PREPARAZIONE OLIMPIADI
(LICEO ROITI 12-02-2014)

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. Iniziamo quindi col richiamare velocemente queste nozioni.

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).

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 $p \mid a_i$.

Dimostrazione.
(1) Se $p \mid a.b$, allora $p.m = a.b$. Sia $m = \prod l_i^{\alpha_i}$ la fattorizzazione di m in fattori primi; nello stesso modo siano $a = \prod p_j^{\beta_j}$, $b = \prod q_t^{\gamma_t}$ le fattorizzazioni di a, b. Allora $p.\prod l_i^{\alpha_i} = \prod p_j^{\beta_j}.\prod q_t^{\gamma_t}$ sono due fattorizzazioni dello stesso numero. Per unicità della fattorizzazione sono uguali. Quindi p è uguale a qualche p_j (e quindi $p \mid a$) o a qualche q_t (e allora $p \mid b$).
(2) Se $p \mid a_1(a_2...a_r)$, allora $p \mid a_1$ (e abbiamo finito) o $p \mid a_2(a_3...a_r)$. Nel secondo caso $p \mid a_2$ o $p \mid a_3(a_4...a_r)$. Andando avanti così si arriva necessariamente a trovare i tale che $p \mid a_i$. □

Osservazione 1.3. *Questo lemma viene chiamato anche "lemma di Euclide" ma è stato Gauss il primo a mettere in evidenza la sua importanza. (In realtà si usa il Lemma di Gauss per dimostrare il TFA, ma questo è un'altra storia! vedere la sotto sezione 1.1).*

La seconda parte segue dalla prima, quindi il Lemma di Gauss è essenzialmente il caso con due fattori. Ovviamente si può dimostrare la seconda parte

con il TFA scrivendo la fattorizzazione di ogni a_i: p deve comparire in una di queste.

Conoscendo la fattorizzazione in primi è facile trovare l'MCD (massimo comune divisore) 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).

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

A questo punto è facile dimostrare la seguente generalizzazione del lemma di Gauss:

Lemma 1.4. *Se $n \mid ab$ e se $(n, a) = 1$ (n e a sono primi tra di loro), allora $n \mid b$.*

Dimostrazione. Abbiamo $nm = ab$, scrivere le fattorizzazioni di ogni numero. Siccome nessun primo divide sia n che a, tutti i fattori primi di n devono comparire (con le loro potenze) nella fattorizzazione di b, quindi $n \mid b$. □

A questo punto vi chiederete forse come si fa a vedere se un numero è primo? Come si fa a trovare dei numeri primi? Sono problemi molto difficili. Osserviamo però le seguenti cose:

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 $1 < d \leq \sqrt{n}$.

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 $\sigma(p^a) = \dfrac{p^{a+1} - 1}{p - 1}$.

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 $(2^3-1).(3^2-1)/2 = 7.4 = 28$.

1.1. **Per i curiosi.**

Questa sezione non è indispensabile ma se siete curiosi ecco velocemente come si può dimostrare il TFA.

- Per prima cosa bisogna mostrare che ogni intero $n > 1$ si scrive come un prodotto di numeri primi, questo è facile.

Usiamo una proprietà "ovvia" dell'insieme $\mathbb{N}$ dei numeri naturali: se $X \subset \mathbb{N}$ è un sotto insieme non vuoto, allora X ammette un elemento minimo (cioè esiste $n_0 \in X$ tale che $\forall n \in X$, $n \geq n_0$).

Supponiamo che esista un intero > 1 che non si scriva come prodotto di primi. L'insieme X di tali interi è quindi non vuoto e per la proprietà del minimo ammette un più piccolo elemento n_0. Chiaramente n_0 non è primo. Quindi $n_0 = a.b$ con $1 < a, b < n_0$. Siccome $a, b \notin X$, a e b si scrivono come prodotti di primi. Quindi anche $n_0 = a.b$ si scrive come prodotto di primi: assurdo. Quindi X è vuoto. Quindi ogni intero $n > 1$ ammette una fattorizzazione $n = p_1^{a_1}...p_r^{a_r}$ in numeri primi.

