# Introduction to Number Theory

CS1800 Discrete Structures; notes by Virgil Pavlu

## 1 modulo arithmetic

All numbers here are integers. The integer division of $a$ at $n > 1$ means finding the unique quotient $q$ and reminder $r \in \mathbb{Z}_n$ such that
$a = nq + r$
where $\mathbb{Z}_n$ is the set of all possible reminders at $n$ : $\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\}$.

"mod $n$" = *reminder at division with* $n$ for $n > 1$ ($n$ it has to be at least 2)
"$a \mod n = r$" means mathematically all of the following :
· $r$ is the reminder of integer division $a$ to $n$
· $a = n * q + r$ for some integer $q$
· $a, r$ have same reminder when divided by $n$
· $a - r = nq$ is a multiple of $n$
· $n \mid a - r$, a.k.a $n$ divides $a - r$

EXAMPLES
21 mod 5 = 1, because 21 = 5*4 +1
same as saying $5 \mid (21 - 1)$

**THEOREM** two numbers $a, b$ have the same reminder mod $n$ if and only if $n$ divides their difference.
We can write this in several equivalent ways:
· $a \mod n = b \mod n$, saying $a, b$ have the same reminder (or modulo)
· $a = b(\mod n)$
· $n \mid a - b$ saying $n$ divides $a - b$
· $a - b = nk$ saying $a - b$ is a multiple of $n$ ($k$ is integer but its value doesnt matter)
EXAMPLES
$21 = 11 \ (\text{mod } 5) = 1 \Leftrightarrow 5 \mid (21 - 11) \Leftrightarrow 21 \mod 5 = 11 \mod 5$
$86 \text{ mod } 10 = 1126 \text{ mod } 10 \Leftrightarrow 10 \mid (86 - 1126) \Leftrightarrow 86 - 1126 = 10k$
**proof:** EXERCISE. Write "$a \mod n = r$" as equation $a = nq + r$, and similar for $b$

**modulo addition** $(a+b) \mod n = (a \mod n + b \mod n) \mod n$
EXAMPLES
17 + 4 mod 3 = (17 mod 3) + (4 mod 3) mod 3 = 2 + 1 mod 3 = 0

**modulo multiplication** $(a \cdot b) \mod n = (a \mod n \cdot b \mod n) modn$
EXAMPLES
17 * 4 mod 3 = (17 mod 3) * (4 mod 3) mod 3 = 2 * 1 mod 3 = 2

**modulo power** is simply a repetition of multiplications
$a^k$ mod $n$ = ($a$ mod $n$ * $a$ mod $n$ ... * $a$ mod $n$ ) mod $n$

EXAMPLE: $13^{100} \mod 11 =?$
$13 \mod 11 = 2$
$13^2 \mod 11 = 2^2 \mod 11 = 4$
$13^4 \mod 11 = (13^2 \mod 11)^2 \mod 11 = 4^2 \mod 11 = 16 \mod 11 = 5$
$13^8 \mod 11 = (13^4 \mod 11)^2 \mod 11 = 5^2 \mod 11 = 25 \mod 11 = 3$
$13^{16} \mod 11 = (13^8 \mod 11)^2 \mod 11 = 3^2 \mod 11 = 9$
$13^{32} \mod 11 = (13^{16} \mod 11)^2 \mod 11 = 9^2 \mod 11 = 4$
$13^{64} \mod 11 = (13^{32} \mod 11)^2 \mod 11 = 4^2 \mod 11 = 5$
$13^{100} = 13^{64} \cdot 13^{32} \cdot 13^4 \mod 11 = (5 * 4 * 5) \mod 11 = 25 * 4 \mod 11 = 25 \mod 11 * 4 \mod 11 = 3 * 4 \mod 11 = 1$

## 2 factorization into primes

Any integer $n \geq 2$ can be uniquely factorized into prime numbers
$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_t$
$12 = 2 \cdot 2 \cdot 3$
$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$

In this product we prefer to group the same primes together, so we usually write each prime only once with an exponent indicating how many times it appears: $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot ... \cdot p_t^{e_t}$

$12 = 2^2 \cdot 3$
$48 = 2^4 \cdot 3$
$36 = 2^2 \cdot 3^2$
$50 = 2 \cdot 5^2$
$1452 = 2^2 \cdot 3 \cdot 11^2$

1 is not a prime number, the primes start at 2
primes sequence: 2,3,5,7,11,13,17,19...

OBSERVATION The product $ab$ factorization is simply enumerating all the primes in $a$ an $b$ with proper counts. If there are exponents or common primes, we can simply write in $ab$ factorization each prime with the exponent made of the sum of exponents of that prime in $a$ and $b$
$300 = 2^2 \cdot 3 \cdot 5^2$
$126 = 2 \cdot 3^2 \cdot 7$
$300 \cdot 126 = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7 = 37800$

**THEOREM** if a prime divides a product of integers, then it divides one of the factors. In other words $p \mid ab \Rightarrow p \mid a \vee p \mid b$
**proof by contradiction** assume $p \nmid a \wedge p \nmid b$. Then neither $a$ nor $b$ contain $p$ in their respective factorizations, thus $p$ cannot appear in the product $ab$

NOTE This is not true for non-primes, for example $p = 4$ :
$4 \mid 6 \cdot 10$, but $4 \nmid 6$ and $4 \nmid 10$

One can obtain the sequence of primes using the *Sieve of Eratosthenes*. Start with a sequence of all positive integers bigger than 1: 2,3,4,5,6,7,8,9,10,...
* the first available number (2) is prime. Remove from the sequence all multiples of 2, so the sequence now is 3,5,7,9,11,13,15...
* repeat: the first available number (3) is prime. remove all multiples of 3; now the sequence of remaining numbers is 5,7,11,13,17,19,23,25,29...
* repeat. We get 5 as prime and after removal of 5 multiples the remaining sequence is 7,11,13,17,19,23,29,...49,..
NOTE that each step gives the next prime number and removes from the sequence its multiples. The next number available is a prime, because it was not removed as a multiple of smaller prime numbers extracted previously.

EXERCISE When the next prime $p$ is extracted, what is the smallest number (other than $p$) that is removed because it is a $p$-multiple?

**THEOREM** There are infinitely many primes.
**proof by contradiction**. Assume prime set is finite $P = \{p_1, p_2, p_3, ..., p_t\}$. Then the number $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_t + 1$ cannot have any prime factors, so it is another prime. But $n$ is not in set $P$, contradiction.

## 3 gcd

Greatest Common Divisor between integers $a$ and $b$ is made of
*the common primes of a and b.*
If they have exponents, each prime in gcd has the lowest exponent between $a$ and $b$ (that is, each exponent gives how many of that prime are in $a$ respectively $b$. The lowest exponent corresponds to the common number of that prime)
$48 = 2^4 \cdot 3$
$36 = 2^2 \cdot 3^2$
gcd(48,36) $= 2^2 \cdot 3 = 12$ (two “2” and one “3” )

$8918 = 2 \cdot 7^3 \cdot 13$
$9800 = 2^3 \cdot 5^2 \cdot 7^2$
gcd(8918,9800) $= 2 \cdot 7^2 = 98$ (one “2”, two “7” )

$60 = 2^2 \cdot 3 \cdot 5$
$50 = 2 \cdot 5^2$
gcd(60,50) $= 2 \cdot 5 = 10$

$60 = 2^2 \cdot 3 \cdot 5$
$637 = 13 \cdot 7^2$
no common primes, so gcd(60,637) $= 1$

**THEOREM** if $q$ divides both $a$ and $b$, then $q \mid gcd(a, b)$
**proof idea**. If $q$ divides both $a$ and $b$ then $q$ can only be made of (factorizes into) the common primes between $a$ and $b$. Since $d = gcd(a, b)$ contains all the common primes, then $d$ will include the entire factorization of $q$, thus $d$ is a multiple of $q$, or $q \mid d = gcd(a, b)$.

**THEOREM** $gcd(a, b)$ is the largest integer who divides both $a$ and $b$
**proof by contradiction** Say $gcd(a, b)$ is not the largest divisor, but instead $f > gcd(a, b)$ is the largest integer that divides both $a$ and $b$. From previous theorem, $f \mid gcd(a, b) \Rightarrow f \leq gcd(a, b)$, contradiction.

