Incontri di teoria dei numeri e aritmetica

Norberto Gavioli
Dipartimento di Matematica Pura ed Applicata
Università dell'Aquila

Ercole Suppa
Liceo Scientifico A. Einstein
Teramo

Rosanna Tupitti
Liceo Scientifico A. Einstein
Teramo

Progetto Lauree Scientifiche
Teramo – Liceo Scientifico A. Einstein
dicembre 2011 – marzo 2012

Indice

Introduzione

In questo documento viene presentata una traccia riassuntiva di alcuni incontri svoltisi tra dicembre 2011 e Marzo 2012 a Teramo presso il Liceo A. Einstein nell'ambito del progetto *Lauree Scientifiche*. L'argomento sviluppato ha riguardato nozioni e tecniche dell'aritmetica ed il loro impiego nello svolgimento di alcuni problemi delle gare delle *Olimpiadi di Matematica*.

Parte I

Incontro del 6 dicembre 2011

Notazioni

Si suppone che il lettore sia familiare con le notazioni insiemistiche, in particolare con quelle che riguardano gli insiemi numerici:

$$\begin{aligned}
\mathbb{N} &= \{\,0,1,2,3,\cdots\} \text{ (numeri naturali)} \\
\mathbb{Z} &= \{\,0,\pm1,\pm2,\pm3,\cdots\} \text{ (numeri interi)} \\
\mathbb{Q} &= \left\{\,\frac{m}{n} \mid m,n\in\mathbb{Z} \text{ e } n\neq 0\,\right\} \text{ (numeri razionali)} \\
\mathbb{R} &\quad \text{(numeri reali)}
\end{aligned}$$

Numeri razionali e frazioni continue

Mostriamo con esempi come è possibile sviluppare in frazione continua i numeri reali. Come primo esempio sviluppiamo il numero $\alpha = \dfrac{51}{29}$. Notiamo innanzitutto che $1 \leq \alpha < 2$ e pertanto la parte intera di α è uguale a 1. Possiamo allora scrivere α nella forma $\alpha = 1 + \beta_1$ dove $0 \leq \beta_1 = \dfrac{22}{29} < 1$. Più esattamente

$$\alpha = 1 + \frac{22}{29}\ .$$

Chiaramente il numero β_1 è l'inverso del numero $\alpha_1 = \dfrac{29}{22}$. Ripetiamo allora lo stesso procedimento ad α_1. La sua parte intera è 1 e pertanto $\alpha_1 = \dfrac{29}{22} = 1+\beta_2$ dove $\beta_2 = \dfrac{7}{22}$. A sua volta β_2 è l'inverso del numero $\alpha_2 = \dfrac{22}{7}$ pertanto:

$$\alpha = 1 + \frac{1}{\alpha_1} = 1 + \cfrac{1}{1+\cfrac{1}{\alpha_2}}\ .$$

Come prima abbiamo $\alpha_2 = \dfrac{22}{7} = 3 + \beta_3$ dove $\beta_3 = \dfrac{1}{7}$ è l'inverso del numero intero $\alpha_3 = 7$ e rappresenta la parte decimale di α_2. Si ottiene infine

$$\alpha = 1 + \cfrac{1}{1+\cfrac{1}{\alpha_2}} = 1 + \cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{7}}}\ .$$

Analizziamo questo processo. Si parte da un numero razionale positivo

$$\alpha = \frac{r_{-1}}{r_0}$$

dove $r_{-1}, r_0 \in \mathbb{Z}$ sono interi positivi. Si costruiscono allora due successioni q_i e r_i di numeri interi di modo che

1) q_i è l'intero che esprime il quoziente della divisione di r_{i-2} per r_{i-1},

2) r_i è il resto della divisione di r_{i-2} per r_{i-1},

3) $\alpha_i = \dfrac{r_{i-1}}{r_i}$

4) $$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{i-1} + \cfrac{1}{q_i + \cfrac{1}{\alpha_i}}}}}}$$

Dal momento che il resto di una divisione tra numeri interi positivi è non negativo e minore del divisore, si ha che r_i è una successione strettamente decrescente di interi non negativi (in particolare $q_i > 0$ per $i \geq 2$). Pertanto esiste un intero positivo n per il quale $r_n = 0$. All'n-simo passo pertanto il processo si arresta e si trova che

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}} \tag{1}$$

Questa espressione si chiama espansione in frazione continua del numero razionale α e si ottiene con un procedimento che si arresta in numero finito di passi.

Il metodo appena presentato può essere generalizzato in modo da poter essere impiegato con un generico numero reale $\alpha > 0$ (non necessariamente razionale). Si considera un numero positivo α che si scrive come somma di parte intera e parte decimale: $\alpha = q_1 + \beta_1$, dove $q_1 \in \mathbb{N}$ e $0 \leq \beta_1 < 1$. Se $\beta_1 \neq 0$ allora, detto $\alpha_1 = \dfrac{1}{\beta_1} > 1$ il suo inverso si ha

$$\alpha = q_1 + \frac{1}{\alpha_1} \ .$$

A questo punto si applica lo stesso procedimento, che abbiamo mostrato per α, al numero $\alpha_1 = q_2 + \beta_2$. Se $\beta_2 \neq 0$ si pone $\alpha_2 = \dfrac{1}{\beta_2}$ e si ottiene:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\alpha_2}} \ .$$

È chiaro che iterando questo procedimento si trova

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{i-1} + \cfrac{1}{q_i + \cfrac{1}{\alpha_i}}}}}} ,$$

dove per ogni i si ha che $q_i \in \mathbb{N}$ e $0 \leq 1/\alpha_i < 1$.

Nota. Abbiamo visto che nel caso di un numero razionale questo procedimento si arresta come in (3). D'altra parte è evidente che viceversa, se questo procedimento si arresta, il numero α è necessariamente razionale.

Quanto appena notato può essere utilizzato per mostrare che alcuni numeri sono irrazionali. Ad esempio applichiamo il procedimento illustrato al numero $\alpha = \sqrt{2}$. La parte intera di α è 1 pertanto:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\sqrt{2} + 1} = 1 + \frac{1}{2 + (\sqrt{2} - 1)} .$$

I due numeri evidenziati in rosso sono $\beta_1 = \dfrac{1}{\alpha_1}$ e $\beta_2 = \dfrac{1}{\alpha_2}$ e questi sono uguali tra loro. Dal momento che ogni α_i si calcola nello stesso modo a partire ad α_{i-1} si trova $\sqrt{2} + 1 = \alpha_1 = \alpha_2 = \cdots = \alpha_n = \cdots$ e quindi il procedimento si ripete senza mai terminare, cosicché il numero $\sqrt{2}$ risulta essere irrazionale:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}} .$$

Divisione e MCD

Tra le proprietà più importanti dei numeri interi, vi è quella di poter eseguire la divisione con resto.

Teorema. *Dati due numeri interi a e $b \neq 0$ esistono e sono univocamente determinati due numeri interi q ed r, detti rispettivamente quoziente e resto della divisione di a per b, tali che*

1) $a = bq + r$,

2) $0 \leq r < |b|$.

Nota. Nel calcolo di quoziente e resto bisogna fare un minimo di attenzione al fatto che il resto è per definizione un numero non negativo. Ad esempio $22 = 2 \cdot 8 + 6$, pertanto il quoziente ed il resto della divisione di 22 per 8 sono rispettivamente 2 e 6. Se si divide 22 per -8, allora, come ci si attenderebbe, il resto rimane invariato uguale a 6 ed il quoziente cambia segno: $22 = (-2) \cdot (-8) + 6$. Se invece si volesse dividere -22 per 8, il quoziente non è l'opposto del quoziente della divisione di 22 per 8; infatti $-22 = (-3) \cdot 8 + 2$, pertanto il quoziente ed il resto della divisione di -22 per 8 sono rispettivamente -3 e 2.

Definizione. Dati due numeri interi a e b, diremo che b è un divisore di a, o, analogamente, che b divide a, se esiste un numero intero c tale che $a = bc$. In tal caso si scrive $b \mid a$.

Nota. È chiaro che un numero $b \neq 0$ divide a se e solo se il resto della divisione di a per b è uguale a 0.

Tra i numeri positivi maggiori di 1 ve ne sono alcuni particolari detti *numeri primi*.

Definizione. Un numero intero $p > 1$ è detto primo se i suoi unici divisori positivi sono 1 e p.

Nota. Si può dimostrare che un numero intero $p > 0$ è primo se e solo se, ogni qualvolta p divide un prodotto di due o più numeri interi, allora o p divide almeno uno dei fattori del prodotto.

Come esercizio facciamo vedere che se p è un numero primo e $1 \leq i \leq p$ allora p divide il simbolo combinatorio $\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!}$. Per far questo notiamo che $\binom{p}{i} \cdot i! \cdot (p-i)! = p! = p \cdot (p-1)!$ pertanto p divide il prodotto $\binom{p}{i} \cdot i! \cdot (p-i)!$. D'altra parte p non divide $i! = 1 \cdot 2 \cdots i$, in quanto p non divide nessuno dei suoi fattori (che sono tutti più piccoli di p). Per lo stesso motivo p non divide $(p-i)!$ e pertanto p deve dividere $\binom{p}{i}$.

I numeri primi sono i mattoni con i quali tramite il prodotto si possono costruire tutti gli altri numeri interi. Euclide ha infatti dimostrato il seguente importante risultato noto come *Teorema Fondamentale dell'Aritmetica*.

Teorema. *Ogni numero positivo n si scrive in modo unico come prodotto di potenze di numeri primi.*

Ad esempio $a = 420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, $b = 308 = 2^2 \cdot 7 \cdot 11$, sono le *scomposizioni in fattori* di a e b.

Definizione. Dati due interi non nulli a e b, viene chiamato massimo comun divisore di a e b quell'unico intero positivo che è il più grande tra i divisori positivi comuni ad a e b. Il massimo comun divisore di a e b viene denotato con $\mathrm{MCD}(a, b)$. Ogni divisore comune di a e b è anche un divisore di $\mathrm{MCD}(a, b)$.

Sin dalle scuole medie si impara che per calcolare il massimo comun divisore d tra a e b, si scompongono a e b in fattori ed allora d è uguale al prodotto di tutte le potenze dei primi comuni (ad entrambe le scomposizioni) prese una sola volta con il minimo tra i due esponenti con cui compaiono nelle scomposizioni di a e b. Ad esempio $\mathrm{MCD}(420, 308) = 2^2 \cdot 7 = 28$.