- Adesso bisogna mostrare che la fattorizzazione è unica, questa è la parte difficile.

Se possiamo usare il lemma di Gauss la questione è semplice:

Supponiamo di avere due fattorizzazioni: $p_1...p_m = q_1...q_t$ (p_i, q_j primi, non necessariamente distinti). Siccome $p_1 \mid q_1...q_t$, per il lemma di Gauss p_1 divide uno dei q_j. Riordinando semmai gli indici possiamo assumere $p_1 \mid q_1$. Siccome p_1 e q_1 sono primi questo implica $p_1 = q_1$. Semplificando per p_1 abbiamo: $p_2...p_m = q_2...q_t$. Ripetendo il ragionamento con p_2 ecc... vediamo che (dopo eventuale riordino degli indici) $m = t$ e $p_i = q_i, \forall i$ (cercate di formalizzare bene questo passaggio). Pertanto la fattorizzazione è unica.

- Siamo quindi ridotti a dimostrare il lemma di Gauss, senza usare il TFA.

Siano m, n due interi, mostriamo che se $d = (m, n)$ (d = MCD di m, n)), allora esistono due interi a, b negativi o positivi tali che $d = an + bm$.

Se abbiamo questo risultato possiamo dimostrare il Lemma di Gauss e quindi il TFA. Infatti sia $p \mid ab$, p primo. Se p non divide a, allora $(a, p) = 1$. Quindi esistono interi x, y (positivi o negativi) tali che: $ax + py = 1$. Moltiplicando per b: $abx + bpy = b$. Siccome $p \mid abx$ (perché $p \mid ab$) e $p \mid bpy$ (perché $p \mid p$), abbiamo $p \mid b$.

- Rimane da dimostrare che se $d = (m, n)$ allora esistono interi u, v (positivi o negativi) tali che $mu + nv = d$.

Sia $I = \{\alpha m + \beta n \mid \alpha, \beta \in \mathbb{Z}\}$ e sia $I_+ = \{m \in I \mid m > 0\}$. L'insieme I_+ è non vuoto perché $m = 1.m + 0.n \in I_+$. Sia d l'elemento minimo di I_+ ("principio del minimo"). Abbaimo $d = um + vn$, $u, v \in \mathbb{Z}$.

Mostriamo che ogni elemento di I_+ è un multiplo di d. Se $a \in I_+$, $a \geq d$ e possiamo fare la divisione euclidea di a per d: $a = dq + r$, dove $r = 0$ o $1 \leq r < d$.

Osserviamo che $r \in I$. Infatti $r = a - dq = (xm + yn) - (um + vn)q = m(x - qu) + n(y - qv)$.

Se $r \neq 0$, allora $r < d$ e $r \in I_+$ (perché $r \in I$ e $r > 0$). Per la definizione di d questo non è possibile. Quindi $r = 0$. Pertanto ogni elemento di I_+ è un multiplo di d. In particolare m e n sono multipli di d, cioè $d \mid m$ e $d \mid n$. Quindi d è un divisore comune di m e n.

Sia adesso s un divisore comune di m e n: $s \mid m$ e $s \mid n$. Siccome $d = um + vy$, abbiamo $s \mid d$, quindi $s \leq d$. Pertanto d è il Massimo Comune Divisore di m e n.

Abbiamo quindi mostrato che se d è il MCD di m e n, allora esistono degli interi u, v (negativi o positivi) tali che $d = mu + nv$.

Questo conclude la dimostrazione del Lemma di Gauss e quindi la dimostrazione del Teorema Fondamentale dell'Aritmetica (TFA).

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).

Quindi per il calcolo modulare possiamo rimpiazzare a con r. Per esempio $13 \equiv 1 \pmod{3}$, quindi $169 = 13^2 \equiv 1.1 \equiv 1 \pmod{3}$, più generalmente

$13^k \equiv 1 \pmod 3$, $\forall k \geq 1$. Questo permetterebbe, per esempio, di risolvere l'esercizio: *mostrare che la somma delle cifre di* 13^{2014} *non è un multiplo di* 3.

Vedere la Sezione 3 per un'altra applicazione.