**THEOREM** Let $gcd(a, b) = gcd(b, a \mod b)$. If $a = bq + r$ (usually the integer division of $a$ to $b$). Then $d = gcd(a, b) = gcd(b, a \mod b) = gcd(b, r)$

Its easy to see how gcd applies to $a = bq + r$ as $q$ subtractions of one from the other:
$gcd(a, b) = gcd(a - b, b) = gcd(a - b - b, b) = ... = gcd(a - qb, b) = gcd(r, b)$

A masonry contractor has to tile a rectangular patio size $a = 22 \times b = 6$. *There is a strict requirement that the tiles have to be squares, and they have to be as big as possible.* What size tile will be used? Answer: d=$gcd(22, 6) = 2$

To see this visually, the contractor draws the patio on a square grid 22 x 6.

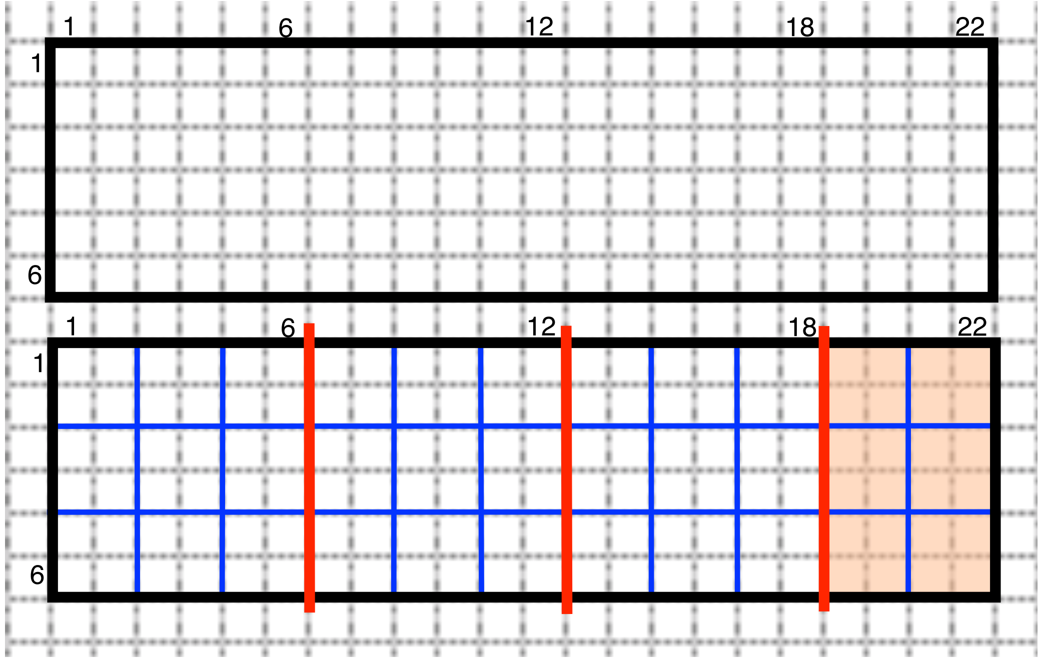

Figure 1: a rectangular patio of size $(a = 22 \times b = 6)$ can be tiled with squares of maximum size $d = gcd(22, 6) = gcd(4, 6) = 2$.

He knows that whatever $d$ is the biggest tile, it can certainly cover 6 x 6, so he chops that square off (figure, vertical red line at column 6). That is
$d = gcd(22, 6) = gcd(22 - 6, 6) = gcd(16, 6)$
Next the contractor chops off the next 6 x 6 square, and he gets
$d = gcd(16, 6) = gcd(16 - 6, 6) = gcd(10, 6)$
Then the last full 6 x 6 is chopped to get
$d = gcd(10 - 6, 6) = gcd(4, 6) = gcd(r, b)$ (since a=22, b=6, q=3, r=4 in equation $a = bq + r$)

EXAMPLE a=51; b=9; d=gcd(51,9)=3
51 division to 9 yields 51=9*5 + 6 ($q = 5$ and $r = 6$)
The theorem states that gcd(51,9) = 3 = gcd(9,6)

**proof** Let $d = gcd(a, b)$ and $d_1 = gcd(b, r)$
$d \mid a$ and $d \mid b \Rightarrow d \mid (a - bq) \Rightarrow d \mid r \Rightarrow d \mid gcd(b, r) = d_1$
$d_1 \mid b$ and $d_1 \mid r \Rightarrow d_1 \mid (bq + r) \Rightarrow d_1 \mid a \Rightarrow d_1 \mid gcd(b, a) = d$
Thus $d \mid d_1$ and $d_1 \mid d \Rightarrow d = d_1$

**Euclid Algorithm** finds gcd$(a, b)$ by reducing the problem $(a, b)$ to a smaller problem $(b, r)$ repeatedly until its trivial.

```
$d$ = PROCEDURE-EUCLID $(a, b)$ : given $a > b \geq 1$, find $d = gcd(a, b)$
1) divide $a$ by $b$ obtain $a = bq + r$
2) if $r = 0$ then b=gcd(a,b), RETURN b, DONE
3) if $r \neq 0$ we have $b > r \geq 1$ and theorem says $gcd(a, b) = gcd(b, r)$
    Call $d$ = PROCEDURE-EUCLID$(b, r)$
4) RETURN d
```

EXAMPLE
gcd(22,6) = gcd(6*3+4, 6)
. *(a=22,b=6,q=3,r=4 reduction to b=6 r=4)*
= gcd(6,4) = gcd( 4*1 +2, 4)
. *(a=6,b=4,q=1,r=2 reduction to b=4 r=2)*
= gcd(4,2) = gcd( 2*2 +0, 2)
. *(r = 0, return b=2 as gcd)*
=2

EXAMPLE
gcd(51,9) = gcd(9*5+6, 9)
. *(a=51,b=9,q=5,r=6 reduction to b=9 r=6)*
= gcd(9,6) = gcd( 6*1 +3, 6)
. *(a=9,b=6,q=1,r=3 reduction to b=6 r=3)*
= gcd(6,3) = gcd( 3*2 +0, 3)
. *(r = 0, return b as gcd)*
=3

NOTE that the problem is always reduced to a smaller one: by reducing $(a, b)$ to $(b, r)$ both values are smaller (closer to 0); thus eventually we are going to hit a trivial problem where $r = 0$.

**lcm**$(a, b)$ **is Least Common Multiple of** $a$ **and** $b$. It is the opposite of gcd regarding $a$ and $b$ prime factorizations:
gcd = intersection of prime factors (smallest counts each prime)
lcm = union of prime factors (largest count for each prime)

$48 = 2^4 \cdot 3$
$36 = 2^2 \cdot 3^2$
gcd(48,36) $= 2^2 \cdot 3 = 12$ (two "2" and one "3" )
lcm(48,36) $= 2^4 \cdot 3^2 = 144$ (four "2" and two "3" )

$8918 = 2 \cdot 7^3 \cdot 13$
$9800 = 2^3 \cdot 5^2 \cdot 7^2$
gcd(8918,9800) $= 2 \cdot 7^2 = 98$ (one "2", two "7" )
lcm(8918,9800) $= 2^3 \cdot 5^2 \cdot 7^3 \cdot 13 = 891800$ (three "2", two "5", three "7", one "13" )

**THEOREM** $a \cdot b = gcd(a, b) \cdot lcm(a, b)$
EXAMPLES
36*48 = gcd(36,48) * lcm (36,48) = 12 * 144
8918* 9800 = gcd(8918,9800) * lcm(8918,9800) = 98 * 891800

**proof idea** $ab$ has the same factorization as gcd*lcm, just organized differently. Take any prime $p^e$ in factorization $ab$. Say $u$ of these $e$ times the prime $p$ comes from $a$, the other $v = e - u$ times it must come from $b$.
Then $p^{min(u,v)}$ appears in $gcd(a, b)$ factorization and $p^{max(u,v)}$ appears in $lcm(a, b)$. The theorem states that overall we have the same number of $p$ occurrences in $ab$ is the same as in $gcd \cdot lcm$, which is same as saying $u + v = min(u, v) + max(u, v)$; easy to verify.

