Θεώρημα 0.0.1 (Lagrange). *Κάθε μη αρνητικός ακέραιος είναι το άθροισμα 4 τέλειων τετραγώνων.*

Απόδειξη. Είναι εύκολο να ελέγξουμε ότι ισχύει η πολυωνυμική ταυτότητα

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

όπου

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2 \\ z_4 &= x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2 \end{aligned}$$

Είναι φανερό λοιπόν ότι αν δύο αριθμοί γράφονται ως άθροισμα τεσσάρων τέλειων τετραγώνων, τότε και το γινόμενο τους είναι επίσης άθροισμα τεσσάρων τέλειων τετραγώνων. Καθώς κάθε αριθμός είναι γινόμενο πρώτων αριθμών, αρκει να δείξουμε το ζητούμενο για κάθε πρώτο αριθμό. Επίσης $2 = 1^2 + 1^2 + 0^2 + 0^2$ και συνεπώς θεωρούμε μόνο περιττούς πρώτους p.

Το σύνολο των τετραγώνων

$$\{a^2 | a = 0, 1, \dots, (p-1)/2\}$$

αντιπροσωπεύει $(p + 1)/2$ διαφορετκές κλάσεις υπολοίπων modulo p. Ομοίως, το σύνολο των ακεραίων

$$\{-b^2 - 1 | b = 0, 1, \dots, (p-1)/2\}$$

αντιπροσωπεύει $(p + 1)/2$ διαφορετκές κλάσεις υπολοίπων modulo p. Καθώς υπάρχουν μόνο p διαφορετκές κλάσεις υπολοίπων modulo p, από την Αρχή του Περιστερώνα πρέπει να υπάρχουν ακέραιοι a και b τέτοιοι ώστε $0 \leqslant a, b \leqslant (p-1)/2$ και

$$a^2 \equiv -b^2 - 1 (mod p),$$

ή ισοδύναμα

$$a^2 + b^2 + 1 \equiv 0 (mod p)$$

Έστω $a^2 + b^2 + 1 = np$. Τότε

$$p \leqslant np = a^2 + b^2 + 1^2 + 0^2 \leqslant 2\left(\frac{p-1}{2}\right)^2 + 1 < \frac{p^2}{2} + 1 < p^2,$$

και έτσι

$$1 \leqslant n < p.$$

Έστω m ο ελάχιστος θετικός ακέραιος τέτοιος ώστε ο mp να είναι το άθροισμα τεσσάρων τέλειων τετραγώνων. Συνεπώς υπάρχουν ακέραιοι x_1, x_2, x_3, x_4 τέτοιοι ώστε

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

και

$$1 \leqslant m \leqslant n < p.$$

Πρέπει να δείξουμε ότι $m = 1$.

Ας υποθέσουμε ότι $m \neq 1$. Τότε $1 < m < p$. Διαλέγουμε ακέραιους y_i ώστε

$$y_i \equiv x_i (modm)$$

και

$$\frac{-m}{2} < y_i < \frac{m}{2}$$

για $i = 1, \ldots, 4$. Έτσι

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0(modm)$$

και

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

για κάποιον μη αρνητικό ακέραιο r. Αν $r = 0$, έχουμε $y_i = 0$ για κάθε i και κάθε x_i διαιρείται από το m^2. Προκύπτει δηλαδή ότι ο mp διαιρείται από τον m^2, και συνεπώς ο p διαιρείται από τον m. Αυτό είναι όμως αδύνατο, καθώς ο p είναι πρώτος και $1 < m < p$. Άρα, $r \geq 1$ και

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \geq 4(m/2)^2 = m^2$$

Επίσης, $r = m$ αν και μονο αν ο m είναι άρτιος και $y_i = m/2$ για κάθε i. Σε αυτήν την περίπτωση, $x_i = m/2(modm)$ για κάθε i, και έτσι $x_i^2 \equiv (m/2)^2(modm^2)$ και

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4(m/2)^2 = m \equiv 0(modm^2).$$

Από αυτό προκύπτει ότι ο p διαιρείται από τον m, το οποίο είναι αντίφαση. Συνεπώς,

$$1 \leqslant r < p < m.$$

Εφαρμόζοντας τώρα την αρχική πολυωνυμική ταυτότητα παίρνουμε

$$m^2rp = (mp)(mr) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

όπου τα z_i καθορίζονται από τις σχέσεις .Καθώς $x_i \equiv y_i(modm)$ από τις σχέσεις αυτές συμπεραίνουμε ότι $z_i \equiv 0(modm)$ για $i = 1, \ldots, 4$. Έστω $w_i = z_i/m$. Τότε οι $w_1, \ldots, w_4$ είναι ακέραιοι και

$$rp = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$

το οποίο αντίκειται στην ελαχιστικότητα του m. Άρα $m = 1$ και ο πρώτος p είναι το άθροισμα τεσσάρων τέλειων τετραγώνων. Αυτό ολοκληρώνει και την απόδειξη του θεωρήματος.

□