Fermat Theorem

Monday, September 29, 2025 9:25 AM

Missing
100 # 2, 7
200 # 6, 7, 11, 24, 27
500 # 2, ~~3, 8, 9, 11~~, 19, 26, 29

Recall : Modular Arithmetic

1] Fermat Little Theorem (§ 2.5 Stallings)

if p is prime and a is co-prime to p then

$$a^{p-1} \equiv 1 \pmod{p}$$

2] e.g. ① $2^4 \equiv 1 \pmod 5$

② $2^5 \equiv 2^4 \cdot 2 = 2 \pmod 5$

③ $27^{15} \equiv (2^4)^3 \cdot 2^3 \pmod 5$

$\equiv 1^3 \cdot 2^3$

mod 4

$\equiv 2^3 \equiv 8 \equiv 3 \pmod 5$

mod 5

3] Exer

① $1234^{512} \pmod{11}$

Soln. $\equiv (2^{10})^{51} \cdot 2^2 \pmod{11}$

mod 10

mod 11

$\equiv 2 \equiv 4 \pmod{11}$

② $7654^{123} \pmod{11}$

$\equiv (-2)^3 \equiv -8 \equiv 3 \pmod{11}$

③ $16^{50} \pmod 7$

5.1^n

$= 2^1$

$3498^{25} \pmod 7$

$\equiv (-2)^1 \equiv 5$

④ $26^{3598} \pmod 7$

$-2 \xrightarrow{\text{mod } 6} 4$

$(-2) \equiv (-2)^4 \equiv 2 \pmod 7$

⑤ $4809^{12345} \pmod{11}$

$2345^{1273} \pmod{11}$ 5

6] What if the mod n is not prime?

e.g.

① $3^{13} \pmod{10}$

$\equiv 3^4 \equiv 81 \equiv 1 \pmod{10}$

Group Theory

1] Def^n.

Let $*$ be a binary operation. Then $*$ is said to be on a set A if $*$ is a function from $A \times A$ to A

$$* : A \times A \longrightarrow A$$

Here, A is said to be closed under the $*$ operation

2] **[2] Definition.** A **group** $(G, \cdot)$ is a nonempty set G together with a binary operation $\cdot$ on G such that the following conditions hold:

(i) *Closure:* For all $a, b \in G$ the element $a \cdot b$ is a uniquely defined element of G

(ii) *Associativity:* For all $a, b, c \in G$, we have

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) *Identity:* There exists an *identity element* $e \in G$ such that for all $a \in G$

$$e \cdot a = a \quad \text{and} \quad a \cdot e = a$$

(iv) *Inverses:* For each $a \in G$ there exists an *inverse* element $a^{-1} \in G$ such that

$$a \cdot a^{-1} = e \quad \text{and} \quad a^{-1} \cdot a = e$$

3] e.g.

① $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ is the multiplicative group modulo 5.

$e = 1$

a	1	2	3	4
a^{-1}	1	3	2	4

② $(\mathbb{Z}_{10}, +)$ is the additive group modulo 10

$e = 0$

a	0	1	2	.....	9
$a^{-1}=-a$	0	9	8	.....	1

③ $(\mathbb{Z}_{10}^{*}, \cdot)$ is the multiplicative group modulo 10

$e = 1$

a	1	3	7	9
a^{-1}	1	7	3	9

4] Notations:

① Juxtaposition: write ab for $a \cdot b$

② Power (superscript): $a^n = \underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{n\text{-times}}$, $a^0 = e$

③ negative power: $a^{-n} = (a^{-1})^n$

④ Note: avoid juxtaposition and power notations if the operation of the group denoted additively.

$+$, $\oplus$

For $3+3+3+3$, avoid 3^4,
write $4(3)$

for $a \oplus b$, avoid ab

Avoid the notation if it causes confusion.

5] Prop. (cancellation Property)

Let G be a group and $a, b, c \in G$.

① if $ab = ac$ then $b = c$.

② if $ac = bc$ then $a = b$

Proof : ① $ab = ac$

$\Rightarrow \quad \bar{a}^{1}(ab) = \bar{a}^{1}(ac)$ multiplying both sides by $\bar{a}^{1}$

$\Rightarrow \quad (\bar{a}^{1}a)b = (\bar{a}^{1}a)c$ by associativity.

$\Rightarrow \quad e\,b = e\,c$ by inverse law

$\Rightarrow \quad b = c$ by identity