Un'altra cosa che può essere utile (cf Sezione 7): 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, $n = 4k^2 + 4k + 1 \equiv 1 \pmod 4$.

3. Febbraio 2005, n. 17

Determinare tutte le coppie (m, n) di interi positivi m, n tali che

$$\frac{3^m + 3}{2^n + 2^{n-1}}$$

sia un numero intero.

1a dimostrazione:
Dobbiamo determinare gli (m, n) tali che: $3^m + 3 = (2^n + 2^{n-1}).a$ dove a è un intero. Abbiamo:

$$3(3^{m-1} + 1) = 2^{n-1}(2 + 1).a$$

perciò l'equazione diventa:

$$3^{m-1} + 1 = 2^{n-1}a$$

Il problema è quindi equivalente a determinare (m, n) tali che 2^{n-1} divida $3^{m-1} + 1$.

Se $n = 1$, $2^{n-1} = 2^0 = 1$ divide ogni numero, quindi $(m, 1)$ $m \geq 1$ conviene.

Se $n = 2$, 2 divide sempre $3^{m-1} + 1$, perché 3^{m-1} è dispari. Quindi $(m, 2)$, $m \geq 1$ conviene.

Se $n = 3$ dobbiamo vedere se $4 \mid 3^{m-1} + 1$. Abbiamo $3 \equiv 3 \pmod 4$ (il resto della divisione di 3 per 4 è 3). Poi $3^2 = 9 \equiv 1 \pmod 4$, quindi $3^3 \equiv 3.(3^2) \equiv 3.1 \equiv 3 \pmod 4$, ecc... Cioè se k è dispari 3^k ha resto 3 nella divisione per 4, se k è pari 3^k ha resto 1.

Se non siete convinti: se $3^k = 4m + 3$, allora $3^{k+1} = 3(4m + 3) = 12m + 9 = 4(3m + 2) + 1$. Se $3^k = 4m + 1$, $3^{k+1} = 12m + 3 = 4(3m) + 3$.

Quindi $3^{m-1} + 1$ ha resto $3 + 1 \equiv 0 \pmod 4$, se $m - 1$ è dispari, mentre ha resto $1 + 1 = 2$ se $m - 1$ è pari. In conclusione $4 \mid 3^{m-1} + 1$ se e solo se $m - 1$ è dispari, cioè se m è pari. Quindi tutte le coppie $(m, 3)$ con $m \geq 2$ pari vanno bene.

Supponiamo $n > 4$, quindi $2^3 \mid 2^{n-1} \mid 3^{m-1} + 1$. Abbiamo $3 \equiv 3 \pmod 8$, poi $3^2 = 9 \equiv 1 \pmod 8$, $3^3 = 3.(3^2) \equiv 3 \pmod 8$, ecc... Come prima vediamo che: 3^k ha resto 3 nella divisione per 8 se k è dispari, mentre ha resto 1 se k è pari. Nel primo caso $3^k + 1$ ha resto 4, nel secondo resto 2. Quindi $3^k + 1$ non è mai divisibile per 8 ($4 \not\equiv 0 \pmod 8$).

Quindi le coppie cercate sono: $(m, 1), (m, 2)$ per ogni intero m e $(m, 3)$ per $m \geq 2, m$ pari. □

2a dimostrazione:
Come prima si tratta di determinare le potenze di 2 che dividono $3^{m-1}+1$, i casi interessanti sono $2^2, 2^3$.

Questa soluzione (che è quella proposta) usa l'identità notevole:

$$x^{2k+1}+y^{2k+1}=(x+y)(x^{2k}-x^{2k-1}y+x^{2k-2}y^2-...-xy^{2k-1}+y^{2k}) \tag{4}$$

Se $m-1=2k+1$ è dispari (cioè se m è pari), scrivendo $3^{2k+1}+1=3^{2k+1}+1^{2k+1}$ viene:

$$3^{2k+1}+1=4(3^{2k}-3^{2k-1}+...-3+1) \tag{5}$$

Vediamo così che $4 \mid 3^{2k+1}+1$.

