Mathesis Nazionale - Scuola estiva

Telese, 27-30 Luglio 2015

Il Gioco nella Didattica della Matematica

Alessio Russo
Seconda Università di Napoli
alessio.russo@unina2.it

"Gli uomini non sono mai più ingegnosi che nell'invenzione dei giochi; l'ingegno si trova a suo agio …. Dopo i giochi che dipendono unicamente dai numeri, vengono i giochi in cui entra la posizione … Dopo i giochi in cui entrano solo il numero e la posizione, verrebbero i giochi in cui entra il moto … Infine, sarebbe desiderabile che si avesse un corso intero di giochi, trattati matematicamente."

(G.W. Leibnitz, 1646-1716)

Questo tipo di matematica è seria e piena di legittimità, tanto è vero che su di essa si può basare una proposta didattica, e una delle più sensate, che ha tanti sostenitori nei più diversi tempi e contesti [...] I giochi non sembrano diversi dai tradizionali esercizi, se non forse perché sono di tipo più logico e linguistico e meno numerico, in generale, e questo argomento gioca tutto a loro favore. La differenza rispetto agli esercizi è che divertono, e non è cosa da poco [...] in primo luogo rappresentano una sfida, e secondariamente la soluzione di solito presenta un elemento di sorpresa. La sorpresa consiste o nel fatto che una risposta proprio ci sia, o nel fatto che la risposta è contraria a ciò che ci si attende. (***G. Lolli***, *Il Riso di Talete*)

“I giochi matematici sono un veicolo quanto mai utile per diffondere la bellezza e l’utilità della matematica e per far capire che bellezza e utilità vanno ben al di là dei confini delle aule scolastiche.” (M. Gardner, 1914-2010)

“La Matematica è un gioco che segue alcune semplici regole, giocato con segni senza senso sulla carta.” (D. Hilbert, 1862-1946)

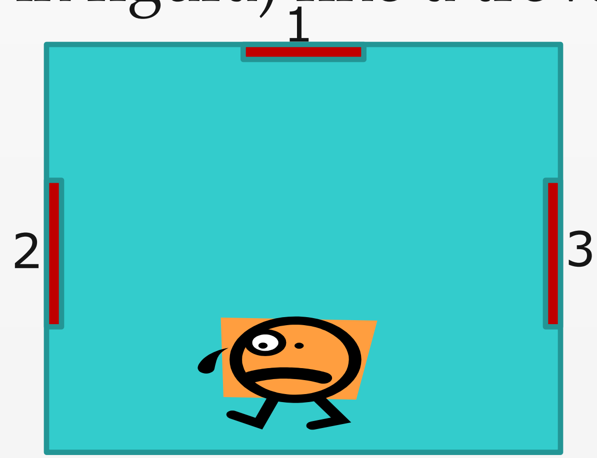
Qualche gioco matematico

Identità nascoste

- Scrivete il vostro numero di cellulare.
- Riscrivetelo invertendo le sue cifre.
- Sottraete il più piccolo dal più grande.
- Sommate le cifre del numero ottenuto.
- Ripetete quest'ultima operazione finché non ottenete un numero di una sola cifra.

Libertà va cercando …

Il nostro eroe è prigioniero in una stanza con tre porte. Su un foglio trova scritto che aprendo due di queste porte è definitivamente perduto. C'è solo una porta che lo conduce alla libertà. Per individuarla deve sostituire dei numeri (***quali?***) al posto delle lettere X e Y (con X>Y) nella formula X^3Y-XY^3. Fatto ciò, deve sommare le cifre del numero ottenuto, ripetendo l'operazione finché non trova un numero di una sola cifra. Infine, utilizzando il numero ottenuto, conta partendo dal numero 1 in senso antiorario (come in figura) fino a trovare la porta giusta.



