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

Example: compute $gcd(963, 657)$

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

$$
\begin{aligned}
&gcd(963, 657) \\
&\quad \| \\
&gcd(657, 306) \\
&\quad \| \\
&gcd(306, 45) \\
&\quad \| \\
&gcd(45, 36) \\
&\quad \| \\
&gcd(36, 9)
\end{aligned}
$$

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

Solve for 9 in terms of 657 & 963

look for $9 = k \cdot 657 + \ell \cdot 963$

$$K \cdot 127 = 1 - l \cdot 963$$

OR

$$K \cdot 127 \equiv 1 \pmod{963}$$

Recall $a \equiv b \pmod{m}$ means (def) $a = b + l \cdot m$ for some $l \in \mathbb{Z}$

$$127 \cdot x \equiv 4 \pmod{963}$$

and

$$127 \cdot 91 \equiv 1 \pmod{963}$$

$$(91 \cdot 127) \cdot x \equiv 91 \cdot 4 \pmod{963}$$

$$1 \cdot x \equiv 364 \pmod{963}$$

In general, if $\gcd(a, m) = 1$

then if $ax \equiv ay \pmod{m}$

then $x \equiv y \pmod{m}$

<u>Pf</u>: $\gcd(a, m) = 1 = k \cdot a + l \cdot m$ so $k \cdot a \equiv 1 \pmod{m}$

so if $ax \equiv ay \pmod{m}$, then $x \equiv (k \cdot a)x \equiv (k \cdot a)y \equiv y \pmod{m}$

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

goal: find k & l

$k \cdot 127 + l \cdot 963 = 1$

$$963 = 7 \cdot 127 + 74 \qquad 74 = 963 - 7 \cdot 127$$

$$127 = 1 \cdot 74 + 53 \qquad 53 = 127 - 74$$

$$74 = 1 \cdot 53 + 21 \qquad 21 = 74 - 53$$

$$53 = 2 \cdot 21 + 11 \Rightarrow 11 = 53 - 2 \cdot 21$$

$$21 = 1 \cdot 11 + 10 \Rightarrow 10 = 21 - 11$$

$$11 = 1 \cdot 10 + 1 \Rightarrow 1 = 11 - 10$$

$$= 2 \cdot 11 - 21$$

$$= 2 \cdot 53 - 5 \cdot 21$$

$$= 7 \cdot 53 - 5 \cdot 74$$

$$= 7 \cdot 127 - 12 \cdot 74$$

$$1 = 11 - 10 = 11 - (21 - 11) = 2 \cdot 11 - 21$$

$$= 2(53 - 2 \cdot 21) - 21 = 2 \cdot 53 - 5 \cdot 21 = 2 \cdot 53 - 5(74 - 53)$$

$$= 7 \cdot 53 - 5 \cdot 74 = 7(127 - 74) - 5 \cdot 74 = 7 \cdot 127 - 12 \cdot 74$$

$$= 7 \cdot 127 - 12(963 - 7 \cdot 127) = 91 \cdot 127 - 12 \cdot 963$$

$k = 91 \quad l = -12$

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.

let $h = n - \phi(n)$

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

$\#\ r \cdot p$ where $1 \le r \le p^{k-1} n$

$\phi(p^k)$

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

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

There is a function called the Euler 'phi' function

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

and are between 1 and n

$\phi(n)$ is even for $n \geq 3$

n	integers between 1 and n which are relatively prime	$\phi(n)$
1	1	1
2	1	$1 = 2^1 - 2^0$ $\quad \phi(p) = p-1$
3	1,2	$2 = 3^1 - 3^0$
4	1,3	$2 = 2^2 - 2^1$ $\quad \phi(2^k) = 2^{k-1}$
5	1,2,3,4	$4 = 5^1 - 5^0$ $\quad \phi(2n) = \phi(n)$
6	1,5	$2 = (3^1-3^0)(2^1-2^0)$ if n is odd
7	1,2,3,4,5,6	$6 = 7^1 - 7^0$
$2^3 = 8$	1,3,5,7	$4 = (2^3 - 2^2)$
$3^2 = 9$	1,2,4,5,7,8	$6 = (3^2 - 3^1)$
$2 \cdot 5 = 10$	1,3,7,9	$4 = (5^1-5^0)(2^1-2^0)$
$11 = 11$	1,2,3,4,5,6,7,8,9,10	$10 = 11^1 - 11^0$
$3 \cdot 2^2 = 12$	1,5,7,11	$4 = (3^1-3^0)(2^2-2^1)$
13	1,2, - - - - - , 12	12
$2 \cdot 7 = 14$	1,3,5,9,11,13	$6 = (7^1-7^0)(2^1-2^0)$
$3 \cdot 5 = 15$	1,2,4,7,8,11,13,14	$8 = (3^1-3^0)(5^1-5^0)$
$2^4 = 16$	1,3,5,7,9,11,13,15	$8 = 2^4 - 2^3$

