

Discrete Mathematics

Number Theory

(The study of properties of the integers)

The Basics

The quotient-remainder theorem:

Let n be an integer, and d be a positive integer. There are unique integers q, r with $0 \leq r < d$ satisfying

$$n = dq + r$$

$$n = 27, d = 6$$

$$27 = 4 \cdot 6 + 3$$

$$q = 4 \text{ and } r = \text{rem}(27, 6) = 3$$

The Basics

The quotient-remainder theorem:

Let n be an integer, and d be a positive integer. There are unique integers q, r with $0 \leq r < d$ satisfying

$$n = dq + r$$

$$n = 27, d = 6$$

$$27 = 4 \cdot 6 + 3$$

$$q = 4 \text{ and } r = \text{rem}(27, 6) = 3$$

Existence of q and r

The Basics

The quotient-remainder theorem:

Let n be an integer, and d be a positive integer. There are unique integers q, r with $0 \leq r < d$ satisfying

$$n = dq + r$$

$$n = 27, d = 6$$

$$27 = 4 \cdot 6 + 3$$

$$q = 4 \text{ and } r = \text{rem}(27, 6) = 3$$

Existence of q and r

Uniqueness of q and r

The Basics

The quotient-remainder theorem:

Let n be an integer, and d be a positive integer. There are unique integers q, r with $0 \leq r < d$ satisfying

$$n = dq + r$$

Proof: Existence

Let S be the set of nonnegative integers of the form $n - dq$, where q is an integer and $n - dq \geq 0$. The set is nonempty since $-dq$ can be made as large as needed. By the well-ordering property, S has a least element $r = n - dq_0$. The integer r is nonnegative. It also must satisfy $r < d$; otherwise, there would be a smaller nonnegative element in S , namely, $n - d(q_0 + 1) = n - dq_0 - d = r - d > 0$. Therefore, there are integers q and r with $0 \leq r < d$. ■

The Basics

The quotient-remainder theorem:

Let n be an integer, and d be a positive integer. There are unique integers q, r with $0 \leq r < d$ satisfying

$$n = dq + r$$

Proof: Uniqueness

Suppose there are two such pairs (q, r) and (q_0, r_0) , so that $a = dq + r$, and $a = dq_0 + r_0$ with $0 \leq r, r_0 < d$. Then $d(q - q_0) = r_0 - r$, and consequently $d \mid (r_0 - r)$. But $|r_0 - r| < d$ (since both r_0 and r are nonnegative integers less than d), we must have $r_0 - r = 0$, i.e., $r = r_0$. Finally, $q = (a - r)/d = (a - r_0)/d = q_0$. ■

The Basics

The quotient-remainder theorem:

Let n be an integer, and d be a positive integer. There are unique integers q, r with $0 \leq r < d$ satisfying

$$n = dq + r$$

$$n = 24, d = 6$$

$$24 = 4 \cdot 6 + 0$$

$$q = 4 \text{ and } \text{rem}(27, 6) = 0$$

The Basics

Divisibility. d divides n , $d|n$ if and only if $n = qd$ for some $q \in \mathbb{Z}$.

$$n = 24, d = 6$$

6 divides 24, $6|24$, iff $24 = 4 \cdot 6$ where 4 is an integer.

The Basics

Primes. $P = \{2, 3, 5, 7, 11, \dots\} = \{ p \mid p \geq 2 \text{ and the only positive divisors of } p \text{ are } 1 \text{ and } p \}$

The Basics

Division Facts

1. $d|0$.
2. If $d|m$ and $d'|n$, then $dd'|mn$.
3. If $d|m$ and $m|n$, then $d|n$.
4. If $d|n$ and $d|m$, then $d|n + m$.
5. If $d|n$, then $xd|xn$ for $x \in \mathbb{N}$.
6. If $d|m + n$ and $d|m$, then $d|n$.

The Basics

Division Facts

1. $d|0$.
2. If $d|m$ and $d'|n$, then $dd'|mn$.
3. If $d|m$ and $m|n$, then $d|n$.
4. If $d|n$ and $d|m$, then $d|n + m$.
5. If $d|n$, then $xd|xn$ for $x \in \mathbb{N}$.
6. If $d|m + n$ and $d|m$, then $d|n$.

Proof:

$0 = 0 \cdot d$ ($q = 0$), so $d|0$. ■

The Basics

Division Facts

1. $d|0$.
2. If $d|m$ and $d'|n$, then $dd'|mn$.
3. If $d|m$ and $m|n$, then $d|n$.
4. If $d|n$ and $d|m$, then $d|n + m$.
5. If $d|n$, then $xd|xn$ for $x \in \mathbb{N}$.
6. If $d|m + n$ and $d|m$, then $d|n$.

Proof:

Suppose $d|m$ and $d'|n$, so $m = qd$ and $n = q'd'$.

Then $mn = (qq')dd'$. That is $dd'|mn$ (quotient = qq'). ■

The Basics

Division Facts

1. $d|0$.
2. If $d|m$ and $d'|n$, then $dd'|mn$.
3. If $d|m$ and $m|n$, then $d|n$.
4. If $d|n$ and $d|m$, then $d|n + m$.
5. If $d|n$, then $xd|xn$ for $x \in \mathbb{N}$.
6. If $d|m + n$ and $d|m$, then $d|n$

Proof:

Suppose $d|m$ and $m|n$, so $m = qd$ and $n = q'm$.

Then, $n = q'qd$ so $d|n$ (quotient = $q'q$). ■

The Basics

Division Facts

1. $d \mid 0$.
2. If $d \mid m$ and $d' \mid n$, then $dd' \mid mn$.
3. If $d \mid m$ and $m \mid n$, then $d \mid n$.
4. If $d \mid n$ and $d \mid m$, then $d \mid n + m$.
5. If $d \mid n$, then $xd \mid xn$ for $x \in \mathbb{N}$.
6. If $d \mid m + n$ and $d \mid m$, then $d \mid n$.

Proof:

Suppose $d \mid n$ and $d \mid m$, so $n = qd$ and $m = q'd$.

Then $n + m = (q + q')d$.

That is $d \mid n + m$ (quotient = $q + q'$). ■

The Basics

Division Facts

1. $d|0$.
2. If $d|m$ and $d'|n$, then $dd'|mn$.
3. If $d|m$ and $m|n$, then $d|n$.
4. If $d|n$ and $d|m$, then $d|n + m$.
5. If $d|n$, then $xd|xn$ for $x \in \mathbb{N}$.
6. If $d|m + n$ and $d|m$, then $d|n$.

Proof:

Suppose $d|n$, so $n = qd$.

For $x \in \mathbb{N}$, $xn = qxd$, so $xd|xn$ (quotient = q). ■

The Basics

Division Facts

1. $d|0$.
2. If $d|m$ and $d'|n$, then $dd'|mn$.
3. If $d|m$ and $m|n$, then $d|n$.
4. If $d|n$ and $d|m$, then $d|n + m$.
5. If $d|n$, then $xd|xn$ for $x \in \mathbb{N}$.
6. If $d|m + n$ and $d|m$, then $d|n$

Proof:

Suppose $d|m + n$ and $d|m$, so $m + n = qd$ and $m = q'd$.

Then, $n = qd - m = qd - q'd = (q - q')d$.

That is $d|n$ (quotient = $q - q'$). ■

Greatest Common Divisor

Divisors of 30: {1, 2, 3, 5, 6, 10, 15, 30}.

Divisors of 42: {1, 2, 3, 6, 7, 14, 21, 42}.

Common divisors: {1, 2, 3, 6}.

Greatest common divisor (GCD) = 6.

Greatest Common Divisor

Divisors of 30: {1, 2, 3, 5, 6, 10, 15, 30}.

Divisors of 42: {1, 2, 3, 6, 7, 14, 21, 42}.

Common divisors: {1, 2, 3, 6}.

Greatest common divisor (GCD) = 6.

Let m and n be two integers not both zero. The greatest common divisor $\gcd(m, n)$ is the largest integer that divides both m and n . Any other common divisor, dividing both m and n , is smaller than $\gcd(m, n)$.

That is. (i) $\gcd(m, n) \mid m$ and $\gcd(m, n) \mid n$ and

(ii) $d \mid m$ AND $d \mid n \Rightarrow d \leq \gcd(m, n)$

Note that:

(1) every common divisor divides the GCD, and

(2) $\gcd(m, n) = \gcd(n, m)$.

Greatest Common Divisor

Relatively Prime. If $\gcd(m, n) = 1$, then m, n are relatively prime.

6 and 35 are relatively prime because $\gcd(6, 35) = 1$.

Greatest Common Divisor

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

Proof:

We prove it in two steps:

- (i) Show $\gcd(m, n) \leq \gcd(r, n)$ and
- (ii) Show $\gcd(m, n) \geq \gcd(r, m)$.

