PREPARAZIONE OLIMPIADI
(LICEO ROITI 05-11-2014)

PH. ELLIA

Indice

Introduzione.

Gli esercizi dimostrativi sono generalmente di due tipi: aritmetici o geometrici. Qui ci occuperemo degli esercizi di aritmetica. La conoscenza del Teorema Fondamentale dell'Aritmetica (fattorizzazione in numeri primi), del Lemma di Gauss e le prime nozioni sulle congruenze possono essere molto utili nella risoluzione dei problemi. Rimandiamo agli appunti ([1], scaricabili dal sito www.unife.it/utenti/philippe.ellia) dell'incontro del 12-02-2014 per le dimostrazioni non esposte qui.

1. Il Teorema Fondamentale dell'Aritmetica.

Ricordiamo che un numero intero $n > 1$ è *primo* se i suoi unici divisori sono 1 e n (esempio: $2, 3, 5, 7$ sono i primi < 10).

Quindi un numero intero $n > 1$ *non è primo* se e solo se $n = ab$ con $1 < a \leq b < n$ (n ammette dei divisori non banali).

Sia $Div(n) = \{d_1 = 1, d_2, ..., d_r = n\}$ l'insieme dei divisori di n con $1 < d_2 < ... < d_r$. Allora d_2 è sempre un numero primo. Infatti se non lo fosse si avrebbe $d_2 = ab$ con $1 < a, b < d_2$. Ma $a \mid d_2$ e $d_2 \mid n \Rightarrow a \mid n$, contro la definizione di d_2 ($1 < a < d_2$). Quindi *il più piccolo divisore > 1 di un intero $n > 1$ è sempre un numero primo. In particolare ogni numero > 1 ammette un divisore primo.*

I divisori di un numero, n, sono simmetrici rispetto a $\sqrt{n}$: se $n = ab, a \leq b$, allora $a \leq \sqrt{n}$ (altrimenti $ab \geq a^2 > n = (\sqrt{n})^2$). Nello stesso modo $b \geq \sqrt{n}$. Quindi se $\tau(n)$ indica il numero di divisori di n abbiamo: $\tau(n)$ è dispari $\Leftrightarrow n$ è un quadrato. Detto ciò: *n è primo $\Leftrightarrow n$ non ammette nessuno divisore d con $1 < d \leq \sqrt{n}$.*

Il teorema fondamentale dell'aritmetica (TFA) afferma che ogni intero $n > 1$ si scrive in modo unico (a meno dell'ordine dei fattori) come un prodotto di numeri primi. Per esempio $12 = 2.2.3 = 2^2.3$, $15 = 3.5$ ecc...

Teorema 1.1. *Ogni intero $n > 1$ si scrive in modo unico (a meno dell'ordine dei fattori) come un prodotto di numeri primi:*

$$n = p_1^{a_1}.p_2^{a_2}...p_r^{a_r}\ ;\ a_i \geq 1 \forall i. \tag{1}$$

Se decidiamo di ordinare i primi p_i in modo crescente: $p_1 < p_2 < ... < p_r$, allora la fattorizzazione è unica.

Questo risultato permette di capire alcune cose interessanti sui numeri. Per esempio:

Lemma 1.2. (Lemma di Gauss.)
(1) Se un numero primo p divide un prodotto di due fattori, allora divide uno dei due fattori, cioè se $p \mid a.b$, allora $p \mid a$ o $p \mid b$ ($m \mid k$ significa m divide k).
(2) Più generalmente, se un numero primo divide un prodotto, allora divide uno dei fattori, cioè se $p \mid a_1a_2...a_r$, allora esiste i tale che $p \mid a_i$.

(3) Più generalmente ancora: se $n \mid ab$ *e se* $(n, a) = 1$ *(*n *e* a *sono primi tra di loro), allora* $n \mid b$.

Gli interi a, b sono *primi tra di loro* se il loro MCD (massimo comune divisore) vale uno (in simboli: $(a, b) = 1$). Questo è equivalente a dire che non esiste nessun primo p che divide sia a che b.

Conoscendo la fattorizzazione in primi è facile trovare l'MCD di due numeri a, b. Possiamo sempre scrivere $a = p_1^{a_1} ... p_r^{a_r}$, $b = p_1^{b_1} ... p_r^{b_r}$, $a_i, b_i \geq 0$ (usiamo tutti i primi che compaiono in a o in b, se p_i compare in a ma non in b, allora $b_i = 0$).

Allora $(a, b) = p_1^{c_1} ... p_r^{c_r}$, dove $c_i = min\{a_i, b_i\}$ (qui $(a, b) =$ MCD di a e b).

Invece il minor comune multiplo (mcm) è $p_1^{d_1} ... p_r^{d_r}$, dove $d_i = max\{a_i, b_i\}$.

Nel corso della dimostrazione del TFA è dimostrato ([1], p.5) che se d è l'MCD di a e b allora esistono due numeri u, v (positivi o negativi) tali che $d = au + bv$. Il viceversa non è vero: sia $a = 12, b = 3$, allora $6 = 1.12 - 2.3$, ma $(12, 3) = 3 \neq 6$. Quello che è vero è: se $d = au + bv$, allora $M \mid d$, dove M è l'MCD di a, b.

L'interesse della faccenda è che se si riesce a trovare u, v tali che $1 = au + bv$, allora si può concludere che $(a, b) = 1$. Per esempio due interi consecutivi $n, n + 1$ sono sempre primi tra di loro $(1.(n + 1) - 1.n = 1)$.

