

# EQUAZIONI DIOFANTEE

Salvatore Siciliano

Dipartimento di Matematica "E. De Giorgi"

Università del Salento

salvatore.siciliano@unisalento.it

Maglie, 7 Gennaio 2011

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

# Equazioni diofantee di grado arbitrario in una incognita

In teoria dei numeri, un'equazione algebrica a coefficienti interi di cui si cercano soluzioni intere viene detta *diofantea*.

## Notazioni

$\mathbb{Z}$ : insieme dei numeri interi;

$\mathbb{N}$ : insieme degli interi positivi;

$\mathbb{Q}$ : insieme dei numeri razionali.

Se  $m$  e  $n$  sono due numeri interi, scriveremo  $m|n$  per intendere che  $m$  divide  $n$ .

Data un'equazione diofantea, i tipici problemi a cui si cerca di dare una risposta sono i seguenti:

- 1 Esiste qualche soluzione intera?
- 2 Il numero di soluzioni intere è finito o infinito?
- 3 Determinare tutte le soluzioni intere dell'equazione data.

Data un'equazione diofantea, i tipici problemi a cui si cerca di dare una risposta sono i seguenti:

- 1 Esiste qualche soluzione intera?
- 2 Il numero di soluzioni intere è finito o infinito?
- 3 Determinare tutte le soluzioni intere dell'equazione data.

Data un'equazione diofantea, i tipici problemi a cui si cerca di dare una risposta sono i seguenti:

- 1 Esiste qualche soluzione intera?
- 2 Il numero di soluzioni intere è finito o infinito?
- 3 Determinare tutte le soluzioni intere dell'equazione data.

Data un'equazione diofantea, i tipici problemi a cui si cerca di dare una risposta sono i seguenti:

- 1 Esiste qualche soluzione intera?
- 2 Il numero di soluzioni intere è finito o infinito?
- 3 Determinare tutte le soluzioni intere dell'equazione data.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo di voler determinare le eventuali soluzioni *razionali* di un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (1)$$

dove  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  e  $a_n \neq 0$ .

Osserviamo che non è limitativo supporre  $a_0 \neq 0$ . Infatti, qualora  $a_0 = 0$ , denotato con  $m$  il minimo numero naturale per cui  $a_m \neq 0$ , la (1) si scriverebbe come

$$x^m (a_n x^{n-m} + a_{n-1} x^{n-m-1} + \cdots + a_m) = 0$$

e, una volta considerata la soluzione  $x = 0$  con molteplicità  $m$ , il problema è ricondotto alla situazione precedente.

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .  
Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .  
Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

Supponiamo ora che un numero razionale  $q$  sia soluzione della nostra equazione. Siano  $r \in \mathbb{Z}$  e  $s \in \mathbb{N}$  tale che  $q = \frac{r}{s}$  e  $\text{mcd}(r, s) = 1$ .

Dalla (1) otteniamo:

$$a_n r^n = -(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \cdots + a_0 s^{n-1}) s,$$

$$a_0 s^n = -(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) r.$$

Dalla prima relazione segue che  $s | a_n r^n$  e, poiché  $\text{mcd}(r, s) = 1$ , concludiamo che  $s | a_n$ . Analogamente, dalla seconda relazione otteniamo che  $r | a_0$ .

Le eventuali soluzioni intere si ottengono in corrispondenza di  $s = 1$ .

## Esempio

Consideriamo l'equazione

$$x^7 + x + 2 = 0.$$

I divisori del termine noto sono 1,  $-1$ , 2 e  $-2$ . Pertanto, si verifica immediatamente che l'unica soluzione intera (e, in questo caso, anche l'unica razionale) è costituita da  $-1$ .

## Esempio

Consideriamo l'equazione

$$x^7 + x + 2 = 0.$$

I divisori del termine noto sono 1,  $-1$ , 2 e  $-2$ . Pertanto, si verifica immediatamente che l'unica soluzione intera (e, in questo caso, anche l'unica razionale) è costituita da  $-1$ .

## Esempio

Consideriamo l'equazione

$$x^7 + x + 2 = 0.$$

I divisori del termine noto sono 1,  $-1$ , 2 e  $-2$ . Pertanto, si verifica immediatamente che l'unica soluzione intera (e, in questo caso, anche l'unica razionale) è costituita da  $-1$ .