Spesso la scomposizione in fattori non è il metodo più efficiente per il calcolo del massimo comun divisore, diventa infatti particolarmente arduo fattorizzare numeri con qualche decina di cifre decimali. Euclide ha trovato un modo molto pratico e veloce per il calcolo del massimo comun divisore tra gli interi.

Supponiamo ad esempio di voler calcolare il massimo comun divisore tra due numeri positivi a e b. Possiamo supporre (a meno di scambiarli) che $a \geq b$ e che b non sia un divisore di a (altrimenti si ha già che $\mathrm{MCD}(a, b) = b$). Chiamiamo q ed r il quoziente ed il resto della divisione di a per b così che si abbia $a = bq + r$. Se d è un divisore comune ad a e b allora potremo scrivere $a = a'd$ e $b = b'd$ ottenendo che d è un divisore comune di b ed r per il fatto che $r = a - bq = a'd - b'dq = d(a' - b'q)$. Viceversa se e è un divisore comune di b ed r allora possiamo scrivere b ed r nella forma $b = b''e$ ed $r = r''e$, ottenendo in tal modo che che $a = bq + r = b''eq + r''e = e(b''q + r'')$ è divisibile per e.

Ne consegue che l'insieme dei divisori comuni ad a e b coincide con l'insieme dei divisori comuni di b ed r e pertanto $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$. Si passa allora dal calcolo del massimo comun divisore della coppia (a, b) al massimo comun divisore della coppia (b, r) che è una coppia *più piccola* di interi positivi, in quanto $a > b$ e $b > r$. Si continua allora reiterando il processo sulla coppia (b, r). È chiaro che questo procedimento termina in un numero finito di passi.

Come esempio calcoliamo il massimo comun divisore tra $a = 51$ e $b = 29$. Il resto della divisione tra 51 e 29 è 22. Scriviamo allora $\mathrm{MCD}(51, 29) = \mathrm{MCD}(29, 22)$. Proseguiamo notando che il resto della divisione di 29 per 22 è 7, pertanto $\mathrm{MCD}(29, 22) = \mathrm{MCD}(22, 7)$. Proseguiamo e vediamo che il resto della divisione di 22 per 7 è 1 e ancora possiamo scrivere $\mathrm{MCD}(22, 7) = \mathrm{MCD}(7, 1)$. A questo punto abbiamo terminato perché 1 è un divisore di 7 e quindi $\mathrm{MCD}(51, 29) = \mathrm{MCD}(7, 1) = 1$. Se guardate poche pagine indietro vi rendete conto che le divisioni che abbiamo effettuato sono esattamente le stesse che abbiamo utilizzato per l'espansione in frazione continua del numero $\dfrac{51}{29}$.

Nota. Il massimo comun divisore tra a e b può essere sempre scritto come somma di un multiplo di a ed un multiplo di b.

Usiamo l'esempio appena esposto per illustrare questo fatto. Vogliamo sempre calcolare il massimo comun divisore tra $a = 51$ e $b = 29$ indicando con r_i l'i-esimo resto ottenuto nel procedimento.

Divisione di 51 per 29:	$51 = 29 \cdot 1 + 22$	$r_1 = 22 = 51 - 29 = a - b$;
Divisione di 29 per 22:	$29 = 22 \cdot 1 + 7$	$r_2 = 7 = 29 - 22 = b - r_1 = 2b - a$;
Divisione di 22 per 7:	$22 = 7 \cdot 3 + 1$	$r_3 = 1 = 3r_2 - r_1 = 7b - 4a$.

Si trova così

$$\mathrm{MCD}(a, b) = r_3 = 1 = -7 \cdot 29 + 4 \cdot 51 = -7b + 4a,$$

come richiamato nella nota. Il metodo illustrato funziona in generale e permette di scrivere MCD(a, b) come somma di un multiplo di a e di un multiplo di b. Per approfondimenti si veda il testo in bibliografia [Sci89].

Congruenze

Definizione 1. Dati due numeri interi a e b ed un intero positivo n, diremo che a è congruo a b modulo n, e scriveremo indifferentemente $a \equiv b \mod n$ oppure $a \equiv_n b$, se la differenza $a - b$ è divisibile per n. Equivalentemente a è congruo a b modulo n se e solo se sono tra loro uguali i resti delle divisioni di a e b per n.

Nota. La relazione $a \sim b \iff a \equiv_n b$ è una relazione di equivalenza in $\mathbb{Z}$. Le classi di equivalenza di questa relazione sono dette classi di resto modulo n e sono esattamente in numero uguale ad n (tante quante i possibili resti nella divisione per n). L'insieme delle classi di congruenza modulo n viene spesso denotato con il simbolo $\mathbb{Z}/n\mathbb{Z}$.

La relazione di congruenza è compatibile con somma e prodotto nel senso del seguente teorema

Teorema. *Se $a \equiv_n b$ e $c \equiv_n d$ allora*

1) $a + c \equiv_n b + d$,

2) $ac \equiv_n bd$.

Esercizi

Vediamo ora come applicare le nozioni esposte ad alcuni esercizi proposti in alcune competizioni connesse alle olimpiadi di matematica.

Esercizio (Giochi di Archimede 2011 – triennio n.3)**.** Su ogni vertice di una piramide a base ottagonale è scritto un numero, che può essere 1, 2 oppure 3, in modo che per ogni faccia (inclusa la base) la somma dei numeri scritti sui suoi vertici sia divisibile per tre. Sapendo che i numeri non sono tutti uguali a 3, quanto vale la somma di tutti i numeri scritti sui vertici?

(A) 12, (B) 14, (C) 15, (D) 18, (E) 21.

Denotiamo con $b_1, \ldots, b_8$ i numeri scritti sui vertici dell'ottagono di base e con v il numero scritto sul vertice della piramide. Abbiamo allora le seguenti

relazioni:

$$\begin{aligned} B = \sum_{i=1}^{8} b_i &\equiv_3 0 \\ b_1 + b_2 + v &\equiv_3 0 \\ b_2 + b_3 + v &\equiv_3 0 \\ b_3 + b_4 + v &\equiv_3 0 \\ b_4 + b_5 + v &\equiv_3 0 \\ b_5 + b_6 + v &\equiv_3 0 \\ b_6 + b_7 + v &\equiv_3 0 \\ b_7 + b_8 + v &\equiv_3 0 \\ b_8 + b_1 + v &\equiv_3 0 \end{aligned}$$

Sommando le ultime otto relazioni si trova

$$0 \equiv_3 2\sum_{i=1}^{8} b_i + 8v = 2B + 8v \equiv_3 2 \cdot 0 + 2v = 2v$$

Pertanto $2v$, essendo congruo a 0 modulo 3, deve essere divisibile per 3. Dal momento che 2 non è divisibile per 3 si ricava che 3 deve dividere v e quindi che $v = 3$. Per quanto stabilito nel testo del problema, non tutti i b_i possono essere divisibili per 3 e le ultime 8 congruenze nella tabella sopra diventano:

$$b_1 \equiv_3 -b_2 \equiv_3 b_3 \equiv_3 -b_4 \equiv_3 b_5 \equiv_3 -b_6 \equiv_3 b_7 \equiv_3 -b_8$$

Ne deduciamo che nessuno dei b_i è uguale a 3 e che su due vertici consecutivi della base non possono esserci gli stessi numeri, pertanto quattro vertici della base riportano il numero 1 e quattro il numero due. Se ne conclude che la somma di tutti i numeri scritti sui vertici è uguale a $v + \sum_{i=1}^{8} b_i = 3 + 4 \cdot 1 + 4 \cdot 2 = 15$.

Esercizio (Giochi di Archimede 2011 – triennio 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.

La risposta corretta è la (A) in quanto un numero divisibile per 2 e per 5 è anche divisibile per 10 e pertanto la sua ultima cifra decimale deve essere uguale a 0.

Questo esercizio ci dà uno uno spunto per parlare di alcuni criteri di divisibilità.

Esercizio. Verificare che un numero è divisibile per 3 se e solo se la somma delle sue cifre decimali è un numero è divisibile per 3.

Notiamo che che $10 \equiv_3 1$. Giacché le congruenze sono compatibili con il prodotto si ha $10^n = \underbrace{10 \times \cdots \times 10}_{n \text{ volte}} \equiv_3 \underbrace{1 \times \cdots \times 1}_{n \text{ volte}} = 1$ per ogni intero non negativo n. Il numero intero x che in forma decimale si scrive in cifre come $c_n c_{n-1} \cdots c_1 c_0$ è uguale a $x = c_n \times 10^n + c_{n-1} \times 10^{n-2} + \cdots + c_\times 10 + c_0 \equiv_3 c_n \times 1 + c_{n-1} \times 1 + \cdots + c_1 \times 1 + c_0 = c_n + c_{n-1} + \cdots + c_1 + c_0$. Troviamo allora che i due numeri x e $y = c_n + c_{n-1} + \cdots + c_1 + c_0$ (che è la somma delle cifre di x) hanno lo stesso resto nella divisione per 3 e pertanto sono l'uno divisibile per 3 se e solo se lo è l'altro.

Esercizio (fatelo voi!)**.** Verificare che un numero è divisibile per 9 se e solo se la somma delle sue cifre decimali è un numero è divisibile per 9.

Esercizio (fatelo voi!)**.** Perchè se la prova del nove fallisce in un prodotto allora il risultato del prodotto è errato?

Parte II

Incontro del 20 dicembre 2011

I quadrati modulo 4

Cerchiamo di determinare i possibili resti nella divisione per 4 del quadrato x^2 di un numero intero x.

Se $x = 2h$ è un numero pari allora $x^2 = 4h^2$ è divisibile per quattro e pertanto $x^2 \equiv 0 \bmod 4$. Il resto nella divisione di x^2 per 4 è quindi 0.

Se $x = 2h + 1$ è un numero dispari allora $x^2 = 4h^2 + 4h + 1 \equiv 1 \bmod 4$. Ne consegue che il resto della divisione di x^2 per 4 è 1.

Riassumendo si trova

$$x^2 \equiv \begin{cases} 0 \bmod 4 & \text{se } x \text{ è pari} \\ 1 \bmod 4 & \text{se } x \text{ è dispari} \end{cases} \tag{2}$$

Le terne pitagoriche

Un problema molto antico è quello di determinare tutti i possibili triangoli rettangoli aventi i lati di lunghezza intera. La soluzione, nota già ad Euclide, si ottiene determinando tutte le terne (x, y, z) di interi positivi tali che $x^2+y^2 = z^2$. Queste si possono parametrizzare come segue:

$$\begin{cases} x = d(u^2 - v^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases} \tag{3}$$

dove d, u e v sono interi positivi e u e v sono primi tra loro. Diamo una dimostrazione seguendo [Sam70, Cap. 1 §2].

