3 Interi somma di due quadrati

Uno dei primi problemi che Fermat prese in esame fu quello della rappresentazione dei numeri naturali come somma di due quadrati di interi, cercando di chiarire alcuni passaggi dell'*Arithmetica* di Diofanto che trattavano di tale argomento. Anche F. Viète, C. Bachet e A. Girard, suoi contemporanei, si occuparono di tale questione anche se, come Fermat, non diedero dimostrazioni complete dei risultati a cui pervennero.

Diamo alcuni esempi delle questioni esaminate da Diofanto:

- determinare $a, b, c \in \mathbb{Z}$ tali che $a + b = 1$ e che $a + c$ e $b + c$ sono entrambi quadrati; in tale situazione, dunque, $2c + 1$ è la somma di due quadrati;
- 15 non è mai somma di due quadrati;
- determinare $a, b, c, d \in \mathbb{Z}$ in modo tale che, posto $q := (a + b + c + d)^2$, $q \pm a$, $q \pm b$, $q \pm c$, $q \pm d$ sono tutti quadrati.

Diofanto osserva che quest'ultima questione può essere facilmente risolta se si trovano quattro diversi triangoli pitagorici aventi la stessa ipotenusa o, ciò che è equivalente, se si trova un quadrato che può essere espresso in quattro modi diversi come somma di due quadrati. A questo proposito, Fermat enunciò che, se p è un primo del tipo $4k + 1$, allora p è sempre uguale al quadrato della lunghezza dell'ipotenusa di un unico triangolo a cateti interi (cfr. i successivi Teorema 3.4 e Corollario 3.6).

Il problema che vogliamo esaminare in questo paragrafo è quello di trovare gli interi n per i quali l'equazione diofantea in due indeterminate

$$X^2 + Y^2 = n$$

è risolubile. I principali risultati di questo paragrafo furono dimostrati completamente per la prima volta da Euler.

Il seguente enunciato era verosimilmente già noto a Diofanto e veniva comunque riportato da Leonardo da Pisa (detto Fibonacci) nel suo celebre *Liber Abaci* del 1202.

Proposizione 3.1. *Siano $n, m \in \mathbb{N}^+$. Se n e m possono essere scritti come somma di due quadrati di interi, allora anche nm può essere scritto come somma di due quadrati di interi.*

Dimostrazione. Semplice conseguenza della seguente identità:

$$(a^2 + b^2)(c^2 + d^2) = (ac \mp bd)^2 + (ad \pm bc)^2 \ .$$

□

Osservazione 3.2. La dimostrazione data da Euler nel 1770 del risultato precedente (con la scelta "superiore" dei segni) si basa sul fatto che tale relazione esprime, con linguaggio moderno, la proprietà moltiplicativa della norma nell'anello degli interi di Gauss. (Cioè, se $\alpha := a+bi, \beta := c+di \in \mathbb{Z}[i]$, allora $\mathrm{N}(\alpha) = a^2 + b^2$, $\mathrm{N}(\beta) = c^2 + d^2$ e $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta) = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.)

Proposizione 3.3. *Sia p un numero primo. Se $p \equiv 3 \pmod 4$, allora p non può essere scritto come somma di due quadrati di interi.*

Dimostrazione. Se per assurdo $x^2 + y^2 = p$, allora $x^2 + y^2 \equiv 3 \pmod 4$ e ciò è assurdo in quanto, come ben noto, x^2 e y^2 sono congrui a 0 oppure a 1 (mod 4).

□

Il risultato seguente fu comunicato in una lettera da Fermat a Mersenne nel 1640. Tuttavia una proprietà analoga era stata enunciata precedentemente da Girard. La prima dimostrazione completa di tale risultato fu data da Euler nel 1747.

Teorema 3.4. (P. Fermat, 1640) *Un primo p è esprimibile come somma di due quadrati di interi se, e soltanto se, $p = 2$ oppure $p \equiv 1$ (mod 4).*

Dimostrazione. Se p è un primo esprimibile come somma di due quadrati, allora, per la Proposizione 3.3, $p \not\equiv 3 \pmod 4$. Viceversa, se $p = 2$ allora $2 = 1^2 + 1^2$; non è dunque restrittivo supporre che $p \equiv 1 \pmod 4$. In tal caso, sappiamo che la congruenza $X^2 \equiv -1 \pmod p$ ammette soluzioni (cfr. Proposizione I.6.6 (h)). Sia a una soluzione di tale congruenza, sia cioè $a^2 + 1 = hp$, con $h \geq 1$. Se ne deduce subito che $\mathrm{MCD}(a, p) = 1$. Consideriamo la congruenza lineare:

$$aX \equiv Y \pmod p$$

ed utilizziamo il seguente:

Lemma 3.5. (A. Thue, 1902) *Sia p un primo e a un intero tale che* $\mathrm{MCD}(a,p)=1$. *Allora la congruenza*

$$aX \equiv Y \pmod{p}$$

ammette una soluzione x_0, y_0, con $x_0, y_0 \in \mathbb{Z}$ tali che

$$0 \lneqq |x_0| \lneqq \sqrt{p} \qquad 0 \lneqq |y_0| \lneqq \sqrt{p}\ .$$

Tale lemma è una semplice applicazione del seguente:

Principio di Dirichlet (noto anche come ***Principio delle gabbie di piccioni o delle caselle postali***). *Se un insieme di n elementi (piccioni) deve essere ripartito in m sottoinsiemi (gabbie), cioè se ogni elemento (piccione) deve essere assegnato ad un sottoinsieme (gabbia), e se $n \gneqq m \geq 1$, allora un sottoinsieme (almeno) contiene più di un elemento (cioè, in una stessa gabbia debbono trovarsi almeno due piccioni).*

Pur essendo intuitivamente ovvio, il Principio di Dirichlet è un "teorema" e come tale necessita di una dimostrazione. Sia, per assurdo, falso e sia n il minimo intero positivo per cui è falso. Necessariamente risulta $n \geq 2$. Sia quindi S un insieme con n elementi e supponiamo che questi siano ripartiti in m sottoinsiemi, $S_1, \ldots, S_m$, $n \gneqq m \geq 1$, in modo tale che nessun sottoinsieme contenga due o più elementi di S. Ovviamente $m > 1$. Se a è un elemento di S, allora a appartiene esattamente ad un sottoinsieme, diciamo S_1 (per fissare le idee). Consideriamo allora l'insieme $S' := S \setminus \{a\}$. Gli elementi di S' rimangono ripartiti nei sottoinsiemi $S_2, \ldots, S_m$, in modo tale che nessun sottoinsieme contiene due o più elementi di S'. Ma S' ha $n-1$ elementi e questo contraddice la minimalità di n.

Dimostrazione del Lemma 3.5. Si ponga $k := [\sqrt{p}] + 1$ e si consideri l'insieme $S := \{ax - y : 0 \leq x \leq k-1,\ 0 \leq y \leq k-1\}$.

È ovvio che $\#S \leq k^2$.

Se $\#S < k^2$, siamo arrivati perché $ax_1 - y_1 = ax_2 - y_2$, per una qualche scelta delle coppie $(x_1, y_1) \neq (x_2, y_2)$; quindi basta porre $x_0 := x_1 - x_2$, $y_0 := y_1 - y_2$.

Se $\#S = k^2$, essendo $k^2 \gneqq p$, per il Principio di Dirichlet, devono esistere due elementi $ax_1 - y_1$, $ax_2 - y_2 \in S$ in modo tale che

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{\text{p}}$$

con $x_1 \neq x_2$ oppure $y_1 \neq y_2$. Quindi

$$a(x_1 - x_2) \equiv y_1 - y_2 \pmod{\text{p}}\ .$$

La conclusione si ottiene ponendo $x_0 := x_1 - x_2$, $y_0 := y_1 - y_2$. Infatti, essendo $\mathrm{MCD}(a, p) = 1$ e non potendo essere x_0 e y_0 entrambi nulli, si ricava facilmente che $x_0 \neq 0$ e $y_0 \neq 0$.

□

Fine della dimostrazione del Teorema 3.4. Sia (x_0, y_0), con $x_0, y_0 \in \mathbb{Z}$, una soluzione della congruenza $aX \equiv Y \pmod{p}$ tale che $0 \lneqq |x_0|, |y_0| \lneqq \sqrt{p}$. Dunque $-x_0^2 \equiv a^2 x_0^2 \equiv y_0^2 \pmod{p}$, ovvero $x_0^2 + y_0^2 \equiv 0 \pmod{p}$. Pertanto, esiste un intero $t \geq 1$, in modo tale che $x_0^2 + y_0^2 = tp$. Dal momento che $|x_0|$, $|y_0| \lneqq \sqrt{p}$, allora $tp = x_0^2 + y_0^2 \lneqq 2p$, dunque necessariamente $t = 1$.

□

Corollario 3.6. (L. Euler, 1754) *Ogni primo p, tale che $p \equiv 1 \pmod{4}$, può essere scritto come somma di due quadrati di interi positivi in modo unico, a meno dell'ordine degli addendi.*

Dimostrazione. Supponiamo che $p = a^2 + b^2 = c^2 + d^2$, dove a, b, c, d sono interi positivi. Allora, si ha

$$p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 \ .$$

D'altra parte:

$$p(d^2 - b^2) = (a^2 + b^2)d^2 - (c^2 + d^2)b^2 = a^2 d^2 - c^2 b^2 \equiv 0 \pmod{p} \ ,$$

quindi $(ad - cb)(ad + cb) \equiv 0 \pmod{p}$. Dunque,

$$ad \equiv cb \pmod{p} \quad \text{oppure} \quad ad \equiv -cb \pmod{p} \ .$$

Essendo $0 \lneqq a, b, c, d \lneqq \sqrt{p}$, allora si ha:

$$ad - cb = 0 \quad \text{oppure} \quad ad + cb = p \ .$$

Se $p = ad + cb$, allora essendo:

$$p^2 = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2 \ ,$$

si ricava che $ac - bd = 0$. Dunque, si ha che:

$$ad - cb = 0 \quad \text{oppure} \quad ac - bd = 0 \ .$$

Supponiamo, per esempio, che $ad = bc$, allora $a \mid bc$ e $\mathrm{MCD}(a, b) = 1$, dunque $a \mid c$. Quindi $ah = c$, per qualche intero $h \geq 1$, e $d = bh$, donde