## Esempio

Consideriamo l'equazione

$$x^7 + x + 2 = 0.$$

I divisori del termine noto sono 1,  $-1$ , 2 e  $-2$ . Pertanto, si verifica immediatamente che l'unica soluzione intera (e, in questo caso, anche l'unica razionale) è costituita da  $-1$ .

## Esempio

Consideriamo l'equazione

$$x^7 + x + 2 = 0.$$

I divisori del termine noto sono 1,  $-1$ , 2 e  $-2$ . Pertanto, si verifica immediatamente che l'unica soluzione intera (e, in questo caso, anche l'unica razionale) è costituita da  $-1$ .

## Esempio

Consideriamo l'equazione

$$x^7 + x + 2 = 0.$$

I divisori del termine noto sono 1,  $-1$ , 2 e  $-2$ . Pertanto, si verifica immediatamente che l'unica soluzione intera (e, in questo caso, anche l'unica razionale) è costituita da  $-1$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 < r_1 < b; \\
 b &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\
 &\vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\
 r_{n-1} &= r_nq_{n+1}.
 \end{aligned} \tag{2}$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 < r_1 < b; \\
 b &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\
 &\vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\
 r_{n-1} &= r_nq_{n+1}.
 \end{aligned} \tag{2}$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$a = bq_1 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2;$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_nq_{n+1}. \quad (2)$$

Allora si dimostra che  $r_n = \text{mcd}(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$a = bq_1 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2;$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_nq_{n+1}. \quad (2)$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$a = bq_1 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2;$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_nq_{n+1}. \quad (2)$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$a = bq_1 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2;$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_nq_{n+1}. \quad (2)$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$a = bq_1 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2;$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_nq_{n+1}. \quad (2)$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 < r_1 < b; \\
 b &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\
 &\vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\
 r_{n-1} &= r_nq_{n+1}.
 \end{aligned} \tag{2}$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 < r_1 < b; \\
 b &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\
 &\vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\
 r_{n-1} &= r_nq_{n+1}.
 \end{aligned} \tag{2}$$

Allora si dimostra che  $r_n = \gcd(a, b)$ .

# L'equazione $ax + by = c$

Siano  $a, b \in \mathbb{N}$  con  $a > b$ . Mediante divisioni successive otteniamo:

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 < r_1 < b; \\
 b &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\
 &\vdots \\
 r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}; \\
 r_{n-1} &= r_nq_{n+1}.
 \end{aligned} \tag{2}$$

Allora si dimostra che  $r_n = \text{mcd}(a, b)$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

## Esempio

Determiniamo  $\text{mcd}(364, 124)$  mediante l'algoritmo euclideo. Abbiamo:

$$364 = 124 \cdot 2 + 116;$$

$$124 = 116 \cdot 1 + 8;$$

$$116 = 8 \cdot 14 + 4;$$

$$8 = 4 \cdot 2.$$

Possiamo quindi concludere che  $\text{mcd}(364, 124) = 4$ .

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

Proveremo ora che esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + by = \text{mcd}(a, b).$$

Infatti, dalla prima relazione di (2) otteniamo

$$r_1 = a - bq_1$$

da cui, sostituendo nella seconda:

$$r_2 = b - r_1q_2 = b - aq_2 + bq_1q_2 = a(-q_2) + b(1 + q_1q_2).$$

Chiaramente, tale procedimento può essere ripetuto per i successivi resti  $r_3, r_4, \dots, r_n$ , ottenendo all'ultimo passo un'espressione della forma

$$r_n = ax + by$$

con  $x$  e  $y$  numeri interi. Poiché  $r_n$  coincide col massimo comun divisore tra  $a$  e  $b$ , ciò è quanto si desiderava provare.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$\begin{aligned} 4 &= 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42 \\ &= 364 \cdot 15 + 124 \cdot (-44). \end{aligned}$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$4 = 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42$$

$$= 364 \cdot 15 + 124 \cdot (-44).$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$4 = 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42$$

$$= 364 \cdot 15 + 124 \cdot (-44).$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$4 = 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42$$

$$= 364 \cdot 15 + 124 \cdot (-44).$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$4 = 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42$$

$$= 364 \cdot 15 + 124 \cdot (-44).$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$\begin{aligned} 4 &= 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42 \\ &= 364 \cdot 15 + 124 \cdot (-44). \end{aligned}$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$4 = 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42$$

$$= 364 \cdot 15 + 124 \cdot (-44).$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Esempio

Torniamo all'esempio precedente, con  $a = 364$  e  $b = 124$ . Risulta:

$$116 = 364 \cdot 1 + 124 \cdot (-2);$$

$$8 = 124 - 116 = 124 - 364 + 124 \cdot 2 = 364 \cdot (-1) + 124 \cdot 3;$$

$$4 = 116 - 8 \cdot 14 = 364 - 124 \cdot 2 + 364 \cdot 14 - 124 \cdot 42$$

$$= 364 \cdot 15 + 124 \cdot (-44).$$

## Nota

La proprietà appena vista vale più in generale anche nell'ipotesi in cui  $a$  e  $b$  siano numeri interi non necessariamente positivi.

