1 is not eligible to be prime --
history: Caldwell + Xiong, "What is the smallest prime?"

Euclid's lemma: if p is prime
and $p \mid ab$ then $p \mid a$ or $p \mid b$

non-example: 6 is not prime.
$6 \mid 3 \cdot 4$ but $6 \nmid 3$ and $6 \nmid 4$.

Def: two numbers a, b are relatively prime
or coprime if $\gcd(a, b) = 1$.

example: 6 and 35 are not prime
but they're relatively prime to each other.

key fact: then can write $1 = am + bn$
for some $m, n \in \mathbb{Z}$

Modular Arithmetic

Fix an integer $m > 0$.

Def: $a \equiv b \pmod{m}$ "a is congruent to b modulo m"

means $m \mid b - a$

Example: $76 \equiv 22 \pmod{18}$

one asked: $18 \overline{)\,76}$ (4, remainder 72, 4) remainder is 4, not 22! what gives?

Well, also true that $76 \equiv 4 \pmod{18}$

and $22 \equiv 4 \pmod{18}$

$-14 \equiv 4 \pmod{18}$

congruence mod m is an equivalence relation:

reflexive: $a \equiv a \pmod{m}$

symmetric: if $a \equiv b \pmod{m}$
then $b \equiv a \pmod{m}$

transitive: if $a \equiv b \pmod{m}$
and $b \equiv c \pmod{m}$.
then $a \equiv c \pmod{m}$

↳ proof:

write $b - a = km$
and $c - b = \ell m$.
then $c - a = c - b + b - a$
$= km + \ell m$
$= (k + \ell) m$.

arithmetic is well-defined mod m:

if $a \equiv a' \pmod{m}$
and $b \equiv b' \pmod{m}$
then $a + b \equiv a' + b' \pmod{m}$
and $ab \equiv a'b' \pmod{m}$

pf: write $a - a' = km$ $\quad b - b' = \ell m$

then $(a+b) - (a'+b') = (a - a') + (b - b')$
$= km + \ell m$
$= (k + \ell) m$

and $ab - a'b' = ab - ab' + ab' - a'b'$

$= a(b-b') + (a-a')b'$

$= a \cdot lm + km \cdot b'$

$= (al + kb')m$ ∎

Claim: if N is a square then the last digit of its decimal expansion is $0, 1, 4, 5, 6,$ or 9.

eg. 910987 is not a square.

proof: any $n \equiv$ either $0, 1, 2, 3, 4, 5$, $-4, -3, -2,$ or $-1 \pmod{10}$

$0^2 \equiv 0 \pmod{10}$

$1^2 \equiv 1$ "

$2^2 \equiv 4$ "

$3^2 \equiv 9$ "

$4^2 \equiv 6 \pmod{10}$

$5^2 \equiv 5 \pmod{10}$

$(-4)^2 \equiv 6$ "

$(-3)^2 \equiv 9$ "

$(-2)^2 \equiv 4$ "

$(-1) \equiv 1$ "

So $n^2 \equiv 0, 1, 4, 9, 6,$ or $5. \pmod{10}$

next: if N is a sum of two squares ($N = m^2 + n^2$) then $N \equiv 0, 1,$ or $2 \pmod 4$

why?

$0^2 \equiv 0 \pmod 4$
$1^2 \equiv 1 \pmod 4$
$2^2 \equiv 0 \pmod 4$
$3^2 \equiv 1 \pmod 4$

if $N = m^2 + n^2$ then $N \equiv$ sum of two of those $\pmod 4$

$0, 1,$ or 2, but not 3.

e.g. $910987 \equiv 87 \equiv 3 \pmod 4$

so not a sum of 2 squares.