Vediamo anche che 8 non divide $3^{2k+1}+1$, infatti da (5) se $8 \mid 3^{2k+1}+1$, allora $2 \mid (3^{2k}-3^{2k-1}+...-3+1)$, ma abbiamo una somma di un numero dispari $(=2k+1)$ di termini dispari, quindi la somma è un numero dispari.

Abbiamo $3^{2k+2}+1=3(3^{2k+1}+1)-2$. Siccome $4 \mid 3^{2k+1}+1$, possiamo scrivere $3^{2k+1}+1=4t$. Quindi $3^{2k+2}+1=12t-2$, che non è divisibile per 4 e a fortiori non per 8. Questo mostra che $4 \nmid 3^{m-1}+1$ se m è dispari.

In realtà la soluzione proposta è un po' più "articolata" e fa uso dell'identità:

$$x^n-y^n=(x+y)(x^{n-1}-x^{n-2}y+...+xy^{n-2}-y^n) \tag{6}$$

valida per n pari.

Usando questa equazione abbiamo $3^{2k}-1=4(3^{2k-1}-...+3-1)$. Quindi $3^{2k}-1$ è multiplo di 4, pertanto $3^{2k}+1=(3^{2k}-1)+2$ non è multiplo di 4. □

Osservazione 3.1. *La prima dimostrazione usa soltanto le congruenze e ci dispensa dal conoscere le identità notevoli. Va detto però che è meglio conoscerle!*

A questo proposito notiamo l'identità:

$$x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+...+xy^{n-2}+y^{n-1})$$

valida per ogni n. Ponendo $y=1$ abbiamo x^n-1, quindi 1 è radice cioè $(x-1) \mid x^n-1$ e questo fornisce la fattorizzazione qui sopra. Se n è pari allora anche -1 è radice quindi $(x+1) \mid x^n-1$ e questo fornisce la fattorizzazione (6).

Finalmente se n è dispari allora -1 è radice di x^n+1 e si ritrova (4).

4. Febbraio 2007, n. 17

Un intero positivo si dice triangolare se si può scrivere nella forma $\frac{n(n+1)}{2}$ *per qualche intero positivo* n*. Quante sono le coppie* (a, b) *di numeri triangolari tali che* $b - a = 2007$*? (Si ricorda che 223 è un numero primo).*

Dimostrazione:
Dobbiamo quindi determinare le coppie (n, m) tali che:

$$\frac{n(n+1)}{2} - \frac{m(m+1)}{2} = 2007$$

Infatti se a è triangolare $a = n(n+1)/2$ e a è determinato da n (a non può essere triangolare in due modi diversi perché $n(n+1)/2 \neq m(m+1)/2$ se $n \neq m$).

Ovviamente a questo punto ci preme capire come utilizzare il suggerimento: 223 è primo. Dopo un attimo di conti vediamo che: $2007 = 9 \times 223 = 3^2 \times 223$.

Siccome $n > m$, poniamo $n = a + m$ e l'equazione diventa:

$$(m + a)(m + a + 1) - m(m + 1) = 2 \times 3^2 \times 223$$

Abbiamo: $(m + a)(m + 1 + a) = m(m + 1) + ma + a(m + 1 + a)$ e l'equazione diventa:

$$a(2m + a + 1) = 2 \times 3^2 \times 223$$

Ci rimane da vedere in quanti modi possiamo scrivere $2 \times 3^2 \times 223$ come prodotto $a.B, a < B$ ($B = 2m + a + 1$). Se a ha un unico fattore primo allora le possibilità sono:

- $a = 2$, $B = 3^2.223$
- $a = 3$, $B = 2.3.223$

Se a ha due fattori primi:

- $a = 2.3$, $B = 3.223$
- $a = 3^2$, $B = 223$

Se a ha tre fattori primi:

- $a = 2.3^2$, $B = 223$

A queste possibilità bisogna aggiungere $a = 1$, $B = 2.3^2.223$. In conclusione ci sono 6 coppie di numeri triangolari la cui differenza vale 2007. □

4.1. **Numeri triangolari ($1+2+...+n=n(n+1)/2$).**

Perché i numeri della forma $n(n+1)/2$ sono detti "triangolari"? Il motivo è che: $1+2+3+...+n=n(n+1)/2$.

