Lecture 12

Tuesday, September 29, 2020 12:05 PM

Lecture 12: SOLVING PROBLEMS USING MODULO n

Problem 1. Find the last digit of $(89134753)^{10262020}$

the last digit of a number is the same as the remainder of dividing by 10

altern. mod 2 & mod 5

$(89134753)^{10262020} \equiv 1 \bmod 5$ $a^q \equiv a$, $a^{q-1} \equiv 1$ if $a \not\equiv 0$, $q = 5$

Soln: What we want $(89134753)^{10262020} \overset{?}{\equiv}$ modulo 10.

Since modulo 10 we have $89134753 \equiv 3 \bmod 10$. we have $(89134753)^{10262020} \equiv 3^{10262020} \bmod 10$.

what are powers of 3 mod 10 ?

$3^1 \equiv 3 \bmod 10$, $3^2 = 9 \equiv 9 \equiv -1$, $3^3 = 27 \equiv 7 \equiv -3$, $3^4 = 81 \equiv 1$, $3^5 \equiv 3 \bmod 10$ ($\times 3$ at each step)

→ pattern is $3, -1, -3, 1$ and repeat with period 4

$\Rightarrow 3^{10262020}$ must end in 3, 9, 7 or 1 $\longrightarrow 3^{10262020}$ must end in 1, because $3^{4 \cdot k} \equiv (3^4)^k \equiv 1^k \equiv 1 \bmod 10$.

4 divides 10262020

∎

Problem 2. Show $\nexists\, x, y, z \in \mathbb{Z}$ s.t. $x^2 + y^2 - 21z^2 = 0$. → smells of mod 3, 7 or 21.

↳ gcd(x,y) = 1 assume.

Sol^n: Let's try modulo 3: the equation reduces to $x^2 + y^2 - \underbrace{21}_{\equiv 0} z^2 \equiv 0 \bmod 3$, so we have

$$\boxed{\underbrace{x^2}_{0 \text{ or } 1} + \underbrace{y^2}_{0 \text{ or } 1} \equiv 0 \bmod 3}.$$

Now a square x^2 modulo 3 can be only 0 or 1 (but not 2).

$0 \to 0^2 \equiv 0$

$1 \to 1^2 \equiv 1$ mod 3

$2 \to 2^2 \equiv 1$

↳ 2 does not appear as a square!

Alternatively, Fermat's little thm say $x^2 \equiv 1$ if $x \not\equiv 0 \bmod 3$.

(1) if $x^2 + y^2 \equiv 0 \bmod 3$, with $\left.\begin{array}{l} x \equiv 0 \\ y \equiv 0 \end{array}\right\} \Rightarrow$ gcd(x,y) would not 1 bc $3 \mid x$, $3 \mid y$

(2) Else $x^2 \equiv 1$, $y^2 \equiv 0$, then $x^2 + y^2 \equiv 1$ not 0. NOT POSSIBLE

(3) Else $x^2 \equiv 1$, $y^2 \equiv 1$, then $x^2 + y^2 \equiv 2 \bmod 3$, not 0. NOT POSSIBLE!

Problem 3. Show $\nexists\, x, y \in \mathbb{Z}$ s.t. $x^3 + 117y^3 = 5$ → what modulo n should we use?

Sol^n: Let's try modulo 9: then $117 \equiv 0 \bmod 9$. So $x^3 + 117y^3 \equiv 5 \bmod 9$ is the same as $x^3 \equiv 5 \bmod 9$. So the question is: which cubes x^3 are allowed mod 9?

mod 9

$0^3 \equiv 0$

$1^3 \equiv 1$

$2^3 \equiv 8 \equiv -1$

$3^3 \equiv 0$

$4^3 \equiv 1$

$5^3 \equiv (-4)^3 \equiv -1$

$6^3 \equiv (-3)^3 \equiv 0$

$7^3 \equiv (-2)^3 \equiv 1$

$8^3 \equiv (-1)^3 \equiv -1$

$\Rightarrow$ cubes mod 9 must be $0, \pm 1$ $\overset{\text{never } 5}{\Longrightarrow}$ $x^3 \equiv 5 \bmod 9$ has no solution $\Rightarrow x^3 + 117y^3 \equiv 5 \bmod 9$ has no solution

$\Rightarrow x^3 + 117y^3 = 5$ has no solution.

∎

Problem 4. Show that 11 divides $n^{11} - n^{10} + 22n^5 - 242n^3 - 34n + 122$, $\forall n \in \mathbb{N}$.

$11 \nmid n$.

Sol^n: Here we want $n^{11} - n^{10} + 22n^5 - 242n^3 - 34n + 122 \overset{?}{\equiv} 0 \bmod 11$. (#)

Let's simplify: use $n^{11} \equiv n \bmod 11$ and $n^{10} \equiv 1 \bmod 11$.

simplify

$$\underbrace{n^{11}}_{\equiv\, n} - \underbrace{n^{10}}_{\equiv\, 1} + \underbrace{22}_{\equiv\, 0} n^5 - \underbrace{242}_{\equiv\, 0} n^3 - \underbrace{34}_{\equiv\, 1} n + \underbrace{122}_{\equiv\, 1} \overset{?}{\equiv} 0 \bmod 11.$$

$$n - 1 + 0 - 0 - n + 1 \equiv 0 \bmod 11$$

!

$\Leftrightarrow (n-1) - (n-1) \equiv 0 \bmod 11$ this is true! $\Rightarrow$ (#) holds

∎