Definition $a \equiv b \ (mod \ \ m)$ means that $m$ divides $a - b$ or there exists a $k$ such that $km = a - b$.

$\equiv \ (mod \ \ m)$ is an equivalence relation since

- $a \equiv a \ (mod m)$ or $m$ divides $a - a$. (reflexive)

- if $a \equiv b \ (mod \ \ m)$, then $b \equiv a \ (mod \ \ m)$ since if $m$ divides $a - b$ then it divides $b - a$. (symmetric)

- if $a \equiv b \ (mod m)$ and $b \equiv c \ (mod \ \ m)$, then $a \equiv c \ (mod \ \ m)$. (transitive)

It is defined on the integers and so it can easily be shown that for any integer $k$,

- $a \equiv b \ (mod \ m)$ if and only if $a + k \equiv b + k \ (mod \ m)$.

- if $a \equiv b \ (mod \ m)$, then $ka \equiv kb \ (mod \ m)$.

if $ka \equiv bk \ (mod \ m)$, then sometimes $a \not\equiv b \ (mod \ m)$.
e.g. $2 \cdot 3 \equiv 2 \cdot 0 \ (mod \ 6)$, but $3 \not\equiv 0 \ (mod \ 6)$.
e.g. $4 \cdot 5 \equiv 4 \cdot 2 \ (mod \ 12)$, but $5 \not\equiv 2 \ (mod \ 12)$.

When $gcd(k, m) = 1$, if $ka \equiv kb \ (mod \ m)$, then $a \equiv b \ (mod \ m)$

$$
\begin{aligned}
gcd(a, b) &= \text{greatest common divisor of } a \text{ and } b \\
&= \text{largest divisor of both } a \text{ and } b \\
&= \text{if } d \text{ divides } a \text{ and } b, \text{ then } d \text{ also divides } gcd(a, b)
\end{aligned}
$$

Example: compute $gcd(963, 657)$

$$
\begin{aligned}
963 &= 1 \cdot 657 + 306 \\
657 &= 2 \cdot 306 + 45 \\
306 &= 6 \cdot 45 + 36 \\
45 &= 1 \cdot 36 + 9 \\
36 &= 4 \cdot 9
\end{aligned}
$$

Conclusion: $gcd(963, 657) = 9$

$$\begin{aligned} gcd(963,657) = 9 &= -36 + 45 \\ &= -(306 - 6 \cdot 45) + 45 \\ &= -306 + 7 \cdot 45 \\ &= -306 + 7(657 - 2 \cdot 306) \\ &= -15 \cdot 306 + 7 \cdot 657 \\ &= -15(963 - 657) + 7 \cdot 657 \\ &= -15 \cdot 963 + 22 \cdot 657 \end{aligned}$$

In general we can always use these equations to write

$$gcd(a,b) = k \cdot a + \ell \cdot b$$

for some integers $k$ and $\ell$.

Example solve $127x \equiv 4 \ (mod\ 963)$

$$
\begin{aligned}
963 &= 7 \cdot 127 + 74 \\
127 &= 1 \cdot 74 + 53 \\
74 &= 1 \cdot 53 + 21 \\
53 &= 2 \cdot 21 + 11 \\
21 &= 1 \cdot 11 + 10 \\
11 &= 1 \cdot 10 + 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 11 - 10 = 11 - (21 - 11) = 2 \cdot 11 - 21 \\
&= 2(53 - 2 \cdot 21) - 21 = 2 \cdot 53 - 5 \cdot 21 = 2 \cdot 53 - 5(74 - 53) \\
&= 7 \cdot 53 - 5 \cdot 74 = 7(127 - 74) - 5 \cdot 74 = 7 \cdot 127 - 12 \cdot 74 \\
&= 7 \cdot 127 - 12(963 - 7 \cdot 127) = 91 \cdot 127 - 12 \cdot 963
\end{aligned}
$$

Conclusion, because $91 \cdot 127 - 12 \cdot 963 = 1$,

$$91 \cdot 127 \equiv 1 \ (mod\ 963)$$

Therefore if we have

$$127x \equiv 4 \ (mod\ 963)$$

$$x \equiv 1 \cdot x \equiv 91 \cdot 127x \equiv 91 \cdot 4 \equiv 364 \ (mod\ 963)$$

Computational elements that we will use in some new cryptosystems

- Compute $a^k \ (mod\ \ m)$ using only squaring operations and multiplication by $a$.

- $gcd(a, b)$ using the Euclidean algorithm

- Find $k$ and $\ell$ such that

$$ka + \ell b = gcd(a, b)$$

- If $gcd(a, m) = 1$, then there is a $k$ such that

$$ak \equiv 1 \ (mod\ \ m)$$

There is a function called the Euler 'phi' function

$$\phi(n) = \# \text{ of integers relatively prime (i.e. } gcd(k, n) = 1)$$
$$\text{and are between 1 and } n$$

| $n$ | integers between 1 and n which are relatively prime | $\phi(n)$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 1 | 1 |
| 3 | 1,2 | 2 |
| 4 | 1,3 | 2 |
| 5 | 1,2,3,4 | 4 |
| 6 | 1,5 | 2 |
| 7 | 1,2,3,4,5,6 | 6 |
| 8 | 1,3,5,7 | 4 |
| 9 | 1,2,4,5,7,8 | 6 |
| 10 | 1,3,7,9 | 4 |
| 11 | 1,2,3,4,5,6,7,8,9,10 | 10 |
| 12 | 1,5,7,11 | 4 |
| 14 | 1,3,5,9,11,13 | 6 |

Let $[a, b]$ represent the interval of integers $\{a, a+1, \ldots, b-1, b\}$. Notice that

$$\begin{aligned}\phi(p) &= \# \text{ of integers in [1,p] that have common factor with } p \\ &= \# \text{ of integers [1,p)} \\ &= p - 1\end{aligned}$$

Also,

$$\begin{aligned}\phi(p^k) &= p^k - \# \text{ of integers in } [1,p^k] \text{ divisible by } p \\ &= p^k - \# \text{ of } r \cdot p \text{ where } 1 \leq r \leq p^{k-1} \\ &= p^k - p^{k-1}\end{aligned}$$

Say that $p$ does not divide $n$. Then let $h$ be the number of integers in $[1, n]$ that have a common factor with $n$.

$$\begin{aligned}\phi(p^k n) &= np^k - \#\text{ of integers in } [1, np^k] \text{ with a common} \\ &\qquad \text{factor with } n \text{ or } p \\ &= np^k - \#\text{ in } [1, np^k] \text{ with a common factor with } n \\ &\qquad - \#\text{ in } [1, np^k] \text{ with a common factor with } p \\ &\qquad + \#\text{ in } [1, np^k] \text{ with a factor with both } n \text{ and } p \\ &= np^k - hp^k - np^{k-1} + hp^{k-1} \\ &= (n-h)(p^k - p^{k-1}) = \phi(n)(p^k - p^{k-1})\end{aligned}$$

if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $p_i$ are all distinct primes, then

$$\phi(n) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - k})$$