo a volte un numero primo, quindi il test risulta valido per ogni numero primo e per ogni numero dispari non primo che non ha fattori comuni con 7 e/o con 3.

In definitiva solo nel caso 1) noto come teorema di Wilson, la congruenza $(p-1)!+1 \equiv 0 (\text{mod } p)$, rappresentando una condizione necessaria e sufficiente affinché *p* sia primo, costituisce l'unica proprietà caratteristica dei numeri primi, per cui abbiamo che "un numero *p* è primo se soddisfa a questa congruenza", cioè se $(p-1)!+1$ è divisibile per *p*.

Tanto nel caso 2) che nel 3) si può verificare la divisibilità per un *p* primo ma anche per un numero dispari composto da due o più fattori primi diversi da *p* in 2) e diversi da 7 o da 3 nel caso 3). Analoghe primeita` parziali abbiamo riscontrate con altre due congruenze per $p \neq 5, \text{in } p^4 - 1 = 0 (\text{mod} 5)$ e per $p \neq 3$, in $3(p^2 - 1) \equiv 0 (\text{mod } 9)$ e con il teorema di Fermat di parziali possiamo trovarne quante ne vogliamo.

.

Generalità delle argomentazioni esposte

Tutto quanto esposto avanti trova fondamento nella teoria dell'aritmetica modulare ed anche nella teoria dei gruppi.
Il fatto che siano venuti fuori tutti 1 dalle quarte potenze dei primi mod 10 e mod 12, o dalle seste potenze dei numeri primi mod 9 non è affatto una singolarità, perché ad es. anche le potenze di 8 dei primi mod 20 danno sempre 1; infatti se prendiamo i numeri della relativa classe di resti 1,3,7,9,11,13,17,19 che sono nel numero di otto e li eleviamo ad 8, avremo sempre 1 come resto. Ciò accade per tutti gli infiniti moduli *x* per il motivo che cercheremo di spiegare qui di seguito.
Sia dato $d \in N$ con $d \geq 2$, perché due numeri *a, b* < *d*, con *a* e *b* primi con *d*, $(a \cdot b)$ è primo con *d*, allora $\text{res}_d (a \cdot b)$ è primo con *d*. Infatti $a \cdot b = q \cdot d + \text{res}_d (a \cdot b)$.
In aggiunta, precisiamo che *a* è primo con *d*, ma ciò non significa che $\text{res}_d (a) = 1$, perché è $\text{res}_d (a) = c \neq 1$, quindi *a* è primo con *d* se e solo se $\text{rest}_d (a)$ è primo con *d* : ad esempio se *a*=14 e *d*=9 abbiamo *c*=5, non c=1. Quanto detto trova fondamento nel fatto che se $a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ e *d*=*x*, da $a = q \cdot d + \text{res}_d (a)$, con $0 \leq \text{res}_d (a) < d$, ad esempio per *a*=44, *q*=3, *d*=12 e $\text{res}_d (a) = 8$ abbiamo $44 = 3 \cdot 12 + 8$.

Inoltre osserviamo che ogni numero che costituisce la classe dei resti di ogni modulo *x*, ad es. del mod 9, cioè 1, 2, 4, 5, 7, 8, moltiplicato per tutti gli altri dà sempre un numero della stessa classe, come si può riscontrare da 4x1=4, 4x2=8, 4x4=7, 4x5=2, 4x7=1, 4x8=5, come abbiamo dai prodotti di un numero della classe dei resti mod 8 per tutti gli altri della stessa classe che sono 1, 3, 5, 7 , cioè ad es. se prendiamo il fattore 7 abbiamo 7x1=7, 7x3=5, 7x5=3, 7x7=1, i cui prodotti sono sempre nella stessa classe di resti, ecc.
Se ora ci rifacciamo alla "Teoria dei gruppi" e consideriamo ad es. $(G, \cdot)$ con ***G*** un insieme e (.) un'operazione binaria di ***G*** , si dice che $(G, \cdot)$ e` un gruppo quando:
l'operazione (.) è associativa, cioe` $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
in ***G*** c'e` un elemento neutro indicato con 1;
$\forall a \in G$, in ***G*** c'è un inverso *b* di *a* indicato con a^{-1} con $a \neq b$, per cui $a \cdot b = 1 = b \cdot a$.

Richiamando il teorema che dice "In un gruppo ogni elemento è cambiabile, da $a \cdot b = a \cdot c$ si ottiene $b = c$, in quanto possiamo moltiplicare per a^{-1} entrambi i membri ed avere $a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c$, cioè, come detto, *b*=*c*.

Ora, essendo per il teorema di Wilson $(p-1)!+1 \equiv 0 \bmod p$, da $(p-1)!+1-p \equiv 0 \bmod p$ abbiamo $(p-1)! = p-1$, ad es. per *p=7* abbiamo $(7-1)! = 7-1; (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)_7 = 6$, ovvero $720 \equiv 6 \bmod 7$, cioè con 6 che è il resto della divisione 720: 7; da $1 \cdot_7 2 \cdot_7 3 \cdot_7 4 \cdot_7 5 \cdot_7 6 = 6$, a parte gli estremi 1 e 6 che sono accoppiati con gli inversi di se stessi, gli altri numeri sono accoppiati a due a due in modo da essere l'uno inverso dell'altro, per cui dai prodotti abbiamo sempre 1. Quanto detto sopra possiamo verificarlo con gli accoppiamenti $(2 \cdot 4)_7 = 1$ e $(3 \cdot 5)_7 = 1$.

Riportiamo un altro esempio per *p=11* , con il prodotto mod 11, cioè
$1 \cdot_{11} 2 \cdot_{11} 3 \cdot_{11} 4 \cdot_{11} 5 \cdot_{11} 6 \cdot_{11} \cdot 7_{11} \cdot 8 \cdot_{11} 9 \cdot_{11} 10 = 10$, da cui a parte gli accoppiamenti estremi di se stessi 1 e 10 si hanno altri quattro accoppiamenti $(2 \cdot 6)_{11} = 1$, $(3 \cdot 4)_{11} = 1$, $(5 \cdot 9)_{11} = 1$, $(7 \cdot 8)_{11} = 1$.
Infine dal teorema di Wilson $(p-1)!+1 \equiv 0 (\bmod p)$ abbiamo $(p-1)!+1-p \equiv 0 (\bmod p)$, per cui possiamo scrivere $(p-1)!_p = p-1$ e quindi $\forall p$, $(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod p$, che da` $p^2 - 2p \equiv 0 \pmod p$, cioè col binomio p^2-$2p$ che e' divisibile per *p*, ma ciò è possibile per ogni numero naturale.

Conclusioni

Dopo aver redatto il presente articolo constatiamo di aver detto quasi nulla di originale, ma crediamo che l'esposizione dei vari argomenti con le varie osservazioni potranno essere una esercitazione didattica per un lettore desideroso di informarsi.

Lecce, gennaio 2010

Bibliografia

G. Aprile,V. Marseguerra, A. Pietrosanti, S. Villatico – "Matematiche Complementari". Vol. II. Edizioni Giorgio Baryes. Roma 1961
G. Carolla – "Alcune regolarità dai numeri primi", pubblicato sui siti: www.gruppoeratostene.com e www.maecla.it . 2009.