Consideriamo una tabella $n \times n$. La tabella contiene n^2 entrate. Consideriamo le seguenti entrate

$$\begin{array}{cc} 1 & \left(\begin{array}{ccccc} \mathbf{0} & & & & \\ 0 & \mathbf{0} & & & \\ 0 & 0 & \mathbf{0} & & \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & \mathbf{0} \end{array} \right) \\ 2 & \\ 3 & \\ \vdots & \\ n & \end{array}$$

I tondini sulla diagonale (in grassetto) più quelli sotto la diagonale rappresentano esattamente la somma $t_n = 1+2+3+...+n$. Vediamo quindi che $t_n := 1+2+...+n$ "rappresenta" un triangolo.

Sulla diagonale abbiamo n tondini (perché ogni riga interseca la diagonale in un unico punto, quindi ci sono altrettanto punti sulla diagonale che il numero di righe). Se togliamo la diagonale dalla tabella rimangono n^2-n entrate: quelle sotto la diagonale (S_t) e quelle sopra la diagonale (S_p). Per simmetria $S_t = S_p$, quindi $n^2-n = S_t+S_p = 2S_t$, pertanto $S_t = (n^2-n)/2$. Quindi i tondini sulla diagonale più quelli sotto la diagonale sono $n+(n^2-n)/2 = n(n+1)/2$. Cioè $1+2+..+n = n(n+1)/2$.

Un altro modo più veloce di dimostrare questa formula è il seguente: scriviamo i nostri numeri da 1 a n su una riga e riscriviamoli sulla riga sotto ma nell'ordine opposto e facciamo le somme per colonne:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n & n-1 & n-2 & \cdots & 1 \\ - & - & - & \cdots & - \\ n+1 & n+1 & n+1 & \cdots & n+1 \end{array}$$

Abbiamo n pacchetti la cui somma vale sempre $n+1$, quindi $2t_n = n(n+1)$, ossia $t_n = n(n+1)/2$.

5. Febbraio 2000, n. 15

Qual'è il più piccolo numero intero positivo che possiede esattamente 15 divisori?
Nota: Per divisori di un numero intero positivo si intendono i divisori positivi, includendo 1 e il numero stesso. Per esempio, il numero 6 ha esattamente 4 divisori: 1,2,3,6.

1a dimostrazione:
Sia n il numero cercato. Osserviamo che n è un quadrato. Infatti i divisori di un numero, m, sono simmetrici rispetto a $\sqrt{m}$: se $m = ab, a \leq b$, allora $a \leq \sqrt{m}$ (altrimenti $ab \geq a^2 > m = (\sqrt{m})^2$). Nello stesso modo $b \geq \sqrt{m}$. Quindi se $d(m)$ indica il numero di divisori di m abbiamo: $d(m)$ è dispari $\Leftrightarrow m$ è un quadrato.

Quindi $n = a^2$.

Se a è un numero primo p, allora $n = p^2$ i cui divisori sono: $Div(p^2) = \{1, p, p^2\}$. Quindi 3 divisori, non va bene.

Se $a = p^2$, p primo, allora $n = p^4$ i cui divisori sono $Div(p^4) = \{1, p, p^2, p^3, p^4\}$. Quindi 5 divisori, non va bene.

Se $a = pq$ è un prodotto di due primi, allora $n = p^2q^2$ e

$$Div(n) = \{1, p, p^2, pq, pq^2, q, qp, qp^2, p^2q^2\}.$$

Quindi 9 divisori, non va bene.

A questo punto abbiamo eliminato $a = 1, 2, 3, 4 = 2^2, 5, 6 = 2.3, 7, 9 = 3^2, 10 = 2.5, 11$. Se $a = 8 = 2^3$, allora $n = 2^6 = 64$. In generale i divisori di p^6, p primo, sono 7 $(1, p, p^2, ..., p^6)$. Quindi $a \geq 12 = 2^2 \times 3$.

Se $a = p^2q$, allora $n = p^4q^2$ i cui divisori sono:

$$1, p, p^2, p^3, p^4, q, q^2, pq, p^2q, p^3q, p^4q, pq^2, p^2q^2, p^3q^2, p^4q^2$$

E sono proprio 15! Il numero cercato è: $12^2 = 144$. □

2a dimostrazione:
Questa soluzione (che è poi quella proposta) richiede il TFA.