A volte ritornano

- Considerate un numero di tre cifre abc.
- Affiancatelo a se stesso, ottenendo il numero abcabc.
- Dividete questo numero per 7.
- Dividete il numero ottenuto per 11.
- Infine, dividete l’ultimo numero per 13.

Tutte le strade portano …
allo stesso numero

- Considerate un numero di 3 cifre abc con la sola condizione che a>c+1.
- Scrivetelo in ordine inverso, quindi sottraete il più piccolo dal più grande.
- Sia x è il numero ottenuto.
- Invertite le cifre di x e sommate il numero ottenuto ad x.

Divisibilità

Siano a e b dei numeri interi. Si dice che a divide b (e si scrive $a|b$) se esiste un intero t tale che $b=at$.

Proprietà - Siano a,b,c dei numeri interi. Allora:

1. $a|a$.
2. Se $a|b$ e $b|c$, allora $a|c$.
3. Se $a|b$ e $b|a$, allora $a\in\{b,-b\}$.
4. Se $a|b$ e $a|c$, allora $a|bx+cy$, per ogni $x,y\in Z$.

Algoritmo della divisione euclidea

Siano $a, b \in Z$, con $b \neq 0$. Allora esistono degli interi q ed r tali che $a = bq + r$ e $0 \leq r < |b|$.
Inoltre, i numeri q ed r sono univocamente determinati dalle precedenti condizioni.

Gli interi q ed r si chiamano rispettivamente quoziente e resto della divisione di a e b.

Massimo comune divisore

Siano a e b dei numeri interi non nulli. Si dice massimo comune divisore di a e b , e si denota col simbolo (a,b), un intero non nullo d tale che:

1. $d \mid a$ e $d \mid b$.
2. Se c è un intero tale che $c \mid a$ e $c \mid b$, allora $c \mid d$.

Gli interi a e b si dicono coprimi se 1 e -1 sono i soli divisori ad essi comuni.

Si dimostra che dati gli interi non nulli a e b esistono due soli massimi comuni divisori d e –d . Inoltre, sussiste la seguente identità di Bezout: $d=ax+by$, con x e y interi opportuni. Infine, se a e b sono numero interi coprimi che dividono un numero c, allora anche $ab \mid c$.

Alcuni esercizi

1. Sia z un numero intero. Provare che esiste un intero q tale che $z \in \{3q, 3q-1, 3q+1\}$.
2. Provare che tra tre numeri interi consecutivi uno di essi è divisibile per 3.
3. Provare che per ogni intero n risulta $3 \mid n^3-n$.
4. Provare che $3 \mid x^3y-xy^3$ per ogni $x,y \in Z$.
   Spiegare il gioco "Libertà va cercando …".
5. Provare che se a e b sono numeri pari consecutivi, allora uno di essi è multiplo di 4.
6. Provare che il prodotto di 6 interi consecutivi è divisibile per $2^4 \cdot 3^2 \cdot 5$.

7. (Gare Provinciali, 2009) – Determinare il massimo intero positivo k tale che $k^2 \mid n!/(n-6)!$ per ogni $n>6$.

Risoluzione – Poniamo $f(n)=n!/(n-6)!=(n-5)(n-4)(n-3)(n-2)(n-1)n$. Per l'Esercizio 6 si ha che $2^4 \cdot 3^2 \cdot 5 \mid f(n)$ per ogni $n>6$. Sia m il massimo intero positivo tale che $m \mid f(n)$ per ogni $n>6$. Allora $2^4 \cdot 3^2 \cdot 5 \leq m$. D'altra parte, posto $a=7$ e $b=13$, risulta $f(a)=2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7= 2^4 \cdot 3^2 \cdot 5 \cdot 7$ e $f(b)=8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13=2^5 \cdot 3^3 \cdot 5 \cdot 11 \cdot 13$. Poiché $m \mid f(a)$ e $m \mid f(b)$, ed inoltre il massimo comune divisore di f(a) e f(b) è dato da $2^4 \cdot 3^2 \cdot 5$, allora $m= 2^4 \cdot 3^2 \cdot 5$. Ne segue che $k^2= 2^4 \cdot 3^2$ e quindi $k= 2^2 \cdot 3 \cdot$

Definizione – Un numero intero p si dice **primo** se p>1 e gli unici divisori di p sono -1, +1, -p e p. Sia $\mathcal{P}$ l'insieme dei numeri primi.