Greatest Common Divisor

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

Proof:

We prove it in two steps:

- (i) Show $\gcd(m, n) \leq \gcd(r, m)$ and
- (ii) Show $\gcd(m, n) \geq \gcd(r, m)$.

(i) $\gcd(m, n)$ divides $r = n - qm$ because it divides n and m (the RHS).
Therefore, $\gcd(m, n)$ is a common divisor of r and m , which means $\gcd(m, n) \leq \gcd(r, m)$.

Greatest Common Divisor

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

Proof:

We prove it in two steps:

- (i) Show $\gcd(m, n) \leq \gcd(r, m)$ and
- (ii) Show $\gcd(m, n) \geq \gcd(r, m)$.

- (i) $\gcd(m, n)$ divides $r = n - qm$ because it divides n and m (the RHS).
Therefore, $\gcd(m, n)$ is a common divisor of r and m , which means $\gcd(m, n) \leq \gcd(r, m)$.
- (ii) $\gcd(r, m)$ divides $n = qm + r$ because it divides m and r (the RHS).
Therefore, $\gcd(r, m)$ is a common divisor of m and n . which means $\gcd(r, m) \leq \gcd(m, n)$. ■

Euclid's Algorithm

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

$$\gcd(42, 108) = \gcd(24, 42) \quad 24 = 108 - 2 \cdot 42$$

Euclid's Algorithm

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\ &= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108}\end{aligned}$$

Euclid's Algorithm

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\ &= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108} \\ &= \gcd(6, 18) & \color{red}{6} &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot \mathbf{108} - 5 \cdot \mathbf{42}\end{aligned}$$

Euclid's Algorithm

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\ &= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108} \\ &= \gcd(6, 18) & \color{red}{6} &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot \mathbf{108} - 5 \cdot \mathbf{42} \\ &= \gcd(0, 6) & \color{red}{0} &= 18 - 3 \cdot 6\end{aligned}$$

Euclid's Algorithm

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\ &= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108} \\ &= \gcd(6, 18) & \color{red}{6} &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot \mathbf{108} - 5 \cdot \mathbf{42} \\ &= \gcd(0, 6) & \color{red}{0} &= 18 - 3 \cdot 6 \\ &= 6 & \gcd(0, n) &= n\end{aligned}$$

Euclid's Algorithm

Theorem: $\gcd(m, n) = \gcd(r, m)$ where $r = \text{rem}(n, m)$.

Input: Two positive integers, m and n .

Output: The greatest common divisor, \gcd of m and n .

Internal computation:

1. If $m > n$, exchange m and n .
2. Divide n by m and get the remainder, r . If $r=0$, report n as the GCD of m and n .
3. Replace n by m and replace m by r . Return to the previous step.

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & 24 &= 108 - 2 \cdot 42 \\ &= \gcd(18, 24) & 18 &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot 42 - 108 \\ &= \gcd(6, 18) & 6 &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot 108 - 5 \cdot 42 \\ &= \gcd(0, 6) & 0 &= 18 - 3 \cdot 6 \\ &= 6 & \gcd(0, n) &= n\end{aligned}$$

Euclid's Algorithm

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\ &= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108} \\ &= \gcd(6, 18) & \color{red}{6} &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot \mathbf{108} - 5 \cdot \mathbf{42} \\ &= \gcd(0, 6) & \color{red}{0} &= 18 - 3 \cdot 6 \\ &= 6 & \gcd(0, n) &= n\end{aligned}$$

Remainders in Euclid's algorithm are integer linear combinations of 42 and 108.

Euclid's Algorithm

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\&= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108} \\&= \gcd(6, 18) & \color{red}{6} &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot \mathbf{108} - 5 \cdot \mathbf{42} \\&= \gcd(0, 6) & \color{red}{0} &= 18 - 3 \cdot 6 \\&= 6 & \gcd(0, n) &= n\end{aligned}$$

Remainders in Euclid's algorithm are integer linear combinations of 42 and 108.

In particular, $\gcd(42, 108) = 6 = 2 \times 108 - 5 \times 42$.

Euclid's Algorithm

$$\begin{aligned}\gcd(42, 108) &= \gcd(24, 42) & \color{red}{24} &= \mathbf{108} - 2 \cdot \mathbf{42} \\ &= \gcd(18, 24) & \color{red}{18} &= 42 - 24 = 42 - \underbrace{(108 - 2 \cdot 42)}_{24} = 3 \cdot \mathbf{42} - \mathbf{108} \\ &= \gcd(6, 18) & \color{red}{6} &= 24 - 18 = \underbrace{(108 - 2 \cdot 42)}_{24} - \underbrace{(3 \cdot 42 - 108)}_{18} = 2 \cdot \mathbf{108} - 5 \cdot \mathbf{42} \\ &= \gcd(0, 6) & \color{red}{0} &= 18 - 3 \cdot 6 \\ &= 6 & \gcd(0, n) &= n\end{aligned}$$

Remainders in Euclid's algorithm are integer linear combinations of 42 and 108.

In particular, $\gcd(42, 108) = 6 = 2 \times 108 - 5 \times 42$.

This will be true for $\gcd(m, n)$ in general:

$$\gcd(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Bezout's Identity

From Euclid's Algorithm,

$$\gcd(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Bezout's Identity

From Euclid's Algorithm,

$$\gcd(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Can any smaller positive number z be a linear combination of m and n ?

suppose: $z = mx + ny > 0.$

Bezout's Identity

From Euclid's Algorithm,

$$\gcd(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Can any smaller positive number z be a linear combination of m and n ?

$$\text{suppose:} \quad z = mx + ny > 0.$$

$\gcd(m, n)$ divides RHS $\rightarrow \gcd(m, n) | z$, i.e. $z \geq \gcd(m, n)$ (because $\gcd(m, n) | m$ and $\gcd(m, n) | n$).

Bezout's Identity

From Euclid's Algorithm,

$$\gcd(m, n) = mx + ny \quad \text{for some } x, y \in \mathbb{Z}.$$

Can any smaller positive number z be a linear combination of m and n ?

$$\text{suppose:} \quad z = mx + ny > 0.$$

$\gcd(m, n)$ divides RHS $\rightarrow \gcd(m, n) | z$, i.e. $z \geq \gcd(m, n)$ (because $\gcd(m, n) | m$ and $\gcd(m, n) | n$).

Bezout's Identity. The GCD of m and n is the smallest positive linear combination of m and n with integer coefficients. For some integers x, y , $\gcd(m, n) = mx + ny$.

Bezout's Identity

The GCD of m and n is **the smallest positive linear combination** of m and n with integer coefficients. For some integers x, y , $\gcd(m, n) = mx + ny$.

Proof:

Let $g = \gcd(m, n)$ and d be the smallest positive linear combination of m and n .

We want to show that $g = d$, that is (i) $g \leq d$ and (ii) $g \geq d$.

Bezout's Identity

The GCD of m and n is **the smallest positive linear combination** of m and n with integer coefficients. For some integers x, y , $\gcd(m, n) = mx + ny$.

Proof:

Let $g = \gcd(m, n)$ and d be the smallest positive linear combination of m and n .

We want to show that $g = d$, that is **(i) $g \leq d$** and **(ii) $d \leq g$** .

(i) Since $g \mid d$, then $g \leq d$.

Bezout's Identity

The GCD of m and n is **the smallest positive linear combination** of m and n with integer coefficients. For some integers x, y , $\gcd(m, n) = mx + ny$.

Proof:

Let $g = \gcd(m, n)$ and d be the smallest positive linear combination of m and n .

We want to show that $g = d$, that is (i) $g \leq d$ and (ii) $d \leq g$.

(i) Since $g \mid d$, then $g \leq d$.

(ii) To show $d \leq g$, we show that d is a common divisor of m, n , i.e. $\text{rem}(m, d) = \text{rem}(n, d) = 0 \Rightarrow d \mid m$ and $d \mid n$. By the quotient-remainder theorem, $m = qd + r$ where $0 \leq r < d$. Then, $r = m - qd = m - q(mx + ny) = m(1 - qx) - n(qy)$, where r is a positive linear combination of m, n which is less than d . Since d is the smallest, r must be 0. Therefore, $d \mid m$. Similarly, if $n = q'd + r'$, then $r' = 0$ and $d \mid n$. ■

GCD Facts

Every common divisor of m, n divides $\gcd(m, n)$.

Proof.

$\gcd(m, n) = mx + ny$. Any common divisor divides the RHS and so also the LHS. ■

Example: 1,2,3,6 are common divisors of 30,42 and all divide the GCD 6

GCD Facts

For $k \in \mathbb{N}$, $\gcd(km, kn) = k \cdot \gcd(m, n)$.

