

Chpt 9.

Fermat's little theorem:

p prime, $a \not\equiv 0 \pmod{p}$

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

We're first going to make an observation:

$a \not\equiv 0 \pmod{p}$, then

$$\{a, 2a, 3a, \dots, (p-1)a\} = \\ = \{1, 2, 3, \dots, (p-1)\} \pmod{p}$$

maybe reordered is all

check this for $a \equiv 5 \pmod{7}$

i.e

$$\text{look at } \{5 \cdot 1, 5 \cdot 2, 5 \cdot 3, \dots, 5 \cdot 6\} \pmod{7}$$

$$= \{5, 3, 1, 6, 4, 2\}$$

$$= \{1, 2, 3, 4, 5, 6\}$$

look at $a \equiv 3 \pmod{7}$

$$\{3 \cdot 1, 3 \cdot 2, \dots, 3 \cdot 6\} \pmod{7}$$

$$= \{3, 6, 2, 5, 1, 4\} \pmod{7}$$

Proof of the observation:

We only need to show that
all the numbers in
 $\{a \cdot 1, \dots, a \cdot (p-1)\}$ are

distinct, since then the size of the
set is $p-1$, so it must have all
 $1 \dots p-1$ numbers mod p .

So suppose

$$ab_i \equiv ab_j \pmod{p}$$

$$\Rightarrow ab_i - ab_j \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid ab_i - ab_j$$

$$\Rightarrow p \mid a(b_i - b_j)$$

but $p \nmid a$ and $-(p-1) \leq b_i - b_j \leq p-1$

so $p \nmid b_i - b_j$ unless $b_i - b_j = 0$

$$\therefore b_i = b_j$$

so $ab_i \equiv ab_j \pmod{p} \Rightarrow b_i = b_j$, so

all the ab_i 's are distinct. ✓

so now this means that

$$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot \dots \cdot a \cdot (p-1)$$

$$\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

$$\Rightarrow a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

but $\gcd(1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1), p) = 1$, so can cancel it.

Thus

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

eg

$$11^{306} \equiv ? \pmod{7}$$

$$4^{306} \equiv ? \pmod{7}$$

$$(4^6)^{51} \equiv ? \pmod{7}$$
$$1^{51} \equiv ? \pmod{7}$$

$$\text{Thus } 11^{306} \equiv 1 \pmod{7}.$$

$$\gcd(a, p) = 1$$

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

our $p=7$
 $p-1=6$

$$4^6 \equiv 1 \pmod{7}$$

$$\frac{51}{6}$$

306

eg
find $3 = X^{641} \pmod{7}$ if $\gcd(x, 7) = 1$



$$\begin{array}{r} 106 \\ 6 \overline{) 641} \\ \underline{36} \\ 5 \end{array}$$

$$X^{6 \cdot 106 + 5} \pmod{7}$$

so $641 = 6 \cdot 106 + 5$

$$(X^{6 \cdot 106})^5 \pmod{7} = 1^5 \cdot X^5 \pmod{7} = X^5 \pmod{7}$$

$$X^5 = 3 \pmod{7}$$

$$\begin{aligned} &= (2 \cdot 3)^5 \\ &= 2^5 \cdot 3^5 \\ &= 4 \cdot 5 \\ &= 20 \\ &= 6 \end{aligned}$$

$$\begin{aligned} 5^{10} &= 2 \\ 6+4 &= 2 \\ 2^6 \cdot 2^4 &= 2^4 = 16 = 2 \end{aligned}$$

$$\begin{array}{cccccc} 5 & 5 & 5 & 5 & 5 & \\ 1 & 2 & 3 & 4 & 5 & 6 \\ & & 3^2=9=2 & \parallel & \parallel & \\ 1 & 4 & \downarrow & 2 & 3 & 6 \\ & & 5 & & & \end{array}$$

$$3^5 = 3 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3$$

$$\begin{aligned} 5^2 &= 4 \\ 5^5 &= 5^2 \cdot 5^2 \cdot 5 \\ &= 4 \cdot 4 \cdot 5 \\ &= 16 \cdot 5 \\ 2 \cdot 5 &= 10 = 3 \end{aligned}$$

Chpt 10.