# 4 relative prime ("coprime")

Integers $a, b$ are coprime if they have no common prime factors. In other words gcd(a,b)=1
Note: a or b or both can be non prime individually, and still be coprime to each other: neither 12 or 25 is prime but
$12 = 2^2 \cdot 3$
$25 = 5^2$
gcd(12,25) =1 so they are coprime

Also an integer $a$ can be coprime with $b$ but not with $c$ : 12 is coprime with 25, but not with 16 because gcd(12,16) =4

**THEOREM** if $n$ divides a product of integers, and it is coprime with one of them, then it divides the other. In other words
$n \mid ab; gcd(n, a) = 1 \Rightarrow n \mid b$
**proof idea** if $n$ factorizes into prime factors $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot ... \cdot p_t^{e_t}$, then none of these primes appear in factorization of $a$ (because $gcd(n, a) = 1$ there are no common primes between $n$ and $a$ ).
But $ab = k \cdot n = k \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot ... \cdot p_t^{e_t}$
so each prime with its exponent like $p_1^{e_1}$ must appear in $b$ factorization. Thus $n \mid b$

**THEOREM** If $d = gcd(a, b)$ then $u = \frac{a}{d}$ and $v = \frac{b}{d}$ are coprime integers, i.e. $gcd(u, v) = 1$
EXAMPLE $a = 6, b = 9, gcd(a, b) = 3$. Then $u = \frac{6}{3} = 2; v = \frac{9}{3} = 3$ and $gcd(\frac{6}{3}, \frac{9}{3}) = gcd(2, 3) = 1$

**proof idea**. Assume $gcd(u, v)$ contains prime $p > 1$. Then $a$ and $b$ both contain $d \cdot p$ in their respective factorizations. That means $d = gcd(a, b)$ should have included $d \cdot p$, since gcd includes all common factors. Thus $dp|d \Rightarrow p = 1$ contradiction.

**formal proof by contradiction**. Assume $gcd(u, v)$ contains prime $p > 1$.

Then $u = pf; v = pg \Rightarrow a = du = dpf; b = dv = dpg \Rightarrow dp \mid a; dp \mid b \Rightarrow dp \mid gcd(a, b) \Rightarrow dp|d \Rightarrow p = 1$ contradiction.

APPLICATION: reduction of rational fractions. Say we want to simplify a fraction of two integers $f = \frac{a}{b}$ as much as possible, i.e until no simplification is possible. That is achieved by dividing both numerator $a$ and denominator $b$ by their gcd; after that the new fraction cannot be simplified further.

$$f = \frac{72}{132}$$

We compute $gcd(72, 132) = gcd(2^3 \cdot 3^2, 2^2 \cdot 3 \cdot 11) = 2^2 \cdot 3 = 12$ and simplify by dividing both numbers by 12

$$f = \frac{72}{132} = \frac{12 \cdot 6}{12 \cdot 11} = \frac{6}{11}$$

which is *irreductible* (not simplifiable)

**THEOREM** if two coprimes divide a number, then their product also divides that number. In other words
$n \mid a; m \mid a; gcd(n, m) = 1 \Rightarrow nm \mid a$
EXAMPLE : $6 \mid 120; 5 \mid 120; gcd(5, 6) = 1$. Then $5 \cdot 6 \mid 120$

This is not necessarily true if $gcd(m, n) > 1$, for example:
$6 \mid 72; 9 \mid 72$. But $6 \cdot 9 \nmid 72$; the theorem doesnt hold here because $gcd(6, 9) \neq 1$

**proof 1.** $n \mid a \Rightarrow a = nk$.
Then $m \mid nk; gcd(m, n) = 1 \Rightarrow m \mid k \Rightarrow k = mt$
We now can write $a = kn = tmn \Rightarrow mn \mid a$

**proof 2**. Lets consider factorization into primes
$nm = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot ... \cdot p_t^{e_t}$.
Take one of these factors, say $p_1^{e_1}$. Since $gcd(n, m) = 1$ all $e_1$ occurrences of prime $p_1$ must be in $n$ or all in $m$; in other words we cannot have some of $p_1$ in $n$ and the rest of them (up to $e_1$) in $m$ because that would cause $p_1$ to be part of $gcd(n, m)$.
Suppose they are in $n$, then since $a$ is multiple of $n$ we have that $p_1^{e_1}$ appears in $a$ factorization. This is true for all primes in $nm$ factorization, so $a$ is a multiple of all of them, thus a multiple of $nm$.

# 5 modulo inverse

In $\mathbb{Z}_n$ some elements have an *inverse*: multiplying with the *inverse* gives 1 mod $n$. We write $a$'s inverse in $\mathbb{Z}_n$ as $a^{-1} \mod n$
DEFINITION $a \in \mathbb{Z}_n$ has inverse $b = a^{-1} \in \mathbb{Z}_n$ iff $ab = 1$ mod $n$.
If $b$ exists, then $a = b^{-1}$ is $b$'s inverse mod $n$, since $ba$=$ab$ = 1 mod $n$

EXAMPLES :
2 has inverse 3=$2^{-1}$ mod 5, because $2 \cdot 3 = 6 = 1$ mod 5
9 has inverse 3=$9^{-1}$ mod 13, because $9 \cdot 3 = 27 = 1$ mod 13

Not all elements in $\mathbb{Z}_n$ have an inverse. Examples:
* $2 \in \mathbb{Z}_8$ has no inverse because gcd(2,8)$\neq 1$. An inverse $b = 2^{-1}$ would mean $2b = 1$ mod $8 \Leftrightarrow \exists k \in Z, 2b = 8k + 1$
which is impossible because $2 \mid 2b$ but $2 \nmid 8k + 1$

* $3 \in \mathbb{Z}_{12}$ has no inverse in $\mathbb{Z}_{12}$ because gcd(3,12)$\neq 1$. An inverse $b = 3^{-1}$ would mean
$3 \cdot b = 12k + 1 \Rightarrow 3 \mid 12k + 1 \Rightarrow 3 \mid 1$ contradiction !

* 0 does not have an inverse in $\mathbb{Z}_n$ (for any $n$), because $0 \cdot b = 0 \neq 1, \forall b \in \mathbb{Z}_n$

$\mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{0\} = \{1, 2, 3, ...n - 1\}$ is the set of all reminders mod $n$ except 0.
**THEOREM** if $a, n$ coprime $gcd(a, n) = 1$, then multiplying all non-zero reminders (mod $n$) with $a$ gives back the set of non-zero reminders.
$\{1a, 2a, 3a, ..., (n - 1)a\} \mod n = \{1, 2, 3, ...n - 1\}$.
In other words:
$S = a \cdot \mathbb{Z}_n^* \mod n = \{1a, 2a, 3a, ..., (n - 1)a\} \mod n = \mathbb{Z}_n^*$
**proof** First, the left set $S$ is a subset of $\mathbb{Z}_n$, and does not contain the reminder 0 : if 0 would be in it, thats saying there is a $t \in \mathbb{Z}_n^*$ with $a \cdot t = 0$ mod $n \Rightarrow n \mid at$. Since $(a, n)$ are coprime, $n$ must divide the other factor, so $n|t$; but this is impossible for $0 < t < n$
Second, $S$ enumerates $n - 1$ elements, and all of them are distinct reminders mod $n$. Suppose there are two distinct $u, v \in \mathbb{Z}_p^*$ such that $au = av$ mod $n \Rightarrow n \mid a(u - v) \Rightarrow n \mid a(u - v)$. Since $(a, n)$ are coprime, $n$ must divide the other factor, $n \mid (u - v) \Rightarrow u = v$ (because $-n < u - v < n$) contradiction.
So $S$ is a subset of $\mathbb{Z}_n^*$ with all its $n - 1$ elements. It means $S = \mathbb{Z}_n^*$.

EXAMPLE n=9, a=4 coprime
$\{1 \cdot 4, 2 \cdot 4, 3 \cdot 4, 4 \cdot 4, 5 \cdot 4, 6 \cdot 4, 7 \cdot 4, 8 \cdot 4\} \mod 9 =$
$\{4, 8, 12, 16, 20, 24, 28, 32\} \mod 9 = \{4, 8, 3, 7, 2, 6, 1, 5\} = \mathbb{Z}_9^*$

**THEOREM** Multiplicative inverse $b = a^{-1} \mod n$ exists if and only if $a, n$ are coprime, i.e. $gcd(a, n) = 1$
The inverse, when exists, is a power of $a \mod n$.
**proof (⇒)** if $a$ has inverse $b$ mod $n$ then $ab = nk + 1$. Let $d = gcd(a, n)$, then
$d \mid ab; d \mid nk \Rightarrow d \mid ab - nk \Rightarrow d \mid 1 \Rightarrow d = 1$

**proof (⇐) 1.** Apply the previous theorem:
$\{1a, 2a, 3a, ..., (n-1)a\} \mod n = \{1, 2, 3, ...n-1\}$
note that 1 is in the set on the right side, so there must be on the left set. Thus there is some value $b \in \{1, 2, ..., n-1\}$ such that $ab = 1 \mod n$
NOTE this proof gives no idea how to actually find the inverse.