Poiché $d^2(u^2-v^2)^2+4d^2u^2v^2 = d^2(u^2+v^2)^2$, si ha che la formula (3) fornisce effettivamente soluzioni dell'equazione $x^2 + y^2 = z^2$.

Verifichiamo ora che viceversa ogni soluzione in interi positivi all'equazione $x^2 + y^2 = z^2$ è della forma (3). Supponiamo che (x, y, z) sia una tale soluzione e chiamiamo d il massimo comun divisore tra x, y e z. Abbiamo allora che $x = d\bar{x}$, $y = d\bar{y}$ e $z = d\bar{z}$ dove $\bar{x}$, $\bar{y}$ e $\bar{z}$ sono interi positivi senza divisori primi comuni tali che $\bar{x}^2 + \bar{y}^2 = \bar{z}^2$. Quest'ultima eguaglianza mostra che $\bar{x}$, $\bar{y}$ e $\bar{z}$ sono a due a due coprimi (ogni primo che divida una coppia di essi deve necessariamente dividere il terzo). In particolare solo uno tra $\bar{x}$, $\bar{y}$ e $\bar{z}$ può essere pari. Inoltre $\bar{x}$, $\bar{y}$ e $\bar{z}$ non possono essere tutti e tre dispari in quanto si troverebbe che $\bar{z}^2 = \bar{x}^2 + \bar{y}^2$ dovrebbe essere contemporaneamente dispari (è il quadrato di un numero dispari) e pari (è la somma di due numeri dispari). Quindi tra i numeri $\bar{x}$, $\bar{y}$ e $\bar{z}$ ce n'è esattamente uno che è pari. Quale? Certamente non $\bar{z}$, perché, se così fosse si avrebbe (in base a quanto detto sui quadrati modulo 4) la contraddizione:

$$0 \equiv \bar{z}^2 = \bar{x}^2 + \bar{y}^2 \equiv 2 \bmod 4.$$

Allora deve essere pari uno solo tra i due interi $\bar{x}$ o $\bar{y}$. A meno di scambiare i nomi di $\bar{x}$ e $\bar{y}$ (senza cambiare l'equazione $\bar{x}^2 + \bar{y}^2 = \bar{z}^2$) possiamo supporre che $\bar{y} = 2h$ sia pari. Otteniamo allora $\bar{y}^2 = 4h^2 = \bar{z}^2 - \bar{x}^2 = (\bar{z} - \bar{x})(\bar{z} + \bar{x})$.

Sappiamo inoltre che $\bar{z}$ e $\bar{x}$ sono entrambi dispari, pertanto sia $\bar{z}-\bar{x}$ che $\bar{z}+\bar{x}$ sono pari. Possiamo allora scrivere $\bar{z}-\bar{x}=2r$ e $\bar{z}+\bar{x}=2s$, dove r ed s sono interi positivi. Troviamo anche che

$$\begin{cases} \bar{x} &= \frac{1}{2}[-(\bar{z}-\bar{x})+(\bar{z}+\bar{x})] = -r+s \\ \bar{z} &= \frac{1}{2}[(\bar{z}-\bar{x})+(\bar{z}+\bar{x})] = r+s \end{cases} \tag{4}$$

Ne deduciamo che i numeri r ed s devono essere primi tra loro, in quanto ogni loro divisore comune è anche un divisore comune di $\bar{x}$ e $\bar{z}$. Riprendiamo l'equazione

$$\bar{y}^2 = 4h^2 = \bar{z}^2 - \bar{x}^2 = (\bar{z}-\bar{x})(\bar{z}+\bar{x}) = 4rs,$$

dal momento che r ed s sono coprimi ne consegue che se p^{2n} è la massima potenza (di esponente necessariamente pari) di un primo p che divide $\bar{y}^2$, essa dovrà dividere uno (ed uno solo) tra r o s. Per il teorema fondamentale dell'aritmetica se ne deduce che gli esponenti dei numeri primi che compaiono nella fattorizzazione di r ed s sono tutti pari, pertanto $r=v^2$ ed $s=u^2$ sono quadrati di numeri interi (positivi) u e v necessariamente primi tra loro. Se ne conclude che $\bar{x}=u^2-v^2$ e $\bar{y}=u^2+v^2$ e $\bar{z}=2u^2v^2$.

Esercizio (Giochi di Archimede 2011)**.** Quante terne ordinate (p,q,r), formate da numeri primi minori di 100, verificano $p^2+q^2=r$? [1 non è un numero primo.]

(A) 2, (B) 4, (C) 6, (D) 8, (E) 16.

Non si tratta di terne pitagoriche, ma la discussione precedente può darci qualche idea di come giungere rapidamente alla soluzione dell'esercizio. Non possiamo avere $r=2$ in quanto 2, come somma di quadrati di numeri positivi può essere scritto nella forma $2=1^2+1^2$, e il numero 1 non è primo. Pertanto r è un primo dipari. Allora p e q sono necessariamente uno pari e l'altro dispari. Supponiamo che quello pari sia p, abbiamo $p=2$.

Inoltre $q^2 < p^2+q^2 = r < 100$, cosicché $q<10$. Le possibilità per q si riducono a $q=3,5,7$ dando luogo alle soluzioni $2^2+3^2=13$, $2^2+5^2=29$ e $2^2+7^2=53$. Considerando il fatto che p e q hanno un ruolo simmetrico nell'equazione, accanto alle soluzioni determinate

$$(p,q,r) = \begin{cases} (2,3,13) \\ (2,5,29) \\ (2,7,53) \end{cases}$$

abbiamo anche

$$(p,q,r) = \begin{cases} (3,2,13) \\ (5,2,29) \\ (7,2,53) \end{cases}$$

Ci sono quindi 6 soluzioni in totale per l'equazione proposta.

Nota. Lo studio delle soluzioni intere dell'equazione $x^2 + y^2 = n$, dove $n > 0$ è un numero naturale fissato, può essere svolto utilizzando la fattorizzazione unica nell'ambito dei numeri complessi a coordinate intere. Si può dimostrare che il numero di soluzioni di tale equazione è uguale a $4(d_1 - d_3)$, dove d_i rappresenta il numero di divisori positivi di n congrui ad i modulo 4 (si veda [IR90, Cap. 16 §6]).

Equazioni lineari

Esercizio. Ci sono punti a coordinate intere sulle rette r ed s di equazione $r : y = \frac{3}{5}x + \frac{4}{5}$ ed $s : y = \frac{2}{5}x + \frac{4}{15}$, e in caso di risposta positiva quanti sono?

Eliminando i denominatori il problema si riduce a determinare le eventuali soluzioni intere delle equazioni:

$$3x - 5y = -4 \tag{5}$$
$$10x - 15y = -4 \tag{6}$$

Si verifica immediatamente che l'equazione (6) non può avere soluzioni intere in quanto, se le avesse, il primo membro risulterebbe essere un multiplo di 5, mentre il secondo non lo è. Pertanto la retta s non ha punti a coordinate intere.

Diverso è il caso dell'equazione (5). Poiché $1 = \mathrm{MCD}(3, 5)$ sappiamo che esistono due numeri interi a e b (ad esempio $a = -3$ e $b = 2$) tali che $3a+5b = 1$. Moltiplichiamo quest'ultima eguaglianza per -4 così da ottenere $3 \cdot (-4a) - 5 \cdot (4b) = -4$. Si scopre quindi che $x = -4a = 12$ e $y = 4b = 8$ formano una soluzione dell'equazione (5) e quindi sono le coordinate intere di un punto che appartiene alla retta r la cui equazione, in forma implicita, è $3x - 5y + 4 = 0$. Notiamo ora che per ogni numero intero h si ha banalmente $3(5h) - 5(3h) = 0$. Pertanto, sommando membro a membro, si trova

$$\begin{array}{lll} 3 \cdot 8 & -5 \cdot 8 & +4 = 0 \\ \underline{3 \cdot (5h)} & \underline{-5 \cdot (3h)} & \underline{= 0} \\ 3 \cdot (12 + 5h) & -5 \cdot (8 + 3h) & +4 = 0 \end{array}$$

Pertanto, al variare di $h \in \mathbb{Z}$, gli infiniti punti a coordinate intere

$$(x_h, y_h) = (12 + 5h, 8 + 3h) \tag{7}$$

appartengono alla retta r.

Esercizio. Mostrare la formula (7) fornisce tutte le soluzioni dell'equazione (5).

Con metodi simili si può dimostrare il seguente risultato generale

Teorema. *Siano a, b e c tre numeri interi senza divisori primi comuni. L'equazione*

$$ax + by = c$$

ammette una soluzione a coordinate intere (x_0, y_0) *se solo se* $\mathrm{MCD}(a, b) = 1$. *In tal caso esistono infinite soluzioni e sono tutte delle forma* (x_h, y_h), *al variare di* $h \in \mathbb{Z}$, *dove*

$$\begin{cases} x_h = x_0 - hb \\ y_h = y_0 + ha \end{cases}$$

Parte III

Incontro del 26 gennaio 2012

Alcuni esercizi

Esercizio (Giochi di Archimede 2011)**.** Un canguro e una rana si trovano inizialmente sullo stesso vertice di un poligono regolare di 41 lati, e cominciano a fare dei salti. La rana salta sempre da un vertice a quello adiacente, in senso antiorario, mentre il canguro salta dal vertice in cui si trova a quello in cui c'è la rana. La sequenza dei salti è questa: la rana fa un salto, il canguro fa un salto; la rana fa due salti, il canguro fa un salto; la rana fa tre salti, il canguro fa un salto, e così via. Dopo che il canguro ha fatto 40 salti, quante volte è tornato sul vertice di partenza?

Numeriamo i vertici del poligono da 0 a 40 in senso antiorario, allora la posizione attuale della rana è determinata dal numero del vertice in cui si trova e questo numero è uguale al resto della della divisione del numero di salti compiuti per 41.

Dopo che che il canguro ha compiuto n salti la rana ne ha compiuti

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

e pertanto se denotiamo con x la sua posizione dopo $n = 40$ salti del canguro si trova

$$x \equiv \frac{40 \cdot 41}{2} \equiv 0 \bmod 41.$$

Ne deduciamo che sia la rana che il canguro stanno ripassando dal punto di partenza. Possono esserci già passati un'altra volta in precedenza? La risposta è no. Infatti se dopo n salti del canguro si trovassero entrambi al punto di partenza, si avrebbe

$$\frac{n(n+1)}{2} \equiv 0 \bmod 41$$

Poiché 41 è un numero primo dispari, deve dividere il numeratore della frazione $\frac{n(n+1)}{2}$ e peritando deve dividere n o $n+1$. D'altra parte $n \leq 40$ e quindi n non può essere divisibile per 41. Si deve allora avere $n + 1 = 41$, ossia $n = 40$.

