$a \equiv b \pmod m$ means $m \mid a-b$
m divides $a-b$

if $m=5$
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

$0 \equiv 5 \equiv 10 \equiv 15 \equiv \cdots \bmod 5$
$1 \equiv 6 \equiv 11 \equiv 16 \equiv \cdots \bmod 5$
$2 \equiv 7 \equiv \cdots \bmod 5$
$3 \equiv 8 \equiv \bmod 5$
$4 \equiv \cdots \bmod 5$

Given any m natural number $0,1,2,3,\cdots,m-1$ they are all distinct mod m
$0 \le a, b \le m-1$
if $a \neq b$, say $a<b$
then $0<b-a<m \Rightarrow b-a$ is not divisible by m.
for any a- natural numbers $\Rightarrow$ there is $0 \le b \le m-1$
such that $a \equiv b \pmod 5$
$\Rightarrow$ there are exactly m possible equivalence cases mod m
because we can divide with remainder
given a $\Rightarrow$ divide a by m with remainder

$a = qm + r \Rightarrow a \equiv r \pmod m$
r: remainder, $0 \le r \le m-1$

ex: $263 \equiv 3 \pmod 5$
$263 = 260 + 3 = 52 \cdot 5 + 3$
$0 \le 3 < 4$

Last time: a number is divisible by 9 $\Leftrightarrow$ the sum of its digits is divisible by 9

divisibility by 11 $n = \overline{a_k a_{k-1} \cdots a_0}$
a_i – digits of n
$0 \le a_i \le 9$

Claim: n is divisible by 11 $\Leftrightarrow a_0 - a_1 + a_2 - a_3 + \cdots (-1)^k a_k$ is divisible by 11.
ex: $121 = 11^2$
$1-2+1=0$ divisible by 11
99 is divisible by 11
$20801 : 2-0+8-0+2=11$

$10^0 \equiv 1 \mod 11$

$10 \equiv -1 \mod 11$

$10^2 \equiv (-1)^2 = +1 \mod 11$

$10^3 \equiv (-1)^3 \equiv -1 \mod 11$

...

$10^k \equiv (-1)^k \mod 11$

$n = a_0 + 10^1 a_1 + 10^2 a_2 + \cdots + 10^k a_k$

$237 = 7 + 3 \cdot 10^1 + 2 \cdot 10^2$

$10^k \equiv (-1)^k \mod 11$

$10^k a_k \equiv (-1)^k \mod 11$

$\Rightarrow a_0 + 10a_1 + \cdots + 10^k a_k \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11}$

mod 7

$n = a_0 + a_1 10^1 + \cdots + a_k 10^k$

$10^0 \equiv 1 \mod 7$

$10^1 \equiv 3 \mod 7$

$10^2 \equiv 3 \cdot 3 = 9 \equiv 2 \mod 7$

$10^3 \equiv 3 \cdot 2 = 6 \mod 7 \equiv -1 \mod 7$

$10^4 \equiv (-1) \cdot 3 \equiv -3 \mod 7$

$10^5 \equiv 4 \cdot 3 = 12 \equiv 5 \mod 7$

$10^6 \equiv 5 \cdot 3 = 15 \equiv 1 \mod 7$

$10^{6k} \equiv 1 \mod 7$

$10^{6k+1} \equiv 3 \mod 7$

$10^{6k+2} \equiv 2 \mod 7$

$10^{6k+3} \equiv -1 \mod 7$

$10^{6k+4} \equiv -3 \mod 7$

$10^{6k+5} \equiv -2 \mod 7$

$n = a_0 + 10^1 a_1 + 10^2 a_2 + 10^3 a_3 + \cdots$

$\equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 \cdots \mod 7$

We proved by induction that

$n^3 + 5n$ is divisible by 3 for any n.

Different proof using modular arithmetic

Look at $n \mod 3$: 0, 1, 2 are all possible values

$n \equiv 0 \mod 3$ or i.e. n is divisible by 3 $\Rightarrow n^3 + 5n$ is also divisible by 3

or

$n \equiv 1 \mod 3$

$n^3 \equiv 1^3 \mod 3$

$n^3 \equiv 1 \mod 3$

$5n \equiv 5 \cdot 1 = 5 \mod 3$

$n^3 + 5n \equiv 1 + 5 = 6 \equiv 0 \mod 3$

or

$n \equiv -1 \mod 3$

$n^3 \equiv (-1)^3 = -1 \mod 3$

$5n \equiv -5 \mod 3$

$n^3 + 5n \equiv -1 + (-5)$

$\equiv -6$

$\equiv 0 \mod 3$

Ex:

Prove that 10003 can not be written as $a^2 + b^2$ where a, b are natural numbers.

Hint: consider numbers mod 4

If a is an integer what values can $a^2 \mod 4$ take?

All possible numbers mod 4 are 0, 1, 2, 3

$a \equiv 0 \mod 4 \Rightarrow a^2 \equiv 0^2 \equiv 0 \mod 4$

1	$1 \equiv 1 \mod 4$
2	$4 \equiv 0 \mod 4$
3	$9 \equiv 1 \mod 4$

For any $a \Rightarrow a^2 \equiv 0$ or $1 \bmod 4$

a^2+b^2 can be $0+0=0$
a, b any integers $0+1=1$
$1+0=1$
$1+1=2$

a^2+b^2 can only be $0, 1, 2$ or 4
but cannot be $3 \bmod 4$.

$10,003 = 10000+3 \equiv 3 \bmod 4$
↳ divisible by 4
$\Rightarrow$ cannot write it as a^2+b^2