Esercizio 1. *(1) Sia* p *un numero primo. Per ogni intero* n, $(n + p, n)$ *vale* 1 *o* p. *Se* $n < p$, $(n + p, n) = 1$.
(2) Mostrare che $(60, 161) = 1$.

Dimostrazione. (1) Abbiamo $(n + p) - n = p$, quindi se $d \mid n + p$ e $d \mid n$, allora $d \mid p$, quindi $d = 1$ o $d = p$. Se $n < p$, allora $p \nmid n$, quindi $(n + p, n) = 1$.
(2) Abbiamo $161 - 60 = 101$ e 101 è primo (basta verificare che nessun numero dispari < 10 divide 101, cioè 3,5,7,9 quindi basta verificare che 3,5,7 non dividono 101). Quindi $(60, 161) = (60, 60 + 101) = 1$ (siamo nel caso $n = 60, p = 101$ con $n < p$).

In un altro modo: $60 = 2^2 \times 3 \times 5$, $161 = 7 \times 13$; non hanno fattori primi comuni, quindi sono primi tra di loro (in realtà, trovata la fattorizzazione di 60, basta verificare che 2,3,5 non dividono 161). $\square$

1.1. **I divisori di un numero.**

Un'altra cosa interessante: se $n = p_1^{a_1}...p_r^{a_r}$ è la fattorizzazione di n (quindi $a_i > 0$) , allora $d \mid n$ se solo se $d = p_1^{c_1}...p_r^{c_r}$, con $0 \leq c_i \leq a_i$ (nb: bisogna autorizzare $c_i = 0$, per esempio se $c_i = 0, \forall i$ si ottiene $d = 1$ che divide ogni n). Siccome ci sono a_i+1 possibilità per c_i e siccome i c_i determinano univocamente d, vediamo che il numero di divisori di n è: $(a_1 + 1)(a_2 + 1)...(a_r + 1)$. Per esempio $12 = 2^2.3$ ha $3.2 = 6$ divisori che sono $1, 2, 3, 4, 6, 12$.

Se $n = p^a$ è una potenza di un numero primo i suoi divisori sono $1, p, p^2, ..., p^a$. Siccome $1 + p + p^2 + ... + p^a = \dfrac{p^{a+1} - 1}{p - 1}$, se indichiamo con $\sigma(n)$ la somma di tutti i divisori di n, abbiamo $\sigma(p^a) = \dfrac{p^{a+1} - 1}{p - 1}$.

Abbiamo usato:

Lemma 1.3. *Se $a \neq 1$ allora $1 + a + a^2 + ... + a^n = \dfrac{a^{n+1} - 1}{a - 1}$.*

Dimostrazione. Abbiamo $(a-1)(1+a+...+a^n) = (a+...+a^n+a^{n+1}) - (1+a+...+a^n) = a^{n+1} - 1$. Se $a \neq 1$ si ottiene il risultato. □

Adesso sia $n = p_1^{a_1}...p_r^{a_r}$ la fattorizzazione di n. Se svolgiamo il prodotto:

$$(1 + p_1 + ... + p_1^{a_1})(1 + p_2 + ... + p_2^{a_2})...(1 + p_r + ... + p_r^{a_r})$$

otteniamo $\sum p_1^{c_1}...p_r^{c_r}$ dove la somma è fatta su tutti i possibili c_i tali che $0 \leq c_i \leq a_i$, cioè otteniamo la somma di tutti i divisori di n. Quindi

$$\sigma(n) = \prod_{i=1}^{r} \sigma(p_i^{a_i}) = \prod_{i=1}^{r} \frac{(p_i^{a_i+1} - 1)}{(p_i - 1)}.$$

Per esempio la somma dei divisori di $12 = 2^2.3$ è $(2^3-1).(3^2-1)/2 = 7.4 = 28$.

2. Congruenze.

Due numeri a, b hanno la stessa parità se 2 divide $a-b$, ossia se a e b hanno lo stesso resto nella divisione per 2. I resti possibili nella divisione per 2 sono $0, 1$. Indichiamo con $\overline{0}$ la classe dei numeri pari (quelli che hanno resto 0 nella divisione per 2) e con $\overline{1}$ la classe dei numeri dispari. Allora: $\overline{0}+\overline{0}=\overline{0}$, $\overline{0}+\overline{1}=\overline{1}$ e $\overline{1}+\overline{1}=\overline{0}$. La prima relazione significa che la somma di due numeri pari è un numero pari, la seconda dice che sommando un pari con un dispari si ottiene un dispari e finalmente la terza dice che la somma di due dispari è un pari. Analogamente abbiamo: $\overline{1}.\overline{1}=\overline{1}$, $\overline{1}.\overline{0}=\overline{0}$.

Questo è l'esempio più semplice di *aritmetica modulare*, detta anche aritmetica dell'orologio.

Più generalmente se $n > 1$ è un intero si dice che due numeri a, b sono *congruenti modulo* n se $n \mid a-b$. Questo è equivalente a dire che a e b hanno lo stesso resto nella divisione per n. Si scrive $a \equiv b \pmod n$ (e si legge a equivalente (o uguale) b modulo n). I resti possibili nella divisione per n sono $0, 1, 2, ..., n-1$. Quindi ogni intero a è equivalente modulo n ad un unico numero $r \in \{0, 1, 2, ..., n-1\}$: $a \equiv r \pmod n$ (si dice che r è la classe di resto di a mod. n). Funziona anche se a è negativo. Per esempio $-1 = 3(-1)+2$ quindi $-1 \equiv 2 \pmod 3$.