## Teorema

Siano  $a, b, c \in \mathbb{Z}$ . L'equazione diofantea

$$ax + by = c$$

ammette soluzioni se e solo se  $\text{mcd}(a, b) | c$ .

## Teorema

Siano  $a, b, c \in \mathbb{Z}$ . L'equazione diofantea

$$ax + by = c$$

ammette soluzioni se e solo se  $\text{mcd}(a, b) | c$ .

## Teorema

Siano  $a, b, c \in \mathbb{Z}$ . L'equazione diofantea

$$ax + by = c$$

ammette soluzioni se e solo se  $\text{mcd}(a, b) | c$ .

## Teorema

Siano  $a, b, c \in \mathbb{Z}$ . L'equazione diofantea

$$ax + by = c$$

ammette soluzioni se e solo se  $\text{mcd}(a, b) | c$ .

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data.  $\square$

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

## Dimostrazione

Poniamo  $d = \text{mcd}(a, b)$ . Se  $ax + by = c$  per qualche  $x, y \in \mathbb{Z}$ , poiché  $d|a$  e  $d|b$ , segue necessariamente che  $d|c$ .

Viceversa, se  $d|c$  allora esiste  $k \in \mathbb{Z}$  tale che  $c = kd$ . Siano  $\hat{x}, \hat{y} \in \mathbb{Z}$  tali che

$$a\hat{x} + b\hat{y} = d$$

e poniamo

$$\bar{x} = k\hat{x}, \quad \bar{y} = k\hat{y}.$$

Risulta

$$a\bar{x} + b\bar{y} = k(a\hat{x} + b\hat{y}) = kd = c$$

e quindi  $(\bar{x}, \bar{y})$  è una soluzione intera dell'equazione data. □

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Supponiamo ora che  $(\bar{x}, \bar{y})$  sia una soluzione dell'equazione diofantea

$$ax + by = c \quad (3)$$

e proponiamoci di determinare tutte le altre. Osserviamo che se  $(\hat{x}, \hat{y})$  è un'altra soluzione di (3) allora abbiamo

$$a(\hat{x} - \bar{x}) + b(\hat{y} - \bar{y}) = a\hat{x} + b\hat{y} - (a\bar{x} + b\bar{y}) = c - c = 0$$

e quindi  $(\hat{x} - \bar{x}, \hat{y} - \bar{y})$  è una soluzione dell'equazione

$$ax + by = 0. \quad (4)$$

Viceversa, se  $(x_0, y_0)$  è una soluzione di (4) allora

$$a(x_0 + \bar{x}) + b(y_0 + \bar{y}) = ax_0 + by_0 + a\bar{x} + b\bar{y} = c.$$

Pertanto, la soluzione generale di (3) è rappresentata da tutte le coppie  $(x_0 + \bar{x}, y_0 + \bar{y})$  con  $(x_0, y_0)$  soluzione di (4).

Ora, la soluzione generale della (4) è data da

$$x_0 = \frac{kb}{d}, \quad y_0 = -\frac{ka}{d}$$

dove  $k$  è un arbitrario numero intero e  $d = \text{mcd}(a, b)$ .

In conclusione, la soluzione generale di (3) è data da:

$$x = \bar{x} + \frac{kb}{d}, \quad y = \bar{y} - \frac{ka}{d}$$

con  $k \in \mathbb{Z}$ .

Ora, la soluzione generale della (4) è data da

$$x_0 = \frac{kb}{d}, \quad y_0 = -\frac{ka}{d}$$

dove  $k$  è un arbitrario numero intero e  $d = \text{mcd}(a, b)$ .

In conclusione, la soluzione generale di (3) è data da:

$$x = \bar{x} + \frac{kb}{d}, \quad y = \bar{y} - \frac{ka}{d}$$

con  $k \in \mathbb{Z}$ .