**proof (⇐) 2.** if gcd(a,n)=1, consider the sequence of powers of a in $\mathbb{Z}_n$ : $a^1, a^2, a^3 ...(\mod n)$. This is an infinite sequence but $\mathbb{Z}_n$ is finite, so some of these powers are bound to be the same value in $\mathbb{Z}_n$; in other words there will be different exponents $u, u+v$ such that $a^u = a^{u+v}$ mod $n$. That means
$n \mid a^{u+v} - a^u \Rightarrow n | a^u(a^v - 1)$
but $gcd(n, a) = 1 \Rightarrow gcd(n, a^u) = 1$. So a previous theorem says $n$ has to divide the other factor, or
$n \mid (a^v - 1) \Rightarrow a^v = nk + 1 \Rightarrow a \cdot a^{v-1}$ mod $n$ =1
So we found the inverse of $a$, it is $a^{-1} = a^{v-1}$ mod $n$. It is inefficient for a large $n$ to try consecutive powers to find the root

EXAMPLE: 4 should have an inverse in $\mathbb{Z}_9$ because gcd(4,9)=1. We can find it by trying powers of 4 modulo 9:
$4^2 \mod 9 = 16 \mod 9 = 7$
$4^3 \mod 9 = 64 \mod 9 = 1$
So $4 * 4^2 = 1 \mod 9$, or $4^2 \mod 9$ is the inverse of 4 in $\mathbb{Z}_9$. That inverse value is $4^2 \mod 9 = 7$.

EXAMPLE: 5 should have an inverse in $\mathbb{Z}_{26}$ because gcd(5,26)=1. We can find it by trying powers of 5 modulo 26 until we get 1:

$5^2 \mod 26 = 25 \mod 26 = -1 \mod 26$
$5^3 = (5^2)5 = (-1) * 5 = -5 = 21 \mod 26$
$5^4 = (5^2)^2 = (-1)^2 = 1 \mod 26$
So $5 * 5^3 = 1 \mod 26$, or $5^3 \mod 26 = 21$ is the inverse of 5 in $\mathbb{Z}_{26}$.
Verify: 5*21 = 105 = 1 mod 26

The first way to get the inverse (when exists) is to use the modulo power until we get reminder 1. The second way is to find the linear coefficients that give the gcd, recursively from problem (a,b) to smaller problem (b,r) similarly with the strategy in Euclid algorithm.

**THEOREM of gcd-coefficients.** For any integers $a, b$ there exists integer coefficients $k, h$ such that
$ak + bh = gcd(a, b)$ (“*gcd equation*”)
$k, h$ are called “gcd-coefficients” or “Bézout coefficients” for $(a, b)$.

Further, any integer coefficients $k, h$ produce a linear combination of $ak + bh$ that is a multiple of $d = gcd(a, b)$. In particular, such linear combinations cant produce positive integers smaller than $d$. In fact these two sets are the same:
$\{ak + bh | \forall k, h \in \mathbf{Z}\}$ = multiples of $d = \{..., -3d, -2d, -d, 0, d, 2d, 3d, 4d...\}$

EXAMPLE: $a = 60, b = 36, gcd(60, 36) = 12$
We can pick $k = -1, h = 2$ to get
$ak + bh = 60 \cdot (-1) + 36 \cdot 2 = -60 + 72 = 12$
The coefficients are not unique; we could pick instead $k = 2, h = -3$ to get
$ak + bh = 60 \cdot 2 + 36 \cdot (-3) = 120 - 108 = 12$
The second part of the theorem states that for any $k, h$ the integer $ak + bh$ has to be a multiple of 12, thus at least 12 (if positive) or at most -12 (if negative) or 0.

EXAMPLE: $a = 51, b = 9, gcd(51, 9) = 3$
For $k = 11, h = -62$ we get $ak + bh = 51 \cdot (11) + 9 \cdot (-62) = 561 - 558 = 3$

EXAMPLE: $a = 22, b = 6, gcd(22, 6) = 2$
For $k = -1, h = 4$ we get $ak + bh = 22 \cdot (-1) + 6 \cdot (4) = -22 + 24 = 2$

**proof** Say $d = gcd(a,b)$. We know from previous theorem $gcd(\frac{a}{d}, \frac{b}{d}) = 1$, and then from another previous theorem that in this case $\frac{a}{d}$ should have an inverse modulo $\frac{b}{d}$. Lets call that inverse k:

$$\frac{a}{d} \cdot k = 1 \mod \frac{b}{d}$$

thats same as saying is an integer $t$ such that

$$\frac{ak}{d} = \frac{b}{d} \cdot t + 1$$

Then $ak = bt + d \Rightarrow ak - bt = d$. Let $h = -t$ to obtain $ak + bh = d = gcd(a,b)$.

INVERSE FROM GCD-COEFFICIENTS. If $gcd(a,b) = 1$, $a$ has an inverse in $\mathbb{Z}_b$ and viceversa. In this particular case of coprimes $a, b$ gcd-coefficients theorem guarantees the coefficients $k, h$ such that
$ak + bh = 1$
These are indeed the inverses we are looking for:
$k = a^{-1} \mod b$ ; $h = b^{-1} \mod a$

EXERCISE explain why $k$ is the inverse of $a$ in $\mathbb{Z}_b$ ( $ak = 1 \mod b$)

The finding-inverse problem then comes down to finding these coefficients $k, h$. Euclid-Extended Algorithm does just this, by reducing the problem to a smaller one until its easy to solve.

**Euclid Extended Algorithm** finds gcd-coefficients $k$ and $h$ for the given integers $a$,$b$, such that $ak + bh = d = gcd(a, b)$. It works recursively by reducing the problem$(a, b)$ to a smaller problem until it becomes trivial.

$k, h =$ PROCEDURE-EUCLID-EXTENDED $(a, b)$ : given $a > b \geq 1$, return coefficients $k, h$ such that $ak + bh = gcd(a, b)$

```
1) divide $a$ by $b$ obtain $a = bq + r$
2) if $r = 0$, $b = gcd(a, b)$ and coefficients are $k = 1, h = 1 - q$
                                        **exercise**: $k = 0, h = 1$ also work
    RETURN 1, $1 - q$. DONE
3) If $r > 0$ then $b > r \geq 1$
    Call $k_1, h_1 =$ PROCEDURE-EUCLID-EXTENDED (b,r) to obtain
    $bk_1 + rh_1 = gcd(b, r) = gcd(a, b)$
4) compute $k, h$ from $a, b, q, r, k_1, h_1$
    $k = h_1$; $h = k_1 - qh_1$
                                        **exercise**: verify these $k, h$ calculations
5) RETURN $k, h$
```

```
EXAMPLE $a = 51, b = 9$
$k, h$=gcd-coef(51,9) = gcd-coef(9*5+6, 9)
.                                             *(a=51,b=9,q=5,r=6 call b=9 r=6)*
    $k_1, h_1$=gcd-coef(9,6) = gcd( 6*1 +3, 6)
.                                             *(a=9,b=6,$q_1$=1,r=3 call b=6 r=3)*
        $k_2, h_2$=gcd(6,3) = gcd( 3*2 +0, 3)
.                                             *(r = 0,$q_2$=2 return coef 1, 1-$q_2$)*
        $k_2 = 1; h_2 = 1 - q_2 = -1$
        RETURN $k_2, h_2$ for a=6,b=3
.                                             *verify* $6 * k_2 + 3 * h_2 = gcd$
    $k_1 = h_2 = -1; h_1 = k_2 - q_1 h_2 = 2$
    RETURN $k_1, h_1$ for a=9,b=6
.                                             *verify* $9 * k_1 + 6 * h_1 = gcd$
$k = h_1 = 2; h = k_1 - qh_1 = -11$
RETURN $k, h$ for a=51,b=9
.                                             *verify* $51 * k + 9 * h = gcd$
```

OBSERVATION: $k, h$ are not unique. The procedure found $k = 2, h = -11$, but $k = -1, h = 6$ would have worked too: 51*-1 + 9*6 = 3 = gcd(51,9)

# 6 Fermat's Little Theorem

We now know that when $a$ has an inverse mod $n$, that inverse is a power of $a$: $\exists v, a^v = 1 \mod n \Rightarrow a^{-1} = a^{v-1} \mod n$.
We would like to get our hands on a power $v$ such that $a^v = 1 \mod n$. This is like solving a modulo-root equation but for the exponent. We call the smallest such $v$ the multiplicative *root* (or *order*) of $a \mod n$.
**The good:** if $v$ is such a power that produces $a^v = 1 \mod n$, then any multiple of $v$ has the same property : $a^{vk} = (a^v)^k = 1^k = 1 \mod n$
So we dont need the smallest root $v$, any multiple of $v$ would be fine. We know how to obtain such a multiple that works for any $a$, in other words to act like an root for all $a$; in the next section will call that root-for-all $\phi(n)$.