L'interesse della faccenda è che possiamo calcolare, come abbiamo fatto con i numeri pari e dispari, con le classi di resto modulo n. Il calcolo "modulare" funziona come quello usuale prendendo ogni volta il resto mod. n. Per esempio se $n = 12$, stiamo calcolando sull'orologio: le 14 sono le 2 ecc... Abbiamo:

$$a \equiv b \pmod n \Leftrightarrow a+k \equiv b+k \pmod n \tag{2}$$

abbiamo anche:

$$a \equiv b \pmod n \Rightarrow a.k \equiv b.k \pmod n \tag{3}$$

ATTENZIONE: se $a.k \equiv b.k \pmod n$ NON si può concludere che $a \equiv b \pmod n$. Per esempio: $6.6 \equiv 6.4 \equiv 0 \pmod{12}$, ma $4 \not\equiv 6 \pmod{12}$.

Quindi l'implicazione inversa di (3) è falsa in generale (si può mostrare che è vera se $k \not\equiv 0 \pmod n$ e se n è primo).

Per il calcolo modulo a si può rimpiazzare n con il suo resto nella divisione per a.

Si ricorda la regola: *un numero è divisibile per 3 se e solo se la somma delle sue cifre è divisibile per 3.* Abbiamo $10 \equiv 1 \pmod 3$, quindi $100 = 10 \times 10 \equiv 1.1 \equiv 1 \pmod 3$; vediamo così che $10^k \equiv 1 \pmod 3$. Sia $n = abcd$ (scrittura decimale $a, b, c, d \in \{0, 1, .., 9\}$). Abbiamo $n = a.1000 + b.100 + c.10 + d = a.10^3 + b.10^2 + c.10 + d \equiv a + b + c + d \pmod 3$. Quindi $n \equiv 0 \pmod 3$ (cioè n è divisibile per 3) se e solo se $a + b + c + d \equiv 0 \pmod 3$.

Nello stesso modo un numero è divisibile per cinque se e solo se la sua ultima cifra è 0 o 5. Finalmente e ovviamente, sempre per lo stesso motivo, l'ultima cifra di un numero pari deve essere un numero pari.

Esercizio 2. *Mostrare che la somma delle cifre di* 13^{2014} *non è un multiplo di* 3.

Dimostrazione. Abbiamo $13 \equiv 1 \pmod 3$, quindi $169 = 13^2 \equiv 1.1 \equiv 1 \pmod 3$, più generalmente $13^k \equiv 1 \pmod 3$, $\forall k \geq 1$. Quindi $13^{2014} \equiv 1 \pmod 3$, 13^{2014} non è divisibile per 3 (ha resto uno nella divisione per 3). Pertanto la somma delle sue cifre non è un multiplo di 3. □

Un'altra cosa che può essere utile: un quadrato è congruo a 0 o 1 modulo 4. Infatti sia $n = a^2$. Se $a = 2k$ è pari, $n = 4k^2$, se $a = 2k + 1$ è dispari, $n = 4k^2 + 4k + 1 \equiv 1 \pmod 4$.

Esercizio 3. *Mostrare che 1026 non è un quadrato.*

Proof. Abbiamo $1026 = 4 \times 256 + 2$ quindi $1026 \equiv 2 \pmod 4$ e pertanto non può essere un quadrato. □

3. La formula del binomio.

Consociamo tutti la formula $(x+y)^2 = x^2+2xy+y^2$. Abbiamo anche: $(x+y)^3 = x^3+3x^2y+3xy^2+y^3$. Cosa possiamo dire di $(x+y)^4, (x+y)^5$, più generalmente esiste una formula per $(x+y)^n$? La formula esiste ed è la *formula del binomio*. Prima di enunciarla alcune notazioni. Se $n > 0$ è un intero si pone $n! = 1 \times 2 \times 3 \times ... \times n$ ($n!$ si legge n *fattoriale*). Quindi $1! = 1, 2! = 2, 3! = 6, 4! = 24, 5! = 120, 6! = 720, 7! = 5040$. Come potete vedere $n!$ cresce molto velocemente. Per convenzione $0! = 1$.

Il coefficiente binomiale $\binom{n}{k}$ è definito per $0 \leq k \leq n$ tramite:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{4}$$

Con queste notazioni abbiamo la formula del binomio:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \tag{5}$$

Ci sono vari modi di dimostrare questa formula. Facciamo prima alcune osservazioni. La formula è simmetrica in x, y, quindi il coefficiente di $x^{n-k}y^k$ deve essere uguale a quello di $x^k y^{n-k}$. In effetti si può verificare che $\binom{n}{k} = \binom{n}{n-k}$. Un'altra osservazione più preoccupante: $(x+y)^n = (x+y)(x+y)...(x+y)$, se svolgiamo il prodotto degli n fattori del membro di destra e poi raggruppiamo i termini $x^{n-k}y^k$ è chiaro che il coefficiente che otteniamo è un intero. Cioè $\binom{n}{k}$ è un intero per ogni $k, 0 \leq k \leq n$. Questo non è immediato dalla definizione (4)!