Ora, la soluzione generale della (4) è data da

$$x_0 = \frac{kb}{d}, \quad y_0 = -\frac{ka}{d}$$

dove  $k$  è un arbitrario numero intero e  $d = \text{mcd}(a, b)$ .

In conclusione, la soluzione generale di (3) è data da:

$$x = \bar{x} + \frac{kb}{d}, \quad y = \bar{y} - \frac{ka}{d}$$

con  $k \in \mathbb{Z}$ .

Ora, la soluzione generale della (4) è data da

$$x_0 = \frac{kb}{d}, \quad y_0 = -\frac{ka}{d}$$

dove  $k$  è un arbitrario numero intero e  $d = \text{mcd}(a, b)$ .

In conclusione, la soluzione generale di (3) è data da:

$$x = \bar{x} + \frac{kb}{d}, \quad y = \bar{y} - \frac{ka}{d}$$

con  $k \in \mathbb{Z}$ .

# Esempi

L'equazione

$$3x + 6y = 22$$

non ha soluzioni intere perchè  $3 = \text{mcd}(3, 6)$  non divide 22.

# Esempi

L'equazione

$$3x + 6y = 22$$

non ha soluzioni intere perchè  $3 = \text{mcd}(3, 6)$  non divide 22.

# Esempi

L'equazione

$$3x + 6y = 22$$

non ha soluzioni intere perchè  $3 = \text{mcd}(3, 6)$  non divide 22.

Consideriamo l'equazione

$$7x + 11y = 13.$$

Per il Teorema, l'equazione data ammette delle soluzioni intere. Ora, risulta

$$11 = 1 \cdot 7 + 4;$$

$$7 = 1 \cdot 4 + 3;$$

$$4 = 1 \cdot 3 + 1;$$

$$1 = 1 \cdot 1$$

e quindi

$$1 = 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 = (11 - 7) \cdot 2 - 7 = 7(-3) + 11 \cdot 2.$$

Consideriamo l'equazione

$$7x + 11y = 13.$$

Per il Teorema, l'equazione data ammette delle soluzioni intere. Ora, risulta

$$11 = 1 \cdot 7 + 4;$$

$$7 = 1 \cdot 4 + 3;$$

$$4 = 1 \cdot 3 + 1;$$

$$1 = 1 \cdot 1$$

e quindi

$$1 = 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 = (11 - 7) \cdot 2 - 7 = 7(-3) + 11 \cdot 2.$$

Consideriamo l'equazione

$$7x + 11y = 13.$$

Per il Teorema, l'equazione data ammette delle soluzioni intere. Ora, risulta

$$11 = 1 \cdot 7 + 4;$$

$$7 = 1 \cdot 4 + 3;$$

$$4 = 1 \cdot 3 + 1;$$

$$1 = 1 \cdot 1$$

e quindi

$$1 = 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 = (11 - 7) \cdot 2 - 7 = 7(-3) + 11 \cdot 2.$$

Consideriamo l'equazione

$$7x + 11y = 13.$$

Per il Teorema, l'equazione data ammette delle soluzioni intere. Ora, risulta

$$11 = 1 \cdot 7 + 4;$$

$$7 = 1 \cdot 4 + 3;$$

$$4 = 1 \cdot 3 + 1;$$

$$1 = 1 \cdot 1$$

e quindi

$$1 = 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 = (11 - 7) \cdot 2 - 7 = 7(-3) + 11 \cdot 2.$$

Pertanto, una soluzione intera dell'equazione assegnata è

$$\bar{x} = -3 \cdot 13 = -39, \quad \bar{y} = 2 \cdot 13 = 26.$$

Le altre soluzioni sono date da

$$x = -39 + 11k, \quad y = 26 - 7k$$

dove  $k$  è un arbitrario numero intero.

Pertanto, una soluzione intera dell'equazione assegnata è

$$\bar{x} = -3 \cdot 13 = -39, \quad \bar{y} = 2 \cdot 13 = 26.$$

Le altre soluzioni sono date da

$$x = -39 + 11k, \quad y = 26 - 7k$$

dove  $k$  è un arbitrario numero intero.

Pertanto, una soluzione intera dell'equazione assegnata è

$$\bar{x} = -3 \cdot 13 = -39, \quad \bar{y} = 2 \cdot 13 = 26.$$

Le altre soluzioni sono date da

$$x = -39 + 11k, \quad y = 26 - 7k$$

dove  $k$  è un arbitrario numero intero.

