Mivel $(a-b)(a^2+ab+b^2)=a^3-b^3$, és $a-b$ nem lehet osztható p-vel, a $p \mid a^2+ab+b^2$ feltétel ekvivalens az $a^3 \equiv b^3 \pmod{p}$ feltétellel. Ezen kívül többször felhasználjuk, hogy $p \geq 7$.

Ismeretes, hogy minden p prímszámhoz létezik olyan g egész szám (úgynevezett primitív gyök modulo p), amelyre az $1, g, g^2, \ldots, g^{p-2}$ számok p-vel való osztási maradékai között az $1, 2, \ldots, p-1$ számok mindegyike pontosan egyszer fordul elő, továbbá $g^{p-1} \equiv 1 \pmod{p}$ (a Fermat-tételnek megfelelően). (A bizonyítást lásd pl. *Niven–Zuckermann:* Bevezetés a számelméletbe, 49–50. old.) Ennek következménye, hogy tetszőleges $3k+1$ alakú p prímszámra létezik olyan h egész szám, amely nem kongruens 1-gyel modulo p, viszont $h^3 \equiv 1 \pmod{p}$; ilyen szám például a $g^{\frac{p-1}{3}}$.

Azt állítjuk, hogy léteznek olyan x, y egész számok, amelyekre $0 < x$, $|y| < \sqrt{p}$, valamint $hx \equiv h \pmod{p}$. Tekintsük a $hu-v$ alakú számokat, ahol $0 \leq u$, $v \leq [\sqrt{p}]$ egészek. Ez összesen $([\sqrt{p}]+1)^2 > p$ darab egész szám, van közöttük kettő, amelyek ugyanabba a p szerinti maradékosztályba esnek: $hu_1 - v_1 \equiv hu_2 - v_2 \pmod{p}$, vagyis $p \mid (u_1-u_2)h-(v_1-v_2)$. Legyen $x=u_1-u_2$ és $y=v_1-v_2$. Ekkor az $|x|$, $|y| < \sqrt{p}$, $hx \equiv y \pmod{p}$ feltételek teljesülnek, és az általánosság megszorítása nélkül feltehetjük, hogy $x>0$, mert x-et és y-t kicserélhetjük $(-x)$-re és $(-y)$-ra. Még azt kell megmutatnunk, hogy x és y különbözőek, és egyikük sem 0. Tegyük fel, hogy $y=0$; ekkor $p \mid hx$. Mivel h nem osztható p-vel, ebből $p \mid x$ következik, viszont $|x|<p$ miatt ez csak $x=0$ esetén lehetséges. Ha viszont $x=y=0$, az ellentmond annak, hogy az (u_1,v_1) és (u_2,v_2) számpárok különbözők. Az $x=0$ esetben hasonlóképpen jutunk ellentmondásra. Ha x és y nem lennének különbözőek, akkor $p \mid (h-1)x$ lenne, viszont sem $h-1$, sem x nem osztható p-vel.

Mivel

$$(x-y)\left(x^2+xy+y^2\right) = x^3-y^3 \equiv (hx)^3-y^3-(hx-y)\left(h^2x^2+hxy+y^2\right) \equiv 0 \pmod{p},$$

és $0<|x-y|<2\sqrt{p}<p$, így $p \mid x^2+xy+y^2$. Ha megmutatjuk, hogy $y>0$ is teljesül, kész vagyunk: x, y közül a kisebbiket a-nak, a nagyobbikat b-nek választva megfelelő számpárt nyerünk.

Tegyük fel, hogy $y<0$. Ekkor $x \leq |y|$ esetén

$$x^2+xy+y^2 \leq x|y|+xy+y^2 = y^2 < p,$$

$x>|y|$ esetén pedig

$$x^2+xy+y^2 \leq x^2+xy+x|y| = x^2 < p.$$

Viszont

$$x^2+xy+y^2 = \frac{1}{2}\left(x^2+y^2+(x+y)^2\right) > 0,$$

és így x^2+xy+y^2 nem lehet osztható p-vel.

Frenkel Péter (Fazekas M. Főv. Gyak. Gimn., IV. o.t.)

Megjegyzések. 1. Többen észrevették, hogy $0 < a$, $b < \sqrt{p}$ teljesülése esetén $p \mid a^2+ab+b^2$ ekvivalens azzal, hogy $a^2+ab+b^2=p$. Ez azért igaz, mert $0<a^2+ab+b^2<3p$, és $a^2+ab+b^2=2p$ nem lehetséges. (Ebben az esetben ugyanis a és b is páros kellene legyen, viszont $2p$ nem osztható 4-gyel.)

2. Legyen $\varrho = \frac{1}{2}+\frac{\sqrt{3}}{2}i$ az első hatodik komplex egységgyök. Az $x+y\varrho$ (x, y egészek) alakú komplex számokat Euler-egészeknek nevezik. Egyszerű számolással ellenőrizhető, hogy $|x+y\varrho|^2 = x^2+xy+y^2$. A feladat tehát, figyelembe véve az előbbi megjegyzést, olyan $a+b\varrho$ Euler-egész létezésének bizonyítása volt, amelyre $|a+b\varrho|^2=p$, valamint $0<a<b<\sqrt{p}$.

Ismeretes (lásd pl. *Gyarmati–Turán:* Számelmélet, 431–432. old.), hogy ha p $3k+1$ alakú prím, akkor pontosan 12 olyan Euler-egész létezik, amelyek abszolút értékének négyzete éppen p. Ezek közül hat egymásból úgy kapható, hogy egy megfelelő hatodik egységgyökkel megszorozzuk őket, a többi hat pedig ezek konjugáltja. A $0<a<b$ feltétel azzal ekvivalens, hogy a keresett Euler-egész argumentuma (szöge) $0°$ és $30°$ közé esik. Az ilyen egész létezése az előbbiekből következik. Végül a $b<\sqrt{p}$ feltétel is teljesül, mert $b^2<a^2+ab+b^2=p$.