Proof.

$\gcd(km, kn) = kmx + kny = k(mx + ny)$. The RHS is the smallest possible, so there is no smaller positive linear combination of m, n .

That is $\gcd(m, n) = (mx + ny)$. ■

Example. $\gcd(6, 15) = 3 \rightarrow \gcd(12, 30) = 2 \times 3 = 6$

GCD Facts

if $\gcd(\ell, m) = 1$ and $\gcd(\ell, n) = 1$, then $\gcd(\ell, mn) = 1$.

Proof.

$$1 = \ell x + my \text{ and } 1 = \ell x' + ny'.$$

$$\begin{aligned} \text{Multiplying, } 1 &= (\ell x + my)(\ell x' + ny') \\ &= \ell \cdot (\ell x x' + n x y' + m y x') + mn \cdot (y y'). \end{aligned}$$

Example. $\gcd(15, 4) = 1$ and $\gcd(15, 7) = 1 \rightarrow \gcd(15, 28) = 1$

GCD Facts

if $d|mn$ and $\gcd(d, m) = 1$, then $d|n$.

Proof.

$$dx + my = 1 \rightarrow ndx + nmy = n.$$

Since $d|mn$, d divides the LHS,
hence $d|n$, the RHS. ■

Example. $\gcd(4, 15) = 1$ and $4|(15 \times 16) \rightarrow 4|16$

Die Hard: The movie

<https://www.youtube.com/watch?v=2vdF6NASMiE>

The diabolical Simon G ruber asks John McClane & Zeus Carver to use 3 and 5-gallonjugs to measure 4 gallons, or else a bomb explodes.

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

(0, 0)

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0) \xrightarrow{1} (3, 0)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)1: \rightarrow (3, 3)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)1: \rightarrow (3, 3)2: \rightarrow (1, 5)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)1: \rightarrow (3, 3)2: \rightarrow (1, 5)3: \rightarrow (1, 0)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)1: \rightarrow (3, 3)2: \rightarrow (1, 5)3: \rightarrow (1, 0)2: \rightarrow (0, 1)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)1: \rightarrow (3, 3)2: \rightarrow (1, 5)3: \rightarrow (1, 0)2: \rightarrow (0, 1)1: \rightarrow (3, 1)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0)1: \rightarrow (3, 0)2: \rightarrow (0, 3)1: \rightarrow (3, 3)2: \rightarrow (1, 5)3: \rightarrow (1, 0)2: \rightarrow (0, 1)1: \rightarrow (3, 1)2: \rightarrow (0, 4)$

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1) \xrightarrow{1} (3, 1) \xrightarrow{2} (0, 4)$

After the 3-gallon jug is emptied into the 5-gallon jug, the state is $(0, \ell)$, where

$\ell = 3x - 5y$.

(the 3-gallon jug has been emptied x times and
the 5-gallon jug y times)

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1) \xrightarrow{1} (3, 1) \xrightarrow{2} (0, 4)$

After the 3-gallon jug is emptied into the 5-gallon jug, the state is $(0, \ell)$, where

$\ell = 3x - 5y$.

(the 3-gallon jug has been emptied x times and the 5-gallon jug y times)

Since ℓ is integer linear combination of 3, 5 and Since $\gcd(3, 5) = 1$ we can get $\ell = 1$,

$1 = 3 \cdot 2 - 5 \cdot 1$

(after emptying the 3-gallon jug 2 times and the 5 gallon jug once, there is 1 gallon)

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1) \xrightarrow{1} (3, 1) \xrightarrow{2} (0, 4)$

After the 3-gallon jug is emptied into the 5-gallon jug, the state is $(0, \ell)$, where

$\ell = 3x - 5y$.

(the 3-gallon jug has been emptied x times and the 5-gallon jug y times)

Since ℓ is integer linear combination of 3, 5 and Since $\gcd(3, 5) = 1$ we can get $\ell = 1$,

$1 = 3 \cdot 2 - 5 \cdot 1$

(after emptying the 3-gallon jug 2 times and the 5 gallon jug once, there is 1 gallon)

$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1)$

Do this 4 times and you have 4 gallons (guaranteed). (Actually fewer pours works.)

Die Hard: The movie

Given 3 and 5-gallon jugs, measure exactly 4 gallons.

1: Repeatedly fill the 3-gallon jug.

2: Empty the 3-gallon jug into the 5-gallon jug.

3: If ever the 5-gallon jug is full, empty it by discarding the water.

$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1) \xrightarrow{1} (3, 1) \xrightarrow{2} (0, 4)$

After the 3-gallon jug is emptied into the 5-gallon jug, the state is $(0, \ell)$, where

$\ell = 3x - 5y$.

(the 3-gallon jug has been emptied x times and the 5-gallon jug y times)

Since ℓ is integer linear combination of 3, 5 and Since $\gcd(3, 5) = 1$ we can get $\ell = 1$,

$1 = 3 \cdot 2 - 5 \cdot 1$

(after emptying the 3-gallon jug 2 times and the 5 gallon jug once, there is 1 gallon)

$(0, 0) \xrightarrow{1} (3, 0) \xrightarrow{2} (0, 3) \xrightarrow{1} (3, 3) \xrightarrow{2} (1, 5) \xrightarrow{3} (1, 0) \xrightarrow{2} (0, 1)$

Do this 4 times and you have 4 gallons (guaranteed). (Actually fewer pours works.)

For any jug problem with jugs of capacities X and Y with $g = \gcd(X, Y)$, you can only end up with quantities of water that are multiples of g after any number of operations

Fundamental Theorem of Arithmetic

Euclid's Lemma:

For primes $p, q_1, q_2, \dots, q_\ell$, if $p \mid q_1 q_2 \dots q_\ell$ then p is one of the q .

Fundamental Theorem of Arithmetic

Euclid's Lemma:

For primes $p, q_1, q_2, \dots, q_\ell$, if $p \mid q_1 q_2 \dots q_\ell$ then p is one of the q .

Proof:

If $p \mid q_\ell$ then $p = q_\ell$. If not, $\gcd(p, q_\ell) = 1$ and $p \mid q_1 \cdot \dots \cdot q_{\ell-1}$. ■

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Let $a > 1$ be the smallest integer that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the p_i and q_j are all primes. (We allow repetitions among the p_i and q_j . That way, we don't have to use exponents.)

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Let $a > 1$ be the smallest integer that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the p_i and q_j are all primes. (We allow repetitions among the p_i and q_j . That way, we don't have to use exponents.)

Then $p_1 \mid a = q_1 \cdots q_t$. Since p_1 is prime, by the Euclid's Lemma, $p_1 \mid q_j$ for some j . Since q_j is prime and $p_1 > 1$, this means that $p_1 = q_j$. For convenience, we may renumber the q_j so that $p_1 = q_1$.

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Let $a > 1$ be the smallest integer that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the p_i and q_j are all primes. (We allow repetitions among the p_i and q_j . That way, we don't have to use exponents.)

Then $p_1 \mid a = q_1 \cdots q_t$. Since p_1 is prime, by the Euclid's Lemma, $p_1 \mid q_j$ for some j . Since q_j is prime and $p_1 > 1$, this means that $p_1 = q_j$. For convenience, we may renumber the q_j so that $p_1 = q_1$.

We can now cancel p_1 from both sides of the equation above to get $p_2 \cdots p_s = q_2 \cdots q_t$.

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Let $a > 1$ be the smallest integer that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the p_i and q_j are all primes. (We allow repetitions among the p_i and q_j . That way, we don't have to use exponents.)

Then $p_1 \mid a = q_1 \cdots q_t$. Since p_1 is prime, by the Euclid's Lemma, $p_1 \mid q_j$ for some j . Since q_j is prime and $p_1 > 1$, this means that $p_1 = q_j$. For convenience, we may renumber the q_j so that $p_1 = q_1$.

We can now cancel p_1 from both sides of the equation above to get $p_2 \cdots p_s = q_2 \cdots q_t$. But $p_2 \cdots p_s < a$ and by assumption a is the smallest positive integer with a non-unique prime factorization. It follows that $s = t$ and that $p_2 \cdots p_s$ are the same as $q_2 \cdots q_t$, except possibly in a different order.

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Let $a > 1$ be the smallest integer that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the p_i and q_j are all primes. (We allow repetitions among the p_i and q_j . That way, we don't have to use exponents.)

Then $p_1 \mid a = q_1 \cdots q_t$. Since p_1 is prime, by the Euclid's Lemma, $p_1 \mid q_j$ for some j . Since q_j is prime and $p_1 > 1$, this means that $p_1 = q_j$. For convenience, we may renumber the q_j so that $p_1 = q_1$.