Pertanto, una soluzione intera dell'equazione assegnata è

$$\bar{x} = -3 \cdot 13 = -39, \quad \bar{y} = 2 \cdot 13 = 26.$$

Le altre soluzioni sono date da

$$x = -39 + 11k, \quad y = 26 - 7k$$

dove  $k$  è un arbitrario numero intero.

## Teorema

Siano  $a_1, a_2, \dots, a_n, b \in \mathbb{Z}$ . Allora l'equazione

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

ammette soluzioni intere se e solo se  $\text{mcd}(a_1, a_2, \dots, a_n) | b$ .

## Teorema

Siano  $a_1, a_2, \dots, a_n, b \in \mathbb{Z}$ . Allora l'equazione

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

ammette soluzioni intere se e solo se  $\text{mcd}(a_1, a_2, \dots, a_n) | b$ .

## Teorema

Siano  $a_1, a_2, \dots, a_n, b \in \mathbb{Z}$ . Allora l'equazione

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

ammette soluzioni intere se e solo se  $\text{mcd}(a_1, a_2, \dots, a_n) | b$ .

# L'equazione $x^2 + y^2 = z^2$

Vogliamo determinare tutte le soluzioni intere dell'*equazione di Pitagora*

$$x^2 + y^2 = z^2. \quad (5)$$

# L'equazione $x^2 + y^2 = z^2$

Vogliamo determinare tutte le soluzioni intere dell'*equazione di Pitagora*

$$x^2 + y^2 = z^2. \quad (5)$$

# L'equazione $x^2 + y^2 = z^2$

Vogliamo determinare tutte le soluzioni intere dell'*equazione di Pitagora*

$$x^2 + y^2 = z^2. \quad (5)$$

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

## Nota

È sufficiente considerare le sole soluzioni intere positive. Una terna di numeri naturali  $(x, y, z)$  che sia soluzione della (5) è detta *terna pitagorica*.

Possiamo inoltre limitare l'attenzione alle sole soluzioni *primitive*, ossia quelle per cui risulta  $\text{mcd}(x, y, z) = 1$ .

Infatti, se  $(x, y, z)$  è una soluzione primitiva di (5), allora per ogni  $k \in \mathbb{Z}$  abbiamo che  $(kx, ky, kz)$  è ancora una soluzione di (5).

Viceversa, se  $x, y, z \in \mathbb{N}$  soddisfano la (5), posto  $d = \text{mcd}(x, y, z)$ , esistono  $a, b, c \in \mathbb{N}$  tali che  $x = ad$ ,  $y = bd$  e  $z = cd$ .

Risulta  $\text{mcd}(a, b, c) = 1$  e

$$(a^2 + b^2)d^2 = c^2d^2,$$

quindi  $(a, b, c)$  è una soluzione primitiva.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

Notiamo poi che se  $(x, y, z)$  è una soluzione primitiva allora  $x$  e  $y$  non possono essere né entrambi pari (perché  $\text{mcd}(x, y, z) = 1$ ) né entrambi dispari. Nel secondo caso, avremmo infatti  $x = 2h + 1$  e  $y = 2k + 1$  con  $h, k \in \mathbb{N}$  e quindi

$$z^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + k^2 + h + k) + 2$$

il che è impossibile in quanto ogni quadrato perfetto pari è divisibile per 4.

## Teorema

Siano  $x, y, z \in \mathbb{N}$  con  $x$  pari. Allora  $(x, y, z)$  è una soluzione primitiva dell'equazione diofantea

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

se e solo se esistono  $a, b \in \mathbb{N}$  con  $a > b$  tali che  $a$  e  $b$  hanno parità opposte,  $\text{mcd}(a, b) = 1$  e risulta

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

## Teorema

Siano  $x, y, z \in \mathbb{N}$  con  $x$  pari. Allora  $(x, y, z)$  è una soluzione primitiva dell'equazione diofantea

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

se e solo se esistono  $a, b \in \mathbb{N}$  con  $a > b$  tali che  $a$  e  $b$  hanno parità opposte,  $\text{mcd}(a, b) = 1$  e risulta

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

## Teorema

Siano  $x, y, z \in \mathbb{N}$  con  $x$  pari. Allora  $(x, y, z)$  è una soluzione primitiva dell'equazione diofantea