Cerchiamo di capire quello che succede. Nel svolgere il prodotto $(x+y)(x+y)...(x+y)$ si procede nel seguente modo: nel primo fattore si sceglie x o y, nel secondo pure si sceglie x o y, ecc... fino all'ultimo. Se abbiamo scelto k volte x (e quindi $n-k$ volte y), si ottiene un termine $x^k y^{n-k}$. Facendo questo lavoro per tutte le scelte possibili abbiamo svolto il prodotto. Per esempio per ottenere x^n devo scegliere sempre x (e questa è l'unica possibilità). Quindi il coefficiente di x^n è 1. Idem per y^n. Per ottenere $x^{n-1}y$ devo scegliere sempre x, tranne una volta (che prendo y). Quindi devo prendere y una sola volta. In quanti modi posso farlo: in n modi (prendo y nel primo fattore, prendo y nel secondo fattore,..., prendo y nell'ennesimo fattore). Quindi il coefficiente di $x^{n-1}y$ è n.

Vediamo così che il coefficiente di $x^{n-k}y^k$ è il numero di modi di scegliere k elementi in $\{1,2,3,...,n\}$ (i modi di scegliere k volte y tra gli n fattori). Cioè è il numero, C_k^n, di sotto insiemi con k elementi di un insieme con n elementi. Quindi possiamo scrivere:

$$(x+y)^n = \sum_{k=0}^{n} C_k^n x^{n-k} y^k$$

A questo punto è chiaro che C_k^n è un intero e che $C_k^n = C_{n-k}^n$ (ad ogni sotto insieme con k elementi corrisponde un sotto insieme con $n-k$ elementi: il suo complementare; e viceversa).

Rimane da vedere che $C_k^n = \binom{n}{k}$. Questo risulta essenzialmente dal:

Lemma 3.1. *Per $n > 1$, $C_k^n = C_k^{n-1} + C_{k-1}^{n-1}$.*

Dimostrazione. Sia X un insieme con n elementi e sia $x \in X$. Possiamo dividere i sotto insiemi di X con k elementi in due tipi: (a) quelli che contengono x, (b) quelli che non contengono x.

Se I è un insieme di tipo (a), allora $I \setminus \{x\}$ è un sotto insieme con $k-1$ elementi di $X \setminus \{x\}$, un insieme con $n-1$ elementi. Ci sono C_{k-1}^{n-1} tali sotto insiemi. Ci sono quindi C_{k-1}^{n-1} sotto insiemi di tipo (a).

Se J è un sotto insieme di tipo (b), allora $J \subset X \setminus \{x\}$ e J è un sotto insieme con k elementi di un insieme con $n-1$ elementi. Ci sono C_k^{n-1} tali sotto insiemi. Abbiamo quindi C_k^{n-1} sotto insiemi di tipo (b).

In conclusione $C_k^n = C_{k-1}^{n-1} + C_k^{n-1}$. $\square$

Il Lemma permette di calcolare i numeri C_k^n induttivamente. Per $n = 1$ abbiamo $0 \leq k \leq 1$. Se $X = \{1\}$, c'è un unico sotto insieme con 0 elementi ($\emptyset$, l'insieme vuoto) e un unico sotto insieme con un elemento (X stesso). Quindi $C_0^1 = C_1^1 = 1$.

Osserviamo che $C_0^n = 1$ per ogni n (l'unico sotto insieme con 0 elementi è l'insieme vuoto) e $C_n^n = 1$ per ogni n.

Usando il Lemma: $C_1^2 = 1+1 = 2$. Quindi $C_0^2 = 1, C_1^2 = 2, C_2^2 = 1$ (infatti 1,2,1 sono i coefficienti dello sviluppo di $(x+y)^2$). Per $n = 3$ ricaviamo $1,3,3,1$, per $n = 4$: $1,4,6,4,1$ ecc... Avete riconosciuto il triangolo di Tartaglia (o di Pascal, Newton ecc...).

Per dimostrare che $C_k^n = \binom{n}{k}$ basta verificare con la definizione (4) che:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

(e questo non pone problemi) e che C_k^n e $\binom{n}{k}$ coincidono per i primi valori di n (e k), poi siccome seguono la stessa "legge di formazione", sono uguali (per essere super precisi bisognerebbe fare una doppia induzione su n, k).

Questo dimostra la formula del binomio e anche che $\binom{n}{k}$ è un intero (vedremo un'altra dimostrazione della formula del binomio più avanti (Esercizio 4)).

4. Febbraio 2006, Problemi a risposta multipla n.3

Quale fra le seguenti espressioni è equivalente a $(x+y+z)^3 - x^3 - y^3 - z^3$?
(A) $3x^2(y+z) + 3y^2(x+z) + 3z^2(x+y)$
(B) $3x(y+z)^2 + 3y(x+z)^2 + 3z(x+y)^2$
(C) $3(x+y)(x+z)(y+z)$
(D) $3x(y^2+z^2) + 3y(x^2+z^2) + 3z(x^2+y^2)$
(E) $3xy(1-z) + 3xz(1-y) + 3yz(1-x)$.

