Is any one interested in the last digit of $(1357)^{200}$?

O.K.

Last digit of 1357 ?

7

what is 1357 mod 10 ?

$1357 = 1000 + 300 + 50 + 7$

$\equiv 0 + 0 + 0 + 7 \mod$

$\equiv 7.$

Last digit of a number = number mod 10.

Last digit of $(1357)^{200}$

$= (1357)^{200} \mod 10$

$\equiv (7)^{200} = (7^4)^{50} \equiv 1^{50} \equiv 1 \mod 10$

$\equiv$

7

$7^2 \equiv 9 \mod 10$

$7^3 \equiv 3 \mod 10$

$7^4 \equiv 1 \mod 10$

Yesterday:

- If $\gcd(m, n) = 1$ then we can find $n^{-1} \bmod m$.

Exercise: Convince yourself that if $\gcd(m, n) \neq 1$ then n has no inverse mod m. (i.e. There is no a such that $na \equiv 1 \bmod m$)

Problem

Solve $3x \equiv 13 \bmod 26$

$x \equiv 3^{-1} \cdot 13 \bmod 26$

$x \equiv 9 \cdot 13 \bmod 26$

$x \equiv 13 \bmod 26$

Problem

Solve $4x \equiv 12 \bmod 26$

~~$x \equiv 4^{-1} \cdot 12 \bmod 26$~~

One solution is

$x \equiv 3 \bmod 26$

Another solution is

$$x \equiv 16 \mod 26$$

(Check:

$$4 \cdot 16 = 4 \cdot (3+13)$$
$$\equiv 12 + 0$$
$$\equiv 12 \mod 26$$)

Exercise: Convince yourselves that $x \equiv 3$ and $x \equiv 16$ are the only solutions to $4x \equiv 12 \mod 26$.

Chinese Remainder Theorem

Find the smallest integer x that simultaneously satisfied

$$x \equiv 3 \mod 13$$
$$x \equiv 6 \mod 14$$
$$x \equiv 9 \mod 15$$

Soln

Let $a \equiv 14^{-1} \mod 13$

$b \equiv 15^{-1} \mod 13$

First attempt at a solution:

Take

$$X = 3(14)a(15)b$$

Note:

$x \equiv 3 \pmod{13}$

$x \equiv 0 \pmod{14}$

$x \equiv 0 \pmod{15}$

Now let

$c = 13^{-1} \pmod{14}$

$d = 15^{-1} \pmod{14}$

Take

$y = 6(13)c(15)d$

Note:

$y \equiv 0 \pmod{13}$

$y \equiv 6 \pmod{14}$

$y \equiv 0 \pmod{15}$

Now let

$e = 13^{-1} \mod 15$

$f = 14^{-1} \mod 15$

Take

$Z = 9\,(13)\,e\,(14)\,f$

Note:

$Z \equiv 0 \mod 13$

$Z \equiv 0 \mod 14$

$Z \equiv 9 \mod 15$

Now

Take

$x = X + Y + Z$

note

$x \equiv X+Y+Z = 3+0+0 \equiv 3 \pmod{13}$

$x \equiv X+Y+Z = 0+6+0 \equiv 6 \pmod{14}$

$x \equiv X+Y+Z = 0+0+9 \equiv 9 \pmod{15}$

So

x is a simultaneous solution.

$$x = X+Y+Z$$

$$= 3(14)a(15)b + 6(13)c(15)d + 9(13)e(14)f$$

where

$a = 14^{-1} \pmod{13}$

$\boxed{a = 1}$

Is any one interested in the last digit of $(1357)^{200}$?

O.K.

Last digit of 1357 ?

7

what is 1357 mod 10 ?

$1357 = 1000 + 300 + 50 + 7$

$\equiv 0 + 0 + 0 + 7 \mod$

$\equiv 7.$

Last digit of a number = number mod 10.

Last digit of $(1357)^{200}$

$= (1357)^{200} \mod 10$

$\equiv (7)^{200} = (7^4)^{50} \equiv 1^{50} \equiv 1 \mod 10$

$\equiv$

7

$7^2 \equiv 9 \mod 10$

$7^3 \equiv 3 \mod 10$

$7^4 \equiv 1 \mod 10$

Yesterday:

- If $\gcd(m, n) = 1$ then we can find $n^{-1} \bmod m$.

Exercise: Convince yourself that if $\gcd(m, n) \neq 1$ then n has no inverse mod m. (i.e. There is no a such that $na \equiv 1 \bmod m$)

Problem

Solve $3x \equiv 13 \bmod 26$

$x \equiv 3^{-1} \cdot 13 \bmod 26$

$x \equiv 9 \cdot 13 \bmod 26$

$x \equiv 13 \bmod 26$

Problem

Solve $4x \equiv 12 \bmod 26$

~~$x \equiv 4^{-1} \cdot 12 \bmod 26$~~

One solution is

$x \equiv 3 \bmod 26$

Another solution is

$$x \equiv 16 \mod 26$$

(Check:

$$4 \cdot 16 = 4 \cdot (3+13)$$
$$\equiv 12 + 0$$
$$\equiv 12 \mod 26$$)

Exercise: Convince yourselves that $x \equiv 3$ and $x \equiv 16$ are the only solutions to $4x \equiv 12 \mod 26$.

Chinese Remainder Theorem

Find the smallest integer x that simultaneously satisfied

$$x \equiv 3 \mod 13$$
$$x \equiv 6 \mod 14$$
$$x \equiv 9 \mod 15$$

Soln

Let $a \equiv 14^{-1} \mod 13$

$b \equiv 15^{-1} \mod 13$

First attempt at a solution:

Take

$$X = 3(14)a(15)b$$

Note:

$x \equiv 3 \pmod{13}$

$x \equiv 0 \pmod{14}$

$x \equiv 0 \pmod{15}$

Now let

$c = 13^{-1} \pmod{14}$

$d = 15^{-1} \pmod{14}$

Take

$y = 6(13)c(15)d$

Note:

$y \equiv 0 \pmod{13}$

$y \equiv 6 \pmod{14}$

$y \equiv 0 \pmod{15}$

Now let

$e = 13^{-1} \mod 15$

$f = 14^{-1} \mod 15$

Take

$Z = 9\,(13)\,e\,(14)\,f$

Note:

$Z \equiv 0 \mod 13$

$Z \equiv 0 \mod 14$

$Z \equiv 9 \mod 15$

Now

Take

$x = X + Y + Z$

note

$x \equiv X+Y+Z = 3+0+0 \equiv 3 \pmod{13}$

$x \equiv X+Y+Z = 0+6+0 \equiv 6 \pmod{14}$

$x \equiv X+Y+Z = 0+0+9 \equiv 9 \pmod{15}$

So

x is a simultaneous solution.

$$x = X+Y+Z$$

$$= 3(14)a(15)b + 6(13)c(15)d + 9(13)e(14)f$$

where

$a = 14^{-1} \pmod{13}$

$\boxed{a = 1}$

$b = 15^{-1} \equiv 2^{-1} \equiv 7 \pmod{13}$

$\boxed{b = 7}$

$c = 13^{-1} \equiv (-1)^{-1} \equiv (-1) = 13 \pmod{14}$

$\boxed{c = 13}$

$d = 15^{-1} = 1^{-1} = 1 \pmod{14}$

$\boxed{d = 1}$

etc. for e, f.