Sia $n = p_1^{a_1}p_2^{a_2}...p_r^{a_r}$ la fattorizzazione di n in numeri primi ($p_1 < p_2 < ... < p_r, a_i \geq 1, \forall i$). Un numero d divide n se e solo se $d = p_1^{b_1}p_2^{b_2}...p_r^{b_r}$ con $a_i \geq b_i \geq 0$. Si ammette anche l'esponente 0 perché non tutti i fattori primi

di n devono comparire necessariamente nella scomposizione di d: per esempio se $b_i = 0, \forall i$ si ottiene il divisore $d = 1$.

Ci sono a_1+1 scelte per b_1 ($0 \leq b_1 \leq a_1$), a_2+1 scelte per b_2, ..., a_r+1 scelte per b_r. Siccome d è completamente determinato dai relativi b_i, concludiamo che se $\tau(n)$ indica il numero di divisori di n, allora:

$$\tau(n) = (a_1 + 1)(a_2 + 1)...(a_r + 1)$$

Per avere $\tau(n) = 15 = 3 \times 5$ ci sono solo le seguenti possibilità:

- $r = 1$, $a_1 = 14$, cioè $n = p^{14}$ dove p è primo. Il più piccolo numero di questo tipo è $2^{14} = (2^3)^2 \times (2^3)^2 \times 2^2 = 64^2 \times 4$.
- $r = 2, a_1 = 2, a_2 = 4$, cioè $n = p^2q^4, p < q$ primi. Il più piccolo numero di questo tipo è $2^2 \times 3^4 = 4 \times 81 = 324$
- $r = 2, a_1 = 4, a_2 = 2$, cioè $n = p^4q^2$, $p < q$. Il più piccolo numero di questo tipo è $2^4 \times 3^2 = 12^2 = 144$.

Siccome $64^2 \times 4 > 64 \times 4 > 144$, il numero cercato è 144.

□

6. Febbraio 2000, n. 16

Determinare tutte le coppie ordinate (m, n) di interi positivi che soddisfano l'equazione:

$$\frac{2}{5} = \frac{1}{m} + \frac{1}{n} - \frac{1}{mn}$$

Osservazione 6.1. *Chiaramente qui per "positivi" si intende strettamente positivi: $m, n > 0$.*

Una coppia è sempre ordinata, infatti $(a, b) = (x, y) \Leftrightarrow a = x$ e $b = y$. Quindi per esempio $(2, 3)$ e $(3, 2)$ sono due coppie diverse.

Gli interi m, n hanno ruoli simmetrici: se (m, n) è soluzione, anche (n, m) è soluzione.

1a dimostrazione:
La prima idea è di limitare m o n.

Supponiamo $m \leq n$. Abbiamo:

$$\frac{1}{m} + \frac{1}{n} - \frac{1}{mn} < \frac{2}{m}$$

(Infatti $\frac{1}{n} \leq \frac{1}{m}$ e $\frac{1}{mn} > 0$.) Quindi $\frac{2}{5} < \frac{2}{m}$, ossia: $m < 5$.

A questo punto possiamo risolvere per tutti i valori di m tali che $1 \leq m \leq 4$, oppure cercare una minorazione di $1/m + 1/n - 1/mn$. Per esempio:

$$\frac{1}{m} + \frac{1}{n} - \frac{1}{mn} \geq \frac{1}{m}$$

Infatti $\frac{1}{n} - \frac{1}{mn} = \frac{m-1}{mn} \geq 0$ (nella correzione c'è scritto $>$ ma è sbagliato come mostra il caso $m = 1$). Segue che $\frac{2}{5} \geq \frac{1}{m}$, cioè $2m \geq 5$ e siccome m è un intero: $m \geq 3$. A questo punto basta risolvere per $m = 3, 4$.

Se $m = 4$: $\frac{2}{5} = \frac{1}{4} + \frac{1}{n} - \frac{1}{4n}$, moltiplicando per $20n$: $8n = 5n + 20 - 5 \Leftrightarrow 3n = 15$, quindi $n = 5$.