- Se n è un numero intero maggiore di 1, allora esiste un $p \in \mathcal{P}$ tale che $p \mid n$. In particolare, $\mathcal{P} \neq \emptyset$.
- Teorema di Euclide (300 a. C.)

  Esistono infiniti numeri primi.
- Teorema Fondamentale dell'Aritmetica

  Ogni numero intero n>1 si decompone nel prodotto di numeri primi. Tale decomposizione è unica a meno dell'ordine dei fattori.

8. Determinare tutti i primi p tali che $(p-6)^2+1$ è primo.

Risoluzione – Se $p=2$, allora $(2-6)^2+1=17$ è primo. Sia dunque p dispari. Allora p è del tipo $p=2k+1$, con k intero opportuno. Ne segue che $(p-6)^2+1 =(2k-5)^2+1$ è pari, e dovendo essere primo risulta $(2k-5)^2+1=2$. Allora $2k-5=\pm1$, e quindi $k=2$ oppure $k=3$. Nel primo caso $p=5$, nel secondo $p=7$.

Piccolo Teorema di Fermat (1640)

Sia p un numero primo. Allora per ogni numero intero a risulta che p è un divisore a^p-a. In particolare, se a e p sono coprimi, allora $p \mid a^{p-1}-1$.

Si dimostra che per ogni intero a risulta $561 \mid a^{561}-a$. D'altra parte, $561=3\cdot 11\cdot 17$ non è un numero primo. Pertanto, il Piccolo Teorema di Fermat non è un Criterio di Primalità.

9. (Cortona, 1991) Determinare tutti i numeri primi p tali che $p | 2^p+1$.

Risoluzione – Per il Piccolo Teorema di Fermat $p | 2^p-2$. D'altra parte, poiché $p | 2^p+1$, allora $p | (2^p+1-(2^p-2))$. Allora $p=3$.

10. Siano n e p numeri primi tali che $p | 2^n-1$. Provare che $n | p-1$.

Risoluzione – Per il Piccolo Teorema di Fermat $p | 2^{p-1}-1$. D'altra parte, poiché $p | 2^n-1$, allora p divide il massimo comune divisore di $2^{p-1}-1$ e 2^n-1. Ma $(2^{p-1}-1, 2^n-1)=2^{(p-1,n)}-1$ (provarlo!). Inoltre n è primo, e quindi $(p-1,n)$ è 1 oppure $n | p-1$. Nella prima eventualità si ha la contraddizione $p | 1$. Dunque $n | p-1$.

Qual è il più grande primo attualmente conosciuto?

$$2^{57885161}-1$$

Un numero primo della forma 2^n-1 si dice primo di Mersenne.

11. Provare che se 2^n-1 è primo di Mersenne, allora anche n è primo.

- E’ il 48° primo di Mersenne.
- E’ costituto da 17.425.170 cifre.
- Sono necessarie circa 10000 pagine di un normale testo per contenerlo.
- E’ il risultato del lavoro di centinaia di volontari tramite Internet.

(Progetto GIMPS: www.mersenne.org)

- E’ stato trovato il 25 gennaio 2013 da C. Cooper della University of Central Missouri.

