Consider the finite field $\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$

For addition ($p \in \mathbb{P}$)

+	0	1	2	3	...	p-2	p-1
0	0	1	2	3	...	p-2	p-1
1	1	2	3	4	...	p-1	0
2	2	3	4	5	...	0	1
3	3	4	5	6	...	1	2
⋮	⋮	⋮	⋮	⋮		⋮	⋮
p-2	p-2	p-1	0	1	...	p-4	p-3
p-1	p-1	0	1	2	...	p-3	p-2

For multiplication ($p = 7$)

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Lemma 1: For $p \in \mathbb{P}$ (the primes) and $s \in \{1, 2, \ldots, p-1\}$ consider the equation $s^2 \equiv -1 \pmod{p}$

1. For $p = 2$, $s = 1$ is the unique soln
2. For $p \equiv 1 \pmod 4$, $\exists$ two solns in $\{1, 2, \ldots, p-1\}$
3. For $p \equiv 3 \pmod 4$, no soln exists

Pf: (3) Suppose $s^2 \equiv -1 \equiv p-1 \pmod p$

Since $p \equiv 3 \pmod 4$, $p = 3 + 4k$, for some $k \in \mathbb{Z}$.

So $s^2 = (3+4k) - 1 = 4k + 2 = 2(2k+1)$

This is impossible, s^2 cannot be 2 times an odd number. ($\not\Rightarrow$) $\Rightarrow s^2 \equiv -1 \pmod p$ has no solution. ▲

(2) Suppose $s^2 \equiv -1 \equiv p-1 \pmod p$

Since $p \equiv 1 \pmod 4$,

$p = 1 + 4k$ for some $k \in \mathbb{Z}$

So $s^2 = (1+4k) - 1 = 4k$

$\Rightarrow s = 2\ell$, where $\ell^2 = k$.

The solutions are $s = \pm 2\ell$ or $s = 2\ell$ and $s = p - 2\ell$

Ex) If $\ell = 3$, $k = 9$, $p = 37$

So for $p = 37$, the two solns are $s = 6$ and $s = 31$.

($s = \pm 2\ell$).

Lemma 2: No integer of the form $n = 4m+3$ $(n \equiv 3 \pmod 4)$ can be written as the sum of two squares: $n \neq i^2 + j^2$ for any $i, j \in \mathbb{Z}$.

Pf: Suppose i is even; so $i = 2k$.

Then $i^2 = 4k^2 \equiv 0 \pmod 4$

Suppose i is odd; so $i = 2k+1$.

Then $i^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$

Similar for j. In any case,

$i^2 + j^2 \not\equiv 3 \pmod 4$.