$p = c^2 + d^2 = h^2(a^2 + b^2) = h^2 p$. Ne segue che $h = 1$, cioè $a = c$ e $b = d$. Un ragionamento analogo, nel caso in cui $ac = bd$, permette di concludere. □

Prima di enunciare il teorema fondamentale di questo paragrafo osserviamo che ogni intero positivo n può essere rappresentato in una ed una sola maniera nella forma $n = \ell^2 m$ con ℓ, m interi positivi ed m privo di fattori quadratici (semplice conseguenza del Teorema Fondamentale dell'Aritmetica).

Teorema 3.7. *Sia $n = \ell^2 m > 0$ un intero positivo ed m un intero positivo privo di fattori quadratici. Allora n può essere rappresentato come somma di due quadrati di interi se, e soltanto se, per ogni primo dispari p tale che $p \mid m$, risulta $p \equiv 1 \pmod 4$.*

Dimostrazione. Sia $m = p_1 \dots p_r$ la fattorizzazione in primi (non necessariamente distinti) di m. Supponiamo che per ogni primo p_i, $1 \leq i \leq r$, risulti $p_i \equiv 1 \pmod 4$ oppure $p_i = 2$. Per induzione su r, applicando il Teorema 3.4 e la Proposizione 3.1, si ha che m è una somma di due quadrati e quindi, poiché $\ell^2 = \ell^2 + 0^2$, anche n è una somma di due quadrati.

Viceversa, se $n = a^2 + b^2 = \ell^2 m$ con $a, b \geq 0$, allora, posto $d := \mathrm{MCD}(a, b)$ e $a = da'$, $b = db'$, dove $\mathrm{MCD}(a', b') = 1$, allora

$$n = d^2(a'^2 + b'^2) = \ell^2 m \ .$$

Sia p un fattore primo dispari di m (senza perdere di generalità, si può supporre che m ne possieda uno, altrimenti la conclusione sarebbe immediata). Quindi,

$$a'^2 + b'^2 = (\ell/d)^2 m = tp$$

per qualche $t > 0$. Inoltre, risulta $\mathrm{MCD}(a', p) = 1$, infatti se $p \mid a'$, allora $p \mid b'$ e $\mathrm{MCD}(a', b') \neq 1$. Dunque, deve esistere un intero α' in modo tale che $a'\alpha' \equiv 1 \pmod p$. Essendo $a'^2 + b'^2 \equiv 0 \pmod p$, moltiplicando per α'^2 si ottiene $1 + (\alpha' b')^2 \equiv 0 \pmod p$, cioè $\left(\frac{-1}{p}\right) = 1$ e quindi, (cfr. Proposizione I.6.6 (h)), si ricava che $p \equiv 1 \pmod 4$.

□

Osservazione 3.8. A. Von Wijngarden nel 1950 aveva prodotto una tavola delle rappresentazioni di $n = x^2 + y^2$ con $x, y \in \mathbb{N}$, $0 \leq x \leq y$, per $n \leq 10.000$. Con l'uso di mezzi di calcolo sempre più potenti è possibile ora trovare rappresentazioni di n come somma di due quadrati per valori di n molto grandi.

Corollario 3.9. (P. Fermat, 1640) *Sia $n > 0$ un intero tale che $n = x^2 + y^2$ con $x, y \in \mathbb{N}$ e sia p un numero primo dispari.*

(a) *Se* $\mathrm{MCD}(x, y) = 1$ *e* $p \mid n$, *allora risulta* $p \equiv 1 \pmod 4$ *e la congruenza* $X^2 \equiv -1 \pmod n$ *è risolubile.*

(b) *Se* $p \mid n$ *e* $p \equiv 3 \pmod 4$, *allora una potenza di* p *con esponente pari deve dividere* n *, più precisamente:*

$$n = p^{2k} n' = (p^k x')^2 + (p^k y')^2$$

dove k, n', x', y' *sono interi opportuni, con* $k, n' > 0$.

Dimostrazione. (a) Ragionando come nella dimostrazione del Teorema 3.7, poiché $p \mid n$ e $\mathrm{MCD}(x, y) = 1$, si ha che $p \nmid x$. Quindi, esiste un intero x^* tale che $xx^* \equiv 1 \pmod p$ ed, essendo $x^2 + y^2 \equiv 0 \pmod p$, si ottiene $1 + (x^* y)^2 \equiv 0 \pmod p$, da cui $p \equiv 1 \pmod 4$ (cfr. Proposizione I.6.6 (h)) e $1 + (x^* y)^2 \equiv 0 \pmod n$ (cfr. Teorema I.6.36).