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

se e solo se esistono  $a, b \in \mathbb{N}$  con  $a > b$  tali che  $a$  e  $b$  hanno parità opposte,  $\text{mcd}(a, b) = 1$  e risulta

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

## Teorema

Siano  $x, y, z \in \mathbb{N}$  con  $x$  pari. Allora  $(x, y, z)$  è una soluzione primitiva dell'equazione diofantea

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

se e solo se esistono  $a, b \in \mathbb{N}$  con  $a > b$  tali che  $a$  e  $b$  hanno parità opposte,  $\text{mcd}(a, b) = 1$  e risulta

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

## Teorema

Siano  $x, y, z \in \mathbb{N}$  con  $x$  pari. Allora  $(x, y, z)$  è una soluzione primitiva dell'equazione diofantea

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

se e solo se esistono  $a, b \in \mathbb{N}$  con  $a > b$  tali che  $a$  e  $b$  hanno parità opposte,  $\text{mcd}(a, b) = 1$  e risulta

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2 \nmid x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2 \nmid x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\gcd(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\gcd(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2|x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2|x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2|x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2|x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2|x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2|x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2 \nmid x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2 \nmid x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

## Dimostrazione

Supponiamo prima che  $(x, y, z)$  sia una soluzione primitiva.

Poiché  $2 \nmid x$  si ha che  $y$  e  $z$  sono dispari, pertanto  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono interi positivi e, inoltre,  $\text{mcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ .

Dalla relazione

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$$

segue quindi che  $\frac{z-y}{2}$  e  $\frac{z+y}{2}$  sono entrambi quadrati perfetti.

Esistono allora  $a, b \in \mathbb{N}$  tali che

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2.$$

Evidentemente, abbiamo che  $a > b$  e  $\text{mcd}(a, b) = 1$  e, dal momento che  $a^2 + b^2 = z$ , segue anche che  $a$  e  $b$  hanno parità opposte.

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte.  $\square$

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte.  $\square$

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte.  $\square$

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte.  $\square$

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

Reciprocamente, se  $a$  e  $b$  verificano le condizioni dell'enunciato, abbiamo subito che  $x, y, z \in \mathbb{N}$ ,  $x$  è pari e

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Rimane da dimostrare che  $\text{mcd}(x, y) = 1$ . Supponiamo per assurdo che  $\text{mcd}(x, y) > 1$  e, quindi, che esista un numero primo  $p$  che divida sia  $x$  che  $y$ . Allora  $p$  divide anche  $z$  e poiché

$$y = a^2 - b^2, \quad z = a^2 + b^2$$

segue che  $p|2a^2$  e  $p|2b^2$ .

Ma  $\text{mcd}(a, b) = 1$ , dunque necessariamente  $p = 2$ .

Ne concludiamo che  $y$  è pari e ciò è assurdo in quanto  $a$  e  $b$  hanno parità opposte. □

## Questione (Pierre de Fermat, 1637)

L'equazione

$$x^n + y^n = z^n$$

dove  $n$  è un numero naturale maggiore di 2, può ammettere soluzioni costituite da terne di interi positivi?

Andrew Wiles: *Modular elliptic curves and Fermat's Last theorem*,  
Annals of Mathematics **141** (1995), 443-551.

## Questione (Pierre de Fermat, 1637)

L'equazione

$$x^n + y^n = z^n$$

dove  $n$  è un numero naturale maggiore di 2, può ammettere soluzioni costituite da terne di interi positivi?

Andrew Wiles: *Modular elliptic curves and Fermat's Last theorem*,  
Annals of Mathematics **141** (1995), 443-551.

## Questione (Pierre de Fermat, 1637)

L'equazione

$$x^n + y^n = z^n$$

dove  $n$  è un numero naturale maggiore di 2, può ammettere soluzioni costituite da terne di interi positivi?

Andrew Wiles: *Modular elliptic curves and Fermat's Last theorem*,  
Annals of Mathematics **141** (1995), 443-551.

## Problema 1

Determinare le soluzioni intere dell'equazione

$$(x + y + z)^3 = x^3 + y^3 + z^3.$$

## Problema 1

Determinare le soluzioni intere dell'equazione

$$(x + y + z)^3 = x^3 + y^3 + z^3.$$

## Problema 1

Determinare le soluzioni intere dell'equazione

$$(x + y + z)^3 = x^3 + y^3 + z^3.$$

## Soluzione

Abbiamo

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

da cui otteniamo

$$(x+y+z)^3 - (x^3 + y^3 + z^3) = 3(x+y)(x+z)(y+z).$$

Così, l'equazione assegnata è equivalente a

$$(x+y)(x+z)(y+z) = 0$$

la quale ammette come soluzioni intere tutte e sole le terne del tipo

$$(m, -m, n), \quad (m, n, -m), \quad (m, n, -n)$$

con  $m, n \in \mathbb{Z}$ .