Sistemi di numerazione

Sia b un numero intero >1. Una rappresentazione in base b di un numero naturale n è una (k+1)-pla ordinata $(a_0,a_1,\ldots,a_k)$ tale che k è un intero non negativo, per ogni $i\in\{0,1, \ldots ,k\}$ $0\le a_i<b$, $a_k\neq 0$ e

$$n=a_kb^k+a_{k-1}b^{k-1}+\ldots+a_1b+a_0.$$

Per indicare l'espressione precedente si scrive $n=(a_ka_{k-1}\ldots a_1a_0)_b$. In particolare, se b=10, allora si scrive semplicemente $n= a_ka_{k-1}\ldots a_1a_0$.

Teorema

Fissato un numero naturale $b>1$ e un intero $n>0$, esiste una rappresentazione in base b di n. Inoltre, se

$$a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 = n = c_l b^l + c_{l-1} b^{l-1} + \ldots + c_1 b + c_0$$

sono rappresentazioni in base b di n, allora $k=l$ e per ogni $i \in \{0,1, \ldots ,k\}$ risulta $a_i=c_i$.

Un esempio

$$366 = 2 \cdot 183 + 0$$
$$183 = 2 \cdot 91 + 1$$
$$91 = 2 \cdot 45 + 1$$
$$45 = 2 \cdot 22 + 1$$
$$22 = 2 \cdot 11 + 0$$
$$11 = 2 \cdot 5 + 1$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$
$$1 = 2 \cdot 0 + 1.$$

Pertanto $366=(101101110)_2$

12. Sia b un intero >3. Si dimostri che $(1331)_b=[(11)_b]^3$.

13. (Gara Nazionale, 1998) Provare che nel sistema di numerazione in base 9 tutti i termini della successione 1, 11, 111,…, 11…11 (n cifre) sono "triangolari", cioè del tipo k(k+1)/2 con k numero intero.

Risoluzione – Poniamo a_n=11…11 (n cifre). Poiché tale numero è scritto in base 9, allora risulta $a_n=1+9+\ldots+9^{n-1}=$
$=(9^n-1)/8=(3^n-1)(3^n+1)/8$. Sia k un intero tale che $3^n-1=2k$.
Allora $3^n+1=2(k+1)$, da cui l'asserto.

14. Spiegazione del gioco "A volte ritornano".

Risulta:

$$abcabc=c+b10+a10^2+c10^3+b10^4+a10^4=$$

$$(1+10^3)c+(1+10^3)10b+(1+10^3)10^2a = (1001)(abc).$$

Inoltre, $1001= 7{\cdot}11{\cdot}13$.

$$(1001)^0=1$$
$$(1001)^1=1001$$
$$(1001)^2=1002001$$
$$(1001)^3=1003003001$$
$$(1001)^4=1004006004001$$

.....

15. Spiegazione del gioco "Tutte le strade portano allo … stesso numero".

Risulta:

$$abc=c+b10+a10^2 \text{ e } cba=a+b10+c10^2.$$

Da ciò segue:

$$x=abc-cba=a10^2+b10+c-(c10^2+b10+a)=$$
$$(a-1)10^2+10^2+(b-1)10+(10+c)-(c10^2+b10+a)=$$
$$(a-1)10^2+(10+b-1)10 +(10+c)-(c10^2+b10+a)=$$
$$(a-1-c)\ 10^2+9\cdot 10+(10+c-a).$$

Posto $y=(10+c-a)10^2+9\cdot 10+(a-1-c)$, si ha:

$$x+y= 9\cdot 10^2+18\cdot 10+9=9\cdot 10^2+10^2+8\cdot 10+9=10^3+0\cdot 10^2+8\cdot 10+9=$$

1089

Simpatici collegamenti

Sia $\boldsymbol{p=abc}$ un numero primo di tre cifre (in base 10). Sia poi $\boldsymbol{f=ax^2+bx+c}$ il polinomio avente per coefficienti le cifre di $\boldsymbol{p}$.

- Cosa si può dire riguardo all'irriducibilità di f in $\boldsymbol{Z[x]}$? E in $\boldsymbol{Q[x]}$ e in $\boldsymbol{R[x]}$?
- E' possibile generalizzare le considerazioni precedenti?