(b) Supponiamo che $p^h \mid n$ e $p^{h+1} \nmid n$. Poiché $p \equiv 3 \pmod 4$ si ha, per il punto (a), che $\mathrm{MCD}(x, y) = d \gneqq 1$. Ponendo $x = dx_1$, $y = dy_1$ e $N = n/d^2$, allora si ha $N = x_1^2 + y_1^2$ con $\mathrm{MCD}(x_1, y_1) = 1$. Se $p^k \mid d$ e $p^{k+1} \nmid d$, allora $p^{h-2k} \mid N$. Ciò è assurdo (cfr. (a)) a meno che $h = 2k$.

□

3 Esercizi e complementi

3.1. Siano $a, b \in \mathbb{N}^+$ tali che $\mathrm{MCD}(a,b) = 1$. Mostrare che, se a non è somma di due quadrati di interi, allora ab non è somma di due quadrati di interi.

[*Suggerimento*. Si noti che $ab = p_1^{e_1} \dots p_t^{e_t} q_1^{f_1} \dots q_r^{f_r}$, dove $a = \prod_{i=1}^{t} p_i^{e_i}$, $b = \prod_{j=1}^{r} q_j^{f_j}$ sono le fattorizzazioni in primi distinti di a e b ed inoltre risulta $p_i \neq q_j$ per ogni i e per ogni j, perché $\mathrm{MCD}(a,b) = 1$.

Si osservi che l'ipotesi $\mathrm{MCD}(a,b) = 1$ è essenziale. Infatti se $a = 3$ e $b = 6$, allora a non è somma di due quadrati di interi, però $a \cdot b = 18 = 3^2 + 3^2$.]

3.2. Sia $a \in \mathbb{N}^+$. Mostrare che se a non è somma di due quadrati di interi, allora a non può essere neanche somma di due quadrati di numeri razionali.

[*Suggerimento*. Se, per assurdo, $a = \left(\frac{x}{y}\right)^2 + \left(\frac{z}{w}\right)^2$ con $x, y, z, w \in \mathbb{Z}$, $yw \neq 0$, allora $a(yw)^2 = (xw)^2 + (yz)^2$. Utilizzando il Teorema 3.7 si giunge facilmente ad una contraddizione.]

3.3. Mostrare che:

(a) Un numero razionale $\alpha = a/b$, con $a, b \in \mathbb{Z}$, $b \neq 0$, è somma di due quadrati di numeri razionali se, e soltanto se, ab è somma di due quadrati di interi.

(b) Un numero razionale $\alpha = a/b$, con $a, b \in \mathbb{Z}$, $b \neq 0$, $\mathrm{MCD}(a,b) = 1$, è somma di due quadrati di numeri razionali se, e soltanto se, a e b sono entrambi somma di due quadrati di interi.

(c) Se un numero razionale è somma di due quadrati di numeri razionali, allora esso ha una infinità di rappresentazioni distinte come somma di due quadrati di numeri razionali (positivi).

[*Suggerimento*. (a) Se $\frac{a}{b} = \left(\frac{c}{d}\right)^2 + \left(\frac{e}{f}\right)^2$ allora $ab(df)^2 = (bcf)^2 + (bde)^2$ e quindi per il Teorema 3.7, ab deve essere somma di due quadrati. Se $ab = x^2 + y^2$ allora $\frac{a}{b} = \left(\frac{x}{b}\right)^2 + \left(\frac{y}{b}\right)^2$.

(b) Si noti che, per il Teorema 3.7, se $\mathrm{MCD}(a,b) = 1$ allora ab è somma di due quadrati se e soltanto se a e b sono entrambi somma di due quadrati.

(c) Se $\gamma = \alpha^2 + \beta^2$ con $\alpha, \beta \in \mathbb{Q}$ e $\alpha, \beta > 0$ allora si può verificare che

$$\gamma = \alpha_k^2 + \beta_k^2$$

con $\alpha_k := \left(\frac{(k^2-1)\alpha - 2k\beta}{k^2+1}\right)^2$, $\beta_k := \left(\frac{(k^2-1)\beta - 2k\alpha}{k^2+1}\right)^2$, con $k \geq 1$ intero.]

3.4. Mostrare che, preso comunque $r \in \mathbb{N}^+$:

(a) Il numero naturale $n = a^2$, dove

$$a = (3^2+1)(4^2+1)\dots((r+2)^2+1)$$

è somma di due quadrati di interi non negativi in (almeno) r maniere distinte. Più precisamente:

$$n = a_k^2 + b_k^2 \ , \quad \text{per } k = 3, 4, \ldots, r+2 \ ,$$

dove

$$a_k = (k^2-1)a/(k^2+1) \ , \quad b_k = 2ka/(k^2+1) \ .$$

(b) Esistono sempre almeno r triangoli pitagorici distinti, aventi la stessa ipotenusa.

[*Suggerimento*. (a) Verifica diretta; (b) segue da (a)].

