The \textit{gcd} (greatest common divisor) of two numbers (or highest common factor), is the largest number that is a factor of both numbers.

Two numbers are \textit{relatively prime} if they have no common factor apart from 1. That is, their gcd is 1.
Calculating GCD

If we have the prime factorization of the two numbers, then to calculate their gcd:

*take the smaller power of each common prime and multiply together*
Let $d$ be a positive integer. The value $c \mod d$ is the remainder when $c$ is divided by $d$. 
Euclid’s Algorithm

To calculate gcd of $a$ and $b$:

if $b$ is a factor of $a$, then answer is $b$
else repeat with $b$ and $a \mod b$

Extended Euclid says that:
If $c$ is the gcd of $a$ and $b$, then there exist integers $s$ and $t$ such that

$$s \times a + t \times b = c.$$
Modular Addition and Multiplication

In arithmetic *modulo* \( n \), when we add, subtract, or multiply two numbers, we take the answer mod \( n \).

Specifically, \( \mathbb{Z}_n \) is the set \( \{0, 1, \ldots, n - 1\} \) with two operations:

\[
\begin{align*}
a +_n b &= (a + b) \mod n \\
a \cdot_n b &= (a \times b) \mod n
\end{align*}
\]
Modular arithmetic obeys the usual rules/laws for addition and multiplication.

We can write down *tables* for modular arithmetic.
Complete Rows in Tables

In the row for $a$ in the multiplication for $\mathbb{Z}_n$, all values are present if and only if $a$ and $n$ are relatively prime.
The **inverse** of $b$, written $b^{-1}$, is a number $y$ in $\mathbb{Z}_n$ such that $b \cdot_n y = 1$.

$b^{-1}$ exists if and only if $b$ and $n$ are relatively prime.

If an inverse exists, then it is unique.

It can sometimes be used to solve a modular equation.
Modular Exponentiation and Dexpo

The *modular exponentiation* problem is to compute $g^A \mod n$, given $g$, $A$, and $n$.

dexpo($g,A,n$) :
  if $A = 0$ then answer is 1
  else if $A$ odd
    take $z = dexpo(g, A - 1, n)$ and multiply by $g$
  else
    take $z = dexpo(g, A/2, n)$ and square it
Fermat’s little theorem says. If \( p \) is a prime, then for \( a \) with \( 1 \leq a \leq p - 1 \),
\[
a^{p-1} \mod p = 1.
\]

Extended by Euler’s theorem: \( a^\phi \mod n = 1 \) where \( \gcd(a, n) = 1 \) and \( \phi \) is how many have \( \gcd = 1 \).
**RSA Described**

The RSA cryptosystem allows Alice to send messages secretly to Bob.

1. Bob picks primes $p$ and $q$.
   
   Bob calculates $n = pq$ and $\phi = (p - 1)(q - 1)$.

2. Bob picks $a$ relatively prime to $\phi$ and uses Extended Euclid to get $b = a^{-1}$ modulo $\phi$.
   
   Bob publishes $n$ and $a$.

3. To send message $M$, Alice calculates and sends $M^a \mod n$.

4. To decrypt $N$, Bob calculates $N^b \mod n$. 

*testlet3sum: 11*