Aritmetica dell'orologio

Fare i calcoli, anziché con i numeri interi, con "blocchi" di numeri.

Gauss, 1801, Disquisitiones Arithmeticae.

Definizione

Sia n un numero intero. Si dice che dei numeri interi a e b sono congrui modulo n, e si scrive

$$a \equiv b \pmod{n},$$

se n divide $a - b$.

Esempi: $37 \equiv 1 \pmod{12}$

$35 \equiv 3 \pmod{8}$

Proprietà fondamentali

Siano a,b,c e d dei numeri interi. Se n è un intero non nullo, allora risulta:

- $a \equiv a \pmod{n}$.
- Se $a \equiv b \pmod{n}$, allora $b \equiv a \pmod{n}$.
- Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, allora $a \equiv c \pmod{n}$.
- $a \equiv \mathrm{rest}(a,n) \pmod{n}$, dove rest(a,n) è il resto della divisione euclidea di a e n.
- Se $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, allora $a + c \equiv b + d \pmod{n}$ e $a \cdot c \equiv b \cdot d \pmod{n}$.

Queste ultime proprietà (leggi di compatibilità) rendono la congruenza simile, nei calcoli, all'*uguaglianza*.

Qualche applicazione

- 47 divide $2^{23} - 1$

Si ha $23=2 \cdot 10+3$. Ora $2^{10} \equiv 37 \pmod{47}$, e così $2^{20} \equiv 37^2 \equiv 6 \pmod{47}$. Ne segue che $2^{23} \equiv 6 \cdot 2^3 \equiv 1 \pmod{47}$.

- 341 divide $2^{341} - 2$

Poiché $2^{10} \equiv 1 \pmod{341}$, allora risulta anche $2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}$. Ma ovviamente, $2 \equiv 2 \pmod{341}$, e quindi $2^{341} \equiv 2 \pmod{341}$.

16. Qual è la cifra delle unità del numero

$$2^{(2^1)} + 2^{(2^2)} + 2^{(2^3)} + \cdots + 2^{(2^{2012})} ?$$

Risoluzione – Osserviamo innanzitutto che dato un numero

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

allora $n \equiv a_0 \pmod{10}$, sicché $a_0 = \mathrm{rest}(n,10)$. Denotiamo con n il nostro numero. Poiché ogni addendo di n (a partire dal secondo) è il quadrato del precedente, ed inoltre $2^4 \equiv 6 \pmod{10}$ e $6^2 \equiv 6 \pmod{10}$, allora $n \equiv 4 + 2011 \cdot 6 \pmod{10}$.
Ma $2011 \equiv 1 \pmod{10}$, e quindi $n \equiv 0 \pmod{10}$. Dunque, la cifra delle unità di n è 0.

Qualche Criterio di Divisibilità

Chiaramente, se n e d sono numeri naturali, allora

$$d \mid n \Leftrightarrow n \equiv 0 \pmod{d}.$$

Ne segue che se t è un numero naturale tale che $n \equiv t \pmod{d}$, allora

$$d \mid n \Leftrightarrow d \mid t.$$

Sia n>1 un numero naturale che abbia la seguente rappresentazione decimale:

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

Poiché $10 \equiv 1 \pmod 9$ e $10 \equiv 1 \pmod 3$, allora, utilizzando le leggi di compatibilità, si ha:

Criterio di divisibilità per 3 e per 9

Il numero naturale $n= a_k a_{k-1} \ldots a_1 a_0$ è divisibile per 3 (rispettivamente, per 9) se e solo se $3 \mid a_k+a_{k-1}+\ldots+a_1+a_0$ (rispettivamente, $9 \mid a_k+a_{k-1}+\ldots+a_1+a_0$.