3.5. Verificare che, se $n = x^2 + y^2$, con $x, y \in \mathbb{Z}$, allora:

$$2n = (x+y)^2 + (x-y)^2 \ .$$

[La verifica è immediata.]

3.6. (**P. Fermat**, 1640). Mostrare che se p è un primo dispari del tipo $x^2 + 2$, allora p non può dividere un intero n del tipo $y^2 - 2$.

[*Suggerimento*. Si noti che $x^2 + y^2 = (x^2+2) + (y^2-2)$, quindi se $p = x^2+2$ divide $y^2 - 2$, allora $p \mid (x^2 + y^2)$. Essendo $p = x^2 + 2$ dispari deve essere $x^2 \equiv 1 \pmod 4$, quindi $p \equiv 3 \pmod 4$.]

3.7. Per ogni $n \geq 1$, si ponga:

$$r_2(n) := \#\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : \ x^2 + y^2 = n\} \ .$$

Da un punto di vista "geometrico" la funzione $r_2(n)$ esprime il numero dei punti del piano a coordinate intere che giacciono sulla circonferenza di equazione

$$X^2 + Y^2 = n \ , \quad n > 0 \, . \tag{3.7.1}$$

Evidentemente, se un punto (x, y) giace sulla circonferenza di equazione (3.7.1), allora anche i punti $(-x, y)$, $(x, -y)$, $(-x, -y)$ vi giacciono. Inoltre, tali punti sono tutti distinti se, e soltanto se, $xy \neq 0$. Se invece (x, y) è una soluzione intera di (3.7.1), con $xy = 0$, allora, e soltanto allora, n è un quadrato. In tal caso, $n = a^2$ con $a \in \mathbb{Z}$ e quindi $(x, y) \in \{(a, 0), (0, a), (-a, 0), (0, -a)\}$.

Per ogni $n \in \mathbb{N}^+$, si ponga:

$${}_2r(n) := \#\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 = n \ , \quad 0 \leq x \ , \quad 0 \lneqq y\} \ .$$

Da un punto di vista geometrico, ${}_2r(n)$ esprime il numero dei punti a coordinate intere *del primo quadrante* che giacciono sulla circonferenza di equazione (3.7.1). Evidentemente:

$$r_2(n) = 4 \cdot {}_2r(n) \ .$$

Mostrare che:

(a) $r_2(1) = 4$, $r_2(2) = 4$, $r_2(3) = 0$, $r_2(4) = 4$, $r_2(5) = 8$, $r_2(6) = 0$, $r_2(7) = 0$, $r_2(8) = 4$, $r_2(9) = 4$, $r_2(10) = 8$.

(b) $r_2(n) \leq 4\sqrt{n}$.

(c) Non esiste una costante K in modo tale che, per ogni $n \in \mathbb{N}^+$, risulti $r_2(n) \leq K$.

(d) Per ogni $n \in \mathbb{N}^+$, $r_2(n) = r_2(2n)$.

(e) Se p è un numero primo, allora:

$$r_2(p) = \begin{cases} 4 & \text{se } p = 2 \\ 8 & \text{se } p \equiv 1 \pmod 4 \\ 0 & \text{se } p \equiv 3 \pmod 4 \ . \end{cases}$$

(f) ${}_2r(n)$ è una funzione (aritmetica) moltiplicativa, mentre $r_2(n)$ è una funzione aritmetica che non è in generale moltiplicativa.

[*Suggerimento*. (a) La verifica è diretta. (b) Basta mostrare che ${}_2r(n) \leq \sqrt{n}$. Ciò è semplice conseguenza del fatto che $x^2 + y^2 = n \ \Rightarrow \ |x| \leq \sqrt{n}$ (e, poi, $|y| = \sqrt{n - x^2}$). L'affermazione (c) discende dal precedente Esercizio 3.4 (a). L'enunciato (d) è una conseguenza del precedente Esercizio 3.5. (e) Dal punto (a) si ha che $r_2(2) = 4$ e dal Teorema 3.7 discende che $r_2(p) = 0$ se $p \equiv 3 \pmod 4$. Se $p \equiv 1 \pmod 4$, si ha che ${}_2r(p) = 2$. Infatti, per il Corollario 3.6, le due soluzioni si determinano scambiando l'ordine delle coordinate. (f) $r_2(n)$ non è moltiplicativa perché $r_2(10) = 8 \neq r_2(2)r_2(5) = 4 \cdot 8$ (cfr. (a)). L'affermazione che ${}_2r(n)$ è una funzione moltiplicativa discende immediatamente dalla Proposizione 3.1 .]

3.8. (a) Mostrare che se $n \in \mathbb{N}$, $n \geq 2$, è tale che la congruenza:

$$X^2 \equiv -1 \pmod n \tag{3.8.1}$$

è risolubile, allora ogni soluzione a di (3.8.1) determina un'unica coppia di interi (x, y) in modo tale che:

(i) $n = x^2 + y^2$, $x > 0$, $y > 0$, $\mathrm{MCD}(x, y) = 1$,

(ii) $ax \equiv y \pmod n$.

