Teoria dei Numeri
Teorema di Eulero

Alessandra Bernardi

15 marzo 2016, Trento

Teorema di Eulero

Theorem

Un primo p dispari si scrive come somma di due quadrati se e solo se $p \equiv 1$ (mod 4).

Dimostrazione.

L'implicazione " $\Rightarrow$ " l'abbiamo già vista. Vediamo " $\Leftarrow$ " .
Sappiamo già che $\exists\, m > 0$ t.c. per $x > 0$

$$mp = x^2 + 1. \tag{1}$$

Osserviamo che possiamo scegliere $x < p$ infatti se $x \geq p$ allora $x = kp + x'$, quindi $x'^2 \equiv x^2 \equiv -1 \pmod{p}$.
Anzi possiamo addirittura prendere $x < p/2$ infatti se $x \geq \frac{p+1}{2}$ allora $y = p - x$ perciò di nuovo $y^2 \equiv x^2 \equiv -1$ (mod p).
Se quindi $x < p/2$ allora $m = \frac{x^2+1}{p} < p$ *(basta fare i conti).* □

Teorema di Eulero

Theorem

Un primo p dispari si scrive come somma di due quadrati se e solo se $p \equiv 1$ (mod 4).

Dimostrazione.

L'implicazione " $\Rightarrow$ " l'abbiamo già vista. Vediamo " $\Leftarrow$ " .

Sappiamo già che $\exists\, m > 0$ t.c. per $x > 0$

$$mp = x^2 + 1. \tag{1}$$

Osserviamo che possiamo scegliere $x < p$ infatti se $x \geq p$ allora $x = kp + x'$, quindi $x'^2 \equiv x^2 \equiv -1 \pmod{p}$.
Anzi possiamo addirittura prendere $x < p/2$ infatti se $x \geq \frac{p+1}{2}$ allora $y = p - x$ perciò di nuovo $y^2 \equiv x^2 \equiv -1$ (mod p).
Se quindi $x < p/2$ allora $m = \frac{x^2+1}{p} < p$ *(basta fare i conti).* □

Teorema di Eulero

Theorem

Un primo p dispari si scrive come somma di due quadrati se e solo se $p \equiv 1$ (mod 4).

Dimostrazione.

L'implicazione " $\Rightarrow$ " l'abbiamo già vista. Vediamo " $\Leftarrow$ " .
Sappiamo già che $\exists\, m > 0$ t.c. per $x > 0$

$$mp = x^2 + 1. \tag{1}$$

Osserviamo che possiamo scegliere $x < p$ infatti se $x \geq p$ allora $x = kp + x'$, quindi $x'^2 \equiv x^2 \equiv -1 \pmod{p}$.
Anzi possiamo addirittura prendere $x < p/2$ infatti se $x \geq \frac{p+1}{2}$ allora $y = p - x$ perciò di nuovo $y^2 \equiv x^2 \equiv -1$ (mod p).
Se quindi $x < p/2$ allora $m = \frac{x^2+1}{p} < p$ *(basta fare i conti).* □

Teorema di Eulero

Theorem

Un primo p dispari si scrive come somma di due quadrati se e solo se $p \equiv 1$ (mod 4).

Dimostrazione.

L'implicazione " $\Rightarrow$ " l'abbiamo già vista. Vediamo " $\Leftarrow$ " .
Sappiamo già che $\exists\, m > 0$ t.c. per $x > 0$

$$mp = x^2 + 1. \tag{1}$$

Osserviamo che possiamo scegliere $x < p$ infatti se $x \geq p$ allora $x = kp + x'$, quindi $x'^2 \equiv x^2 \equiv -1 \pmod{p}$.
Anzi possiamo addirittura prendere $x < p/2$ infatti se $x \geq \frac{p+1}{2}$ allora $y = p - x$ perciò di nuovo $y^2 \equiv x^2 \equiv -1$ (mod p).
Se quindi $x < p/2$ allora $m = \frac{x^2+1}{p} < p$ *(basta fare i conti).* □

Teorema di Eulero

Theorem

Un primo p dispari si scrive come somma di due quadrati se e solo se $p \equiv 1$ (mod 4).

Dimostrazione.

L'implicazione " $\Rightarrow$ " l'abbiamo già vista. Vediamo " $\Leftarrow$ " .
Sappiamo già che $\exists\, m > 0$ t.c. per $x > 0$

$$mp = x^2 + 1. \tag{1}$$

Osserviamo che possiamo scegliere $x < p$ infatti se $x \geq p$ allora $x = kp + x'$, quindi $x'^2 \equiv x^2 \equiv -1 \pmod{p}$.
Anzi possiamo addirittura prendere $x < p/2$ infatti se $x \geq \frac{p+1}{2}$ allora $y = p - x$ perciò di nuovo $y^2 \equiv x^2 \equiv -1$ (mod p).
Se quindi $x < p/2$ allora $m = \frac{x^2+1}{p} < p$ *(basta fare i conti).* □

Teorema di Eulero

Theorem

Un primo p dispari si scrive come somma di due quadrati se e solo se $p \equiv 1$ (mod 4).

Dimostrazione.

