Thm: $\sqrt{2} \notin \mathbb{Q}$

Pf (contradiction): Suppose $\sqrt{2} \in \mathbb{Q}$, which means that it can be written as $\sqrt{2} = p/q$ where $p, q \in \mathbb{Z}^+$, and p and q have no common divisors. Then $\sqrt{2}\, q = p$ and consider the square

$2q^2 = p^2$. This means $2 \mid p^2 \Rightarrow 2 \mid p$.

So $\exists\, k \in \mathbb{Z}^+$ s.t. $p = 2k \Rightarrow p^2 = 4k^2$

$\Rightarrow \cancel{2}q^2 = \cancel{4}^{2}k^2 \Rightarrow q^2 = 2k^2 \Rightarrow$

$2 \mid q^2 \Rightarrow 2 \mid q$ $(\rightarrow\leftarrow)$.

(✱) **Thm** (Fermat): If $n \in \mathbb{Z}^+$, then $n = k^2 + m^2$ for some $k, m \in \mathbb{Z}^+$ iff every prime factor p of n where $p \equiv 3 \pmod 4$ appears in the factorization of p with an even exponent.

Chapter IV: When can $n \in \mathbb{Z}^+$ be written as the sum of two squares?

$1 = 0^2 + 1^2$
$2 = 1^2 + 1^2$
$3 =$ No
$4 = 0^2 + 2^2$
$5 = 1^2 + 2^2$
$6 =$ No
$7 =$ No
$8 = 2^2 + 2^2$
$9 = 0^2 + 3^2$
$10 = 1^2 + 3^2$
$11 =$ No
$12 =$ No
$13 = 2^2 + 3^2$
$14 =$ No
$15 =$ No
$16 = 0^2 + 4^2$
$17 = 1^2 + 4^2$
$18 = 3^2 + 3^2$
$19 =$ No
$20 = 2^2 + 4^2$
$21 =$ No
$22 =$ No
$23 =$ No
$24 =$ No

Notice that:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
$n \equiv 0 \pmod 4$			$n \equiv 3 \pmod 4$

Twin Primes

Notice that if p is prime then

1. $p = 2$
2. $p \equiv 1 \pmod 4$
3. $p \equiv 3 \pmod 4$

(✱) See left panel.

$n = 3 + 4j$

Lemma 1: For $p \in \mathbb{P}$, consider the congruence equation $s^2 \equiv -1 \pmod{p}$

For $s \in \{1, 2, 3, \ldots, p-1\}$, one of three things is true.

① For $p = 2$, $s = 1$ is the unique soln.

② For $p \equiv 1 \pmod{4}$, $\exists$ exactly two soln's.

③ For $p \equiv 3 \pmod{4}$, $\nexists$ any solution.