Reminder: Public Key Cryptography

- **Idea.** Use a **public key** which is used for encryption and a **private key** used for decryption.
- Alice encrypts her message with Bob’s public key and sends it.
Reminder 2: GCD

- We say that \( d \) is a common divisor of \( a \) and \( b \) (where \( a, b, d \in \mathbb{N} \)) if \( d \mid a \) and \( d \mid b \).
- The greatest common divisor of \( a \) and \( b \), denoted \( \text{GCD}(a, b) \), is a common divisor \( c \) of \( a \) and \( b \), such that:
  - If \( d \mid a \) and \( d \mid b \) then \( d \leq c \).
  - Equivalently, if \( d \mid a \) and \( d \mid b \) then \( d \mid c \).

- Claim. If \( a = bq + r \) then

\[
\text{GCD}(a, b) = \text{GCD}(b, r).
\]

Reminder 3: The Euclidean Algorithm

- **Input.** Two numbers \( a, b \in \mathbb{N} \).
- **Output.** \( \text{GCD}(a, b) \).

\[
\begin{align*}
r &\leftarrow a \mod b. \\
\text{While } r \neq 0: \\
&\quad a \leftarrow b. \\
&\quad b \leftarrow r. \\
&\quad r \leftarrow a \mod b. \\
\text{Output } b.
\end{align*}
\]

\[
\begin{array}{c|c c}
\text{a} & \text{b} & \text{r} \\
\hline
78 & 45 & 33 \\
45 & 33 & 12 \\
33 & 12 & 9 \\
12 & 9 & 3 \\
9 & 3 & 0
\end{array}
\]
Warm-up: The Fibonacci Numbers

- **Fibonacci numbers**: 
  
  \[ F_0 = F_1 = 1 \quad F_i = F_{i-1} + F_{i-2}. \]

  1, 1, 2, 3, 5, 8, 13, 21, 34, ...

- How many rounds of the algorithm are required to compute \( GCD(F_n, F_{n-1}) \)?

  ◦ Round 1: \( r = F_n - F_{n-1} = F_{n-2} \).
  ◦ Round 2: \( r = F_{n-1} - F_{n-2} = F_{n-3} \).
  ◦ ...
  ◦ **Round n**: \( r = F_1 - F_0 = 0 \).
More GCDs

• **Theorem.** For any \( a, b \in \mathbb{N} \), there exist \( s, t \in \mathbb{Z} \) such that

\[
GCD(a, b) = as + bt.
\]

\[
GCD(18, 27) = 9 \quad -1 \cdot 18 + 1 \cdot 27 = 9
\]

\[
GCD(25, 65) = 5 \quad 8 \cdot 25 - 3 \cdot 65 = 5
\]

The Extended Euclidean Algorithm

• Build a matrix: First two rows are \((a, 1, 0)\) and \((b, 0, 1)\).

• Every other row is obtained by subtracting the two rows above it, to obtain the next value of \( b \).

\[
\begin{pmatrix}
78 & 1 & 0 \\
45 & 0 & 1 \\
33 & 1 & -1 \\
12 & -1 & 2 \\
9 & 3 & -5 \\
3 & -4 & 7
\end{pmatrix}
\]

\[
\begin{align*}
\text{ } & a = 78 \quad b = 45 \\
\text{ } & a = 45 \quad b = 33 \quad r = 33 \\
\text{ } & a = 33 \quad b = 12 \quad r = 12 \\
\text{ } & a = 12 \quad b = 9 \quad r = 9 \\
\text{ } & a = 9 \quad b = 3 \quad r = 3 \\
\text{ } & a = 9 \quad b = 3 \quad r = 0
\end{align*}
\]
The Extended Euclidean Algorithm

- Build a matrix: First two rows are \((a, 1,0)\) and \((b, 0,1)\).
- Every other row is obtained by subtracting the two rows above it, to obtain the next value of \(b\).

\[
\begin{pmatrix}
78 & 1 & 0 \\
45 & 0 & 1 \\
33 & 1 & -1 \\
12 & -1 & 2 \\
9 & 3 & -5 \\
3 & -4 & 7 \\
\end{pmatrix}
\]

In every step, we have
\[a = qb + r,\]
and then
\[a \leftarrow b, \quad b \leftarrow r.\]

If \(R_i\) denotes the \(i\)'th row:
\[R_i = R_{i-2} - qR_{i-1}.\]

\[
33 = 2 \cdot 12 + 9 \quad \text{so} \quad R_5 = R_3 - 2R_4
\]
Proof by Algorithm!