Possiamo allora rispondere al quesito dicendo che canguro e rana passando per il punto iniziale esattamente una volta sola e questo avviene al quarantesimo salto del canguro.

Esercizio (Giochi di Archimede 2011)**.** Gabriella scrive una successione di 10 numeri (eventualmente negativi), in modo che ciascun numero della successione, dal terzo in poi, sia la somma dei due che lo precedono. Il primo numero della successione è 34 mentre l'ultimo è 0. Quanto vale la somma di tutti i numeri della successione?

Scriviamo a rovescio la successione di Gabriella (ogni termine è somma dei due successivi), chiamando a il penultimo numero da lei scritto. Troviamo:

$$0, a, -a, 2a, -3a, 5a, -8a, 13a, -21a, 34a$$

Si trova che $a = 1$ e che la somma richiesta è uguale a

$$0 + 1 - 1 + 2 - 3 + 5 - 8 + 13 - 21 + 34 = 22.$$

Esercizio (Giochi di Archimede 2011)**.** Diciamo che una coppia di numeri naturali (a, b) è bella se comunque si scelga una coppia di numeri naturali (c, d) tali che $ab = cd$, vale $a + b = c + d$. Quante sono le coppie belle?

(A) Nessuna, (B) una, (C) cinque, (D) sette, (E) più‘ di otto.

Sono infinite: ogni coppia della forma $(1, p)$ dove p è un numero primo, è bella.

La domanda può essere ampliata chiedendosi quali sono le coppie di numeri naturali (a, b) per le quali il prodotto ab determina la somma $a+b$. Notiamo che se le coppie $(ab, 1)$, (a, b) hanno lo stesso prodotto delle coordinate, ci chiediamo quando $ab+1 = a+b$. Si trova $1 = ab-a-b = (a-1)(b-1)+1$ e se ne deduce che $a = 1$ o $b = 1$. Pertanto le coppie belle sono della forma $(a, 1)$ o $(1, b)$. Per quanto appena mostrato sia a che b devono necessariamente essere primi.

Esercizio (Giochi di Archimede 2011)**.** Marta ha scritto sulla lavagna un numero intero pari. Per 12 volte Marta sostituisce il numero scritto sulla lavagna con il suo quadrato aumentato di 5. Con quali cifre può terminare il numero che si trova scritto sulla lavagna alla fine dei calcoli di Marta?

(A) 0 oppure 4, (B) 0, 4 oppure 6, (C) 0 oppure 6, (D) 4 oppure 6, (E) può terminare con una qualsiasi cifra pari.

Analizziamo due passi consecutivi della successione scritta da Marta. Supponiamo che alla lavagna compaia il numero pari $x_n = 2a$, dopo due passi comparirà $x_{n+2} = ((2a)^2 + 5)^2 + 5 = 16a^4 + 40a^2 + 30 \equiv (2a)^4 \bmod 10$. Elenchiamo ora le quarte potenze dei numeri pari modulo 10:

$$\begin{aligned}
0^4 &= 0 && \equiv 0 \bmod 10\\
2^4 &= 16 && \equiv 6 \bmod 10\\
4^4 &= 16^2 \equiv 6^2 = 36 && \equiv 6 \bmod 10\\
6^4 &= (6^2)^2 = (36)^2 \equiv 6^2 = 36 && \equiv 6 \bmod 10\\
8^4 &= (8^2)^2 = (64)^2 \equiv (4)^2 = 16 && \equiv 6 \bmod 10
\end{aligned}$$

Pertanto, qualunque sia il numero pari x_0, si trova che x_2, x_4, $\ldots$, x_{12} hanno come ultima cifra 0 o 6.

Esercizio (Giochi di Archimede 2011)**.** Abbiamo una sequenza di 2011 numeri, di cui indichiamo con an il termine n-esimo. Sapendo che $a_1 = 1$, e che per ogni $n \geq 2$, $a_n = a_{n-1}(3n + 1)$, trovare le ultime quattro cifre del termine a_{2011}.

(A) 0000, (B) 3400, (C) 6000, (D) 6031, (E) 6034.

Basta notare che $a_n \neq 0$ e che a_{2011} è divisibile per a_n se $1 \leq n \leq 2010$. Inoltre $a_3 = 10a_2$ è divisibile per 10 e $a_{333} = 1000a_{332}$ è divisibile per 1000. Pertanto a_{2011} è non nullo e divisibile per 10000 e le sue ultime quattro cifre sono quindi 0000.

Elementi invertibili modulo n

Si supponga di dover determinare tutte le soluzioni intere dell'equazione

$$7x + 15y = 9. \tag{8}$$

Sappiamo dal paragrafo precedente che questa equazione ha infinite soluzioni. Una sua formulazione equivalente è

$$7x \equiv 9 \bmod 15. \tag{9}$$

notiamo che $13 \cdot 7 = 91 = 1 + 15 \cdot 4 \equiv 1 \bmod 15$. Supposto che x sia una soluzione della congruenza (9), troviamo

$$x = 1 \cdot x \equiv_{15} (13 \cdot 7)x = 13 \cdot (7x) \equiv_{15} 13 \cdot 9 = 117 \equiv_{15} 12.$$

Viceversa se x è un intero tale che $x \equiv 12 \bmod 15$, allora, moltiplicando entrambi i membri per 7 si ottiene

$$7x \equiv 7 \cdot 12 = 84 \equiv 9 \bmod 15.$$

Abbiamo quindi scoperto che *x è la prima coordinata di una soluzione (x, y) dell'equazione (8) se e solo se $x \equiv 12 \bmod 15$*. È facile a questo punto determinare anche la seconda coordinata y. Sappiamo che $x = 12 + 15h$ e $15y = 9 - 7x = 9 - 84 - 105h = -75 - 105h = 15(-5 - 7h)$, da cui $y = -5 - 7h$. Le soluzioni dell'equazione proposta sono quindi tutte e sole quelle della forma $(x_h, y_h) = (12 + 5h, -5 - 7h)$ al variare di $h \in \mathbb{Z}$, come previsto dal teorema del paragrafo precedente.

Il nuovo approccio consiste nell'aver notato che $13 \cdot 7 \equiv 1 \bmod 15$. Più in generale si dà la seguente definizione.

Definizione. Sia n un numero positivo. Un numero intero $a \in \mathbb{Z}$ è detto invertibile modulo n se esiste un'altro intero $b \in \mathbb{Z}$, detto inverso di a modulo n, tale che $ab \equiv 1 \bmod n$.

Mostriamo alcune proprietà elementari degli inversi modulo n.

Proposizione. *Dato un intero positivo n ed $a \in \mathbb{Z}$, si supponga che a ammetta un inverso b modulo n allora*

1) $\mathrm{MCD}(a, n) = 1$,

2) $\mathrm{MCD}(b, n) = 1$,

3) b' è un altro inverso di a modulo n se e solo se $b \equiv b' \bmod n$,

4) a è un inverso di b modulo n.

Dimostrazione.

1) La condizione $ab \equiv 1 \bmod n$ si esprime con il fatto che esiste un intero h tale che $ab - 1 = hn$, ossia $ab - hn = 1$, cosicché ogni divisore d comune ad a ed n deve dividere necessariamente 1. Pertanto $d = 1$.

2) Si dimostra come il punto precedente.

3) $b' = b' \cdot 1 \equiv_n b' \cdot (ab) = (b'a)b \equiv_n 1 \cdot b = b$.

4) Questo punto è ovvio. □

Parte IV

Incontro del 23 febbraio 2012

Teorema cinese dei resti

Teorema (Teorema cinese dei resti)**.** *Per ogni k-upla* $(n_1, \ldots, n_k)$ *di interi positivi a due a due primi tra loro e per ogni k-upla* $(a_1, \ldots, a_k)$ *di numeri interi esistono infinite soluzioni del sistema di congruenze*

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ x \equiv a_k \bmod n_k \end{cases} \tag{10}$$

Le soluzioni di detto sistema formano una classe di resto modulo $n = n_1 \cdots n_k$*.*

Utilizziamo il metodo di Lagrange per dare una dimostrazione. Si inizia con il porre $N_i = n/n_i = \prod_{j \neq i} n_j$ e si nota che $\mathrm{MCD}(N_1, \ldots, N_k) = 1$. Dal Teorema di Bezout si deduce che esistono degli interi $e_1, \ldots, e_k$ tali che $\sum_{i=1}^{k} e_i N_i = e_1 N_1 + \cdots + e_k N_k = 1$. Da questa uguaglianza, notando che $N_j \equiv 0 \bmod n_i$ per $i \neq j$, si trova che $N_i e_i \equiv 1 \bmod n_i$ e $N_i e_i \equiv 0 \bmod n_j$ per $j \neq i$ Si pone allora

$$x = \sum_{i=1}^{k} a_i e_i N_i = a_1 e_1 N_1 + \cdots + a_k e_k N_k$$

cosicché $x \equiv a_i (e_i N_i) \equiv a_i \bmod n_i$. Pertanto x è una soluzione del sistema (10).

Come esempio consideriamo il sistema

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 14 \\ x \equiv 11 \bmod 17 \end{cases}$$

e risolviamolo con il metodo di Lagrange. Abbiamo $n_1 = 5$, $n_2 = 14$ e $n_3 = 17$ cosicché $N_1 = n_2 n_3 = 238$, $N_2 = n_1 n_3 = 85$ e $N_3 = n_1 n_2 = 70$. Con l'algoritmo di Euclide possiamo scrivere $17 = \mathrm{MCD}(N_1, N_2) = -N_1 + 3N_2$ e quindi $1 = \mathrm{MCD}(N_1, N_2, N_3) = \mathrm{MCD}(\mathrm{MCD}(N_1, N_2), N_3) = \mathrm{MCD}(17, N_3) = 33 \cdot 17 - 8N_3 = 33(-N_1 + 3N_2) - 8N_3 = -33N_1 + 99N_2 - 8N_3$. Una soluzione particolare è allora $x = -33 \cdot 5 \cdot N_1 + 99 \cdot 4 \cdot N_2 - 8 \cdot 11 \cdot N_3 = 3938$. Riducendo modulo $n = 1190$ si può scegliere $x = 368 = 3938 \bmod 1190$.