We can now cancel p_1 from both sides of the equation above to get $p_2 \cdots p_s = q_2 \cdots q_t$. But $p_2 \cdots p_s < a$ and by assumption a is the smallest positive integer with a non-unique prime factorization. It follows that $s = t$ and that $p_2 \cdots p_s$ are the same as $q_2 \cdots q_t$, except possibly in a different order.

But since $p_1 = q_1$ as well, this is a contradiction to the assumption that these were two different factorizations.

Fundamental Theorem of Arithmetic

Theorem. Uniqueness of Prime Factorization

Every $n \geq 2$ is uniquely (up to reordering) a product of primes.

Proof: Contradiction.

Let $a > 1$ be the smallest integer that has two different prime factorizations, say $a = p_1 \cdots p_s = q_1 \cdots q_t$, where the p_i and q_j are all primes. (We allow repetitions among the p_i and q_j . That way, we don't have to use exponents.)

Then $p_1 \mid a = q_1 \cdots q_t$. Since p_1 is prime, by the Euclid's Lemma, $p_1 \mid q_j$ for some j . Since q_j is prime and $p_1 > 1$, this means that $p_1 = q_j$. For convenience, we may renumber the q_j so that $p_1 = q_1$.

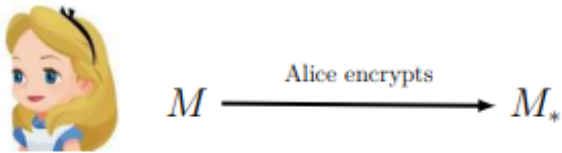
We can now cancel p_1 from both sides of the equation above to get $p_2 \cdots p_s = q_2 \cdots q_t$. But $p_2 \cdots p_s < a$ and by assumption a is the smallest positive integer with a non-unique prime factorization. It follows that $s = t$ and that $p_2 \cdots p_s$ are the same as $q_2 \cdots q_t$, except possibly in a different order.

But since $p_1 = q_1$ as well, this is a contradiction to the assumption that these were two different factorizations.

Thus there cannot exist such an integer a with two different factorizations. ■

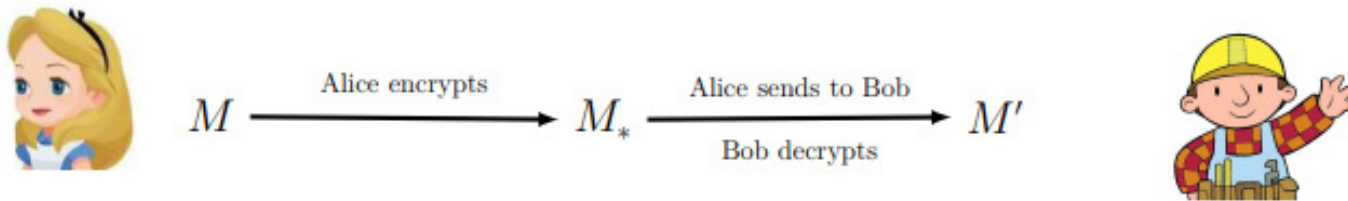
Cryptography 101:

Alice and Bob wish to securely exchange the prime M



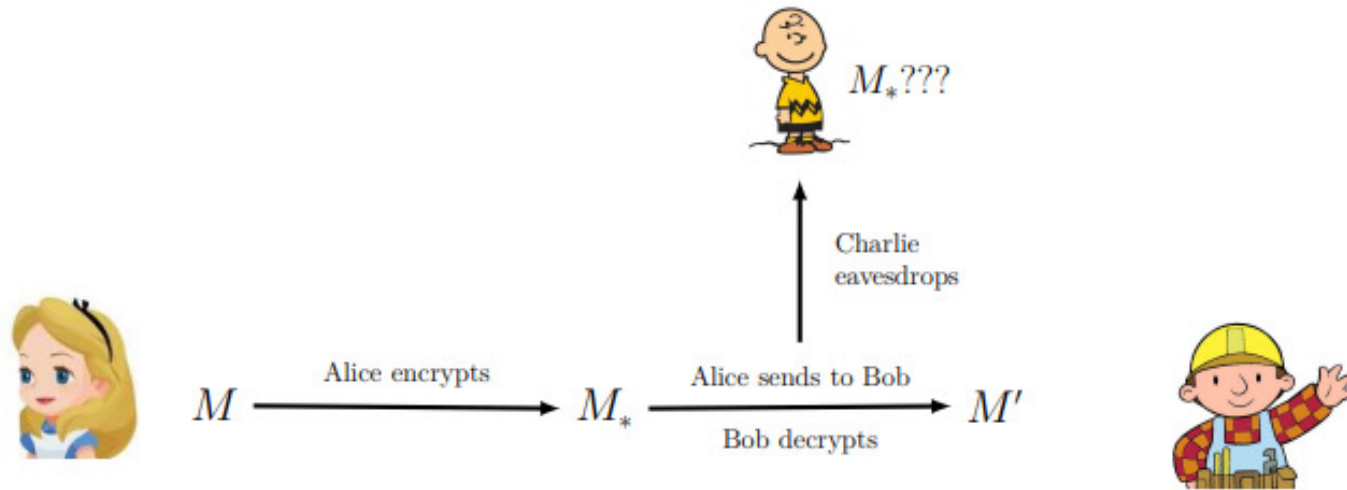
Cryptography 101:

Alice and Bob wish to securely exchange the prime M



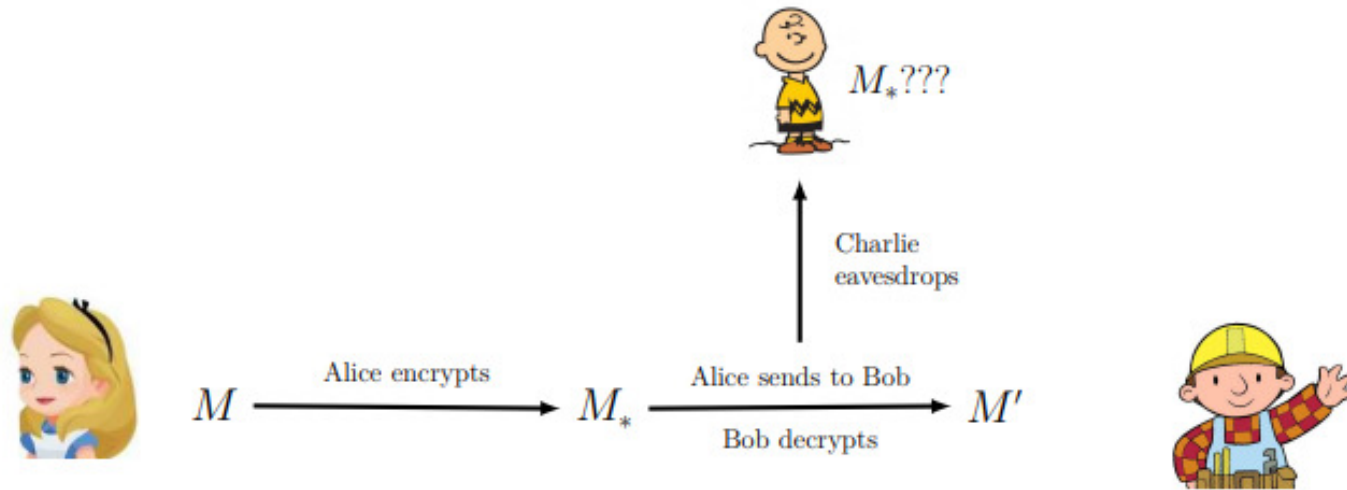
Cryptography 101:

Alice and Bob wish to securely exchange the prime M



Cryptography 101:

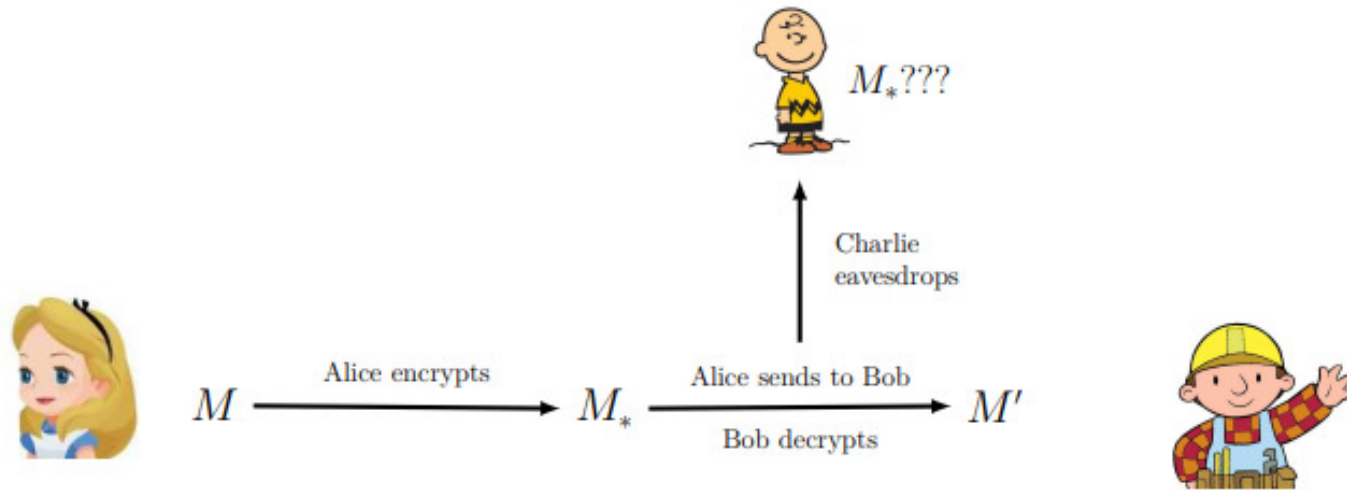
Alice and Bob wish to securely exchange the prime M