Poiché $10 \equiv 0 \pmod{2}$ e $10 \equiv 0 \pmod{5}$, allora per le leggi di compatibilità si ha:

Criterio di divisibilità per 2 e per 5

Il numero naturale $n = a_k a_{k-1} \ldots a_1 a_0$ è divisibile per 2 (rispettivamente, per 5) se e solo se a_0 è pari (rispettivamente, a_0 è 0 o 5).

Poiché $10^s \equiv 0 \pmod 4$ e $10^s \equiv 0 \pmod{25}$ se $s>1$, allora per le leggi di compatibilità si ha:

Criterio di divisibilità per 4 e per 25

Il numero naturale $n= a_k a_{k-1} \ldots a_1 a_0$ è divisibile per 4 (rispettivamente, per 25) se e solo se $a_1 a_0$ è divisibile per 4 (rispettivamente, per 25).

Poiché

$10 \equiv 3 \pmod 7$,

$10^2 \equiv 3\cdot 10 \equiv 2 \pmod 7$,

$10^3 \equiv 2\cdot 10 \equiv 6 \equiv -1 \pmod 7$,

$10^4 \equiv (-1)\cdot 10 \equiv -3 \pmod 7$,

$10^5 \equiv (-3)\cdot 10 \equiv -2 \pmod 7$,

$10^6 \equiv (-2)\cdot 10 \equiv 1 \pmod 7$,

$\ldots\ldots,$

allora $a_0 + a_1 10 + \ldots + a_{k-1}10^{k-1} + a_k 10^k \equiv$

$$a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \ldots \pmod 7.$$

Criterio di divisibilità per 7

Il numero naturale $n=a_k a_{k-1} \ldots a_1 a_0$ è divisibile per 7 se e solo se 7 divide il numero $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \ldots$.

17. (Giochi di Archimede, 1990) Sapendo che un numero di 6 cifre decimali abcdef è divisibile per 7, dimostrare che risulta anche $7 \mid bcdefa$.

Risoluzione – Poniamo m=bcdefa. Per il criterio di divisibilità per 7 esiste un intero k tale che f+3e+2d-c-3b-2a=7k . D'altra parte, m $\equiv$ a+3f+2e-d-3c-2b $\equiv$ a+3(f+3e+2d-c-3b)= a+3(7k+2a)=7(a+3k). Ne segue che 7|m.

Poiché $10 \equiv -1 \pmod{11}$, $10^2 \equiv 1 \pmod{11}$, $10^3 \equiv -1 \pmod{11}$, $10^4 \equiv 1 \pmod{11}$, ecc., allora per le leggi di compatibilità si ha:

Criterio di divisibilità per 11

Il numero naturale $n= a_k a_{k-1} \dots a_1 a_0$ è divisibile per 11 se e solo se 11 divide il numero $a_0 - a_1 + a_2 - a_3 + \dots + (-1)^k a_k$.

18. (Giochi di Archimede, 2003) Un numero $n=a_k a_{k-1} \ldots a_1 a_0$ si dice *palindromo* se $a_k=a_0$, $a_{k-1}=a_1$, e così via. Determinare il più grande numero primo palindromo con un numero pari di cifre.

Risoluzione – Per il criterio di divisibilità per 11 un numero palindromo con un numero pari di cifre è divisibile per 11. Ciò comporta che la risposta è 11.

Il più grande primo palindromo con un numero dispari di cifre, attualmente noto, è stato trovato nel 2014 da David Broadhurst. Ha 320237 cifre!

19. Spiegazione del gioco "Identità nascoste"

Sia $n=a_k a_{k-1} \ldots a_1 a_0 = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0$ il numero di cellulare. Allora

$$n \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod 9.$$

Se m è il numero ottenuto invertendo le cifre (o più in generale, permutandole), allora

$$n - m \equiv 0 \pmod 9.$$

Supponiamo che $n-m \neq 0$. La somma delle cifre di $n-m$ è un multiplo di 9, e se si ripete l'operazione si ottiene sempre un multiplo di 9. Alla fine quindi si otterrà 9.