Come ulteriore esercizio diamo una versione semplificata di un quesito olimpionico.

Esercizio. Si mostri che se a e b sono due interi positivi tali che $4ab - 1$ divide $4a^2 - 1$ allora $a = b$.

Ancora sugli elementi invertibili modulo n

Denotiamo con $\varphi(n)$ il numero degli interi compresi tra 0 ed n che sono invertibili modulo n. La funzione φ viene chiamata φ *di Eulero.*

Come sopra si supponga che $n = n_1 \cdots n_k$ dove $\mathrm{MCD}(n_i, n_j) = 1$ per $i \neq j$. Sappiamo x è un intero invertibile modulo n se e solo se $\mathrm{MCD}(x, n) = 1$. D'altra parte $\mathrm{MCD}(x, n) = 1$ se e solo $\mathrm{MCD}(x, n_1) = \mathrm{MCD}(x, n_2) = \cdots = \mathrm{MCD}(x, n_k) = 1$. Se denotiamo allora con a_1, a_2, ..., a_k i resti delle divisioni di x per n_1, n_2, ..., n_k, si trova che $\mathrm{MCD}(a_i, n_i) = 1$ e che pertanto a_i è invertibile modulo n_i. Viceversa se a_1, a_2, ..., a_k, sono tali che $\mathrm{MCD}(a_i, n_i) = 1$ e se $x \equiv a_i \bmod n_i$ si ha che $\mathrm{MCD}(x, n) = 1$, ossia che x è invertibile modulo n. Dal teorema cinese dei resti si trova allora

Proposizione. *Se* $\mathrm{MCD}(n_i, n_j) = 1$ *per* $i \neq j$ *allora* $\varphi(n) = \varphi(n_1) \cdots \varphi(n_k)$.

Esercizio. Determinare $\varphi(11^7)$.

In base alla definizione bisogna contare quanti sono i numeri positivi più piccoli di 11^7 primi con 11^7, ossia non divisibili per 11. Ci sono 11^7 numeri positivi minori o eguali a 11^7. Fra di essi ce ne sono 11^6 che sono divisibili per 11 (uno ogni 11). Pertanto $\varphi(11^7) = 11^7 - 11^6 = 11^7 \left(1 - \frac{1}{11}\right)$.

In generale, con lo stesso ragionamento, si può vedere che se p è un numero primo allora $\varphi(p^h) = p^h \left(1 - \frac{1}{p}\right)$. Se $n = p_1^{e_1} \cdots p_k^{e_k}$ è la fattorizzazione di n come prodotto di potenze di numeri primi distinti dalla proposizione precedente abbiamo

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_1^{e_1}\right) \cdots \varphi\left(p_k^{e_k}\right) \\
&= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{e_k} \left(1 - \frac{1}{p_k}\right) \\
&= p_1^{e_1} \cdots p_k^{e_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

Diamo ora (senza dimostrazione) il seguente famoso teorema.

Teorema (formula di Eulero)**.** *Se* $n > 1$ *è un numero naturale e* x *è un intero tale che* $\mathrm{MCD}(x, n) = 1$ *allora*

$$x^{\varphi(n)} \equiv 1 \bmod n.$$

Il seguente esercizio può essere utile per risolvere il Problema 5 delle Olimpiadi internazionali di matematica del 2007.

Esercizio. Siano a e b interi positivi tali che $4ab - 1$ divide $(4a^2 - 1)^2$. Dimostrare che $4ab - 1$ divide $(a - b)^2$.

Supponiamo che p sia un numero primo e che $p^h > 1$ sia la più alta potenza di p che divide $4ab - 1$ (che è un numero dispari). Ne deduciamo che p^h è dispari e divide $(4a^2 - 1)^2 = (2a - 1)^2(2a + 1)^2$. Giacché $2a + 1$ e $2a - 1$ hanno come

differenza 2, il loro massimo comun divisore è 2, ne consegue che p^h divide uno ed uno solo tra i due numeri $(2a-1)^2$ e $(2a+1)^2$. Posto

$$2k = \begin{cases} h & \text{se } h \text{ è pari} \\ h+1 & \text{se } h \text{ è dispari} \end{cases}$$

si ha che p^{2k} divide divide uno ed uno solo tra i due numeri $(2a-1)^2$ e $(2a+1)^2$, e quindi che p^k divide divide uno ed uno solo tra i due numeri $2a-1$ e $2a+1$. Si trova allora $2a \equiv \pm 1 \bmod p^k$. Nel caso in cui $a \equiv 1 \bmod p^k$ si ha $0 \equiv 4ab - 1 = 2a \cdot 2b - 1 \equiv 2b - 1 \bmod p^k$, da cui si deduce che $2b \equiv 1 \equiv a \bmod p^k$. Se invece $a \equiv -1 \bmod p^k$ si ha $0 \equiv 4ab - 1 = 2a \cdot 2b - 1 \equiv -2b - 1 \bmod p^k$, da cui si deduce che $2b \equiv -1 \equiv a \bmod p^k$. In ogni caso si trova sempre $a \equiv b \bmod p^k$. Consideriamo ora la scomposizione nel prodotto di potenze di numeri primi distinti del numero $4ab - 1$:

$$4ab - 1 = p_1^{h_1} \cdots p_s^{h_s}.$$

Come sopra poniamo

$$2k_i = \begin{cases} h_i & \text{se } h_i \text{ è pari} \\ h_i+1 & \text{se } h_i \text{ è dispari} \end{cases}$$

ottenendo che $a \equiv b \bmod p_i^{k_i}$. Poiché i primi p_i sono a due a due coprimi tra loro, dal Teorema cinese dei resti si trova che $a \equiv b \bmod p_1^{k_1} \cdots p_s^{k_s}$, o, equivalentemente, che $p_1^{k_1} \cdots p_s^{k_s}$ divide $a - b$. Siccome $4ab - 1 = p_1^{h_1} \cdots p_s^{h_s}$ divide $p_1^{2k_1} \cdots p_s^{2k_s}$ e quest'ultimo numero divide $(a-b)^2$, segue che $4ab - 1$ è un divisore di $(a-b)^2$ come richiesto.

Parte V

Incontro del 22 marzo 2012

Equazioni quadratiche

Il tema principale di questo ultimo incontro riguarda le equazioni quadratiche. Vedremo insieme alcuni esempi di equazioni quadratiche diofantee senza darne una trattazione specifica.

Equazioni quadratiche nelle quali una variabile compare al primo grado

Esercizio. Determinare tutte le soluzioni intere dell'equazione

$$y + 2xy - 14x + 4x^2 - 9 = 0.$$

In questa equazione la variabile y compare al primo grado e possiamo pertanto esplicitarla.

$$y(1 + 2x) - 14x + 4x^2 - 9 = 0$$
$$y = \frac{-4x^2 + 14x + 9}{2x + 1}$$

Eseguendo la divisione di $-4x^2 + 14x + 9$ per $2x + 1$ si trova $-2x + 8$ come quoziente e 1 come resto, ossia $-4x^2 + 14x + 9 = (2x + 1)(-2x + 8) + 1$. Sostituendo quest'espressione nell'equazione si trova:

$$y = \frac{-4x^2 + 14x + 9}{2x + 1} = -2x + 8 + \frac{1}{2x + 1}$$

Dal momento che se x e y sono interi lo sono anche le parti dell'equazione evidenziate in rosso, si evince che (x, y) è una soluzione intera dell'equazione proposta se solo se $\dfrac{1}{2x + 1}$ è un numero intero e quindi se e solo se $2x + 1$ è un divisore di 1. Si ottiene quindi $2x + 1 = \pm 1$ e di conseguenza $x = 0$ o $x = -1$. Le soluzioni intere dell'equazioni sono allora tutte e sole $(x, y) = (0, 9)$ e $(x, y) = (-1, 9)$.

Equazione di Pell

L'equazione di Pell ha una forma generale del tipo

$$x^2 - Dy^2 = 1 \tag{11}$$

dove $D \in \mathbb{Z}$ non è un quadrato perfetto. Un'altro modo equivalente di richiedere che D non sia un quadrato perfetto è che $\sqrt{D}$ sia un numero irrazionale. Per una trattazione generale si veda ad esempio il decimo capitolo di [Hua82] oppure [IR90, §10.9].

È noto che questa equazione ammette sempre infinite soluzioni che possono essere determinate a partire da una soluzione particolare (x_1, y_1), detta anche

soluzione fondamentale. A sua volta la soluzione fondamentale si ricava a partire dallo sviluppo in frazione continua del numero $\sqrt{D}$.

Supponiamo ad esempio di voler determinare la soluzione fondamentale dell'equazione

$$x^2 - 12y^2 = 1 \tag{12}$$

Come abbiamo fatto nel primo incontro sviluppiamo $\alpha = \sqrt{12}$ in frazione continua. Notiamo che $\alpha = 3 + (\alpha - 3)$ dove $0 < \alpha - 3 < 1$. Calcoliamo ora $\dfrac{1}{\alpha - 3} = \dfrac{\alpha + 3}{\alpha^2 - 9} = \dfrac{\alpha + 3}{3} = 1 + \dfrac{\alpha}{3} = 2 + \dfrac{\alpha - 3}{3}$, dove $0 < \dfrac{\alpha - 3}{3} < 1$. Continuiamo calcolando l'inverso di $\dfrac{\alpha - 3}{3}$. Si trova $\dfrac{3}{\alpha - 3} = 3\left(\dfrac{1}{\alpha - 3}\right) = 3\left(2 + \dfrac{\alpha - 3}{3}\right) = 6 + (\alpha - 3)$, dove $0 < \alpha - 3 < 1$. Al passo successivo dovremo calcolare l'inverso di $\alpha - 3$, cosa che abbiamo già fatto e pertanto da questo momento tutti i calcoli successivi si ripetono ciclicamente. Otteniamo quindi

$$\begin{aligned}
\sqrt{12} = 3 + (\alpha - 3) &= 3 + \cfrac{1}{2 + \dfrac{\alpha - 3}{3}} \\
&= 3 + \cfrac{1}{2 + \cfrac{1}{6 + (\alpha - 3)}} \\
&= 3 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{2 + \dfrac{\alpha - 3}{3}}}} \\
&= 3 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{2 + \cfrac{1}{6 + \cfrac{1}{\ddots}}}}}}}
\end{aligned}$$

Se guardiamo i numeri che compaiono a sinistra nei **denominatori** che si susseguono nella frazione continua questi formano una successione periodica: 2, 6, 2, 6, 2,... Fermiamoci alla prima ripetizione (in rosso nell'espressione precedente) e scriviamo la frazione continua troncata risultante **nella forma ridotta ai**

minimi termini:

$$3+\cfrac{1}{2+\cfrac{1}{6+\cfrac{1}{2}}}=\frac{97}{28}$$

Posto $x_0 = 97$ (numeratore della precedente frazione) e $y_0 = -28$ (opposto del denominatore della precedente frazione) si ha

$$x_0^2 - 12y_0^2 = 9409 - 12 \cdot 784 = 1$$

Abbiamo trovato in questo modo la soluzione fondamentale $(x_0, y_0) = (97, -28)$ dell'equazione di Pell proposta.