Example. Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)

Cryptography 101:

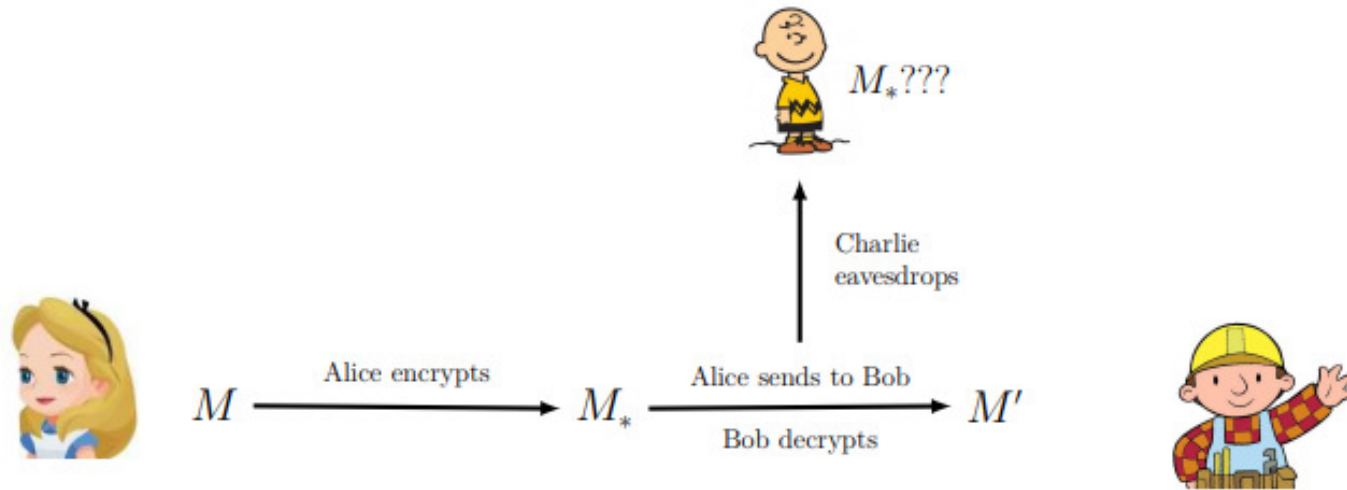
Alice and Bob wish to securely exchange the prime M



Example. Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)
Alice and Bob know k , Charlie does not.

Cryptography 101:

Alice and Bob wish to securely exchange the prime M

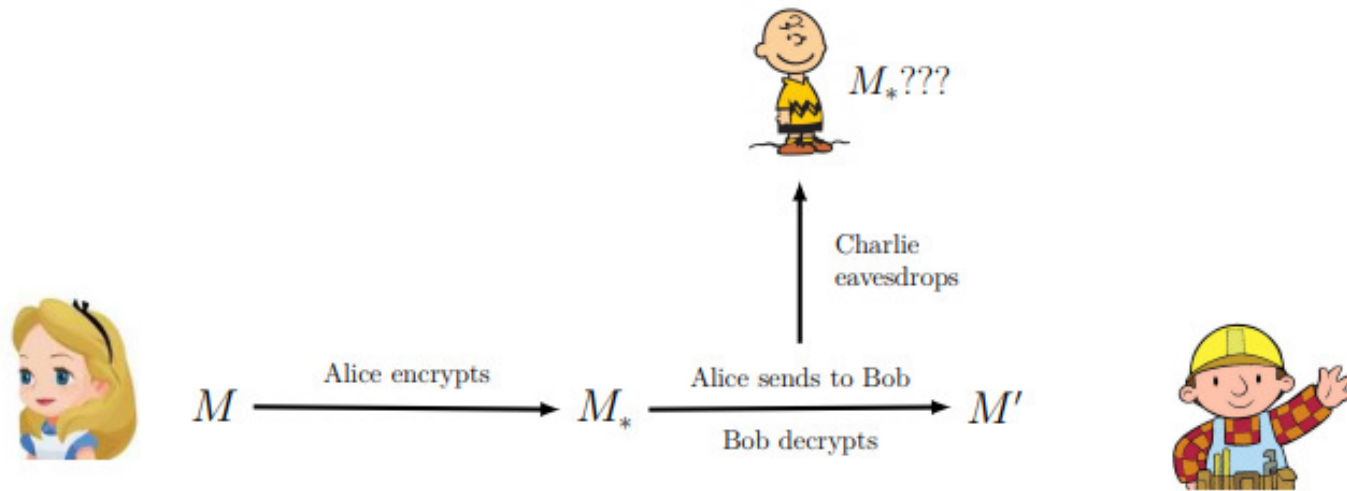


Example. Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)
Alice and Bob know k, Charlie does not.

Bob Decrypts: $M' = M_*/k = M \times k/k = M$. ($M' = M$ and Charlie is in the dark.)

Cryptography 101:

Alice and Bob wish to securely exchange the prime M



Example. Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)

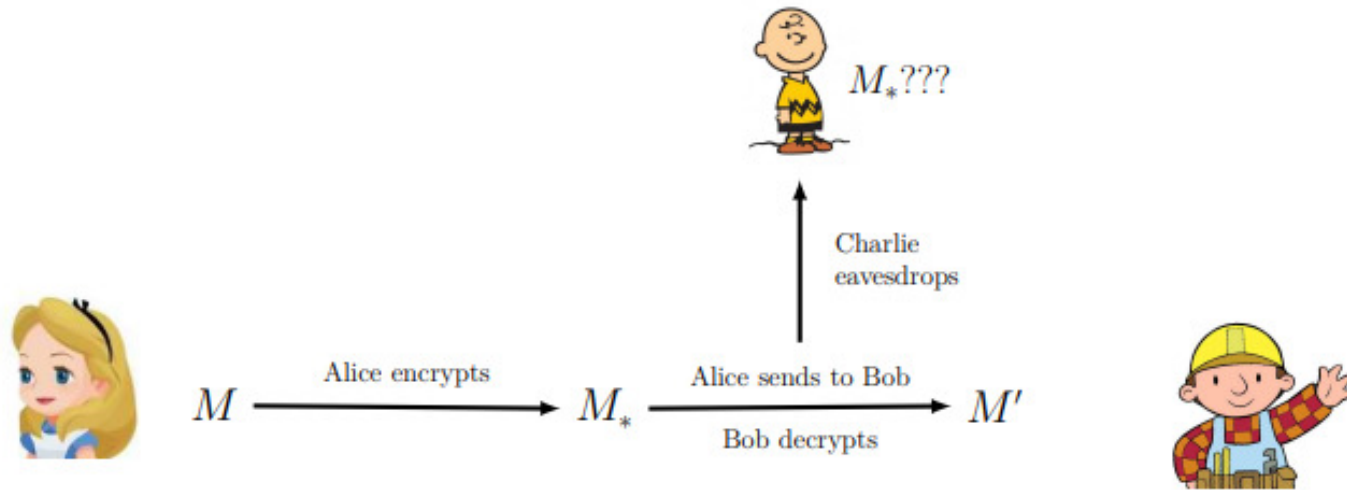
Alice and Bob know k , Charlie does not.

Bob Decrypts: $M' = M_*/k = M \times k/k = M$. ($M' = M$ and Charlie is in the dark.)

Secure as long as Charlie cannot factor M' into k and M . (Factoring is hard)

Cryptography 101:

Alice and Bob wish to securely exchange the prime M



Example. Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)

Alice and Bob know k , Charlie does not.