In here we look at the particular case where $n = p$ is prime. In this case the problem is easier: a known multiple for any $v$ (root for $a$) is $p - 1$. So $p - 1$ acts as an root for every $a$ (mod $p$).

**THEOREM (Fermat)** Let $p$ prime. For any $0 \neq a \in \mathbb{Z}_p$, we have
$a^{p-1} = 1 \text{ mod } p$

EXAMPLES
$p = 7$, $a = 5$
$a^{p-1} = 5^6 = 15625 = 7 * 2232 + 1 = 1(\mod 7)$
The smallest root $v$ for $a = 5$ is $p - 1 = 6$: none of the previous powers of $a = 5$ gives 1 mod 7 : $5, 5^2, 5^3, 5^4, 5^5 \neq 1 \mod 7$

$p = 7$, $a = 4$
$a^{p-1} = 4^6 = (4^2)^3 = 16^3 = 2^3 = 1(\mod 7)$
The smallest root $v$ for $a = 4$ is actually $v = 3$, not $p - 1 = 6$, but of course $p - 1$ must be a multiple of $v$:
$4^3 = 16 \cdot 4 = 2 \cdot 4 = 1(\mod 7)$

$p = 5$, $a = 3$
$a^{p-1} = 3^4 = 81 = 1(\mod 5)$
It turns out that modulo 5, $p - 1 = 4$ is the smallest root $v$ for any $a$ to give $a^v = 1 \mod p$

$p = 11$, $a = 3$
$a^{p-1} = 3^{10} = (3^4)^2 \cdot 3^2 = 81^2 \cdot 9 = 4^2 \cdot 9 = 5 \cdot 9 = 1( \mod 11)$
For $a = 3$, smallest root $v \mod 11$ is actually not $p-1 = 10$, but 5 (a divisor of $p-1$):
$3^5 = 243 = 1( \mod 11)$

**proof.** A previous theorem stated that if (a,p) are coprime then these two sets are the same
$S = \{1a, 2a, 3a, ..., (p-1)a\} = \mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$
Then the product of all elements in $S$ mod $p$ is the same as the product of all elements in $\mathbb{Z}_p^*$ mod $p$:
$a^{p-1} \cdot 1 \cdot 2 \cdot ... \cdot (p-1) = 1 \cdot 2 \cdot ... \cdot (p-1) \mod p$
$a^{p-1}(p-1)! = (p-1)! \mod p$
$\Rightarrow p \mid (p-1)!(a^{p-1} - 1)$
Since $gcd(p, (p-1)!) = 1$, $p$ must divide the other factor, $p \mid (a^{p-1} - 1) \Rightarrow a^{p-1} = 1 \mod p$

EXERCISE: Given the theorem, show that for any integer $a$ and prime $p$, we have $a^p = a$ (mod $p$).

EXERCISE: Explain why $p$ and $(p-1)!$ are coprime, a critical fact used to prove the theorem.

# 7 Primality test

OBSERVATION Fermat's Theorem statement holds sometimes when $p$ is not prime, only for carefully chosen $a$. For example $p = 15, a = 4$ we have
$4^{15-1} = 4^{14} = (4^2)^7 = 16^7 = 1^7 = 1(\mod 15)$
Surprisingly for very special non-prime "Carmichael numbers" Fermat's theorem holds entirely (for any $a$). So its converse its not true. Try it for $p = 561$.

**Fermat's Primality Test** for number $p$ works like this : pick several random positive integers $a < p$ and check for each $a$ if $a^{p-1} = 1 \mod p$.
• if at least one test (for a particular $a$) gives "NO" then we know for sure $p$ is not prime
• if all tests (for all $a$) give "YES", we are not sure, but with high probability $p$ is prime.

Carmichael numbers are the numbers $n$ with the following two properties:
· $n$ is "square free", meaning factorization into primes $n = p_1 \cdot p_2 \cdot ... \cdot p_t$ contains each prime exactly once (no exponents $e > 1$)
· for every prime factor $p$ of $n$, $p - 1 \mid n - 1$

EXAMPLES First few Carmichael numbers are
561= 3*11*17; because 2, 10, 16 divide 560
1105= 5*13*17; because 4, 12, 16 divide 1104
1729 = 7*13*19 ; because 6, 12, 18 divide 1728

**Carmichael numbers pass all Fermat's-primality tests but they are not primes!** But Carmichael numbers are so rare, that we are OK with them passing incorrectly at "primes".

EXERCISE(difficulty ★) Show that a Carmichael number $n$ that satisfies the definiton properties above, while not prime, passes all Fermat's tests: for every $0 < a < n$ we get $a^{n-1} = 1 \mod n$.

EXERCISE(difficulty ★★) A number $n$ passes all Fermat's tests: for every $0 < a < n$ we get $a^{n-1} = 1 \mod n$. Show that either it is prime, or it is a Carmichael number.

# 8 Chinese Reminder - optional

If $N = p \cdot q \cdot r$ (or more factors) then there is a matching of sizes between $(\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r)$ and $\mathbb{Z}_N$.

**THEOREM of Chinese Reminder** If the factors are pairwise coprime, i.e. $gcd(p, q) = gcd(p, r) = gcd(q, r) = 1$,
The following is a one to one mapping : take any triplet of reminders $(a \in \mathbb{Z}_p, b \in \mathbb{Z}_q, c \in \mathbb{Z}_r)$ into a unique $x \in \mathbb{Z}_N$, such that $x \mod p = a; x \mod q = b; x \mod r = c$
This mapping function $h : \mathbb{Z}_{pqr} \to \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$, given by
$h(x) = (x \mod p, x \mod q, x \mod r)$
is called the Chines-Reminder bijection between $\mathbb{Z}_{pqr}$ and $(\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r)$

EXAMPLE $p = 3, q = 4, r = 5; N = 3 \cdot 4 \cdot 5 = 60$
$a = 1, b = 2, c = 1 \Leftrightarrow x = 46$
$a = 1, b = 2, c = 0 \Leftrightarrow x = 10$
$a = 1, b = 1, c = 3 \Leftrightarrow x = 13$
$a = 1, b = 0, c = 2 \Leftrightarrow x = 52$
$a = 2, b = 2, c = 2 \Leftrightarrow x = 2$
$a = 0, b = 0, c = 0 \Leftrightarrow x = 0$
$a = 1, b = 1, c = 1 \Leftrightarrow x = 1$
$a = 2, b = 1, c = 2 \Leftrightarrow x = 17$

NOTE it is critical that $gcd(p, q) = 1$. For example if $p = 4$ and $q = 6$, picking $a = 2, b = 1$ it would be impossible to find $x$ with these reminders mod $p$ and mod $q$

EXERCISE. it is enough to proof the theorem for only 2 factors $N = pq$. Once we have that proof we can extend it to 3 factors, then to 4, then 5, and so on.
From 2 to 3 factors: Say $N = pqr = (pq)r$. Since $gcd(pq, r) = 1$ the theorem for two factors gives us the mapping $h_1(x) = (y, c)$ between $\mathbb{Z}_{pqr}$ and $(\mathbb{Z}_{pq} \times \mathbb{Z}_r)$; with $y \in \mathbb{Z}_{pq}$ and $c \in \mathbb{Z}_r$.
Applying the 2-factor theorem again for $p, q$ we get a second mapping $\mathbb{Z}_{pq}$ and $(\mathbb{Z}_p \times \mathbb{Z}_q)$ : $h_2(y) = (a, b)$ with $a \in \mathbb{Z}_p, b \in \mathbb{Z}_q$. Since both $h_1, h_2$ are bijective (one to one) then we can compound them to obtain the 3-factor theorem

$x \quad -h_1 \rightarrow \quad (y,c) \quad -h_2 \rightarrow \quad (a,b,c)$

**proof 1** based on uniqness (no construction of $x$) for three-factor (works for any number of coprime factors). We want to show that $h(x) = (x \mod p, x \mod q, x \mod r)$ is a bijection (one-to-one) between $\mathbb{Z}_{pqr}$ and $(\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r)$.
First $h$ is an injection because for any $x \neq y$ we have $h(x) \neq h(y)$:
$h(x) = h(y) \Rightarrow x = y \mod p \Rightarrow p \mid x - y$. Similarly $q \mid x - y$, and $r \mid x - y$
But $p, q, r$ are pairwise coprime, so then $pqr \mid x - y \Rightarrow x = y$
Second, $|\mathbb{Z}_{pqr}| = pqr = |\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r|$ (same number of elements). An injection like $h$ between finite sets of equal sizes must be *surjective* (cover all elements in the result set). Then $h$ is bijective, or one-to-one.