Torniamo al problema generale della soluzione dell'Equazione di Pell (11). Consideriamo l'insieme $\mathbb{Q}[\sqrt{D}]$ definito da

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

Se $\alpha = a+b\sqrt{D}$ e $\beta = c+d\sqrt{D}$, dove $a, b, c, d \in \mathbb{Q}$, sono due elementi di $\mathbb{Q}[\sqrt{D}]$ tali che $\alpha = \beta$ allora da $a + b\sqrt{D} = c + d\sqrt{D}$ si ottiene $a - c = (d - b)\sqrt{D}$. Notiamo che che se $d \neq b$ allora $\sqrt{D} = \dfrac{a-c}{d-b} \in \mathbb{Q}$, contro l'ipotesi che $\sqrt{D}$ sia un numero irrazionale. Ne deduciamo che si deve avere $b = d$ e $a = c$. Pertanto se $a, b \in \mathbb{Q}$, allora in numero $\alpha = a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ determina univocamente a e b. Chiameremo allora coniugato di α il numero (ben definito) $\bar{\alpha} = a - b\sqrt{D}$. Notiamo che se $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$ allora $\overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}$.

Definizione. Diremo anche che $\alpha = a + b\sqrt{D}$ è un numero di Pell se $\alpha \cdot \bar{\alpha} = (a+b\sqrt{D})\cdot(a-b\sqrt{D}) = a^2 - Db^2 = 1$, ossia se (a, b) è una soluzione dell'equazione di Pell.

Se α e β sono due numeri di Pell allora $(\alpha\beta)\cdot\overline{(\alpha\beta)} = \alpha\beta\bar{\alpha}\bar{\beta} = (\alpha\cdot\bar{\alpha})(\beta\cdot\bar{\beta}) = 1\cdot 1 = 1$. Pertanto il prodotto di due numeri di Pell è anch'esso un numero di Pell. Anche l'opposto ed il coniugato di un numero di Pell sono numeri di Pell. In particolare se $\alpha_0 = x_0 + y_0\sqrt{D}$ è il numero di Pell che corrisponde alla soluzione fondamentale (x_0, y_0) dell'equazione (11), allora $\alpha_n = \alpha_0^n = x_n + y_n\sqrt{D}$ è ancora un numero di Pell, inoltre si può dimostrare che α_0 è il più piccolo numero di Pell positivo. **Le soluzioni dell'equazione di Pell sono quindi infinite** e, facendo riferimento alla notazione introdotta, sono tutte e sole le coppie della forma

$$(\pm x_n, \pm y_n)$$

associate ai numeri di Pell della forma

$$\pm\alpha_n \text{ e } \pm\bar{\alpha}_n.$$

Si può dare una formula esplicita per x_n e y_n (nelle seguenti formule $\lfloor n \rfloor$ rappresenta la parte intera di n):

$$x_n = \frac{\alpha_0^n + \bar{\alpha}_0^n}{2} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} x_0^{n-2i} y_0^{2i} D^i;$$

$$y_n = \frac{\alpha_0^n - \bar{\alpha}_0^n}{2} = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} x_0^{n-2i-1} y_0^{2i+1} D^i.$$

Problemi riconducibili all'equazione di Pell

Il problema che proponiamo è tratto da [AG09, §3.9].

Esercizio. Il triangolo di lati 3, 4, 5 e quello di lati 13, 14, 15 area intera e i lati che sono tre interi consecutivi. Determinare tutti i possibili triangoli con questa proprietà.

Si comincia porre $a = n - 1$, $b = n$ e $c = n + 1$ e si determina l'area A del triangolo di lati a, b e c tramite la formula di Erone:

$$\begin{aligned} A &= \frac{1}{4}\sqrt{(a+b+c)(a+b-c)(a+c-b)(b+c-a)} \\ &= \frac{1}{4}\sqrt{3n \cdot (n-2) \cdot n \cdot (n+2)} \\ &= \frac{n}{4}\sqrt{3(n^2-4)} \end{aligned}$$

Se n fosse dispari troveremmo che il prodotto $n\sqrt{3(n^2-4)}$ sarebbe dispari e pertanto A non potrebbe essere un numero intero. Viceversa nel caso in cui n fosse pari si troverebbe che anche $\sqrt{3(n^2-4)}$ sarebbe pari cosicché $n\sqrt{3(n^2-4)}$ sarebbe divisibile per 4 ed A sarebbe un numero intero. Possiamo quindi porre $n = 2x$ dove x è un intero. Elevando al quadrato e dividendo per $\frac{x^2}{4}$ si ottiene

$$\frac{A^2}{x^2} = 3(x^2 - 1)$$

Ne deduciamo che $m = \frac{A}{x}$ è un numero intero intero divisibile per 3: poniamo $m = 3y$ dove y è intero. Sostituendo m e semplificando per 3 si trova infine l'equazione di Pell:

$$x^2 - 3y^2 = 1 \tag{13}$$

Le infinite soluzioni di (13) determinano i triangoli richiesti dal problema.

Carattere quadratico di -1

Fissiamo ora un numero primo p dispari e cerchiamo di determinare gli interi x tali che che x sia inverso di sè stesso modulo p. Questa condizione si esprime scrivendo $x \cdot x \equiv 1 \bmod p$, ossia

$$x^2 \equiv 1 \bmod p. \tag{14}$$

Supposto che x soddisfi la condizione (14) si ottiene che p deve essere un divisore di $x^2 - 1 = (x-1)(x+1)$. Ne deduciamo che la condizione (14) è soddisfatta se e solo se $x \equiv \pm 1 \bmod p$.

Notiamo ora che nel prodotto

$$(p-1)! = 1 \cdot 2 \cdots (p-2) \cdot (p-1) \tag{15}$$

Compaiono tutti i rappresentanti modulo p degli interi non divisibili per p. A parte i fattori 1 e $p-1$ che coincidono con i loro inversi modulo p, gli altri fattori possono essere raggruppati in coppie nelle quali ciascuno dei due fattori è inverso dell'altro modulo p. Queste coppie, composte da due numeri il cui prodotto è 1 modulo p, nel prodotto (15) si semplificano (mod p) e pertanto

$$(p-1)! = 1 \cdot 2 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \bmod p$$

Abbiamo ottenuto quindi il famoso

Teorema (di Wilson)**.** *Se p è un numero primo dispari allora*

$$(p-1)! \equiv -1 \bmod p.$$

Continuiamo la nostra analisi. Notiamo che per $i = 1, 2, \ldots, \dfrac{p-1}{2}$ si ha che $p - i \equiv -i \bmod p$. Possiamo allora scrivere

$$\begin{aligned} -1 \equiv_p (p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right) \cdots (p-2) \cdot (p-1) \\ &\equiv_p 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-2) \cdot (-1) \\ &= (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \end{aligned}$$

Nel caso in cui $p \equiv 1 \bmod 4$, ossia $\dfrac{p-1}{2}$ è un numero pari, si ottiene

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \bmod p.$$

Viceversa, se esiste un numero intero x tale che $x^2 \equiv -1 \bmod p$ si trova che se $y \in \mathbb{Z}$ non è divisibile per p allora i quattro numeri y, yx, $yx^2 \equiv_p -y$ e $yx^3 \equiv_p -xy$ sono tra loro a due a due incongrui modulo p e sono le quattro radici quarte di y^4 modulo p. Pertanto i $p-1$ resti non nulli modulo p sono ripartiti a 4 a 4 in insiemi di numeri che hanno la stessa quarta potenza. Ne deduciamo che 4 divide $p-1$. Riassumendo troviamo:

Teorema. *Dato un primo dispari p esiste un intero x tale che $x^2 \equiv -1 \bmod p$ se e solo se $p \equiv 1 \bmod 4$.*

Esercizio. Determinare il numero di soluzioni (x, y, z) intere e primitive (ossia per le quali $\mathrm{MCD}(x, y, z) = 1$) dell'equazione

$$x^2 + y^2 = pz^2$$

dove $p \equiv 3 \bmod 4$

Vediamo due metodi per risolvere il problema.
Il primo richiede una riduzione modulo 4, si ottiene

$$x^2 + y^2 \equiv 3z^2 \bmod 4$$

Poiché i quadrati modulo 4 sono congrui a 0 o a 1, l'unica possibilità è che $x \equiv y \equiv z \equiv 0 \bmod 4$. In tal caso 2 divide $\mathrm{MCD}(x, y, z)$ e la soluzione non può essere primitiva. Si deduce che l'equazione non ammette soluzioni primitive.

L'altro metodo consiste nel supporre che una soluzione (x, y, z) primitiva esista e nel ridurre modulo p. Si trova

$$x^2 \equiv -y^2 \bmod p$$

Se y fosse divisibile per p allora lo dovrebbe essere anche x. In tal caso p^2 dovrebbe dividere $x^2 + y^2 = pz$ e pertanto p dividerebbe z e allora la soluzione non sarebbe primitiva. Pertanto y è invertibile modulo p: esiste $u \in \mathbb{Z}$ tale che $uy \equiv 1 \bmod p$. Troviamo allora

$$(ux)^2 \equiv -(uy)^2 \equiv -1 \bmod p$$

Dal precedente teorema deduciamo che $p \equiv 1 \bmod 4$ contro il quanto richiesto dall'esercizio.