## Soluzione

Abbiamo

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

da cui otteniamo

$$(x+y+z)^3 - (x^3 + y^3 + z^3) = 3(x+y)(x+z)(y+z).$$

Così, l'equazione assegnata è equivalente a

$$(x+y)(x+z)(y+z) = 0$$

la quale ammette come soluzioni intere tutte e sole le terne del tipo

$$(m, -m, n), \quad (m, n, -m), \quad (m, n, -n)$$

con  $m, n \in \mathbb{Z}$ .

## Soluzione

Abbiamo

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

da cui otteniamo

$$(x+y+z)^3 - (x^3 + y^3 + z^3) = 3(x+y)(x+z)(y+z).$$

Così, l'equazione assegnata è equivalente a

$$(x+y)(x+z)(y+z) = 0$$

la quale ammette come soluzioni intere tutte e sole le terne del tipo

$$(m, -m, n), \quad (m, n, -m), \quad (m, n, -n)$$

con  $m, n \in \mathbb{Z}$ .

## Soluzione

Abbiamo

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

da cui otteniamo

$$(x+y+z)^3 - (x^3 + y^3 + z^3) = 3(x+y)(x+z)(y+z).$$

Così, l'equazione assegnata è equivalente a

$$(x+y)(x+z)(y+z) = 0$$

la quale ammette come soluzioni intere tutte e sole le terne del tipo

$$(m, -m, n), \quad (m, n, -m), \quad (m, n, -n)$$

con  $m, n \in \mathbb{Z}$ .

## Soluzione

Abbiamo

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

da cui otteniamo

$$(x+y+z)^3 - (x^3 + y^3 + z^3) = 3(x+y)(x+z)(y+z).$$

Così, l'equazione assegnata è equivalente a

$$(x+y)(x+z)(y+z) = 0$$

la quale ammette come soluzioni intere tutte e sole le terne del tipo

$$(m, -m, n), \quad (m, n, -m), \quad (m, n, -n)$$

con  $m, n \in \mathbb{Z}$ .

## Soluzione

Abbiamo

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

da cui otteniamo

$$(x+y+z)^3 - (x^3 + y^3 + z^3) = 3(x+y)(x+z)(y+z).$$

Così, l'equazione assegnata è equivalente a

$$(x+y)(x+z)(y+z) = 0$$

la quale ammette come soluzioni intere tutte e sole le terne del tipo

$$(m, -m, n), \quad (m, n, -m), \quad (m, n, -n)$$

con  $m, n \in \mathbb{Z}$ .

## Problema 2

Determinare le soluzioni intere positive dell'equazione

$$x^2 - y^2 = 60.$$

## Problema 2

Determinare le soluzioni intere positive dell'equazione

$$x^2 - y^2 = 60.$$

## Problema 2

Determinare le soluzioni intere positive dell'equazione

$$x^2 - y^2 = 60.$$

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

## Soluzione

Riscriviamo l'equazione assegnata come

$$(x + y)(x - y) = 60.$$

Poniamo

$$x + y = a, \quad x - y = b.$$

Allora deve aversi  $a, b \in \mathbb{N}$  con  $a > b$  e  $ab = 60$ . I possibili valori di  $a$  e  $b$  verificanti tali richieste sono contenuti nel seguente schema:

| a  | b |
|----|---|
| 60 | 1 |
| 30 | 2 |
| 20 | 3 |
| 15 | 4 |
| 12 | 5 |
| 10 | 6 |

D'altra parte, poiché

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

i valori  $x$  e  $y$  risultano interi se e solo se  $a$  e  $b$  hanno la stessa parità.

Pertanto, le uniche coppie  $(a, b)$  accettabili sono  $(30, 2)$  e  $(10, 6)$ , a cui corrispondono le soluzioni  $(x, y) = (16, 14)$  e  $(x, y) = (8, 2)$ .

D'altra parte, poiché

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

i valori  $x$  e  $y$  risultano interi se e solo se  $a$  e  $b$  hanno la stessa parità.