**proof 2 : construction of $x$ for two factor.** Given $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_q$ we want to find $x \in \mathbb{Z}_{pq}$ such that $x \mod p = a; x \mod q = b$.
$gcd(p,q) = 1 \Rightarrow \exists k, h : pk - qh = 1 \Rightarrow (pk - qh)(b - a) = b - a \Rightarrow pk(b - a) - qh(b - a) = b - a \Rightarrow pk(b - a) + a = qh(b - a) + b$. This is the integer we are looking for $x = pk(b-a) + a = qh(b-a) + b \mod pq$ because it gives precisely $a \mod p$ and $b \mod q$.

# 9 Euler totient function $\phi(n)$ - mandatory

$\phi(n)$ = number of coprimes with $n$ in $\mathbb{Z}_n$.

|  | $n$ | set $C_n$ = coprimes-with-$n$ in $\mathbb{Z}_n$ | $\phi(n) = \lvert C_n \rvert$ |
|---|---|---|---|
| prime | 2 | 1 | 1$= n-1$ |
| prime | 3 | 1,2 | 2$= n-1$ |
|  | 4 | 1,3 | 2 |
| prime | 5 | 1,2,3,4 | 4$= n-1$ |
|  | 6 | 1,5 | 2 |
| prime | 7 | 1:6 | 6$= n-1$ |
|  | 8 | 1,3,5,7 | 4 |
|  | 9 | 1,2,4,5,7,8 | 6 |
|  | 10 | 1,3,7,9 | 4 |
| prime | 11 | 1:10 | 10$= n-1$ |
|  | 15 | 1,2,4,7,8,11,13,14 | 8 |
|  | 16 | 1,3,5,7,9,11,13,15 | 8 |
| prime | 17 | 1:16 | 16$= n-1$ |
|  | 18 | 1,5,7,11,13,17 | 6 |
| prime | 19 | 1:18 | 18$= n-1$ |
|  | 20 | 1,3,7,9,11,13,17,19 | 8 |
| prime | 23 | 1:22 | 22$= n-1$ |

**THEOREM (Euler)** if $gcd(a, n) = 1$ then $a^{\phi(n)} = 1 \mod n$

EXAMPLE $n = 15$
coprime set is $C_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ ; $\phi(15) = |C_{15}| = 8$
Then for every $a \in C_{15}$ we have $a^8 = 1 \mod 15$:
$1^8 = 1 \mod 15$
$2^8 = (2^4)^2 = 16^2 = 1^2 = 1 \mod 15$
$4^8 = (4^2)^4 = (2^4)^4 = 1^4 \mod 15$
$7^8 = (7^2)^4 = 49^4 = 4^4 = 2^8 = 1 \mod 15$
$8^8 = (-7)^8 = 7^8 = 1 \mod 15$
$11^8 = (-4)^8 = 4^8 = 1 \mod 15$
$13^8 = (-2)^8 = 2^8 = 1 \mod 15$
$14^8 = (-1)^8 = 1 \mod 15$

EXERCISE proof Fermat's theorem as a particular case of Euler's theorem for primes by showing that for a prime $p$,
$\phi(p) = p - 1$

EXERCISE Show that if n is a prime square $n = p^2$, then
$\phi(n) = p(p-1)$

**EXERCISE: RSA EQUATION** if $n$ is a product of two primes, $n = pq$, show that
$\phi(n) = (p-1)(q-1) = pq - p - q + 1$
by counting the non-coprimes in $\mathbb{Z}_n \setminus C_n$
NOTE that in this case Euler's theorem says that for any $a < n$, and any integer $k$
$a^{\phi(n)k+1} = a^{(p-1)(q-1)k+1} = a \mod pq$.
This is the equation that makes RSA cryptosystem work. It uses two prime numbers $p, q$ very large (2048 bits each $\approx 10^{600}$ magnitude) to avoid factorization by brute force with present computational ability (as of year 2016).

EXERCISE. Ff $n$ is a product of three primes, $n = pqr$, show that
$\phi(n) = (p-1)(q-1)(q-1)$
by counting the non-coprimes in $\mathbb{Z}_n \setminus C_n$

EXERCISE(difficulty ★, done in textbook) if $n$ is a product of two primes, $n = pq$, then we know from previous exercise that $\phi(n) = (p-1)(q-1)$
Prove Euler's theorem in this particular case
$a^{(p-1)(q-1)} = 1 \mod pq$; for any $a, n$ coprimes
by following these two steps:
· use Fermat's theorem for $a$, separately mod $p$ and then mod $q$
· use the Chinese reminder theorem to get the result of $a^{(p-1)(q-1)} \mod pq$

EXERCISE (RSA-1-factor). RSA is hard to break because breaking it comes down to one of the following notoriously difficult problems:
• Given $n = pq$ ($p, q$ unknown), find $p$ and $q$; or
• Given $n = pq$ ($p, q$ unknown) and $e$, find $e$'s inverse modulo $(p-1)(q-1)$ without finding $p$ and $q$
Suppose one wants to implement an RSA-like cryptosystem based on Fermat's theorem with only one prime $n = p$. The equation is
$a^{(p-1)k+1} = a \mod p$.

and so encoding and decoding would work correctly with two keys $e$(public) and $e^{-1} \mod p-1$ (private). What is wrong with this encryption schema? Hint: Finding private key is easy.

EXERCISE(difficulty ★ RSA-3-factors). Suppose one wants to implement an RSA-like cryptosystem with three primes $n = pqr$ instead of two. The equation becomes
$a^{(p-1)(q-1(r-1)k+1} = a \mod pqr$.
• Is it correct ? So that encoding and decoding work correctly with two keys $e$(public) and $e^{-1} \mod (p-1)(q-1)(r-1)$ (private).
• Is this encryption schema weaker or stronger than the two-factor RSA?

# 10 Euler totient function $\phi(n)$ - optional ★

$\phi(n) =$ number of coprimes with $n$ in $\mathbb{Z}_n = |C_n|$
**THEOREM (Euler)** if $gcd(a,n) = 1$ then $a^{\phi(n)} = 1 \mod n$
**proof 1 with modulo arithmetic.** We have a theorem that says if $a, n$ coprime $gcd(a,n) = 1$, then multiplying all non-zero reminders (mod $n$) with $a$ gives back the set of non-zero reminders.
$\{1a, 2a, 3a, ..., (n-1)a\} \mod n = \{1, 2, 3, ...n-1\}$.
In other words:$S = a \cdot \mathbb{Z}_n^* \mod n = \{1a, 2a, 3a, ..., (n-1)a\} \mod n = \mathbb{Z}_n^*$
Now we need a version of this theorem, for the coprime reminders set:

**Lemma.** if $a, n$ coprime $gcd(a,n) = 1$, then multiplying all coprime reminders $C_n = \{u_1, u_2, u_3, ..., u_{\phi(n)}\}$ with $a$ gives back the set of coprime reminders: $\{au_1, au_2, au_3, ..., au_{\phi(n)}\} \mod n = \{u_1, u_2, u_3, ..., u_{\phi(n)}\}$.
In other words
$S = a \cdot C_n \mod n = \{ua | u \in C_n\} \mod n = C_n$
**proof for lemma.** To show this result we make a similar argument with the one in the original theorem:
• the left set $S$ is a subset of $C_n$, because every element in $uv \in S$ is a product of two coprimes with $n$ ($u$ and $a$), thus certainly a coprime: we can immediately show that if $u^{-1}, a^{-1}$ are $u$ and $a$ inverses mod $n$, then $u^{-1}a^{-1}$ is the inverse of $ua$, so $ua \in C_n$.
• Second, $S$ enumerates $\phi(n)$ elements, and all of them are distinct reminders mod $n$. Suppose there are two distinct $u_1, u_2 \in C_n$ such that $au_1 = au_2 \mod n \Rightarrow n \mid a(u_1 - u_2) \Rightarrow n \mid a(u_1 - u_2)$. Since $(a,n)$ are coprime, $n$ must divide the other factor, $n \mid (u_1 - u_2) \Rightarrow u_1 = u_2$ (because $-n < u_1 - u_2 < n$) contradiction.
So $S$ is a subset of $C_n$ with all its $\phi(n)$ elements. It means $S = C_n$.