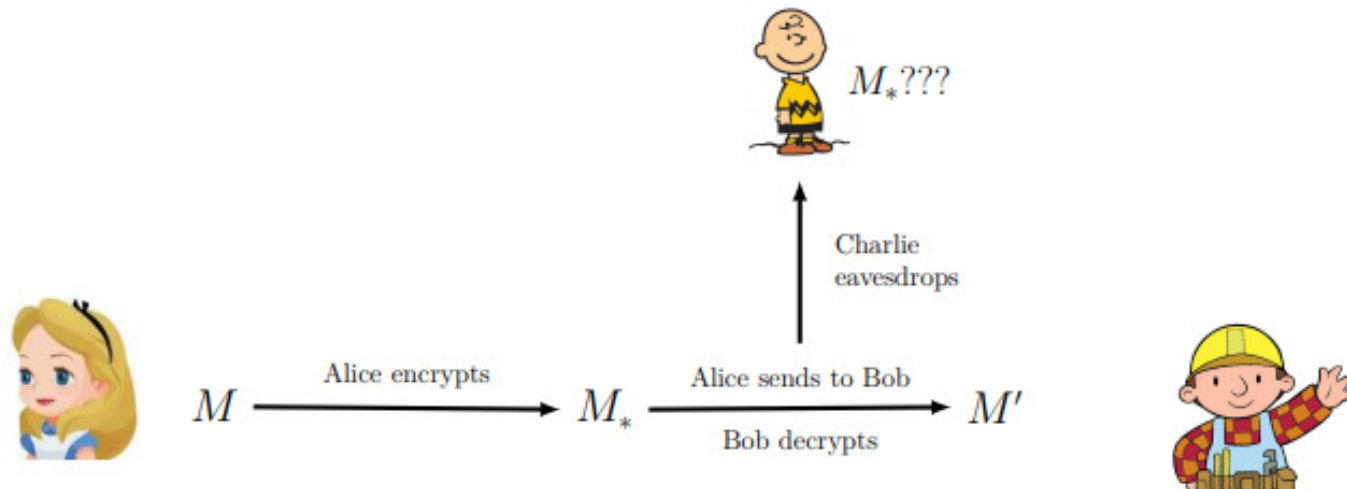
Bob Decrypts: $M' = M_*/k = M \times k/k = M$. ($M' = M$ and Charlie is in the dark.)

Secure as long as Charlie cannot factor M' into k and M . (Factoring is hard)

If Charlie can find $k = \gcd(M_{1*}, M_{2*})$, then this is not secure.

Cryptography 101:

Alice and Bob wish to securely exchange the prime M



Example. Alice Encrypts: $M_* = M \times k$ (k is a shared secret – private key)

Alice and Bob know k, Charlie does not.

Bob Decrypts: $M' = M_*/k = M \times k/k = M$. ($M' = M$ and Charlie is in the dark.)

Secure as long as Charlie cannot factor M' into k and M. (Factoring is hard)

If Charlie can find $k = \gcd(M_{1*}, M_{2*})$, then this is not secure.

To improve, we need modular arithmetic.

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$41 \equiv 79 \pmod{19}$ because $41 - 79 = -38 = -2 \cdot 19$.

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Proof (i)

$$\begin{aligned} ar - bs &= (b + kd)(s + \ell d) - bs \\ &= d(ks + b\ell + k\ell d). \end{aligned}$$

That is $d \mid ar - bs$. ■

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Proof (ii)

$$(a + r) - (b + s) = (b + kd + s + \ell d) - b - s = d(k + \ell).$$

That is $d \mid (a + r) - (b + s)$. ■

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$41 \equiv 79 \pmod{19}$ because $41 - 79 = -38 = -2 \cdot 19$.

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Proof (iii)

Base Case: When $n = 1$, we are given that $a \equiv b \pmod{d}$.

Inductive Hypothesis: Suppose $a^k \equiv b^k \pmod{d}$.

Inductive Step: Applying (a) with $r = a^k$ and $s = b^k$, we get $a^{k+1} \equiv b^{k+1} \pmod{d}$.

By induction, $a^n \equiv b^n \pmod{d}$ for $n \geq 1$. ■

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Example. What is the last digit of 3^{2017} ?

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Example. What is the last digit of 3^{2017} ?

$$3^2 \equiv -1 \pmod{10}$$

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Example. What is the last digit of 3^{2017} ?

$$\begin{aligned} 3^2 &\equiv -1 \pmod{10} \\ (3^2)^{1008} &\equiv (-1)^{1008} \pmod{10} \end{aligned}$$

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Example. What is the last digit of 3^{2017} ?

$$3^2 \equiv -1 \pmod{10}$$

$$(3^2)^{1008} \equiv (-1)^{1008} \pmod{10}$$

$$3 \cdot (3^2)^{1008} \equiv 3 \cdot (-1)^{1008} \pmod{10}$$

Modular Arithmetic

$a \equiv b \pmod{d}$ if and only if $d \mid (a - b)$, i.e. $a - b = kd$ for $k \in \mathbb{Z}$

$$41 \equiv 79 \pmod{19} \quad \text{because} \quad 41 - 79 = -38 = -2 \cdot 19.$$

Modular Equivalence Properties.

Suppose $a \equiv b \pmod{d}$, i.e. $a = b + kd$, and $r \equiv s \pmod{d}$, i.e. $r = s + \ell d$.

(i) $ar \equiv bs \pmod{d}$. (ii) $a + r \equiv b + s \pmod{d}$. (iii) $a^n \equiv b^n \pmod{d}$.

Example. What is the last digit of 3^{2017} ?

$$\begin{aligned} 3^2 &\equiv -1 \pmod{10} \\ (3^2)^{1008} &\equiv (-1)^{1008} \pmod{10} \\ 3 \cdot (3^2)^{1008} &\equiv 3 \cdot (-1)^{1008} \pmod{10} \\ &\equiv 3 \end{aligned}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

$$7 \equiv 22 \pmod{15}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

$$7 \equiv 22 \pmod{15}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

$$7 \equiv 22 \pmod{15}$$

Observe:

$$\gcd(6,12) = 6$$

$$\gcd(6,13) = 1$$

$$\gcd(8,15) = 1$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

Suppose $ac \equiv bc \pmod{d}$. You can cancel c to get $a \equiv b \pmod{d}$ if $\gcd(c, d) = 1$.

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

$$7 \equiv 22 \pmod{15}$$

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

$$7 \equiv 22 \pmod{15}$$

Suppose $ac \equiv bc \pmod{d}$. You can cancel c to get $a \equiv b \pmod{d}$ if $\gcd(c, d) = 1$.

Proof. $d \mid c(a - b)$. By GCD fact, $d \mid a - b$ because $\gcd(c, d) = 1$. ■

Modular Division

$$90 \equiv 78 \pmod{12}$$

$$15 \cdot 6 \equiv 13 \cdot 6 \pmod{12}$$

We cannot conclude that $15 \equiv 13 \pmod{12}$

$$90 \equiv 12 \pmod{13}$$

$$15 \cdot 6 \equiv 2 \cdot 6 \pmod{13}$$

$$15 \equiv 2 \pmod{13}$$

$$56 \equiv 176 \pmod{15}$$

$$7 \cdot 8 \equiv 22 \cdot 8 \pmod{15}$$

$$7 \equiv 22 \pmod{15}$$

Suppose $ac \equiv bc \pmod{d}$. You can cancel c to get $a \equiv b \pmod{d}$ if $\gcd(c, d) = 1$.

Proof. $d \mid c(a - b)$. By GCD fact, $d \mid a - b$ because $\gcd(c, d) = 1$. ■

If d is prime, then division with prime modulus is pretty much like regular division.

Modular Multiplicative Inverse

A Modular Multiplicative Inverse of an integer a modulo d is an integer n such that

$$a \times n \equiv 1 \pmod{d}.$$

Modular Multiplicative Inverse

A Modular Multiplicative Inverse of an integer a modulo d is an integer n such that

$$a \times n \equiv 1 \pmod{d}.$$

Inverse of 3 modulo 7 is n such that:

$$3 \times n \equiv 1 \pmod{7} \quad n = 5$$

Modular Multiplicative Inverse

A Modular Multiplicative Inverse of an integer a modulo d is an integer n such that

$$a \times n \equiv 1 \pmod{d}.$$

Inverse of 3 modulo 7 is n such that:

$$3 \times n \equiv 1 \pmod{7} \quad n = 5$$

Inverse of 8 modulo 15 is n such that:

$$8 \times n \equiv 1 \pmod{15} \quad n = 2$$

Modular Multiplicative Inverse

A Modular Multiplicative Inverse of an integer a modulo d is an integer n such that

$$a \times n \equiv 1 \pmod{d}.$$

Inverse of 3 modulo 7 is n such that:

$$3 \times n \equiv 1 \pmod{7} \quad n = 5$$

Inverse of 8 modulo 15 is n such that:

$$8 \times n \equiv 1 \pmod{15} \quad n = 2$$

Inverse of 12 modulo 15 is n such that:

$$12 \times n \equiv 1 \pmod{15} \quad n = ?$$

Modular Multiplicative Inverse

A Modular Multiplicative Inverse of an integer a modulo d is an integer n such that

$$a \times n \equiv 1 \pmod{d}.$$

Inverse of 3 modulo 7 is n such that:

$$3 \times n \equiv 1 \pmod{7} \quad n = 5$$

Inverse of 8 modulo 15 is n such that:

$$8 \times n \equiv 1 \pmod{15} \quad n = 2$$

Inverse of 12 modulo 15 is n such that:

$$12 \times n \equiv 1 \pmod{15} \quad n = ?$$

Check $\{12n \bmod m : n = 0, 1, 2, \dots\} = \{0, 12, 9, 6, 3\}$.

