

③ Assume contrary. Then let  $p$  be the smallest <sup>(odd)</sup> prime s.t.

(a)  $p \mid a^2 + 2b^2 = N$  for some  $(a,b) = 1$ , but  $p \nmid x^2 + 2y^2$ , for any  $x,y \in \mathbb{Z}$ .

For this  $p$ , let  $N_0$  be the smallest <sup>positive</sup> integer such that

$$p \mid N_0 \quad \text{and} \quad N_0 = a_0^2 + 2b_0^2 \quad \text{for some} \quad (a_0, b_0) = 1.$$

Claim 1:  $N_0 < p^2$

Proof: Choose  $\alpha, \beta \in \mathbb{Z}$  s.t.  $|\alpha| \leq \frac{p-1}{2} \geq |\beta|$ , and

$$\alpha \equiv a_0 \pmod{p}$$

$$\beta \equiv b_0 \pmod{p}$$

Let  $(\alpha, \beta) = d$ . Then, as checked in the book  $(d, p) = 1$ ;

and  $p \mid \left(\frac{\alpha}{d}\right)^2 + 2\left(\frac{\beta}{d}\right)^2 < p^2$  | the minimality of  $N_0$  proves that  $N_0 < p^2$ .

$$\left(\frac{\alpha}{d}, \frac{\beta}{d}\right) = 1$$

□

Claim 2:  $N_0$  is odd

Proof: If  $2 \mid N_0 = a_0^2 + 2b_0^2$ , then  $2 \mid a_0$ . Let  $a_0 = 2a_1$ ,  $b_0 = b_1$ , then

$$p \mid \frac{N_0}{2} = b_1^2 + 2a_1^2, \quad (a_1, b_1) = 1 \quad (\text{b/c } (a_0, b_0) = 1); \text{ again}$$

minimality of  $N_0$  implies  $\frac{N_0}{2} = N_0$ , a contradiction.

Therefore  $2 \nmid N_0$ .

Now let  $q \mid N_0$ ,  $q \neq p$  (Such a prime divisor  $q$  exists since  $N_0 \neq p$  — and this is b/c of the choice of  $p$ ) Since  $q \mid N_0 < p^2$ ,  $q \neq p$  it follows that  $q < p$ . By minimality of  $p$ ,  $q = x^2 + 2y^2$  for some  $x, y \in \mathbb{Z}$ . Therefore, by problem 2,

③