Viceversa, data una coppia di interi (x, y), soddisfacente alla condizione (i), allora questa determina, tramite la congruenza (ii), un'unica soluzione a della congruenza (3.8.1).

(b) Per ogni $n \in \mathbb{N}$, $n \geq 2$, poniamo:

$$p_2(n) := \#\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : \ x^2 + y^2 = n \ , \ \ \mathrm{MCD}(x, y) = 1 \, , \}$$

$${}_2p(n) := \#\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : \ x^2 + y^2 = n \ , \ \ \mathrm{MCD}(x, y) = 1, \ x \geq 0, \ y \gneqq 0\} \, .$$

Mostrare che $p_2(2) = 4$ e, per $n \geq 3$, $p_2(n)$ $(= 4 \cdot {}_2p(n))$ è uguale a quattro volte il numero delle soluzioni della congruenza $X^2 \equiv -1 \pmod{n}$ e cioè:

$$p_2(n) = \begin{cases} 0 & \text{se } 4 \mid n \text{ oppure se qualche primo } p \equiv 3 \pmod 4 \text{ divide } n, \\ 4 \cdot 2^s & \text{se } 4 \nmid n \text{ e nessun primo } p \equiv 3 \pmod 4 \text{ divide } n\ , \end{cases}$$

essendo s il numero di divisori primi dispari distinti di n (cfr. Teorema 3.7).

(c) Mostrare che ${}_2p$ è una funzione (aritmetica) moltiplicativa, mentre p_2 è una funzione aritmetica che non è in generale moltiplicativa,

(d) Per ogni primo p, mostrare che $p_2(p) = r_2(p)$, e cioè:

$$p_2(p) = \begin{cases} 4 & \text{se } p = 2\,, \\ 8 & \text{se } p \equiv 1 \pmod 4\,, \\ 0 & \text{se } p \equiv 3 \pmod 4\,. \end{cases}$$

(e) Mostrare che ${}_2r(n) = \sum_{d^2 \mid n} {}_2p(n/d^2)$.

[*Suggerimento*. (a) Si noti, innanzitutto, che adattando opportunamente la dimostrazione, si può generalizzare il Lemma 3.5 nella forma seguente: *se* $a, n \geq 1$ *e se* $\mathrm{MCD}(a, n) = 1$*, allora la congruenza lineare in due intederminate*

$$aX \equiv Y \pmod n$$

ammette sempre una soluzione (x_0, y_0) *con* $0 < |x_0| < \sqrt{n}$ *e* $0 < |y_0| < \sqrt{n}$.

Si supponga che a sia una soluzione di $X^2 \equiv -1 \pmod{n}$ con $1 \leq a \leq n-1$. Si prenda (x_0, y_0) come nel precedente enunciato e si ponga $x := |x_0|$, $y := |y_0|$. Essendo $y_0^2 \equiv a^2 x_0^2 \pmod n$, quindi si ha che $x^2 + y^2 = x_0^2 + y_0^2 \equiv 0 \pmod n$ con $x > 0$ e $y > 0$. Essendo $0 < x, y < \sqrt{n}$, allora necessariamente $x^2 + y^2 = n$. Se x_0 ed y_0 hanno segni concordi, allora risulta anche $ax \equiv y \pmod n$. Se x_0 ed y_0 hanno segni discordi (ad esempio, per fissare le idee, $x_0 < 0$ ed $y_0 > 0$), allora poiché $a^2 \equiv -1 \pmod n$ risulta $-ay_0 \equiv x_0 \pmod n$. In tal caso, si prende $x' := |y_0|$ e $y' := |x_0| = x_0$ ed allora si avrà $x'^2 + y'^2 = x_0^2 + y_0^2 \equiv 0 \pmod n$, $x' > 0$, $y' > 0$, ed anche $ax' \equiv y' \pmod n$. Essendo $0 < x', y' < \sqrt{n}$, allora necessariamente $x'^2 + y'^2 = n$.

Vogliamo ora dimostrare che $\mathrm{MCD}(x, y) = 1$ (e quindi ovviamente anche $\mathrm{MCD}(x', y') = 1$).

Siano $h, k \in \mathbb{Z}$ tali che:

$$a^2 = -1 + kn \quad \text{e} \quad y = ax + hn$$

allora si vede facilmente che:

$$n = x^2 + y^2 = x^2 + (ax + hn)^2 = x^2(1 + a^2) + axhn + hn(ax + hn) = n(x(kx + ha) + yh)$$

e, quindi, che $x(kx + ha) + yh = 1$. Questo fatto implica che $\mathrm{MCD}(x, y) = 1$.

