

### Proof of Lemma

Suppose

$$\frac{n_1(n_1 + 1)}{2} + \frac{n_2(n_2 + 1)}{2} \equiv (l - 6)(24)^{-1} \pmod{l}.$$

Then

$$(2n_1 + 1)^2 + (2n_2 + 1)^2 \equiv (l - 6)3^{-1} + 2 \pmod{l}.$$

If  $l = 12m + 7$  then  $3^{-1} \equiv -4m - 2$  and

$$(l - 6)3^{-1} + 2 \equiv (12m + 1)(-4m - 2) + 2 = -48m^2 - 28m = -4ml \equiv 0 \pmod{l}$$

while if  $l = 12m + 11$  then  $3^{-1} \equiv 4m + 4$  and

$$(l - 6)3^{-1} + 2 \equiv (12m + 5)(4m + 4) + 2 = 48m^2 + 68m + 22 = (4m + 2)l \equiv 0 \pmod{l}.$$

In either case,

$$(2n_1 + 1)^2 + (2n_2 + 1)^2 \equiv 0 \pmod{l}.$$

Since  $l \equiv 3 \pmod{4}$ , we have either  $2n_1 + 1 \equiv 0 \pmod{l}$  or  $2n_2 + 1 \equiv 0 \pmod{l}$ .

Since  $0 \leq n_1, n_2 \leq l - 1$ ,  $1 \leq 2n_1 + 1, 2n_2 + 1 \leq 2l - 1$ , so either  $2n_1 + 1 = l$  or  $2n_2 + 1 = l$ .

So either  $n_1 = \frac{l - 1}{2}$  or  $n_2 = \frac{l - 1}{2}$ .

QED.