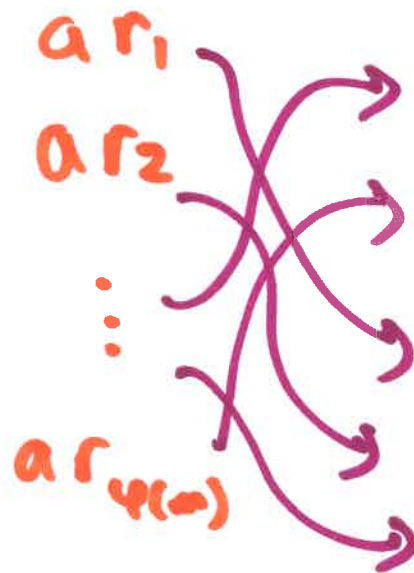


Proof idea:

Let $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ be the set of M.I.s of $\mathbb{Z}_m$. B/c $\gcd(a, m) = 1$, a^{-1} exists in $\mathbb{Z}_m$. If $x, y \in \mathbb{Z}_m$ have M.I.s, then so does $x \cdot y$.

r_1
 r_2
 $\vdots$
 $r_{\varphi(m)}$

mult.
 $\xrightarrow{a}$



Multiplication
by a permutation
(or shuffles) the
M.I.s

(77)

$$(ar_1)(ar_2)\dots(ar_{\varphi(m)}) = a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)}$$

(permute) |||

$$r_1 r_2 \dots r_{\varphi(m)}$$

Thus,

$$r_1 r_2 \dots r_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \pmod{m}$$

$$1 \equiv a^{\varphi(m)} \pmod{m}$$

as needed.

Ex: Find the last two digits of 3^{176} .

$$\frac{3^{176}}{a} \pmod{\frac{100}{m}}$$

We know $\gcd(3, 100) = 1$. We need

$$\begin{aligned}\phi(100) &= \phi(4 \cdot 25) \\ &= \phi(4) \cdot \phi(25) \\ &= \phi(2^2) \cdot \phi(5^2) \\ &= 2^{2-1}(2-1) \cdot 5^{2-1}(5-1) \\ &= 2 \cdot 1 \cdot 5 \cdot 4 = 40.\end{aligned}$$

ETT:

$$3^{40} \equiv 1 \pmod{100}$$

$$176 = 4 \cdot 40 + 16$$

$$3^{176} = 3^{4 \cdot 40 + 16} = (3^{40})^4 \cdot 3^{16} \equiv 3^{16} \pmod{100}$$

(79)

$$3^{176} \equiv 3^{16} \pmod{100}$$

Do the actual arithmetic:

$$3^4 = 81$$

$$3^8 = 81^2 = 6561 \equiv 61 \pmod{100}$$

$$3^{16} = (3^8)^2 \equiv 61^2 = 3721 \equiv 21 \pmod{100}$$

Thus,

$$3^{176} \equiv 21 \pmod{100}.$$

Saw modular arith. used in check sums.

One of its main uses today is cryptography

Mod. crypt.

① RSA

② Elliptic curve crypt.

$$y^2 = x^3 + ax + b$$

Crypt. is the study of keeping secrets.

The original text is plaintext. After encrypt the text is transformed into ciphertext. Decryption reverses this process.

The function that transform plaintext into ciphertext is the encipher (function).
The functions that transforms ciphertext into plaintext is the decipher (function).

We will cover affine ciphers.

Assume

$$A=1, B=2, \dots, Y=25, Z=26 \equiv 0 \quad (26)$$

All chars are elements of $\mathbb{Z}_{26}$.

Affine encipher:

$$f_E(x) = ax + b \quad (26)$$

Because we want to decipher text, we need to undo f_E . In other words, we want f_D such that

$$f_D(f_E(x)) = x.$$

Forget $\mathbb{Z}_{26}$:

$$f_D(x) = cx + d.$$

$$c = a^{-1}$$

$$c(ax+b) + d = x$$

$$acx + (bc + d) = x$$

$$d = -ba^{-1}$$

(83)

We need a to have a mult. inv. in $\mathbb{Z}_{26}$.

$$\varphi(26) = \varphi(2) \cdot \varphi(13) = 12.$$

We have 12 options for a , 26 options for b . In total:

$$12 \cdot 26 = 312 \quad \text{options.}$$

crypt. secure

$$2^{256}, 2^{512}, 2^{2048}$$