Dimostrazione:

Usando la formula del binomio abbiamo $(x+y+z)^3 = ((x+y)^3 + z^3) = (x+y)^3 + 3(x+y)^2 z + 3(x+y)z^2 + z^3 = x^3 + 3x^2y + 3xy^2 + y^3 + 3(x^2 + 2xy + y^2)z + 3xz^2 + 3yz^2$. Quindi:

$$(x+y+z)^3 - x^3 - y^3 - z^3 = 3x^2y + 3xy^2 + 3x^2z + 6xyz + 3y^2z + 3xz^2 + 3yz^2$$

Osserviamo che il risultato è un polinomio omogeneo di grado tre nelle variabili x, y, z (cioè una somma di monomi di grado tre). Vediamo inoltre che c'è un termine $6xyz$. Questo permette di scartare (A) (tutti i monomi hanno un quadrato, non c'è nessun termine in xyz). Anche (B) può essere scartato: il termine in xyz è $18xyz$. Anche (D) è da scartare (tutti i monomi contengono un quadrato: non c'è nessun termine in xyz). Finalmente (E) non è omogeneo di grado tre, quindi va scartato. La risposta è (C). $\square$

5. Archimede.

5.1. **Biennio 2011, n.1.**

Quanti sono i numeri di 6 cifre, formati dalle cifre 1, 2, 3, 4, 5, 6, divisibili per 1, 2, 3, 4, 5, 6?
(A) Nessuno, (B) 1, (C) 18, (D) 120, (E) 360.

Dimostrazione: Sia n il numero in questione. Se $5 \mid n$ l'ultima cifra di n deve essere 5 o 0, quindi 5 sotto le nostre ipotesi. Siccome $2 \mid n$, n è pari e quindi la sua ultima cifra deve essere un numero pari. La risposta è (A). $\square$

5.2. **Biennio 2012, n.1.**

Loretta si reca ogni 13 giorni in un ambulatorio per una cura. Il giovedì, e solo il giovedì, nell'ambulatorio presta servizio Franco, l'infermiere preferito di Loretta. Sapendo che oggi, giovedì, Loretta è andata all'ambulatorio, tra quanti giorni rivedrà Franco?
(A) 14 (B) 35 (C) 53 (D) 65 (E) 91

Dimostrazione: Loretta e Franco s'incontrano in ambulatorio, poi lei torna ogni 13 giorni e lui ogni 7 giorni. Il loro prossimo incontro avverrà un giorno che sarà un multiplo di 13 e un multiplo di 7, più precisamente il minor comune multiplo di 13 e 7 che è $7 \times 13 = 91$. $\square$

5.3. **Triennio 2011, n.**

Un numero si dice palindromo se la sequenza delle sue cifre non cambia che la si legga da sinistra a destra o da destra a sinistra; ad esempio 36563 'e palindromo. Quanti sono i numeri palindromi di 5 cifre tali che la somma delle loro cifre sia pari?
(A) 450, (B) 550, (C) 700, (D) 900, (E) 1000.

Dimostrazione: Un tale numero è della forma *abcba* (scrittura decimale). La somma delle cifre è: $2a+2b+c$ e quindi la somma delle cifre è pari se e solo se c è pari. Abbiamo quindi $a \in \{1,2,...,9\}$ ($a \neq 0$, altrimenti il numero avrebbe meno di 5 cifre), $b \in \{0,1,2,...,9\}$ e $c \in \{0,2,4,6,8\}$. Quindi 9 possibilità per a, 10 per b e 5 per c. Ci sono quindi $9 \times 10 \times 5 = 450$ tali numeri. $\square$

5.4. **Triennio 2012, n.11.**

Determinare la somma delle cifre del numero $(10^{2012}+1)^3$.
(A) 4 (B) 8 (C) 2012 (D) 2013 (E) nessuna delle precedenti

Dimostrazione: Per calcolare la somma delle cifre di un numero bisogna scriverlo in base 10, per esempio $abcd = a.10^3 + b.10^2 + c.10 + d$ e la somma delle cifre è la somma dei vari coefficienti delle potenze di 10, qui $a+b+c+d$.

Per la formula del binomio

$$(10^{2012}+1)^3 = (10^{2012})^3+3(10^{2012})^2+3.10^{2012}+1 = 10^{6036}+3.10^{2024}+3.10^{2012}+1$$

Quindi la somma delle cifre è: 1+3+3+1 = 8. □

5.5. **Biennio 2012, n.6.**

Quanti sono i numeri di tre cifre, tutte diverse da 0, tali che comunque si permutino le loro cifre il numero che si ottiene è divisibile per quattro?
(A) 8 (B) 12 (C) 16 (D) 24 (E) 48

Dimostrazione: Un numero divisibile per 4 è pari. Quindi tutte le cifre del numero devono essere pari. Se $n = abc$, $a, b, c \in \{2, 4, 6, 8\}$.

Supponiamo $n = ab2$. Allora $n = a.100 + b.10 + 2 = a(4.25) + b(4.2 + 2) + 2$. Se $4 \mid n$, allora $4 \mid 2b + 2$, ma nessun $b \in \{2, 4, 6, 8\}$ verifica $4 \mid 2b + 2$. Quindi $a, b, c \in \{4, 6, 8\}$.

Supponiamo $n = ab6$. ragionando come prima si vede che 4 deve dividere $2b + 6$, ma questo non è possibile se $b \in \{4, 6, 8\}$.