Pertanto, le uniche coppie  $(a, b)$  accettabili sono  $(30, 2)$  e  $(10, 6)$ , a cui corrispondono le soluzioni  $(x, y) = (16, 14)$  e  $(x, y) = (8, 2)$ .

D'altra parte, poiché

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

i valori  $x$  e  $y$  risultano interi se e solo se  $a$  e  $b$  hanno la stessa parità.

Pertanto, le uniche coppie  $(a, b)$  accettabili sono  $(30, 2)$  e  $(10, 6)$ , a cui corrispondono le soluzioni  $(x, y) = (16, 14)$  e  $(x, y) = (8, 2)$ .

D'altra parte, poiché

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

i valori  $x$  e  $y$  risultano interi se e solo se  $a$  e  $b$  hanno la stessa parità. Pertanto, le uniche coppie  $(a, b)$  accettabili sono  $(30, 2)$  e  $(10, 6)$ , a cui corrispondono le soluzioni  $(x, y) = (16, 14)$  e  $(x, y) = (8, 2)$ .

D'altra parte, poiché

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

i valori  $x$  e  $y$  risultano interi se e solo se  $a$  e  $b$  hanno la stessa parità.

Pertanto, le uniche coppie  $(a, b)$  accettabili sono  $(30, 2)$  e  $(10, 6)$ , a cui corrispondono le soluzioni  $(x, y) = (16, 14)$  e  $(x, y) = (8, 2)$ .

### Problema 3

Dato un numero primo  $p$ , determinare tutte le coppie ordinate di numeri naturali  $(m, n)$  che verificano l'equazione

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{p}.$$

### Problema 3

Dato un numero primo  $p$ , determinare tutte le coppie ordinate di numeri naturali  $(m, n)$  che verificano l'equazione

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{p}.$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$m = 2p, \quad n = 2p;$$

$$m = p^2 + p, \quad n = p + 1;$$

$$n = p + 1, \quad m = p^2 + p.$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$m = 2p, \quad n = 2p;$$

$$m = p^2 + p, \quad n = p + 1;$$

$$n = p + 1, \quad m = p^2 + p.$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$\begin{aligned} m &= 2p, & n &= 2p; \\ m &= p^2 + p, & n &= p + 1; \\ n &= p + 1, & m &= p^2 + p. \end{aligned}$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$m = 2p, \quad n = 2p;$$

$$m = p^2 + p, \quad n = p + 1;$$

$$m = p + 1, \quad n = p^2 + p.$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$m = 2p, \quad n = 2p;$$

$$m = p^2 + p, \quad n = p + 1;$$

$$m = p + 1, \quad n = p^2 + p.$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$m = 2p, \quad n = 2p;$$

$$m = p^2 + p, \quad n = p + 1;$$

$$m = p + 1, \quad n = p^2 + p.$$

## Soluzione

Posto

$$m = p + a, \quad n = p + b$$

l'equazione data si riscrive nella seguente forma equivalente

$$p(2p + a + b) = (p + a)(p + b)$$

da cui, sviluppando i prodotti e semplificando, si ottiene

$$ab = p^2.$$

Pertanto le uniche possibilità sono  $a = b = p$  o  $a = p^2, b = 1$  oppure  $a = 1, b = p^2$ . Le soluzioni intere positive dell'equazione di partenza sono quindi:

$$m = 2p, \quad n = 2p;$$

$$m = p^2 + p, \quad n = p + 1;$$

$$n = p + 1, \quad m = p^2 + p.$$

## Problema 4

Si dimostri che l'equazione

$$a^2 + b^2 = c^2 + 3$$

ammette come soluzioni infinite terne di interi  $(a, b, c)$ .

## Problema 4

Si dimostri che l'equazione

$$a^2 + b^2 = c^2 + 3$$

ammette come soluzioni infinite terne di interi  $(a, b, c)$ .

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.

## Soluzione

Osserviamo che, se  $a$  e  $b$  sono pari, allora  $c$  deve essere dispari. Posto allora

$$a = 2h, \quad b = 2k, \quad c = 2l + 1$$

l'equazione assegnata può essere riscritta nella forma

$$h^2 + k^2 = l^2 + l + 1$$

la quale risulta in particolare soddisfatta qualora  $k = l = h^2 - 1$ .

Pertanto l'equazione di partenza ammette come soluzioni intere tutte le terne  $(a, b, c) = (2h, 2h^2 - 2, 2h^2 - 1)$  con  $h$  numero intero arbitrario.