The rest of the proof follows the derivation used to prove Fermat's theorem: if $S$ and $C_n$ are the same set, then the product of all elements in $S$ mod $n$ is the same as the product of all elements in $C_n$ mod $n$:
$a^{|C_n|} \prod\{C_n\} = \prod\{C_n\} \mod n$
$a^{\phi(n)} \prod\{C_n\} - \prod\{C_n\} = 0 \mod n$
$(a^{\phi(n)} - 1) \prod\{C_n\} = 0 \mod n$
$n \mid (a^{\phi(n)} - 1) \prod\{C_n\}$
Since $gcd(n, \prod\{C_n\}) = 1$, $n$ must divide the other factor, $n \mid (a^{\phi(n)} - 1) \Rightarrow a^{\phi(n)} = 1 \mod n$.

## 10.1 Group Theory and Lagrange Theorem

DEFINITION A set and an operand like $(\mathbb{Z}_n, \mod +)$ form a *group* because the following are satisfied:
1) the operand result is always in the set : $a, b \in \mathbb{Z}_n \Rightarrow a + b \mod n \in \mathbb{Z}_n$
2) there is a neutral element, $0 + a = a + 0 = a, \forall a \in \mathbb{Z}_n$
3) associativity holds $(a + b) + c = a + (b + c), \forall a, b, c \in \mathbb{Z}_n$
4) every element has an inverse $\forall a, \exists - a, a + (-a) = -a + a = 0$

OBSERVATION $(\mathbb{Z}_n, \mod \times)$ is not a group with multiplicative-mod, because 1 would be the neutral element, and then 0 has no inverse.
But how about $(\mathbb{Z}_n^*, \mod \times)$ - that is, the set of all reminders except 0, with multiplicative-mod as operand? Certainly not a group for all $n$: for example $n = 10$ gives $\mathbb{Z}_{10}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ where 5 has no inverse (there is no element that multiplied with 5 gives 1 mod 10).

EXERCISE Show that conditions 2 and 3 are satisfied for $(\mathbb{Z}_n^*, \mod \times)$ to be a group.

EXERCISE Show that conditions 1 and 4 for $(\mathbb{Z}_n^*, \mod \times)$ are very related in the following sense: for any $x \in \mathbb{Z}_n^*$, either there is an inverse (satisfies condition 4) or there is a particular element $y \in \mathbb{Z}_n^*$ such that $x \times y \mod n = 0 \notin \mathbb{Z}_n^*$ (breaks condition 1), but not both.

**THEOREM** $(\mathbb{Z}_n^*, \mod \times)$ is a group if and only if $n$ is prime.
**proof** EXERCISE
EXAMPLE $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ with operand multiplication modulo 5 forms a group:
1) $a \times b \mod 5 \in \mathbb{Z}_5^*, \forall a, b \in \mathbb{Z}_5^*$
2) 1 is the neutral element
3) $(a \times b) \times c \mod 5 = a \times (b \times c) \mod 5$ in general
4) 1 is its own inverse, 4 is its own inverse, 2 and 3 are eachother's inverse.

**THEOREM** Let $C_n$ be the set of coprimes n from $\mathbb{Z}_n$ (listed in the table above for few $n$). Then $(C_n, \mod \times)$ is a group.
**proof** Lets look at each of the four rules.

1) if $a, b \in C_n$ then we know $ab \mod n \in Z_n$, the only question is if $ab$ is coprime with $n$. Since $gcd(a, n) = gcd(b, n) = 1$, we must have $gcd(ab, n) = 1$; otherwise any prime $p \mid gcd(ab, n)$ will have to be a common prime between $(a, n)$ or common between $(b, n)$ contradicting the premise. So $ab \in C_n$.
2) $1 \in C_n$ is neutral element
3) associativity holds
4) $a \in C_n$ means $a$ has an inverse mod $n$, $a^{-1} \in Z_n$. But this means $a^{-1}$ has inverse $a$, so $a^{-1}$ is coprime with $n$, or $a^{-1} \in C_n$.

**Subgroup**. A group $(G, +)$ has a subgroup $(S, +)$ if the operand $+$ is the same, $S \subset G$, and the $(S, +)$ is a group in itself, a.k.a. the four group-properties hold for $(S, +)$.
Then $|G|$ is a multiple of $|S|$ (the size of a subgroup divides the size of the group).

EXAMPLE $(\mathbb{Z}_6, mod+)$ has a subgroup formed by elements $S = \{0, 2, 4\}$; we can check the four rules:
1) $a, b \in S \Rightarrow a + b \in S$: 2+2 mod 6 =4, 2+4 mod 6=0; 4+4 mod 6 =2 etc
2) 0 is the neutral element
3) associativity holds
4) the inverse of every element in $S$ is also in $S$, because 2 and 4 are eachother's inverse (addition opposite) mod 6.

EXAMPLE $(\mathbb{Z}_7^*, mod\times)$ is a group with modulo-multiplication operand, and has a subgroup formed by elements $S = \{1, 2, 4\}$ :
1) $a, b \in S \Rightarrow a \cdot b \in S : 2 \cdot 2 \mod 7 = 4; 4 \cdot 4 \mod 7 = 2; 2 \cdot 4 \mod 7 = 1$
2) 1 is the neutral element
3) associativity holds
4) the inverse of every element in $S$ is also in $S$, because 2 and 4 are eachother's inverse (multiplication opposite) mod 7.

EXERCISE Another subgroup of $(\mathbb{Z}_6, mod+)$ is given by elements $S = \{0, 3\}$

EXERCISE $(\mathbb{Z}_8, mod+)$ has subgroups $S = \{0, 2, 4, 6\}$ and $S = \{0, 4\}$

EXERCISE $(\mathbb{Z}_{12}, mod+)$ has subgroups $S = \{0, 2, 4, 6, 8, 10\}$, $S = \{0, 4, 8\}$, $S = \{0, 3, 6, 9\}$

**THEOREM (Lagrange)**. A group $(G,+)$ has a subgroup $(S,+)$; we use here "+" as generic operand, can be either addition or multiplication in $\mathbb{Z}_n$. Then $|G|$ is a multiple of $|S|$ (the size of a subgroup divides the size of the group).
**proof** if $S=\{a,b,c,d,...\}$ is a subgroup of $(G,+)$ then we'll prove that $G$ can be partitioned into several sets that look like $h+S=\{h+a,h+b,h+c,h+d...\}$ each corresponding to a key element $h\in G$.
• For $h_1=0$ we get the set $S_1=h_1+S=S$
• Consider an $h_2$ that is not in the first set $h_1+S$. Then $S_2=h_2+S$ will have all brand new elements from $G$, none of them in $h_1+S$.
Proof by contradiction: suppose $\exists a,b\in S$ and $S_2\ni h_2+a=h_1+b\in S$. Then $h_2=h_1+b-a$. But $S$ is a group so $b-a\in S$, which means $h_2\in h_1+S$, contradiction.
Note that $|S_2|=|S|$
• repeat : if the sets generated so far $S_1,S_2,S_3...$ do not fully cover $G$, pick next $h_k$ in $G\setminus S_1\cup S_2\cup S_3$ and repeat the argument from before. The newly generated set $S_k$ will have elements different than the ones in previous sets, and its size will be the same $|S_k|=|S|$
At some point the finite $G$ will be covered by these subsets $G=S_1\cup S_2\cup S_3\cup...\cup S_k$, all disjoint but all of the same size $|S|$. Then $|G|=k|S|$

