Example: $31^{-1} \pmod{87}$

Use EEA to compute s,t such that $1 = s\cdot 31 + t\cdot 87$

87	31	25	6	1
–	–	2	1	4
0	1	2	3	14
1	0	1	1	5

$87 = 2\cdot 31 + 25$

$31 = 1\cdot 25 + 6$

$25 = 4\cdot 6 + 1$

So $1 = 5\cdot 87 - 14\cdot 31$

$\Rightarrow 31^{-1} \equiv -14 \pmod{87} \equiv 73.$

Q: What if $d = \gcd(a,m) \neq 1$?

By EEA $\exists$ (non-unique) $s,t \in \mathbb{Z}$ such that

$$d = s\cdot a + t\cdot m$$

What does it mean "non-unique"?

I.e. if $d = s'\cdot a + t'\cdot m$, what is the relation between (s,t), (s',t')?

$$\begin{aligned} d &= sa + tm \\ d &= s'a + t'm \end{aligned} \Rightarrow \begin{aligned} 1 &= s\cdot \tfrac{a}{d} + t\cdot \tfrac{m}{d} \\ 1 &= s'\cdot \tfrac{a}{d} + t'\, \tfrac{m}{d} \end{aligned}$$

$\Rightarrow s, s'$ are inverses of $\frac{a}{d}$ modulo $\frac{m}{d}$.

$\Rightarrow s' = s + k \cdot \frac{m}{d}$ for some $k \in \mathbb{Z}$.

$\Rightarrow t' = t - k \cdot \frac{a}{d}$ (Ex).

§3.3. Complete and Reduced Systems of Residues.

Definition: A <u>complete system</u> of residues modulo m is a set of integers containing exactly one representative from each congruence class mod m.

The standard complete system is
$$\{0, 1, 2, \dots, m-1\}.$$

Sometimes some other complete systems are more convenient.

We can define $+, -, \times$ for elements of complete system.

Examples a) $m=2$

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

b) $m=5$

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Definition. A <u>reduced set</u> of residues modulo m is a set of integers containing exactly one element from each <u>invertible</u> congruence class mod m (congruence lass of a with $\gcd(a,m)=1$).

The standard reduced set is

$$\{a\in\mathbb{Z} \mid 0\leq a\leq m-1,\ \gcd(a,m)=1\}$$

The size of this set is called Euler's phi-function of m ($\varphi(m)$).

Examples:
a) $m=5$ $\{\cancel{0},1,2,3,4\}$, $\varphi(5)=4$.
b) $m=6$ $\{\cancel{0},1,\cancel{2},\cancel{3},\cancel{4},5\}$, $\varphi(6)=2$
c) $m=\underset{\shortparallel \atop 2^3}{8}$ $\{\cancel{0},1,\cancel{2},3,\cancel{4},5,\cancel{6},7\}$, $\varphi(8)=4$
d) $m=\underset{\shortparallel \atop 3^2}{9}$ $\{\cancel{0},1,2,\cancel{3},4,5,\cancel{6},7,8\}$, $\varphi(9)=6$.

Computation of φ:

a) $m = p$ is prime

$\cancel{0}, 1, 2, \ldots, p-1$

$\Rightarrow \varphi(p) = p-1.$

b) $m = p^k$, power of prime

$\cancel{0}, 1, 2, \ldots, p-1, \cancel{p}, p+1, \ldots, \cancel{2p}, \ldots, \cancel{(p^{k-1})p}, \ldots, p^k - 1$

$\Rightarrow \varphi(p^k) = p^k - p^{k-1}$

c) $\varphi(mn) = \varphi(m)\varphi(n)$ <u>if</u> $\gcd(m,n) = 1$

(proof – later).

§3.4. Powers in modular arithmetics.

Compute powers of 2 mod 21

$a_n \equiv 2^n \pmod{21}$, $a_n \equiv 2a_{n-1} \pmod{21}$

n	0	1	2	3	4	5	6	7	8	9	10	11	
2^n mod 21	1	2	4	8	16	11	1	2	4	8	16	11	...

repetition.

Proposition. Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ with $\gcd(a,m) = 1$. Then there exists $j \in \mathbb{Z}$ $1 \le j \le m$ such that $a^j \equiv 1 \pmod{m}$.

Proof. There are m different residues mod m

$\Rightarrow$ There is a repetition among

$$a^1, a^2, a^3, \dots, a^{m+1} \pmod m.$$

I.e. $\exists\, i, i'$ with $1 \leq i < i' \leq m+1$ with

$$\underbrace{a^i \equiv a^{i'} \equiv a^i}_{\text{can cancel them}} \cdot a^{i'-i} \pmod m$$

$\Rightarrow 1 \equiv a^{i'-i} \pmod m$ $\quad 1 \leq i'-i \leq m.$ $\boxtimes$

Definition: Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ $\gcd(a,m)=1$

The order of a mod m is the smallest $j \in \mathbb{Z}^+$ such that

$$a^j \equiv 1 \pmod m.$$

(Notation: $\mathrm{ord}_m(a)$)

Examples: a) $\mathrm{ord}_{21}(2) = 6$

b) Compute $3^{2017} \pmod{14}$

n	0	1	2	3	4	5	6
3^n mod 14	1	3	9	13 $\equiv -1$	11 $\equiv -3$	5 $\equiv -9$	1

$\Rightarrow \mathrm{ord}_{14}(3) = 6.$

$$3^{2017} \equiv 3^{6 \cdot 336 + 1} \equiv (3^6)^{336} \cdot 3 \equiv 3 \pmod{14}.$$