Nello stesso modo se $m = 3$ si trova $n = 10$. (Abbiamo appena verificato che $(m, n) = (4, 5), (3, 10)$ sono effettivamente soluzioni).

Per la simmetria tra m e n concludiamo che tutte le coppie ordinate cercate sono esattamente: $(4, 5), (3, 10), (5, 4), (10, 3)$. □

Osservazione 6.2. *La cosa importante è la prima disuguaglianza: $m < 5$: non ci vuole molto a vedere che non ci sono soluzioni per $1 \leq m \leq 3$.*

2a dimostrazione:
Moltiplicando per $5mn$ viene:

$$2mn = 5n + 5m - 5$$

Per il Lemma di Gauss, 5 essendo primo, $5 \mid m$ o $5 \mid n$. Diciamo $m = 5a$. L'equazione si riscrive:

$$2an = n + 5a - 1 \Leftrightarrow a(2n - 5) = n - 1$$

Abbiamo $2n-5 > n-1 \Leftrightarrow n > 4$. Siccome $a \geq 1$, l'equazione non ha soluzioni per $n > 4$.

- Se $n = 4$: $3a = 3$, quindi $a = 1$, cioè $m = 5a = 5$.
- Se $n = 3$: $a = 2$, quindi $m = 10$
- Se $n = 2$: $-a = 1$: impossibile
- Se $n = 1$: $-3a = 0$: impossibile ($m > 0$)

Quindi se $m \mid 5$ le soluzioni sono: $(m, n) = (5, 4), (10, 3)$. Siccome m, n giocano ruoli simmetrici (caso $5 \mid n$), tutte le soluzioni possibili sono: $(5, 4), (4, 5)$, $(10, 3), (3, 10)$. □

Osservazione 6.3. *Questa soluzione usa il Lemma di Gauss.*

3a dimostrazione:
Moltiplicando per $10mn$ viene:

$$4mn = 10n + 10m - 10$$

Proviamo a fattorizzare: $4mn - 10m - 10n = (2m - 5)(2n - 5) - 25$, quindi la nostra equazione diventa:

$$(2m - 5)(2n - 5) = 15 = 3 \times 5$$

Supponiamo $m \leq n$. Per il Teorema Fondamentale dell'Aritmetica: $2m - 5 = 3, 2n - 5 = 5$, cioè $(m, n) = (4, 5)$. Sembrerebbe che ci siamo persi una soluzione! No perché c'è anche il caso: $2m - 5 = 1, 2n - 5 = 15$, ossia: $(m, n) = (3, 10)$.

Se non si vuole usare il TFA si può osservare che le uniche coppie di interi (a, b) con $a \leq b$ tali che $ab = 15$ sono $(-15, -1), (-5, -3), (1, 15), (3, 5)$. Provandole tutte si ritrovano le solite soluzioni. □

7. Febbraio 2013, n. 16

Sia n un intero positivo. Una pulce si trova sulla retta reale ed effettua una sequenza di n salti di lunghezza $1, 2, 3, ..., n$. La pulce può scegliere l'ordine delle lunghezze dei salti e per ogni salto può decidere se saltare verso destra o sinistra.
(a) Dimostrare che per $n = 2012$ la pulce può terminare la sequenza di salti nello stesso punto da cui era partita.
(b) Dimostrare che per $n = 2013$ ciò non è possibile.
(c) In generale per quali n può ritornare al punto di partenza?

Dimostrazione:
Capire il problema: si tratta di vedere per quali n è possibile avere $\varepsilon_1 1 + \varepsilon_2 2 + ... + \varepsilon_n n = 0$ dove $\varepsilon_i \in \{\pm 1\}, \forall i$. Se è possibile allora abbiamo $\sum_{i\in I} i = \sum_{j\in J} j$, dove I, J è una partizione di $\{1, 2, ..., n\}$. Poniamo $x = \sum_{i\in I} i = \sum_{j\in J} j$. Allora $2x = 1 + 2 + ... + n = n(n+1)/2$. Cioè $4x = n^2 + n$. Siccome $n^2 \equiv 0, 1 \pmod 4$, viene $n \equiv 0, 3 \pmod 4$. Quindi una condizione necessaria affinché la pulce torni nell'origine è $n \equiv 0, 3 \pmod 4$.