Parte VI

Ulteriori esercizi

Esercizi proposti

Esercizio 1 (Gara Nazionale di Cesenatico 1995, problema 6)**.** Trovare tutte le coppie di interi positivi x, y tali che

$$x^2 + 615 = 2^y.$$

Soluzione. Se (x, y) è una soluzione dell'equazione $x^2 + 615 = 2^y$, il numero y deve essere pari. Infatti da $x^2 + 615 = 2^y$ segue che $x^2 \equiv (-1)^y \pmod 3$ e ciò implica che y è pari altrimenti si avrebbe $x^2 \equiv 2 \pmod 3$ il che è impossibile in quanto gli unici residui quadratici modulo 3 sono 0 ed 1. Posto $y = 2t$ si ha:

$$\left(2^t\right)^2 - x^2 = 615 \quad \Leftrightarrow \quad \left(2^t + x\right)\left(2^t - x\right) = 3 \cdot 5 \cdot 41$$

e allora x, t soddisfano un sistema del tipo

$$\begin{cases} 2^t + x = a \\ 2^t - x = b \end{cases} \quad \Rightarrow \quad \begin{cases} 2^t = \frac{a+b}{2} \\ x = \frac{a-b}{2} \end{cases}$$

con a, b numeri interi positivi che dividono 615 e tali che $a > b$, $a \cdot b = 615$, $a+b = 2^{t+1}$. Gli unici interi positivi che soddisfano tali condizioni sono $a = 123$, $b = 5$ e quindi

$$\begin{cases} 2^t + x = 123 \\ 2^t - x = 5 \end{cases} \quad \Rightarrow \quad \begin{cases} 2^t = \frac{128}{2} = 64 \\ x = \frac{118}{2} = 59 \end{cases} \quad \Rightarrow \quad \begin{cases} x = 59 \\ y = 2t = 12 \end{cases}$$

Gli unici interi positivi che verificano l'equazione $x^2 + 615 = 2^y$ sono $x = 59$, $y = 12$. □

Esercizio 2 (Gara provinciale 1996, problema 5)**.** Il numero n diviso per 1995 dà resto 29. Sapendo che n dà resto 29 anche diviso per 1996 determinare l'ultima cifra di n ?

Soluzione. $n - 29$ è divisibile per 1995 e per 1996, quindi è divisibile per 2 e per 5. Allora $n - 29$ è divisibile per 10 per cui ha l'ultima cifra uguale a 0. Ne segue che l'ultima cifra di n è 9. □

Esercizio 3 (Gara provinciale 1996, problema 13)**.** Un numero è composto da 77 cifre, tutte uguali a 7. Qual è il resto della divisione di questo numero per 101?

Soluzione. Il numero $7777 = 77 \cdot 101$ è divisibile per 101, dunque anche il numero $7777 \cdot 10^n$ è divisibile per 101 per qualsiasi n intero. Il numero dato si può scrivere nella forma

$$7777 \cdot 10^{73} + 7777 \cdot 10^{69} + \cdots + 7777 \cdot 10^5 + 7777 \cdot 10 + 7$$

e dunque è la somma di multipli di 101 più 7. Pertanto il resto della divisione per 101 vale 7. □

Esercizio 4 (Gara provinciale 1997, problema 5)**.** Qual è la cifra delle unità del numero 2^{3^4} ?

Soluzione. Osserviamo che le cifre delle unità delle potenze di 2 si ripetono con periodo 4

$$\begin{aligned} 2^1 &\equiv 2 \pmod{10} \\ 2^2 &\equiv 4 \pmod{10} \\ 2^3 &\equiv 8 \pmod{10} \\ 2^4 &\equiv 6 \pmod{10} \\ 2^5 &\equiv 2 \pmod{10} \\ 2^6 &\equiv 4 \pmod{10} \\ &\dots \end{aligned}$$

Pertanto 2^n e 2^{n+4} hanno la stessa cifra delle unità. Ciò può essere dimostrato osservando che per ogni $n > 1$ risulta

$$2^{n+4} - 2^n = 2^n\left(2^4 - 1\right) = 3 \cdot 10 \cdot 2^{n-1} \quad \Leftrightarrow \quad 2^{n+4} \equiv 2^n \pmod{10}$$

Poichè $3^4 = 81 = 4 \cdot 20 + 1$ abbiamo che

$$2^{3^4} \equiv 2^{81} \equiv 2^{4\cdot 20+1} \equiv 2^1 \equiv 2 \pmod{10}$$

quindi la cifra delle unità di 2^{3^4} è 2. □

Esercizio 5 (Gara provinciale 1998, problema 15)**.** I numeri a e b sono interi positivi. Qual è il minimo valore positivo di $a + b$ affinchè $21ab^2$ e $15ab$ siano entrambi quadrati perfetti?

Soluzione. Un numero è quadrato perfetto se e solo se nella sua fattorizzazione tutti i fattori primi compaiono un numero pari di volte. Pertanto

$$21ab^2 = 3 \cdot 7 \cdot ab^2 = n^2 \quad \Leftrightarrow \quad a = 3 \cdot 7 \cdot u^2 = 21u^2$$

da cui si ottiene

$$15ab = 3^2 \cdot 5 \cdot 7 \cdot u^2 b = m^2 \quad \Leftrightarrow \quad b = 5 \cdot 7 \cdot v^2 = 35v^2$$

Ponendo $u = v = 1$ abbiamo che il valore minimo di $a + b$ è 56. □

Esercizio 6 (Cortona 1998)**.** Determinare tutti gli interi n tali che $n^4 + 4$ sia un numero primo.

Soluzione. $n^4 + 4$ si può scomporre in fattori nel modo seguente

$$n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = \left(n^2 + 2\right)^2 - 4n^2 = \left(n^2 + 2n + 2\right)\left(n^2 - 2n + 2\right)$$

Pertanto $n^4 + 4$ è un numero primo se e solo se

$$n^2 - 2n + 2 = 1 \quad \Leftrightarrow \quad n^2 - 2n + 1 = 0 \quad \Leftrightarrow \quad n = 1$$

□

Esercizio 7 (Gara Nazionale di Cesenatico 2003, problema 1)**.** Trovare tutti i numeri naturali n di tre cifre ($100 \leq n \leq 999$) che sono uguali al numero formato dalle ultime tre cifre di n^2.

Soluzione. Il quadrato di n ha le stesse ultime tre cifre di n se e solo se $n^2 - n = n(n-1)$ è divisibile per $1000 = 2^3 \cdot 5^3$. Poichè n ed $n-1$ sono primi fra loro, solo uno dei due è pari e solo uno dei due può essere divisibile per 5. Abbiamo quindi le seguenti possibilità:

- n è divisibile sia per 2^3 che per 5^3, ossia n è divisibile per 1000. Nessun numero di tre cifre possiede questa proprietà.
- $n-1$ è divisibile sia per 2^3 che per 5^3, ossia $n-1$ è divisibile per 1000. Nessun numero di tre cifre possiede questa proprietà.
- n è divisibile per 2^3 ed $n-1$ è divisibile per 5^3. L'unico numero di 3 cifre con questa proprietà è $n = 376$ ed una verifica diretta fornisce $n^2 = 141376$.
- n è divisibile per 5^3 ed $n-1$ è divisibile per 2^3. L'unico numero di 3 cifre con questa proprietà è $n = 625$ ed una verifica diretta fornisce $n^2 = 390625$.

□

Esercizio 8 (Gara Provinciale 2005, problema 15)**.** Quante sono le coppie ordinate (x, y) di interi positivi x e y che soddisfano la relazione

$$xy + 5(x + y) = 2005$$

Suggerimento. Scrivere la relazione nella forma equivalente

$$(x + 5)(y + 5) = 2030$$

ed utilizzare la fattorizzazione ... □

Esercizio 9 (Gara Nazionale di Cesenatico 2005, problema 2)**.** Dimostrare che, comunque si prendano 18 numeri interi positivi consecutivi minori o uguali a 2005, ce ne è almeno uno divisibile per la somma delle sue cifre.

Soluzione. Tra i 18 numeri considerati vi sono due multipli consecutivi di 9. Per il criterio di divisibilità per 9 la somma delle cifre di questi numeri è multipla di 9. Considerando che la somma massima delle cifre di un numero minore di 2005 è 28 (nel caso di 1999), analizziamo due casi. Se la somma delle cifre di uno di questi numeri è 27, allora questo numero deve essere necessariamente 999, 1899, 1989 o 1998. I numeri 999 e 1998 sono divisibili per 27, mentre i multipli di 9 immediatamente precedenti e immediatamente successivi a 1899 e a 1989, cioè 1890, 1908, 1980 e 1998, sono tutti divisibili per la somma delle loro cifre. Se invece le somme delle cifre dei due multipli consecutivi di 9 sono uguali a 9 o a 18, allora basta notare che uno di essi è pari, e quindi divisibile non solo per 9 ma anche per 2, e quindi per 18. □

Esercizio 10 (Gara Provinciale 2007, problema 17)**.** Un intero positivo si dice *triangolare* se si può scrivere nella forma $n(n+1)/2$ 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).

Suggerimento. Il problema è equivalente a trovare le coppie di interi positivi (n, m) tali che

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

Eliminando i denominatori e fattorizzando l'equazione diventa

$$(n-m)(n+m+1) = 2 \cdot 2007 = 2 \cdot 3^2 \cdot 223 \qquad (*)$$

Considerando tutti i casi possibili ed escludendo i valori non accettabili si trova che l'equazione (*) è verificata se

$$(m, n) \in \{(2007, 2006), (1004, 1002), (670, 667), (337, 331), (227, 218), (120, 102)\}$$

□

Esercizio 11 (Gara Provinciale 2008, problema 15)**.** Si determinino tutte le coppie (x, y) di numeri reali che verificano lequazione

$$\frac{4}{x+y} = \frac{1}{x} + \frac{1}{y}$$

Suggerimento. Dopo aver scritto l'equazione nella forma equivalente $4xy = (x+y)^2$, cioè $(x-y)^2 = 0$ si trova che le coppie cercate sono tutte e sole quelle che soddisfano $x = y$, a cui però va tolta la coppia $(0, 0)$. □

Esercizio 12 (Gara provinciale 2009, problema 9)**.** Determinare tutti i numeri interi positivi n tali che la rappresentazione in base 2 di n coincide con la rappresentazione in base 3 di $2n$.

Soluzione. Sia $n = a_k 2^k + a_{k-1}2^{k-1} + \cdots + 2a_1 + a_0$ con $a_k \neq 0$ la rappresentazione in base 2 di n. I coefficienti a_i sono uguali a 0 oppure 1, quindi vale la disuguaglianza $n < 2^{k+1}$. Supponiamo che $a_0, a_1, \ldots, a_k$ siano anche le cifre della rappresentazione in base 3 di $2n$, ossia che

$$2n = a_k 3^k + a_{k-1}3^{k-1} + \cdots + 3a_1 + a_0$$

Allora vale la stima $2n \geq 3^k$. Si dimostra facilmente per induzione che $3^k > 2^{k+2}$ per ogni $k \geq 4$. Pertanto se fosse $k \geq 4$ avremmo $2n \geq 3^k > 2^{k+2} > 2n$, che non è possibile. Quindi dev'essere $k \leq 3$. Per ipotesi abbiamo

$$27a_3+9a_2+3a_1+a_0 = 2\,(8a_3 + 4a_2 + 2a_1 + a - 0) \quad \Leftrightarrow \quad 11a_3+a_2-a_1-a_0 = 0$$

da cui, tenuto conto che $a_i \in \{0, 1\}$, si deduce subito che $a_3 = 0$. Dunque i coefficienti a_i sono verificano

$$a_2 - a_1 - a_0 = 0$$

uguaglianza che è soddisfatta solo dalle terne $(1, 1, 0)$ ed $(1, 0, 1)$, corrispondenti ai due numeri $n = 5$ ed $n = 6$. □

Esercizio 13 (Gara provinciale 2010, problema 5)**.** Per quanti interi relativi n si ha che $\frac{3n}{n+5}$ è intero e divisibile per 4?