Quindi $a, b, c \in \{4, 8\}$. E' chiaro che ogni numero $n = abc$ con $a, b, c \in \{4, 8\}$ verifica la richiesta dell'esercizio ($n = a.100 + b.10 + c$ e $4 \mid a, b, c$, quindi $4 \mid n$). Ci sono 8 tali numeri: 444, 448, 484, 844, 488, 848, 884, 888. □

5.6. **Triennio 2012, n.12.**

Quale tra i seguenti è il numero più grande che divide n^5-5n^3+4n, qualsiasi sia il numero naturale $n \geq 3$?
(A) 15 (B) 35 (C) 60 (D) 120 (E) 240

Dimostrazione: Abbiamo $P(n) := n^5 - 5n^3 + 4n = n(n^4 - 5n^2 + 4)$. Ponendo $x = n^2$ viene $n(x^2-5x+4)$. Abbiamo $x^2-5x+4 = (x-1)(x-4)$. Riassumendo: $n^5 - 5n^3 + 4n = n(n^2 - 1)(n^2 - 4) = n(n - 1)(n + 1)(n - 2)(n + 2) = (n - 2)(n - 1)n(n + 1)(n + 2)$. Quindi la nostra espressione è il prodotto di cinque numeri > 0 (perché $n \geq 3$) consecutivi.

Un tale prodotto contiene due numeri pari consecutivi cioè: $2k$ e $2(k+1)$. Se $k = 2t$ è pari, $2k = 4t$ è divisibile per 4 (e $2(k+1)$ è divisibile per 2). Se $k = 2t+1$ è dispari $2(k+1) = 2(2t+2) = 4(t+1)$ è divisibile per 4. Quindi $(2k).(2(k+1))$ è divisibile per $2 \times 4 = 8$. Pertanto $8 \mid P(n)$.

Nel prodotto di tre numeri consecutivi $m(m+1)(m+2)$ c'è sempre un multiplo di 3. Infatti questo è chiaro se $m = 3k$. Se m non è multiplo di 3 posso scrivere $m = 3k + r$ con $1 \leq r \leq 2$ (divisione euclidea). Se $r = 1$, $m+2 = 3(k+1)$; se $r = 2$, $m+1 = 3(k+1)$. Quindi il prodotto di tre numeri consecutivi è sempre divisibile per 3.

Nello stesso modo vediamo che il prodotto di cinque numeri consecutivi è sempre divisibile per 5.

In conclusione, per ogni $n > 2$, $P(n)$ è divisibile per $8 \times 3 \times 5 = 120$.

Per $n = 3$, abbiamo $P(3) = 1.2.3.4.5 = 5! = 120$, quindi il numero cercato è 120. □

5.7. **Biennio 2010, n.12.**

Quanto vale la somma: $1 + 2 + 2 + 3 + 3 + 4 + 4 + \ldots + 35 + 35 + 36$?
(A) 990, (B) 1105, (C) 1295, (D) 1395, (E) 1505.

Dimostrazione: Si ricorda la formula $S_n := 1 + 2 + 3 + ... + n = n(n+1)/2$ (vedere [1] per una dimostrazione). La somma cercata vale $S_{36} + (S_{35} - 1) = 36.37/2 + 35.36/2 - 1 = 36(37+35)/2 - 1 = 18.72 - 1 = 1295$.

N.B. La redazione della prima soluzione proposta nelle correzioni è assai confusa per non dire altro. La redazione dice:

Prima soluzione. Chiamiamo S la somma richiesta; osserviamo che il numero di termini della somma è 1 + 34.2 + 1 = 70. Possiamo scrivere
S = 1 + 2 + . . . + 35 + 36
S = 36 + 35 + . . . + 2 + 1 .
Notiamo che la somma di ogni coppia di termini incolonnati è sempre uguale a 37. Qundi se sommiamo termine a termine le due uguaglianze scritte sopra troviamo che 2S è pari alla somma di 70 termini tutti uguali a 37. Dunque 2S = 37 x 70 e quindi S = 37 x 35 = 1295.

Allora: 1) non è vero che la somma cercata, chiamata S, sia uguale a 1+2+3+...+36 = 36.37/2 = 666.
2) Se sommiamo termine a termine le due uguaglianze scritte sopra troviamo

36 somme uguali a 37, quindi 2S = 36 x 37, pertanto S =18 x 37 = 666, come sopra. E' vero invece che la somma cercata è uguale a 2S - 36 -1 = 2 x 666 - 37 = 1295.

La seconda soluzione è più interessante: ogni numero tra 2 e 35 compare due volte e poi abbiamo 1 e 36. Quindi i numeri coinvolti possono essere scritti:

$$\begin{matrix} 1 & 2 & & & & \\ & 2 & 3 & & & \\ & & 3 & 4 & & \\ & & & \ddots & & \\ & & & & 34 & 35 & \\ & & & & & 35 & 36 \end{matrix}$$

La somma nella prima riga è 1+2 = 3, quella della seconda riga è quella della prima +2, ossia 5 (c'è il 2 in comune ma nella prima riga c'è il numero prima di 2 e nella seconda quello dopo, quindi la differenza è 2). In altri termini la somma cercata è: $3 + 5 + 7 + ... + 71 = (1 + 3 + 5 + 7 + .. + 71) - 1$, cioè la somma dei numeri dispari fino a 71 diminuita di uno. La redazione prosegue così:

Osserviamo ora che quando si sommano i numeri dispari consecutivi compresi tra 1 e un certo numero dispari, si trova sempre un quadrato perfetto, e più precisamente, se l'ultimo numero dispari che si è sommato è (2k - 1), si trova k^2. In altre parole vale l'uguaglianza

$$1 + 3 + 5 + 7 + ... + (2k - 1) = k^2$$

Questa può essere facilmente verificata per i primi valori di k = 1, 2, 3,... , e può essere dimostrata per ogni scelta di k usando il principio di induzione.

La soluzione conclude poi così (in sintesi): siccome $71 = 2.36 - 1$, la somma cercata vale $36^2 - 1 = 1295$.

