Lecture 11

Tuesday, September 29, 2020 12:05 PM

Lecture 11 : Fermat's Little Theorem ← Sec. 6.3 & 6.4.

$\boxed{\text{Modular arithmetic}}$ is an incredibly useful tool. For us, it will solve :

(1) Divisibility problems : Does 521 divide $n^{521}-n$ for any $n \in \mathbb{N}$?
→ computing mod 521, $n=521$

(2) Questions about large numbers : What is the last digit of $(1739)^{980145}$?
→ computing mod 10, $n=10$

(3) Non-Existence of Solutions to Diophantine equations : does $\boxed{x^2-3y^2=15}$ have a sol^n with $x,y\in\mathbb{Z}$? ⇝ mod 3, mod 5 or mod 15

§ 1. Modular arithmetic is ARITHMETIC

→ we can + and we can multiply } modulo n

$\equiv$ means $\sim_n$

Prop. 6.25 : Let $n \in \mathbb{N}$. Suppose $a \equiv a' \mod n$, and $b \equiv b' \mod n$. Then

$$a+b \equiv a'+b' \mod n\ , \quad a\cdot b \equiv a'\cdot b' \mod n \quad \blacksquare$$

we can sum ← independent of representative → we can multiply

(we can substract) (division is very tricky)

E.g. $n=16$, $a=7$, $a'=23$ then $a \equiv a' \mod 16$.
$b=2$, $b'=18$, then $b \equiv b' \mod 16$

$$\underbrace{a+b}_{9} \equiv \underbrace{a'+b'}_{41} \mod 16$$

Slogan : " $\equiv 0 \mod n$ means " being a multiple of n, i.e. divisible by n

Example : $49\cdot 598 \equiv ? \mod 5$, answer is 2 (or -3)

Since $49 \equiv 4 \mod 5$, $598 \equiv 3 \mod 5$, so by Prop. $49\cdot598 \equiv 4\cdot 3 \equiv 12 \mod 5$ and $12 \equiv 2 \mod 5$. (Alternative: $49 \equiv -1$, $598 \equiv -2$, so $49\cdot 598 \equiv (-1)(-2) \equiv 2 \mod 5$.)

§ 2. Powers modulo a prime : let p be a prime, LiFE modulo is quite amazing !

Lemma : (Freshman's dream) Let $a,b\in\mathbb{Z}$ and $p \in \mathbb{N}$ a prime.
Then $(a+b)^p \equiv a^p + b^p \mod p$ $\blacksquare$

Proof : By Binomial Thm,

$\binom{p}{0}=1$, $\binom{p}{1}=p \equiv 0 \mod p$, $\binom{p}{2} = \frac{p(p-1)}{2} \equiv 0 \mod p$, ..., $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, $\binom{p}{p}=1$; $p! = p(p-1)! \equiv 0 \mod p$

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = \binom{p}{0} b^p + \binom{p}{1} b^{p-1} a + \dots + \binom{p}{p-1} b a^{p-1} + \binom{p}{p} a^p =$$

$$\equiv a^p + b^p.$$

← implies that mod p the orange terms vanish

$0 \mod p$ bc $p \mid \binom{p}{k}$ if $k=1\dots p-1$

Thm 6.35 : (Little Fermat's theorem) ← p powers modulo p are easy !

Let $p \in \mathbb{N}$ be a prime and $a \in \mathbb{Z}$ an integer.

$$\boxed{a^p \equiv a \mod p} \quad \blacksquare$$

Exercise : Prove this w/ Lemma (hint: by induction on $a \in \mathbb{N}$.)

Application : $p=521$, then $\forall a \in \mathbb{Z}$, $a^{521} \equiv a \mod 521$.

Now this means $a^{521} - a \equiv 0 \mod 521$ ⟶ 521 divides $a^{521}-a$, $\forall a \in \mathbb{Z}$.
↪ Yey ! (see first slide)