L'implicazione " $\Rightarrow$ " l'abbiamo già vista. Vediamo " $\Leftarrow$ " .
Sappiamo già che $\exists\, m > 0$ t.c. per $x > 0$

$$mp = x^2 + 1. \tag{1}$$

Osserviamo che possiamo scegliere $x < p$ infatti se $x \geq p$ allora $x = kp + x'$, quindi $x'^2 \equiv x^2 \equiv -1 \pmod{p}$.
Anzi possiamo addirittura prendere $x < p/2$ infatti se $x \geq \frac{p+1}{2}$ allora $y = p - x$ perciò di nuovo $y^2 \equiv x^2 \equiv -1$ (mod p).
Se quindi $x < p/2$ allora $m = \frac{x^2+1}{p} < p$ *(basta fare i conti)*. □

Dimostrazione.

Siamo quindi arrivati a dire che $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$.
Se $m = 1$ abbiamo finito. Supponiamo quindi $m > 1$.

Con questa ipotesi di $m > 1$ vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. rp è somma di due quadrati.
Se riusciamo a trovare un r con queste proprietà allora potremo applicare il metodo di **discesa infinita** *e dire che se esiste un $m > 1$ tale che mp è somma di due quadrati allora deve esistere un $0 < r < m$ t.c. rp sia somma di due quadrati e quel punto ri-applichiamo lo stesso argomento per r, ma poiché non possiamo andare avanti all'infinito perchè $\mathbb{N}$ ha minimo, dovremo arrivare a dire che $m = 1$.* □

Dimostrazione.

Siamo quindi arrivati a dire che $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$.
Se $m = 1$ abbiamo finito. Supponiamo quindi $m > 1$.

Con questa ipotesi di $m > 1$ vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. rp è somma di due quadrati.
Se riusciamo a trovare un r con queste proprietà allora potremo applicare il metodo di **discesa infinita** *e dire che se esiste un $m > 1$ tale che mp è somma di due quadrati allora deve esistere un $0 < r < m$ t.c. rp sia somma di due quadrati e quel punto ri-applichiamo lo stesso argomento per r, ma poiché non possiamo andare avanti all'infinito perchè $\mathbb{N}$ ha minimo, dovremo arrivare a dire che $m = 1$.* □

Dimostrazione.

Siamo quindi arrivati a dire che $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$.
Se $m = 1$ abbiamo finito. Supponiamo quindi $m > 1$.

Con questa ipotesi di $m > 1$ vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. rp è somma di due quadrati.
Se riusciamo a trovare un r con queste proprietà allora potremo applicare il metodo di **discesa infinita** *e dire che se esiste un $m > 1$ tale che mp è somma di due quadrati allora deve esistere un $0 < r < m$ t.c. rp sia somma di due quadrati e quel punto ri-applichiamo lo stesso argomento per r, ma poiché non possiamo andare avanti all'infinito perchè $\mathbb{N}$ ha minimo, dovremo arrivare a dire che $m = 1$.* □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.

Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Siano $-m/2 \leq u, v \leq m/2$ (*ipotesi non banale se* $m > 1$) tali che

$$u \equiv x \pmod{m} \text{ e } v \equiv y \pmod{m}. \tag{2}$$

Con queste ipotesi è chiaro che $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$ che equivale all'esistenza di un r tale che

$$u^2 + v^2 = rm. \tag{3}$$

Il fatto che $m > 1$ implica che in (3) $r \neq 0$. (Infatti se $r = 0$ allora (3) implicherebbe che $u = v = 0$, ma se $u = v = 0$ allora da (2) si avrebbe che $m \mid x$ e $m \mid y$, ma poiché $mp = x^2 + y^2$ si avrebbe che $m \mid p$, ma se $m \mid p$, poichè p è primo e poichè abbiamo supposto $m < p$, si avrebbe $m = 1$ contro l'ip.) □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che $r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque $m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque
$m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque
$m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □

Dimostrazione.

Sappiamo $\exists\, 0 < m < p$ t.c. $mp = x^2 + y^2$ e supponiamo $m > 1$.
Vogliamo arrivare a dimostrare che $\exists\, 0 < r < m$ t.c. $rp = a^2 + b^2$.
Abbiamo preso $-m/2 \leq u, v \leq m/2$ tali che
$u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$. e abbiamo dimostrato che
$u^2 + v^2 = rm$ con $r \neq 0$.

Poiché abbiamo preso $-m/2 \leq u, v \leq m/2$, si vede che
$r = \frac{u^2+v^2}{m} < m$ *(basta fare i conti)*. Questo mostra che $r < m$.
Ora ci resta solo da dimostrare che anche rp si scrive come somma di due quadrati e poi siamo a posto.

$$(mr)(mp) = (u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2.$$

Ora $(xu + yv)$ è conguro a $x^2 + y^2 \pmod{m}$ perchè $u \equiv x \pmod{m}$ e $v \equiv y \pmod{m}$, Banalmente che $(xv - yu) \equiv 0 \pmod{m}$, quindi sono entrambi congrui a $0 \pmod{m}$. Dunque
$m^2 rp = (ma)^2 + (mb)^2$. Dividendo per m^2 si ha $rp = a^2 + b^2$. □