Recall: "RSA Theorem": Let $m = pq$ with p, q distinct primes. Then

$$a^{k\varphi(m)+1} \equiv a \pmod{m} \quad \text{for any } a, k \in \mathbb{Z}.$$

Proof: By induction.

$k=0$ is obvious

$k=1$ is true by proposition.

Assume true for k and prove for $k+1$.

$$a^{(k+1)\varphi(m)+1} \equiv \underbrace{a^{k\varphi(m)+1}}_{\equiv a} \cdot a^{\varphi(m)} \equiv a^{\varphi(m)+1} \pmod{m}$$

$\equiv a$ (by proposition). $\boxtimes$

Corollary. Let $d \in \mathbb{Z}$ be coprime with $\varphi(m) = (p-1)(q-1)$ and $e \equiv d^{-1} \pmod{\varphi(m)}$. Then the following two functions are inverses to each other:

$$\begin{tikzcd} \{0,1,2,\dots,m-1\} \arrow[r, bend left, "a \to a^d \pmod{m}"] & \{0,1,2,\dots,m-1\} \arrow[l, bend left, "b \to b^e \pmod{m}"] \end{tikzcd}$$

Proof: $(a^d)^e \overset{?}{\equiv} a \pmod{m}$

By construction $ed = 1 + k\varphi(m)$

$$\Rightarrow (a^d)^e = a^{de} = a^{k\varphi(m)+1} \equiv a \pmod{m}$$ $\boxtimes$

§6. Relating Congruences with Different Moduli.

Recall $a \equiv b \pmod{m}$ means

$m \mid b-a$ or

$b = a + km$ for some $k \in \mathbb{Z}$.

§6.1. Principle 1:

Let $m_1, m_2 \in \mathbb{Z}^+$ with $m_1 \mid m_2$.

Then $a \equiv b \pmod{m_2} \Rightarrow a \equiv b \pmod{m_1}$

[Proof: If $m_2 = dm_1$ then

$$b = a + km_2 = a + kdm_1 \Rightarrow b \equiv a \pmod{m_1}]$$

The converse is not true. However the the folowing statement is true:

$$a \equiv b \pmod{m_1} \Rightarrow a \equiv b \pmod{m_2} \text{ or } a \equiv b + m_1 \pmod{m_2}$$
$$\text{or } a \equiv b + 2m_1 \pmod{m_2} \text{ or} \dots$$
$$a \equiv b + m_2 - m_1 \pmod{m_2}).$$

Examples: (a) $x \equiv 1 \pmod{12} \Rightarrow x \equiv 1 \pmod{4}$

(b) $x \equiv 1 \pmod{4} \Rightarrow x \equiv 1$ or 5 or $9 \pmod{12}$

§6.2 Principle 2:

If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$

[Proof: $m \mid b-a \Rightarrow cm \mid c(b-a) = cb - ca$]

The converse is true and is formulated as follows:

Assume $a \equiv b \pmod{m}$. Let $d \mid a$ and $d \mid m$. Then d also divides b and

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

[Check: $b = \underbrace{a + km}_{\text{multiples of } d} \Rightarrow d \mid b$ and $\frac{b}{d} = \frac{a}{d} + k\cancel{d}\frac{m}{d}$].

Examples: (a) $3x \equiv 5 \pmod{12}$ has no solutions
$3 \mid 3$, $3 \mid 12$ but $3 \nmid 5$.

(b) $3x \equiv 6 \pmod{12}$
$\Leftrightarrow x \equiv 2 \pmod{4}$.

Corollary: Any congruence of the form $ax \equiv b \pmod{m}$ either has no solutions in $x \in \mathbb{Z}$ or is equivalent to $x \equiv c \pmod{m'}$ for some $c, m' \in \mathbb{Z}$.

Solution method of such congruences:

(1) Compute $\gcd(a, m) = d$

(2) If $d=1$ then there exists $a^{-1} \pmod{m}$ and $x \equiv a^{-1}b \pmod{m}$

(3) Assume $d>1$

(i) If $d \nmid b$ then there are no solutions

(ii) If $d \mid b$ then

$$ax \equiv b \pmod{m} \iff \frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$$

Now $\gcd(\frac{a}{d}, \frac{m}{d}) = 1$ (because of maximality of d, a common divisor of a and m).

So we go back to (2)

Example: $4x \equiv 6 \pmod{14}$

$\gcd(4, 14) = 2$.

$\iff 2x \equiv 3 \pmod{7}$

Now $\gcd(2, 7) = 1$.

$\iff x \equiv 2^{-1} \cdot 3 \pmod{7} \equiv 4 \cdot 3 \equiv 5 \pmod{7}$.

In other words all integer solutions of $4x \equiv 6 \pmod{14}$ are in the set

$$\{\ldots, -16, -9, -2, 5, 12, 19, \ldots\}$$

which is a congruence class of $5 \pmod{7}$.

§ 6.3 Principle 3, Chinese Remainder Theorem

If $m_1, m_2 \in \mathbb{Z}^+$ such that $\gcd(m_1, m_2) = 1$.

Then $\left.\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{array}\right\} \Rightarrow a \equiv b \pmod{m_1 m_2}$

[Proof: $\begin{array}{l} m_1 \mid b-a \\ m_2 \mid b-a \end{array} \Rightarrow m_1 m_2 \mid b-a$ since $\gcd(m_1, m_2) = 1$]

Ex: Check!

Chinese Remainder Theorem (case of two congruences). Let $m_1, m_2 \in \mathbb{Z}^+$ with $\gcd(m_1, m_2) = 1$

Then the system

$$\begin{array}{l} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{array} \quad \text{for any } b_1, b_2 \in \mathbb{Z} \qquad (*)$$

is equivalent to

$$x \equiv c \pmod{m_1 m_2} \text{ for some } c \in \mathbb{Z}.$$

In other words, the system $(*)$ has a solution $x \in \mathbb{Z}$ which is unique mod $m_1 m_2$