Per quanto riguarda l'unicità, siano (x_1, y_1), (x_2, y_2) due coppie di interi che verificano le condizioni (i) ed (ii), allora è subito visto (applicando la Proposizione 3.1) che

$$n^2 = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2 \ .$$

Pertanto, $0 < x_1x_2 + y_1y_2 \leq n$ ed inoltre:

$$x_1x_2 + y_1y_2 \equiv x_1x_2 + (ax_1)(ax_2) = x_1x_2 + a^2x_1x_2 \equiv 0 \pmod{n} \ .$$

Da ciò si ricava che $x_1x_2+y_1y_2 = n$ e, dunque, $x_1y_2-y_1x_2 = 0$. Poiché $\mathrm{MCD}(x_1, y_1) = 1 = \mathrm{MCD}(x_2, y_2)$, allora si deduce che $x_1 = x_2$ e $y_1 = y_2$.

Viceversa, sia (x, y) una coppia di interi verificante le condizioni (i) e (ii). Dalla relazione $ax \equiv y \pmod{n}$ e dal fatto che $\mathrm{MCD}(x, n) = 1$, si ricava che a è univocamente determinato (mod n), essendo $a \equiv x^*y \pmod{n}$. Inoltre, essendo $0 \equiv x^2 + y^2 \equiv x^2(1 + a^2) \pmod{n}$, si ricava immediatamente che $a^2 \equiv -1 \pmod{n}$.

(b) Utilizzando (a), ${}_2p(n)$ coincide con il numero delle soluzioni incongruenti di $X^2 \equiv -1 \pmod{n}$. Tale numero è stato calcolato nel Corollario I.6.37.

(c) segue facilmente da (b).

(d) è una verifica diretta (cfr. anche Esercizio 3.7 (e))

(e) segue per verifica diretta, utilizzando il fatto che ${}_2p(n)$ e ${}_2r(n)$ sono funzioni moltiplicative.]

3.9. Siano $a, b \in \mathbb{Z}$. Supponiamo che se p è un primo dispari e se $p \mid a$ allora $p \equiv 1 \pmod{4}$.

(a) Mostrare che l'equazione diofantea in due indeterminate:

$$Y^2 + 4a^2 = X^3 + (4b - 1)^3$$

non ha soluzioni.

(b) Mostrare che l'equazione diofantea $Y^2 = X^3 + 11$ non ha soluzioni.

[*Suggerimento*. (a) Sia per assurdo (x, y) una soluzione della equazione diofantea, allora $y^2 \equiv x^3 - 1 \pmod{4}$. Dal momento che $y^2 \equiv 0, 1 \pmod{4}$, allora necessariamente $x \equiv 1 \pmod{4}$ (e, quindi, $y^2 \equiv 0 \pmod{4}$, cioè y deve essere pari) . Poiché:

$$x^3 + (4b - 1)^3 = (x^2 - x(4b - 1) + (4b - 1)^2)(x + (4b - 1))$$

e poiché $x^2 - x(4b-1) + (4b-1)^2 \equiv 3 \pmod{4}$, deve esistere un primo $q \equiv 3 \pmod{4}$ tale che $q \mid x^2 - x(4b - 1) + (4b - 1)^2$ e, quindi, anche $q \mid (y^2 + 4a^2)$. Per il Corollario 3.9 (b), q deve allora dividere sia y che $2a$ e, quindi, q deve dividere a.

(b) Si sommi 16 ad ambo i membri dell'equazione data e si applichi il caso (a).]

3.10. Siano $a, b \in \mathbb{Z}$. Supponiamo che se p è un primo dispari e se $p \mid (2a + 1)$ allora $p \equiv 1 \pmod{4}$.

(a) Mostrare che l'equazione diofantea in due indeterminate:

$$Y^2 + (2a + 1)^2 = X^3 + (4b + 2)^3$$

non ha soluzioni.

(b) Mostrare che la seguente equazione diofantea:

$$Y^2 = X^3 - 17$$

non ha soluzioni.

[*Suggerimento*. (a) Come sopra, se (x, y) è una soluzione allora $x \equiv 1 \pmod 4$ e $x + (4b + 2) \equiv 3 \pmod 4$, da cui si trova un primo $q \equiv 3 \pmod 4$ tale che $q \mid (y^2 + (2a + 1)^2)$ e quindi $q \mid (2a + 1)$.

(b) Si sommi 25 ad ambo i membri dell'equazione.]

Osservazione (Esercizi 3.9 e 3.10). L'equazione diofantea in due indeterminate:

$$Y^2 = X^3 + k \quad \text{con } k \in \mathbb{Z} \tag{3.10.1}$$

è stata a lungo studiata da molti matematici, tra i quali L.J. Mordell attorno al 1913.

Si noti che l'equazione (3.10.1) determina un esempio importante di curva ellittica. Si noti, inoltre, che tale equazione, per $k = -2$, fu considerata da Bachet nel 1621. Fermat affermò che tale equazione diofantea ha soltanto la soluzione $(3, \pm 5)$, ma la sua dimostrazione non fu mai pubblicata (cfr. Esercizio 3.11).