Mostriamo che queste condizioni sono sufficienti:

- Sia $n \equiv 0 \pmod 4$.

Se $n = 4$, allora 1+4 = 2+3. Poi si va avanti così: mettiamoli in colonna e mettiamo i due numeri successivi ognuno in una colonna:

$(1+4)$	$(2+3)$	
5	6	la colonna di destra ha 1 in più, bisogna pareggiare al colpo dopo
8	7	si pareggia mettendo 8 a destra, 7 a sinistra

Vediamo che $1 + 4 + 5 + 8 = 2 + 3 + 6 + 7$, quindi 8 è a posto e si va avanti così, aggiungendo gli altri quattro numeri successivi:

$(1+4)$	$(2+3)$
5	6
8	7
9	10
12	11

ecc... Supponiamo di essere arrivati a $4n$, allora a sinistra si aggiunge $4n + 1, 4n + 4$ e a destra $4n + 2, 4n + 3$ e abbiamo $4(n + 1)$.

- Sia $n \equiv 3 \pmod 4$

Il procedimento è uguale al precedente partendo da $1 + 2 = 3$.

Quindi la risposta al punto (c) è: la pulce può tornare al punto di partenza se e solo se $n \equiv 0, 3 \pmod 4$

(a) Siccome $2012 \equiv 0 \pmod 4$ ($2012 = 4 \times 503$), in questo caso si può tornare al punto di partenza.

(b) Siccome $2013 = 2012 + 1 \equiv 1 \pmod 4$, in questo caso non si può tornare al punto di partenza. □

Osservazione 7.1. *In realtà la soluzione qui sopra è stata ottenuta guardando* prima *i casi piccoli e osservando le uguaglianze: 1+2 = 3, 2+3= 1+4.*

Per risolvere il problema si è usato: $1 + 2 + 3 + ... + n = n(n + 1)/2$ *(cf Sotto sezione 4.1) e il fatto che un quadrato è* $\equiv 0, 1 \pmod 4$ *(cf Sezione 2).*

Un'altra osservazione: le domande non sono nell'ordine giusto! In realtà le risposte a (a) e (b) usano gli argomenti necessari per risolvere (c).

8. Febbraio 2013, n. 15

Determinare tutte le terne di interi strettamente positivi (a, b, c) *tali che:*
$a \leq b \leq c$
$MCD(a, b, c) = 1$
a *è divisore di* $b + c$, b *è divisore di* $c + a$ *e* c *è divisore di* $a + b$.

Osservazione 8.1. *La prima soluzione proposta (decisamente elaborata) pone su due fatti:*

- *Bisogna avere l'idea di vedere che* a, b, c *sono due a due primi tra di loro.*
- *Bisogna sapere che se* a, b, c *sono due a due primi tra di loro e se ognuno divide* N, *allora* $abc \mid N$. *Questo è evidente se uno conosce il teorema fondamentale dell'aritmetica.*

Dimostrazione:
Questa dimostrazione è una semplificazione della seconda soluzione proposta. Abbiamo $c \mid a + b \leq 2c \Rightarrow a + b = c$ o $2c$ ($a + b$ è un multiplo di c).

Se $a + b = 2c$, $2b \geq a + b = 2c \Rightarrow b = c$ e quindi $a = b = c$ e questo implica $a = b = c = 1$ ($MCD(a, b, c) = 1$).

Se $a + b = c$: $b \mid a + c = 2a + b$. Siccome $2a + b \leq 3b$, abbiamo $2a + b = kb$ con $1 \leq k \leq 3$. Non può essere $k = 1$ ($a > 0$). Se $k = 2$, $b = 2a, c = 3a$. Siccome $(a, b, c) = 1$, $a = 1$ e $(a, b, c) = (1, 2, 3)$. Se $k = 3$, allora $a = b$, $c = 2a$, quindi $(a, b, c) = (1, 1, 2)$. □

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