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

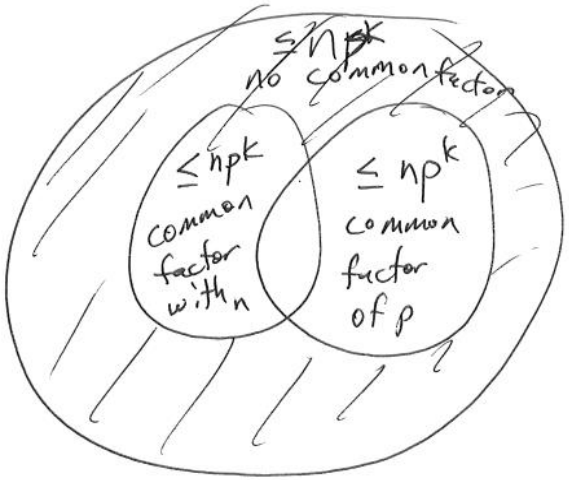
$$\begin{aligned}\phi(p) &= \#\text{ of integers in [1,p] that have common factor with } p \\ &= \#\text{ of integers [1,p)} \\ &= p - 1\end{aligned}$$

Also,

e.g. $\phi(27) = \phi(3^3) = 27 -$ the numbers which are divisible by 3 in $[1, 27]$
$= 27 - 9 = 18$

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

$\phi(27) = \#\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$
$= 27 - 9 = 18$


$\leq np^k$
no common factor
$\leq np^k$
common factor with n
$\leq np^k$
common factor of p

Look at the set of # rel prime to n

$$\{a_1, a_2, a_3, \ldots\ldots, a_{\phi(n)}\}$$

multiply by one of the a_i mod n

Result is that multiplication by an a_i is a permutation of this set.

Is it possible that

$$a_i \cdot a_j \equiv a_i \cdot a_k \pmod{m}?$$

if $j \neq k$

Example: $n=8$

$$\{1,3,5,7\}$$

$\xrightarrow{\times 3}$ $\{3,1,7,5\}$

$\xrightarrow{\times 5}$ $\{5,7,1,3\}$

$\xrightarrow{\times 7}$ $\{7,5,3,1\}$

Take

$$\{a_1, a_2, \ldots, a_{\phi(a)}\}$$

and $a \in \{a_1, a_2, \ldots, a_{\phi(n)}\}$

then

$$\{a_1, a_2, \ldots, a_{\phi(n)}\} \underset{\text{mod } n}{\equiv} \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$$

$$a_1 a_2 \cdots a_{\phi(n)} \equiv (aa_1)(aa_2)(aa_3)\cdots(aa_{\phi(n)}) \pmod{n}$$

$$\equiv a_1 a_2 a_3 \cdots a_{\phi(n)} a^{\phi(n)} \pmod{n}$$

But I can cancel each of the $\phi(n)$ a_i's

$$1 \equiv a^{\phi(n)} \pmod{n}$$

Euler-Fermat theorem.

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

$N = 3465$

Calculate 7^{1442} MOD 3465

$7^2 \equiv 49 \mod 3465$

$7^4 \equiv (49)^2 \equiv 2401 \mod 3465$

$7^8 \equiv 2506 \equiv (7^4)^2$

$7^{16} \equiv (7^8)^2 \equiv 1456$

$7^{32} \equiv (7^{16})^2 \equiv 2821$

$7^{64} \equiv (7^{32})^2 = 2401$

$7^{128} = (7^{64})^2 \equiv 2506$

$7^{256} \equiv (7^{128})^2 \equiv 1456$

$7^{512} \equiv (7^{256})^2 \equiv 2821$

$7^{1024} \equiv (7^{512})^2 \equiv 2401$

$7^{1442} \equiv 7^{1024+418} \equiv 7^{1024+256+128+32+2}$