EXAMPLE ($G=\mathbb{Z}_{12},\ \bmod +$) with $S=\{0,3,6,9\}$. The sets that partion G are
$h_1=0$(neutral element); $S_1=h_1+S=\{0,3,6,9\}$
$h_2=1\in G\setminus S_1$; $S_2=h_2+S=\{1,4,7,10\}$
$h_2=5\in G\setminus S_1\setminus S_2$; $S_2=h_2+S=\{5,8,11,2\}$

EXAMPLE ($G=\mathbb{Z}_7^*=\{1,2,3,4,5,6\},\ \bmod \times$) has subgroup $S=\{1,2,4\}$. The sets that partion G are
$h_1=1$ (neutral element); $S_1=h_1\cdot S=\{1,2,4\}$
$h_2=5\in G\setminus S_1$; $S_2=h_2\cdot S=\{5,3,6\}$

**THEOREM (Euler)** if $gcd(a, n) = 1$ then $a^{\phi(n)} = 1 \mod n$

**proof 2 with group theory.** Let $C_n$ be the set of coprimes-with-$n$ from $\mathbb{Z}_n$, and we know that $(C_n, \mod \times)$ is a group. By definition $\phi(n) = |C_n|$. Now consider the set of elements in $\mathbb{Z}_n$ that are powers of $a$ mod $n$, $A = \{a^1, a^2, a^3 ...\}$. This set $A$ is finite, and the last non-repeated value is $a^v = 1$ (because the next power would be $a$). Then

· $|A| = v$

· $A \subset C_n$ (all elements in $A$ are coprime with $n$)

· $(A, \mod \times)$ is a group, thus a subgroup of $(C_n, \mod \times)$.

The previous theorem says $|A|$ divides $|C_n|$, or equivalently $v \mid \phi(n)$ or $\phi(n) = vk$ which implies

$a^{\phi(n)} \mod n = (a^v)^k \mod n = 1^k \mod n = 1$

EXAMPLE $n = 12, C_n = \{1, 5, 7, 11\} \Rightarrow \phi(n) = 4$.

$1^4 \mod 12 = 1$

$5^4 \mod 12 = 25^2 \mod 12 = 1^2 \mod 12 = 1$

$7^4 \mod 12 = 49^2 \mod 12 = 1^2 \mod 12 = 1$

$11^4 \mod 12 = (-1)^4 \mod 12 = 1$

EXERCISE(difficulty ★) if $n$ is a power of prime, $n = p^k$, then $\phi(n) = p^{k-1}(p - 1)$

EXERCISE(difficulty ★) if $n$ is a product of two coprimes $n = ab$ with $gcd(a, b) = 1$ , then $\phi(n) = \phi(a)\phi(b)$

EXERCISE(difficulty ★) combine the previous two results to show the following. if $n$ factorizes into primes as

$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot ... \cdot p_t^{e_t}$

then

$$\begin{aligned}\phi(n) &= p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \cdot p_3^{e_3-1}(p_3 - 1) \cdot ... \cdot p_t^{e_t-1}(p_t - 1)\\ &= n \cdot (1 - 1/p_1) \cdot (1 - 1/p_2) \cdot (1 - 1/p_3) \cdot ... \cdot (1 - 1/p_t)\end{aligned}$$

# 11 Summary

- division $a$ to $b \geq 2$ : $r = a \mod b \Leftrightarrow a = bq + r$; with quotient $q$ and reminder $r \in Z_b = \{0, 1, 2, ..., b-1\}$

- $n = p_1^{e^1} \cdot p_1^{e^1} \cdot p_1^{e^1} ... p_t^{e^t}$ unique decomposition in to primes

- $gcd(a, b)$ = all common (intersection) primes (each with min exponent)
  $lcm(a, b)$ = union of primes (each with max exponent)
  $ab$ = all primes together (with sum of exponents)

- $gcm(a, b) \cdot lcm(a, b) = ab$

- $a \mid b$ means `‘‘`$a$ `divides` $b$`’’` same as `‘‘`$a$ `is factor of` $b$`’’` same as `‘‘`$b$ `is multiple of` $a$`’’` same as $b = ak$ for some integer $k$

- $a, b$ have the same reminder mod $n$ if and only if $n$ divides their difference : $a \mod n = b \mod n \Leftrightarrow n \mid a - b$

- if prime $p \mid ab$; then $p \mid a \vee p \mid b$

- $a, b$ are `‘‘coprimes’’` (or relatively prime) if they have no common prime factors; then $gcd(a, b) = 1$

- if $n \mid ab$ and $a, n$ coprimes $gcd(a, n) = 1$; then $n \mid b$

- if $n \mid a$ and $m \mid a$ and $gcd(n, m) = 1$; then $nm \mid a$

- after dividing $a, b$ by their $d = gcd(a, b)$, one gets coprime numbers: $gcd(\frac{a}{d}, \frac{b}{d}) = 1$

- $a$ has multiplicative inverse $b = a^{-1} \mod n$ means $ab \mod n = 1$. Thats possible if and only if $gcd(a, n) = 1$

- $a$ inverse mod $n$ (if exists) can be found as $a^{v-1}$ for integer $v$ with property $a^v = 1 \mod n$ ($v$ = root of $a$). Trying powers to obtain the root is inefficient, not practical for large $n$.

• gcd-coefficient $(k, h)$ for $(a, b)$ always exist to give the $gcd(a, b) = ak + bh$.

• if $a, b$ coprime, $1 = gcd(a, b) = ak + bh$. Then $k, h$ are the two inverses
$k = a^{-1} \mod b$ and $h = b^{-1} \mod a$

• Euclid-Extended finds $k, h$ coefficients by transforming the problem$(a, b)$ into problem$(b, r)$ recursively, and then recursively-back computing the coefficients. It is efficient, even for large $a, b$.

• Euler totient $\phi(n)$ is the size of the set $C_n$={reminders coprime with $n$}; in other words $\phi(n)$ = number of coprimes smaller than $n$.
Euler's theorem : $a^{\phi(n)} = 1 \mod n$ for any $a \in C_n$.

• So we have four ways to find $a^{-1}$, the inverse of $a \mod n$:
1) Brute force. Try different values $b < n$ until one works ($ab = 1 \mod n$)
2) Best in practice. $k, h$ = EuclidExtend$(a, n)$. Then $k = a^{-1}$ is the inverse.
3) Find root $v$ for $a$, so $a^v = 1 \mod n$ then $a^{v-1} \mod n$ is the inverse of $a$. Cant do fast exponentiation($v$ unknown); still usually faster than method 1)
4) Best if $\phi(n)$ known. $\phi(n)$ root for $a$ ($a^{\phi(n)} = 1$), so the inverse is $a^{-1} = a^{\phi(n)-1}$. Power modulo $n$ is efficient with fast exponentiation.

• For primes $p$, $\phi(p) = p - 1$ so that theorem becomes Fermats theorem $a^{p-1} = 1 \mod p$ when $(a, p)$ coprimes

• Primality Test for $n$. Try for several $a < n$ to see if $a^{n-1} \mod n = 1$.
if any of the tests(a) gives "NO", then $n$ certainly not prime
if all tests(a) gives "YES", $n$ is likely prime (rare exceptions: Carmichael numbers)

• $n = pq$ (two primes) then $\phi(n) = (p - 1(q - 1)$; so if a coprime with $n$ then $a^{\phi(n)} = a^{(p-1)(q-1)} = 1 \mod n$ or $a^{(p-1)(q-1)k+1} = a \mod n$ for any $k$

• RSA. if $n = pq$ (two large primes); $e$ and $d = e^{-1}$ are eachother inverse mod $(p - 1)(q - 1)$ means $ed = 1 \mod (p - 1)(q - 1)$.
Then $a^{ed} = a^{(p-1)(q-1)k+1} = a \mod n$.
· $n$ is known but the prime factors $p, q$ are not —and hard to find.
· RSA public key for encryption is $e$. ENCRYPT$(a) = a^e \mod n$
· RSA secret key for decryption is $d$. DECRYPT$(a^e) = (a^e)^d \mod n = a$

· RSA signature: verify that one has the correct secret key, by receiving $(a,\, b = a^d)$ and decrypting $b$ with public key $b^e = (a^d)^e \mod n = a$

• Chinese Reminder : if $p, q$ are coprime, any pair of reminders $(a \in Z_p, b \in Z_q)$ corresponds uniquely to a reminder $x \in Z_{pq}$ such that $x \mod p = a$ and $x \mod q = b$