Modular Multiplicative Inverse

A Modular Multiplicative Inverse of an integer a modulo d is an integer n such that

$$a \times n \equiv 1 \pmod{d}.$$

Inverse of 3 modulo 7 is n such that:

$$3 \times n \equiv 1 \pmod{7} \quad n = 5$$

Inverse of 8 modulo 15 is n such that:

$$8 \times n \equiv 1 \pmod{15} \quad n = 2$$

Inverse of 12 modulo 15 is n such that:

$$12 \times n \equiv 1 \pmod{15} \quad n = ?$$

Check $\{12n \bmod m : n = 0, 1, 2, \dots\} = \{0, 12, 9, 6, 3\}$.

Thus 12 has no multiplicative inverse mod 15.

Modular Multiplicative Inverse

For any integer a such that $\gcd(a, m) = 1$, there is an inverse n such that $an \equiv 1 \pmod{m}$.

Modular Multiplicative Inverse

For any integer a such that $\gcd(a, m) = 1$, there is an inverse n such that $an \equiv 1 \pmod{m}$.

$$3 \times n \equiv 1 \pmod{7} \quad n = 5 \quad \gcd(3, 7) = 1$$

$$8 \times n \equiv 1 \pmod{15} \quad n = 2 \quad \gcd(8, 15) = 1$$

$$12 \times n \equiv 1 \pmod{15} \quad n = ? \quad \gcd(12, 15) = 3$$

Modular Multiplicative Inverse

For any integer a such that $\gcd(a, m) = 1$, there is an inverse n such that $an \equiv 1 \pmod{m}$.

Proof : By the Bezout Identity, there are integers x, y such that

$$ax + my = \gcd(a, m) = 1.$$

In other words $ax - 1 = -my$ or equivalently, $ax \equiv 1 \pmod{m}$.

So we may take x to be the inverse we seek. ■

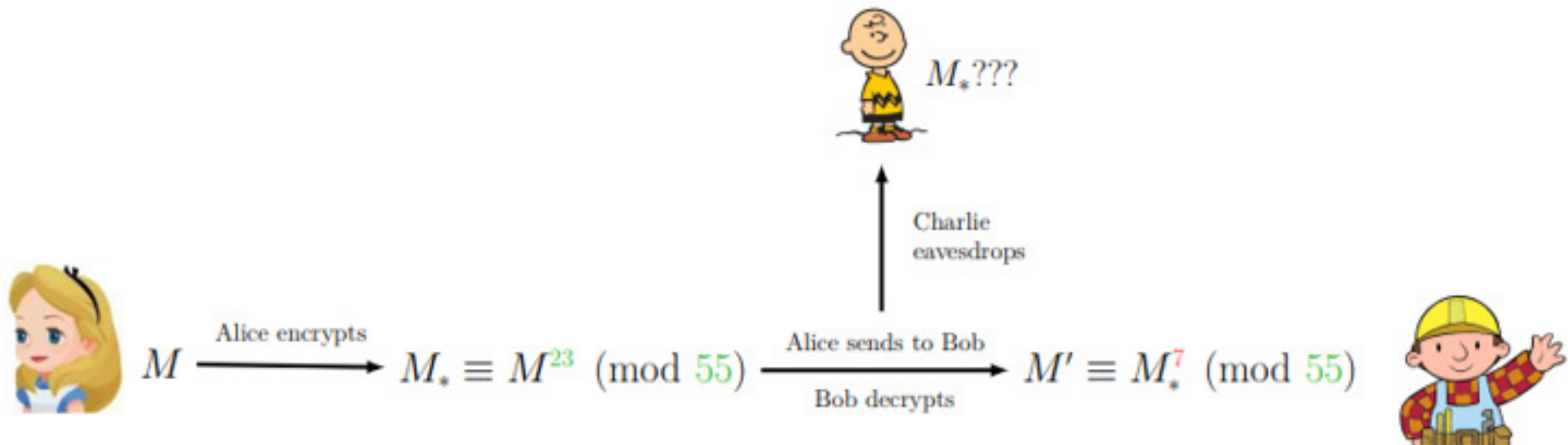
Rivest-Shamir-Adleman

RSA Public Key Cryptography

Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).

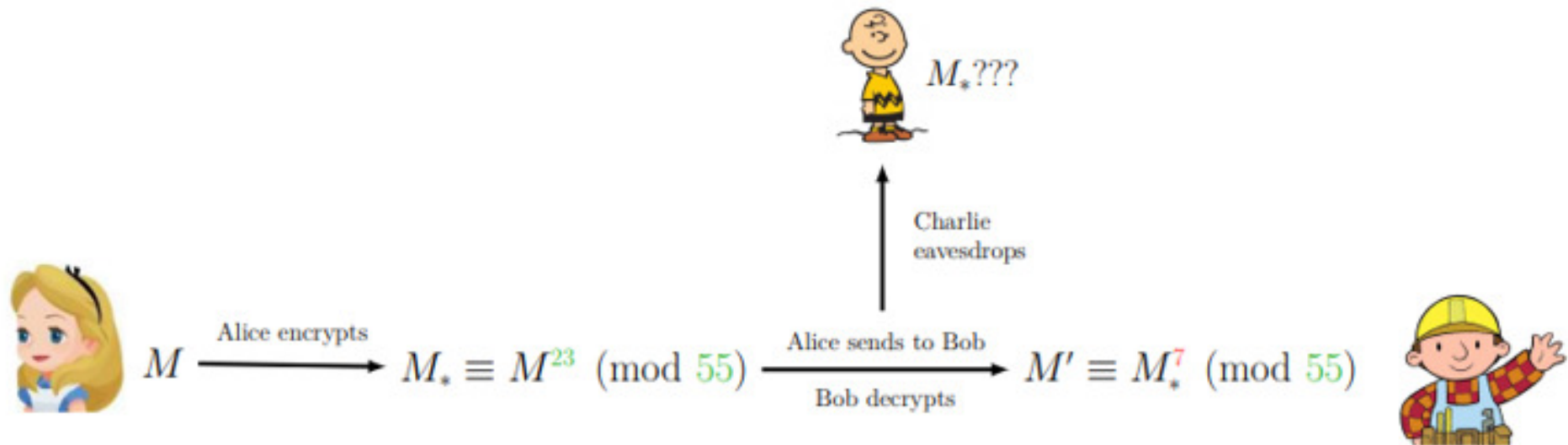
RSA Public Key Cryptography

Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).



RSA Public Key Cryptography

Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).



Examples. Does Bob always decode to the correct message?

$$M = 2$$

$$M_* = 8$$

$$M' = 2$$

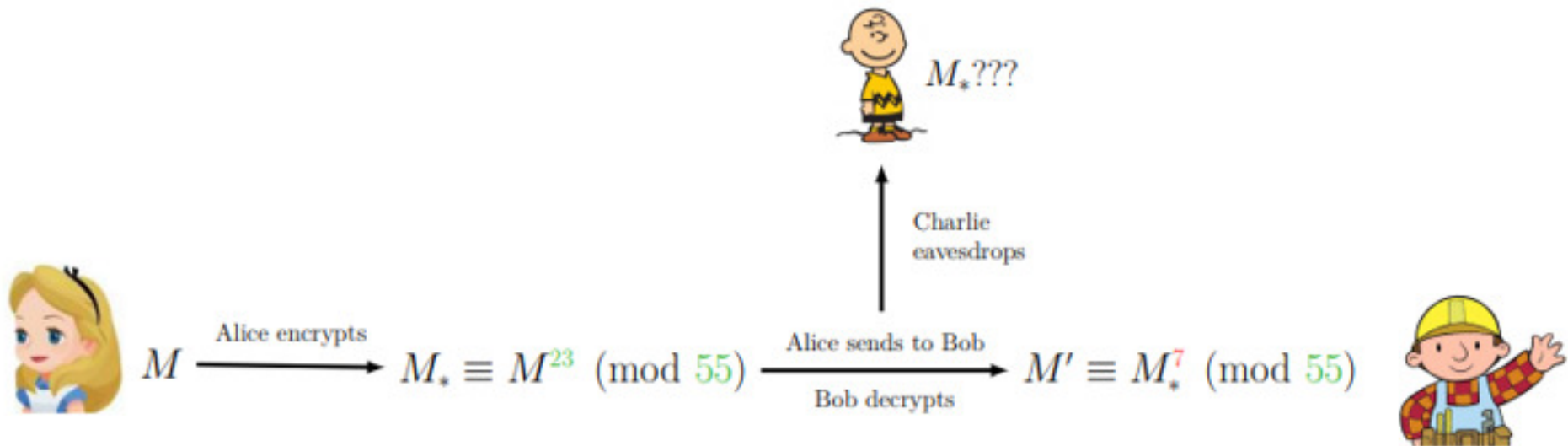
$$M' = M$$

$$2^{23} \equiv 8 \pmod{55}$$

$$8^7 \equiv 2 \pmod{55}$$

RSA Public Key Cryptography

Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).