Questa soluzione offre due spunti interessanti: (a) la formula che dà la somma di tutti i numeri dispari tra 1 e 2k-1, (b) Si parla di *principio di induzione*. Proviamo a vedere queste cose.

□

6. La somma $1+3+5+...+(2k-1)$; il principio di induzione.

Si tratta di dimostrare, per ogni $k \geq 1$ la formula:

$$D(k) := 1+3+5+...+(2k-1) = k^2 \tag{6}$$

Osserviamo che $D(k)$ è la somma dei primi (partendo da 1) k numeri dispari. Abbiamo $D(1) = 1, D(2) = 4 = 2^2$ ecc... Nello stesso modo abbiamo la somma dei primi k numeri pari:

$$P(k) = 2+4+...+2k$$

Conoscendo la formula $1+2+3+...+n = n(n+1)/2$, è facile calcolare $P(k)$. Infatti $P(k) = 2(1+2+...+k) = k(k+1)$ (un rettangolo!). Quindi

$$P(k) = 2+4+6+...+2k = k(k+1) \tag{7}$$

Adesso $P(k)+D(k) = 1+2+3+...+2k = 2k(2k+1)/2 = k(2k+1)$. Pertanto $D(k) = k(2k+1) - k(k+1) = k^2$ e la formula (6) è dimostrata.

Nell'antichità per dimostrare (6) facevano così:

$$1+3=4=2^2 : \quad \begin{array}{cc} \bullet & \star \\ \star & \star \end{array}$$

$$1+3+5=9=3^2 : \quad \begin{array}{ccc} \bullet & \star & \bullet \\ \star & \star & \bullet \\ \bullet & \bullet & \bullet \end{array}$$

Il primo pallino rappresenta 1, le tre stelle 3, i successivi 5 pallini 5. E' chiaro (?) che se abbiamo un quadrato di lato $(k-1)$, aggiungendo una colonna, una riga e completando la diagonale, abbiamo un quadrato di lato k. Abbiamo aggiunto $2(k-1)+1 = 2k-1$. "Quindi" $1+3+5+...+(2k-1) = k^2$, "è vera $\forall k$".

Il passaggio "Quindi"..."è vera $\forall k$", dal punto di vista matematico, deve essere chiarificato. Quello che stiamo dicendo sostanzialmente è questo: sia $F(n)$ una formula (un'asserzione) che dipende da $n \in \mathbb{N}$.

($\star$) Se $F(0)$ è vera e se l'implicazione: $F(n) \Rightarrow F(n+1)$ è vera, allora $F(n)$ è vera per ogni $n \geq 0$.

In soldoni dire che l'implicazione $F(n) \Rightarrow F(n+1)$ è vera torna a dire: se $F(n)$ è vera, allora anche $F(n+1)$ è vera.

Questo risulta dal principio di induzione che si può enunciare così:

Principio di induzione: Sia $X \subset \mathbb{N}$, con $0 \in X$. Se $n \in X \Rightarrow n+1 \in X$, allora $X = \mathbb{N}$.

Il principio è intuitivamente chiaro: abbiamo $0 \in X$. poi $0 \in X \Rightarrow 0+1 = 1 \in X$. Quindi $1 \in X$. Pertanto $1 \in X \Rightarrow 1+1 = 2 \in X$. Quindi $2 \in X$ e si ripete il processo per ottenere $3 \in X$ e poi $4 \in X$, ecc... :ogni $n \in X$ e $X = \mathbb{N}$.

In altri termini se ci rappresentiamo $\mathbb{N}$ come una scala (infinita) a pioli, il principio di induzione dice che se mettiamo il piede sul primo piolo e poi sappiamo che ogni volta che abbiamo il piede su un piolo, possiamo metterlo su quello successivo, allora siamo sicuri di percorrere tutta la scala senza omettere alcun piolo (e questo anche se la scala è infinita!).

Ovviamente possiamo partire dal secondo piolo (o dal piolo numero k), il principio dice che possiamo percorrere tutti i pioli dal secondo (o dal k-esimo) in poi.

Il principio di induzione è equivalente al *principio del minimo*: *ogni sotto insieme non vuoto $X \subset \mathbb{N}$, ammette un elemento minimo*, cioè esiste $n_0 \in X$ tale che $\forall m \in X, m \geq n_0$.

Vediamo adesso come l'affermazione $(\star)$ si deduce dal principio di induzione. Sia $X = \{n \mid F(n) \text{ è vera}\}$. Siccome $F(0)$ è vera, $0 \in X$. Se $n \in X$, quindi $F(n)$ è vera, sappiamo che anche $F(n+1)$ lo è, quindi $n+1 \in X$. per il principio di induzione $X = \mathbb{N}$ e $F(n)$ è vera per ogni $n \in \mathbb{N}$.

Il principio di induzione (o metodo di dimostrazione per induzione) è lo strumento più potente della matematica!

Vediamo come dimostrare la formula $D(k) = k^2$ per induzione. Per $k = 1$: $D(1) = 1^2 = 1$, e questo è vero. Quindi il *caso iniziale* è dimostrato.

Supponiamo di sapere che $D(k) = k^2$ è vera (*ipotesi di induzione*) e mostriamo che questo implica la formula per $k+1$ ($D(k+1) = (k+1)^2$) (questo passaggio si chiama *il passo di induzione*).