Suggerimento. Eseguire la sostituzione $m = n + 5$, ... □

Esercizio 14. Dire quante sono le terne ordinate (x, y, z) di interi positivi che verificano l'equazione

$$15x + 5y + 3z = 2010$$

Soluzione. Posto $w = 3x + y$ l'equazione può essere scritta nel modo seguente

$$5w + 3z = 2010, \qquad w, z \in \mathbb{Z} \tag{*}$$

Una soluzione particolare di (*) è $(w_0, z_0) = (399, 5)$, quindi la soluzione generale è costituita dalle coppie $(w, z) = (399 + 3s, 5 - 5s)$ con $s \in \mathbb{Z}$. Analogamente si trova che la soluzione generale dell'equazione $3x + y = w$ è data dalle coppie $(x, y) = (133 + t, 3s - 3t)$ con $s \in \mathbb{Z}$.

Pertanto i numeri interi positivi x, y, x che verificano l'equazione proposta sono tutte e sole le terne della forma

$$(x, y, z) = (133 + t, 3s - 3t, 5 - 5s)$$

con $-133 < t < s < 1$. Il numero di terne siffatte è $\binom{133}{2} = 8778$. □

Esercizio 15 (IMO 1959, problema 1)**.** Dimostrare che per ogni numero naturale n la frazione $\frac{21n+4}{14n+3}$ è irriducibile.

Suggerimento. Osservare che $3(14n+3) - 2(21n+4) = 1$. □

Esercizio 16. Determinare il più piccolo numero intero positivo avente esattamente 15 divisori.

Soluzione. I numeri interi aventi esattamente 15 divisori sono della forma p^{14} con p primo, oppure della forma p^2q^4 con p, q primi. Tra questi numeri il più piccolo è $2^4 \cdot 3^2 = 144$. □

Esercizio 17. Dimostrare che l'equazione

$$x^2 + y^2 + z^2 = 5xyz$$

non ha soluzioni intere eccetto $x = y = z = 0$.

Soluzione. Supponiamo che l'equazione abbia una soluzione $(a, b, c) \neq (0, 0, 0)$. Osserviamo innanzitutto che a, b, c sono tutti diversi da zero poichè se uno di essi fosse uguale a zero anche gli altri due lo sarebbero. Inoltre a, b, c sono distinti in quanto, se fosse ad esempio $b = c$, sostituendo nell'equazione si avrebbe

$$a^2 = 5ab^2 - 2b^2 = (5a - 2)b^2$$

da cui segue che $a = bd$ per qualche intero d. Pertanto

$$b^2d^2 = (5bd - 2)b^2 \quad \Rightarrow \quad d^2 = 5bd - 2 \quad \Rightarrow \quad 2 = d(5b - d)$$

da cui segue $d = 1$ oppure $d = 2$. In entrambi i casi si ottiene $5b = 3$ il che è impossibile essendo b intero.

Allora a, b, c sono interi distinti e, senza perdita di generalità, possiamo supporre che $a > b > c \geq 1$. Sia a' la seconda radice del polinomio quadratico $P(x) = x^2 - 5bcx + b^2 + c^2$, in modo che (a', b, c) è un'altra soluzione dell'equazione data. Poichè

$$P(b) = 2b^2 + c^2 - 5b^2c < 3b^2 - 5b^2c \leq 3b^2 - 5b^2 < 0$$

abbiamo che b è compreso tra le due radici a e a' del polinomio $P(x)$ e, essendo $b < a$, risulta che $a > b > a'$.

Abbiamo così trovato una nuova soluzione $(a_1, b_1, c_1) = (a', b, c)$ in cui la coordinata più grande è più piccola della coordinata più grande di (a, b, c). La stessa costruzione può essere ripetuta per trovare un'altra soluzione (a_2, b_2, c_2) la cui coordinata maggiore è ancora più piccola. In questo modo potremmo ottenere una successione strettamente decrescente di interi positivi, ma questo è impossibile per il principio della discesa infinita. Possiamo concludere che $(0, 0, 0)$ è l'unica soluzione dell'equazione $x^2 + y^2 + z^2 = 5xyz$. □

Esercizio 18. Dimostrare che un numero ottenuto concatenando un po' di copie di 2010 non può mai essere un quadrato perfetto.

Soluzione. Un numero ottenuto concatenando $m+1$ copie di 2010

$$20102010\cdots 2010 = 2010\left(1+10^4+10^8+\cdots+10^{4m}\right)$$

non può essere un quadrato in quanto è divisibile per 2 ma non per 4, dato che $\left(1+10^4+10^8+\cdots+10^{4m}\right)$ è dispari e $2010 = 2\cdot 3\cdot 5\cdot 67$. □

Esercizio 19. Dimostrare che non esiste nessun intero positivo n tale che $11^n + 2^n + 1$ è un quadrato.

Soluzione. Supponiamo che esista un intero a tale che

$$11^n + 2^n + 1 = a^2 \qquad (*)$$

Allora poichè $11 \equiv -1 \pmod 3$ e $2 \equiv -1 \pmod 3$ abbiamo

$$(-1)^n + (-1)^n + 1 \equiv a^2 \pmod 3$$

Se n fosse dispari, si avrebbe $a^2 \equiv -1 \pmod 3$, il che è impossibile, in quanto gli unici residui quadratici modulo 3 sono 0 e 1. Pertanto n deve essere pari, diciamo $n = 2m$ per un opportuno $m \in \mathbb{Z}$. Sostituendo nella (*) si ottiene $121^m + 4^m + 1 = a^2$. Osservando che

$$\left(11^m\right)^2 = 121^m, \qquad \left(11^m+1\right)^2 = 121^m + 2\cdot 11^m + 1 > 121^m + 4^m + 1$$

abbiamo

$$\left(11^m\right)^2 < a^2 < \left(11^m+1\right)^2 \quad \Leftrightarrow \quad 11^m < a < 11^m + 1$$

ma questo è assurdo essendo 11^m e 11^m+1 due interi consecutivi. Pertanto $11^n + 2^n + 1$ non può essere un quadrato. □

Esercizio 20 (Mathematical Reflection J198)**.** Determinare tutte le coppie (x, y) di interi positivi tali che $x! + y! + 3$ è un cubo perfetto.

Soluzione. Poichè l'espressione $x! + y! + 3$ è simmetrica, senza perdita di generalità, possiamo supporre che $x \geq y$. Consideriamo i seguenti casi:

(a) Se $x \leq 6$, possiamo facilmente verificare che $x! + y! + 3$ è un cubo perfetto solo quando $(x, y) = (5, 2)$ e $(x, y) = (6, 3)$

(b) Se $x > 6$, $y \in \{0, 1, 2, 5, 6\}$, allora $x! + y! + 3 \equiv 3, 4, 5, 6 \pmod 9$. Pertanto $x! + y! + 3$ non può essere un cubo perfetto, poichè $z^3 \equiv 0, 1, 8 \pmod 9$ per ogni $z \in \mathbb{N}$.

x/y	0	1	2	3	4	5	6
0	5	5	6	10	28	124	724
1	5	5	6	10	28	124	724
2	6	6	7	11	29	125	725
3	10	10	11	15	33	129	729
4	28	28	29	33	51	147	747
5	124	124	125	129	147	243	843
6	724	724	725	729	747	843	1443

(c) Se $x > 6$, $y = 3$, abbiamo i seguenti tre sottocasi:

- Se $x = 7$, $y = 3$ allora $x! + y! + 3 = 5049$ che non è un cubo perfetto.
- Se $x = 8$, $y = 3$ allora $x! + y! + 3 = 40329$ che non è un cubo perfetto.
- Se $x \geq 9$, $y = 3$ allora $x! + y! + 3 = x! + 9$ che non è un cubo perfetto poichè $3 \mid x! + 9$, mentre $27 \nmid x! + 9$.

(d) Se $x > 6$, $y = 4$, abbiamo i seguenti 3 sottocasi:

- Se $x = 7$, $y = 4$ allora $x! + y! + 3 = 5067$ che non è un cubo perfetto.
- Se $x = 8$, $y = 4$ allora $x! + y! + 3 = 40347$ che non è un cubo perfetto.
- Se $x \geq 9$, $y = 4$ allora $x! + y! + 3 = x! + 27$. È facile dimostrare per induzione che $x! + 27 > x^3$ per ogni $x \geq 5$. Pertanto se fosse $x! + 27 = z^3$ si avrebbe $x > z$ e, di conseguenza, $z = 3^k$ con $k > 1$. Quindi $x! + 27 = 3^{3k}$, ma ciò è assurdo poiché $81 \mid 3^{3k}$ mentre $81 \nmid x! + 27$.

(e) Se $x > 6$ e $y > 6$ allora $x! + y! + 3$ non può essere un cubo perfetto poichè $x! + y! + 3 \equiv 3 \pmod 9$.

Dunque $x! + y! + 3$ è un cubo perfetto se e solo se

$$(x, y) \in \{(5, 2), (2, 5), (6, 3), (3, 6)\}$$ □

Bibliografia

[AG09] T. Andreescu and R. Gelca, *Mathematical olympiad challenges*, Birkhäuser, 2009.

[Hua82] L. Hua, *Introduction to number theory*, Springer-Verlag, 1982.

[IR90] K.F. Ireland and M.I. Rosen, *A classical introduction to modern number theory*, Graduate texts in mathematics, Springer-Verlag, 1990.

[Sam70] Pierre Samuel, *Algebraic theory of numbers*, Translated from the French by Allan J. Silberger, Houghton Mifflin Co., Boston, Mass., 1970.

[Sci89] B. Scimemi, *Algebretta. un'introduzione al corso di algebra per la laurea in matematica*, Collana di matematica. Testi e manuali, Zanichelli, 1989.