$$ax + by \equiv r \pmod{n} \quad (1)$$

$$cx + dy \equiv \delta \pmod{n} \quad (2)$$

from (1), $ax + by = r + kn$

from (2), $cx + dy = \delta + qn$

(1) $\times\, d$ & (2) $\times\, -b$

$$adx + \cancel{bdy} = rd + kdn \quad (3)$$

$$-bcx - \cancel{bdy} = -b\delta - bqn \quad (4)$$

$$(ad - bc)x = rd - b\delta + (kd - bq)n$$

n%

$$(ad - bc)x \equiv (rd - b\delta) \pmod{n}$$

$$\boxed{\gcd(ad - bc, n) = 1}$$

a) $5x + 3y \equiv 1 \pmod{7}$ (1)

$3x + 2y \equiv 4 \pmod{7}$ (2)

$$(10 - 9)x \equiv -10 \pmod{7}$$

$$x \equiv -10 \pmod{7}$$

$$x \equiv 4 \pmod{7}$$

from (1)

$$20+5y \equiv 1 \pmod{7}$$

$$3y \equiv -19 \pmod{7}$$

$$3y \equiv 2 \pmod{7}$$

$$\boxed{y \equiv 3 \pmod{7}}$$ #

b) $7x+3y \equiv 6 \pmod{11}$

$4x+2y \equiv 9 \pmod{11}$

$x \equiv 9 \pmod{11}$

$y \equiv 3 \pmod{11}$

Modular exponentiation

(b) $11^{644} \bmod 645$

$644 = [1010000100] = a$

$x = 1;$

$Power = 11 \bmod 645 = 11;$

$\boxed{i=0}$

$a(i) = 0$

$Power = (11)^2 \bmod 645 = 121$

$\boxed{i=1}$

$a(i) = 0, \quad Power = (121)^2 \bmod 645 = 451$

$\boxed{i=2}$

$a(i) = 1$

$x = 1 \cdot 451 \bmod 645 = 451$

$Power = (451)^2 \bmod 645 = 226$

$\boxed{i=3}$

$a(i) = 0$

$Power = (226)^2 \bmod 645 = 121$

$\boxed{i=4}$

$a(4) = 0$

$Power = (121)^2 \bmod 645 = 451$

$\boxed{i=5}$

$a(5) = 0, \quad Power = (451)^2 \bmod 645 = 226$

$\boxed{i=6}$

$a(6)=0$

$Power=(226)^2 \bmod 645=121$

$\boxed{i=7}$

$a(i)=1$

$x=(451)(121) \bmod 645=391$

$Power=(121)^2 \bmod 645=451$

$\boxed{i=8}$ $a(i)=0$

$Power=(451)^2 \bmod 645=226$

$\boxed{i=9}$ $a(i)=1$

$x=(391)(226) \bmod 645=\underline{1}$

Fermat's little theorem

Theorem

- p is prime
- $p \nmid a$

$\left.\begin{matrix} \\ \\ \end{matrix}\right\} \therefore a^{p-1} \equiv 1 \pmod{p}$

- Corollary.
- p is pime, $\forall a \in \mathbb{Z}$

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

$\boxed{2}$ Verify that 17 divides $11^{104}+1$

Sol

Find $(11^{104}+1) \bmod 17$

. prove $11^{104}+1 \equiv 0 \pmod{17}$

$11^{104} \equiv ?? \pmod{17}$

$P=17,\ a=11$

$\Rightarrow (11^{16})^{6} \equiv 1^{6} \pmod{17}$

$11^{96} \equiv 1 \pmod{17}$ ①

$11^{2} \equiv 2 \pmod{17}$

$11^{8} \equiv 16 \pmod{17}$ ②

① * ②

$11^{104} \equiv 16 \pmod{17}$

$11^{104} + 1 \equiv 17 \pmod{17}$

$11^{104} + 1 \quad 0 \pmod{17}$

$17 \mid (11^{104} + 1)$.

(4) Derive.

a) $a^{21} \equiv a \pmod{15}, \forall a$

$15 = \boxed{3 \cdot 5}$

- $a^5 \equiv a \pmod 5$ ①
- $a^3 \equiv a \pmod 3$ ②

$\Rightarrow a \mid n,\ b \mid n,\ \gcd(a,b) = 1$

$\longrightarrow ab \mid n$

② $* a^2$

$a^5 \equiv a^3 \pmod{3}$ ③

from ② & ③ by transitivity

$a^5 \equiv a \pmod{3}$ ④

from ① & ④

$a^5 \equiv a \pmod{15}$ ⑤

from ⑤

$(a^5)^4 \equiv a^4 \pmod{15}$

$a^{20} \equiv a^4 \pmod{15}$

$a^{21} \equiv a^5 \pmod{15}$ ⑥

by trans..ivity from ⑤ & ⑥

$a^{21} \equiv a \pmod{15}$

$\cdot\ a^7 \equiv a \pmod{42}, \forall a$

x^2-1

$2*3*7$

$a^2 \equiv a \pmod 2$ (1)

$a^3 \equiv a \pmod 3$ (2)

$a^7 \equiv a \pmod 7$ (3)

$a^2 \equiv a \pmod 2$ (1)

$a^3 \equiv a^2 \pmod 2$

by transitivity

$a^3 \equiv a \pmod 2$

$\vdots$

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

$a^3 \equiv a \pmod 3$

$a^5 \equiv a^3 \pmod 3$

by transitivity

$a^5 \equiv a \pmod 3$

$a^7 \equiv a \pmod 3$ (5)

from 3, 4 & 5

$\therefore\ a^7 \equiv a \pmod{42}$.

⑤ $7^{121} \bmod 13$

$a = 7$, $p = 13$

$\boxed{p \nmid a, \ 13 \nmid 7}$

$7^{12} \equiv 1 \pmod{13}$

$7^{120} \equiv 1^{10} \pmod{13}$

$7^{121} \equiv 7 \pmod{13}$

$\boxed{7}$

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

$a \cdot a^{p-2} \equiv 1 \pmod{p}$

a^{p-2} is a multiplicative Inverse for $a \pmod{p}$.

Find an inverse of 5 modulo 41

a p prime

$$5^{40} \equiv 1 \pmod{41}$$

& $p \nmid a$

$$5 \cdot 5^{39} \equiv 1 \pmod{41}$$

5^{39} is an multiplicative Inverse modulo 41.

1. $7^{12} \equiv 1 \pmod{13}$

2. $7^{12} \equiv 1 \pmod{13}$

10. $7^{12} \equiv 1 \pmod{13}$