Abbiamo

$$D(k+1) = 1+3+5+...+(2k-1)+(2k+1) = [1+3+5+...+(2k-1)]+(2k+1)$$

Per ipotesi di induzione sappiamo che $D(k)$ è vera cioè: $[1+3+5+...+(2k-1)] = k^2$. Quindi $D(k+1) = k^2 + 2k + 1 = (k+1)^2$. La formula è dimostrata per ogni $k \geq 1$.

Esercizio 4. *Dimostrare la formula del binomio per induzione.*

Dimostrazione: la formula è vera per $n = 1$: $x + y = \binom{1}{0}x + \binom{1}{1}y = x + y$. Supponiamo la formula vera per n e mostriamo che questo implica che la formula è vera anche per $n + 1$.

Abbiamo: $(x + y)^{n+1} = (x + y)^n(x + y)$. per ipotesi di induzione $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$, quindi:

$$(x+y)^{n+1} = \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right) .(x+y) = \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1}$$

Poniamo $j = k + 1$, allora:

$$(x + y)^{n+1} = \sum_{j=1}^{n+1} \binom{n}{j-1} x^j y^{n+1-j} + \sum_{j=1}^{n+1} \binom{n}{j-1} x^{j-1} y^{n+1-(j-1)}$$

Cerchiamo adesso il coefficiente del termine $x^t y^{n+1-t}$. Se $t = 0$, y^{n+1} compare solo nella seconda sommatoria, quando $j = 1$ e il coefficiente è: $\binom{n}{0} = 1$. Se $t = n + 1$, x^{n+1} compare solo nella prima sommatoria con il coefficiente $\binom{n}{n} = 1$. Se $0 < t < n + 1$, $x^t y^{n+1-t}$ compare nella prima sommatoria quando $j = t$, con il coefficiente $\binom{n}{t-1}$; e nella seconda quando $j = t + 1$, con il coefficiente $\binom{n}{t}$. Quindi il coefficiente di $x^t y^{n+1-t}$ è $\binom{n}{t-1} + \binom{n}{t} = \binom{n+1}{t}$ (come si vede da un rapido calcolo usando la definizione (4). Quindi $(x + y)^{n+1} = \sum_{t=0}^{n+1} \binom{n+1}{t} x^t y^{n+1-t}$. La formula del binomio è dimostrata. $\square$

Mi direte che l'inconveniente di questo metodo è che bisogna conoscere prima la formula! Vero. ma si può provare a indovinare!

Esercizio 5. *Determinare* $Q(n) := 1^2 + 2^2 + 3^2 + ... + n^2$.

Uno può provare a trovare una dimostrazione *geometrica*, come abbiamo fatto con $S_n = 1 + 2 + 3 + ... + n$ (cf [1]). ma uno può provare a indovinare *per analogia*: abbiamo $S_n = n(n+1)/2$, la formula è data da un polinomio del secondo grado in n. E se qua fosse data da un polinomio del terzo grado? Cioè $Q(n) = an^3 + bn^2 + cn + d$. Come si fa a determinare i coefficienti a, b, c, d? Dando dei valori. Per esempio scrivendo $Q(n) = 0^2 + 1^2 + ... + n^2$, abbiamo $Q(0) = 0$ e quindi $d = 0$. Poi $Q(1) = 1 = a + b + c$, $Q(2) = 5 = 8a + 4b + 2c$, $Q(3) = 14 = 27a + 9b + 3c$. Abbiamo così un sistema lineare di tre equazioni in tre incognite:

$$\begin{cases} a+b+c=1 \\ 8a+4b+2c=5 \\ 27a+9b+3c=14 \end{cases}$$

Risolvendo si trova: $a = 1/3$, $b = 1/2$, $c = 1/6$. Quindi se $Q(n)$ è dato da un polinomio del terzo grado si dovrebbe avere: $Q(n) = P(n)$, dove $P(n) = n(n+1)(2n+1)/6$.

Finora non abbiamo dimostrato niente, abbiamo solo tirato a indovinare!

Ma adesso che abbiamo una formula possiamo cercare di dimostrarla per induzione!

Siccome $P(1) = 1 = Q(1)$, il caso iniziale è vero.

(Passo di induzione:) $Q(n+1) = Q(n) + (n+1)^2$. Per ipotesi di induzione $Q(n) = P(n)$, quindi $Q(n+1) = n(n+1)(2n+1)/6 + (n+1)^2$. Adesso $n(n+1)(2n+1)/6 + (n+1)^2 = (n+1)[(2n+1) + 6(n+1)]/6 = (n+1)(n+2)(2n+3)/6 = P(n+1)$. La nostra formula è dimostrata, abbiamo $Q(n) = P(n), \forall n \in \mathbb{N}$.

(Si può mostrare che, per ogni intero $k \geq 1$, $1^k + 2^k + 3^k + ... + n^k$ è dato da un polinomio di grado $k+1$ in n, ma questo è un'altra storia.)

Questo esempio è tipico del processo creativo in matematica: si cerca di indovinare una risposta (usando il proprio "senso", feeling, matematico, le proprie conoscenze, analogie), quando si pensa di avere la risposta giusta, si cerca di dimostrarla rigorosamente (certe volte si riesce, altre no :-).

Bibliografia

[1] Ellia, Ph.: *Preparazione olimpiadi (Liceo Roiti 12-02-2014)*, www.unife.it/utenti/philippe.ellia

Dipartimento di Matematica, 35 via Machiavelli, 44100 Ferrara
E-mail address: phe@unife.it