Examples. Does Bob always decode to the correct message?

$M = 2$	$M_* = 8$	$M' = 2$	$M' = M$
	$2^{23} \equiv 8 \pmod{55}$	$8^7 \equiv 2 \pmod{55}$	

$M = 3$	$M_* = 27$	$M' = 3$	$M' = M$
	$3^{23} \equiv 27 \pmod{55}$	$27^7 \equiv 3 \pmod{55}$	

RSA Public Key Cryptography

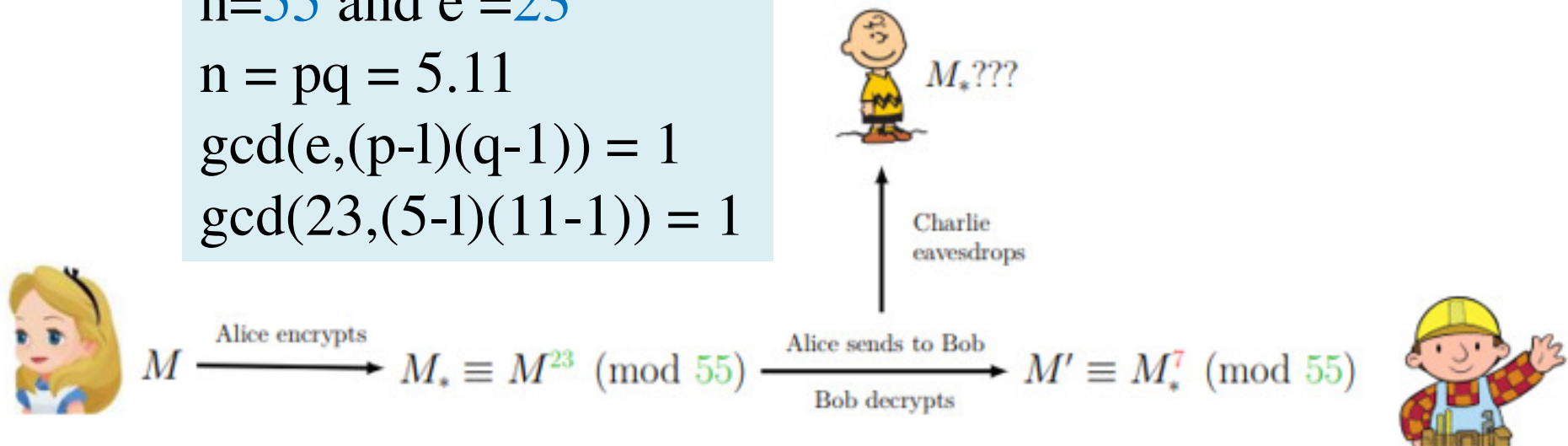
Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).

$$n=55 \text{ and } e=23$$

$$n = pq = 5 \cdot 11$$

$$\gcd(e, (p-1)(q-1)) = 1$$

$$\gcd(23, (5-1)(11-1)) = 1$$



Examples. Does Bob always decode to the correct message?

$M = 2$	$M_* = 8$	$M' = 2$	$M' = M$
	$2^{23} \equiv 8 \pmod{55}$	$8^7 \equiv 2 \pmod{55}$	

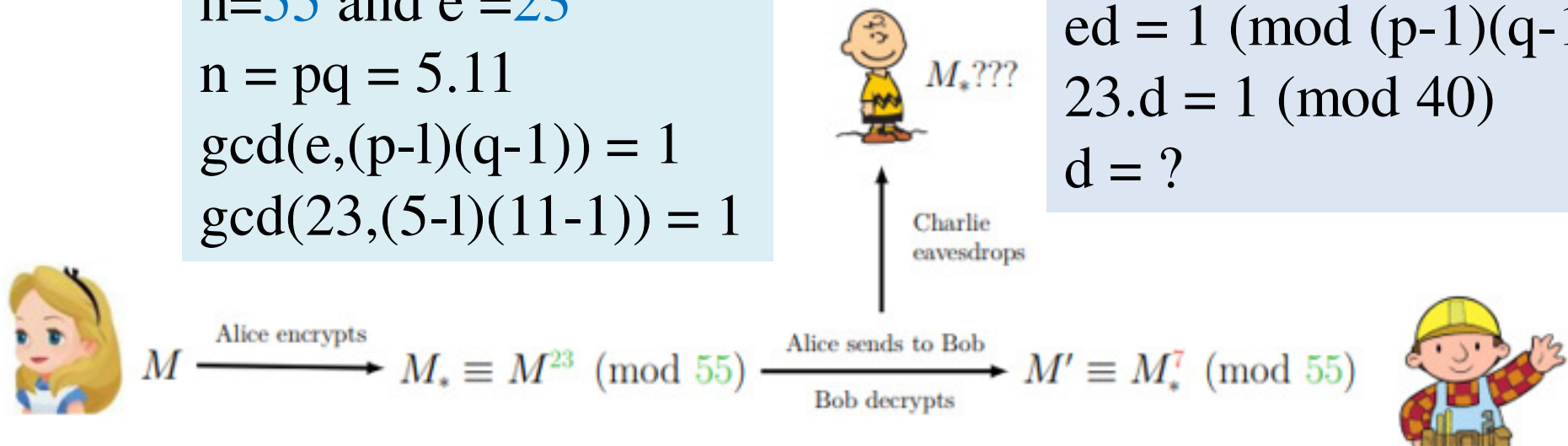
$M = 3$	$M_* = 27$	$M' = 3$	$M' = M$
	$3^{23} \equiv 27 \pmod{55}$	$27^7 \equiv 3 \pmod{55}$	

RSA Public Key Cryptography

Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).

$$\begin{aligned} n &= 55 \text{ and } e = 23 \\ n &= pq = 5 \cdot 11 \\ \gcd(e, (p-1)(q-1)) &= 1 \\ \gcd(23, (5-1)(11-1)) &= 1 \end{aligned}$$

$$\begin{aligned} ed &= 1 \pmod{(p-1)(q-1)} \\ 23 \cdot d &= 1 \pmod{40} \\ d &= ? \end{aligned}$$



Examples. Does Bob always decode to the correct message?

$$\begin{array}{llll} M = 2 & M_* = 8 & M' = 2 & M' = M \\ & 2^{23} \equiv 8 \pmod{55} & 8^7 \equiv 2 \pmod{55} & \end{array}$$

$$\begin{array}{llll} M = 3 & M_* = 27 & M' = 3 & M' = M \\ & 3^{23} \equiv 27 \pmod{55} & 27^7 \equiv 3 \pmod{55} & \end{array}$$

RSA Public Key Cryptography

Bob broadcasts to the world the numbers 23, 55. (Bob's RSA public key).

$$n=55 \text{ and } e=23$$

$$n = pq = 5 \cdot 11$$

$$\gcd(e, (p-1)(q-1)) = 1$$

$$\gcd(23, (5-1)(11-1)) = 1$$

$$ed = 1 \pmod{(p-1)(q-1)}$$

$$23 \cdot d = 1 \pmod{40}$$

$$d = 7$$



Alice encrypts

$$M \longrightarrow M_* \equiv M^{23} \pmod{55}$$

Alice sends to Bob

Bob decrypts

$$M' \equiv M_*^7 \pmod{55}$$



$M_* ???$

Charlie
eavesdrops

Examples. Does Bob always decode to the correct message?

$$M = 2$$

$$M_* = 8$$

$$2^{23} \equiv 8 \pmod{55}$$

$$M' = 2$$

$$M' = M$$

$$8^7 \equiv 2 \pmod{55}$$

$$M = 3$$

$$M_* = 27$$

$$3^{23} \equiv 27 \pmod{55}$$

$$M' = 3$$

$$M' = M$$

$$27^7 \equiv 3 \pmod{55}$$