Mordell ha dimostrato alcuni risultati più generali di quelli enunciati negli esercizi precedenti. Si ponga $k = \beta^3 - \alpha^2$, allora l'equazione diofantea (3.10.1) non ha soluzioni nei seguenti casi:

(1) β dispari, α pari, $3 \nmid \alpha$, $p \mid \text{MCD}(\alpha, \beta) \Rightarrow p \equiv 1 \pmod 4$, $k \not\equiv 7 \pmod 8$
(ad esempio: $k = 13$ $(= 17^3 - 70^2)$, 11 $(= 3^3 - 4^2)$, -3 $(= 1^3 - 2^2)$, -5 $(= (-1)^3 - 2^2)$);

(2) $\beta \equiv 2 \pmod 4$, α dispari, $3 \nmid \alpha$, $p \mid \text{MCD}(\alpha, \beta) \Rightarrow p \equiv 1 \pmod 4$
(ad esempio: $k = 7$ $(= 2^3 - 1^2)$; -9 $(= (-2)^3 - (1)^2)$);

(3) $\beta = 2b$, $\alpha = 2a$, con a dispari, $3 \nmid a$, $b \equiv 3 \pmod 4$, $p \mid \text{MCD}(a, b) \Rightarrow p \equiv 1 \pmod 4$
(ad esempio: $k = 20$ $(= 6^3 - 14^2)$, -12 $(= (-2)^3 - 2^2)$).

Successivamente A. Thue nel 1917 e L.J. Mordell nel 1922 hanno dimostrato che, per ogni $k \neq 0$, (3.10.1) ha al più un numero finito di soluzioni negli interi. Tuttavia, il numero delle soluzioni di (3.10.1) può essere arbitrariamente grande. Non è nota nessuna condizione generale per la risolubilità di (3.10.1) negli interi.

Come nel caso intero, non è noto per quali interi k l'equazione di Mordell (3.10.1) abbia soluzioni razionali. Importanti risultati sono stati ottenuti su tale problematica da Mordell (1969), Cassels (1950), Birch e Swinnerton–Dyer (1963). Il caso razionale differisce sostanzialmente dal caso intero per quanto riguarda il numero delle soluzioni. Infatti, Fueter nel 1930 ha dimostrato che se $k \neq 1, -432$,

se k non possiede fattori con potenza sei, e se (3.10.1) ha una soluzione razionale (x, y), con $xy \neq 0$, allora l'equazione (3.10.1) ha infinite soluzioni razionali. (Se $k = 1$, le soluzioni di (3.10.1) sono soltanto le seguenti $(0, \pm 1)$, $(-1, 0)$, $(2, \pm 3)$; se $k = -432$, l'equazione di Mordell ha un'unica soluzione $(12, \pm 36)$.)

Per maggiori dettagli sull'equazione diofantea di Mordell rinviamo a [9, Chapter 26] e [12, Section 14.4].

3.11. (Fermat, 1658) Mostrare che l'equazione diofantea

$$Y^2 = X^3 - 2$$

ha solamente le soluzioni intere non banali $x = 3$, $y = \pm 5$.

[*Suggerimento*. Si pensi di poter operare nell'anello $\mathbb{Z}[i\sqrt{2}]$ (invece che in $\mathbb{Z}$) che è noto essere anch'esso un dominio euclideo (e quindi, in particolare, un dominio a fattorizzazione unica). Allora, se $x, y \in \mathbb{Z}$ è una soluzione dell'equazione diofantea data, si ha

$$x^3 = (y + i\sqrt{2})(y - i\sqrt{2}) \ .$$

Non è difficile verificare che $\mathrm{MCD}_{\mathbb{Z}[i\sqrt{2}]}(y + i\sqrt{2}, y - i\sqrt{2}) = 1$.

Infatti, se $\alpha := a + bi\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ divide $\beta := y + i\sqrt{2}$ e $\overline{\beta} = y - i\sqrt{2}$, allora esso dovrebbe dividere anche la loro differenza (cioè, $2i\sqrt{2}$) e la loro somma (cioè, $2y$). Quindi $N(\alpha) \mid N(2i\sqrt{2})$ e $N(\alpha) \mid N(2y)$, cioè $N(\alpha) \mid 8$ e $N(\alpha) \mid 4y^2$, dunque $N(\alpha) \mid 4$. Da cui si ricava che $a = \pm 1$ e $b = 0$ oppure $a = 0$ e $b = \pm 1$. È subito visto che nessuna di tali soluzioni determina un divisore proprio di β e $\overline{\beta}$. Pertanto, gli elementi β e $\overline{\beta}$ sono relativamente primi in $\mathbb{Z}[i\sqrt{2}]$.

Essendo $x^3 = \beta\overline{\beta}$ allora necessariamente deve esistere $\gamma := c + id\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ in modo tale che $\beta = \gamma^3$. Dunque, confrontando i coefficienti di $i\sqrt{2}$, deve essere

$$1 = d(3c^3 - 2d^2)$$

pertanto $d = 1$ e $c = \pm 1$. Da cui si ricava che:

$$y + i\sqrt{2} = (\pm 1 + i\sqrt{2})^3$$

ovvero che $y = \pm 5$ e dunque $x = 3$.]