- **Theorem.** If \( c = \gcd(a, b) \), then there exist \( s, t \in \mathbb{Z} \) such that
  \[ as + bt = c. \]

- \( a = 78 \), \( b = 45 \)

\[
\begin{pmatrix}
78 & 1 & 0 \\
45 & 0 & 1 \\
33 & 1 & -1 \\
12 & -1 & 2 \\
9 & 3 & -5 \\
3 & -4 & 7 \\
\end{pmatrix}
\]

\[
\begin{align*}
78 &= 1 \cdot 78 + 0 \cdot 45 \\
45 &= 0 \cdot 78 + 1 \cdot 45 \\
33 &= 1 \cdot 78 - 1 \cdot 45 \\
12 &= -1 \cdot 78 + 2 \cdot 45 \\
9 &= 3 \cdot 78 - 5 \cdot 45 \\
3 &= -4 \cdot 78 + 7 \cdot 45 \\
\end{align*}
\]

Algorithm Correctness

- **Proof Sketch.** By induction.
  - **Induction basis.** Trivial for the first two rows.
  - **Induction step.**
    \[
    \begin{align*}
    R_i &= \begin{pmatrix}
s_1 & s_2 & s_3 \\
t_1 & t_2 & t_3 \\
u_1 & u_2 & u_3 \\
\end{pmatrix} \\
R_{i+1} &= \begin{pmatrix}
s_1 & s_2 & s_3 \\
t_1 & t_2 & t_3 \\
u_1 & u_2 & u_3 \\
\end{pmatrix} \\
R_{i+2} &= \begin{pmatrix}
s_1 &= a \cdot s_2 + b \cdot s_3 \\
t_1 &= a \cdot t_2 + b \cdot t_3 \\
u_1 &= s_1 - qt_1 = a(s_2 - qt_2) + b(s_3 - qt_3) \\
&= a \cdot u_2 + b \cdot u_3. \\
\end{align*}
    \]
Scales Problem

- We need to verify the weights of various objects by using scales.
- We have an unlimited amount of weights with two integer sizes $a$ and $b$.
- For which values of $a$ and $b$ can we measure every possible integer weight?

**Answer.** Whenever $GCD(a, b) = 1$.

Number Theory

- **Number theory**: the study of integers.
- Some famous theorems:
  - **Euclid.** There are infinitely many prime numbers.
  - “Fermat’s last theorem”. The equation $x^n + y^n = z^n$ has no integer solutions when $n > 2$.
  - **Lagrange 1770.** Every natural number can be represented as the sum of four integer squares.

\[ 15 = 1^2 + 1^2 + 2^2 + 3^2 \quad 110 = 10^2 + 3^2 + 1^2 + 0^2 \]
Number Theory (2)

- A couple of famous open problems:
  - **Twin prime conjecture.** There are infinitely many pairs of prime numbers that differ by two (5 and 7, 17 and 19, 41 and 43, ...).
  - **Goldbach's conjecture.** Every even integer greater than 2 can be expressed as the sum of two primes.

Congruent Numbers

- **Recall.** The remainder of dividing $a$ by $m$ can be written as
  \[ r = a \mod m. \]
- If also $r = b \mod m$, we say that “$a$ is congruent to $b$ modulo $m$”, and write \[ a \equiv b \mod m. \]
  - Equivalently, $m|(a - b)$.
- The numbers 3, 10, 17, 73, 1053 are all congruent modulo 7.
Congruence Classes

- If \( m = 2 \), numbers are congruent if they have the same parity.
- If \( m = 3 \), there are three distinct classes of numbers:
  
  \[
  0 \equiv 3 \equiv 6 \equiv 9 \equiv \ldots \quad \text{mod } 3 \\
  1 \equiv 4 \equiv 7 \equiv 10 \equiv \ldots \quad \text{mod } 3 \\
  2 \equiv 5 \equiv 8 \equiv 11 \equiv \ldots \quad \text{mod } 3 
  \]

- In general, we have exactly \( m \) equivalence classes of numbers.

Congruency is Transitive

- Claim 1. If \( a \equiv b \text{ mod } m \) and \( b \equiv c \text{ mod } m \), then \( a \equiv c \text{ mod } m \).

\[
5 \equiv 55 \text{ mod } 10. \\
55 \equiv 95 \text{ mod } 10 \\
\downarrow \\
5 \equiv 95 \text{ mod } 10
\]
Congruency is Transitive

- **Claim 1.** If $a \equiv b \mod m$ and $b \equiv c \mod m$ then $a \equiv c \mod m$.

- **Proof.** If $m|(a - b)$ and $m|(b - c)$ then $m|(a - c)$ since 
  
  $a - c = (a - b) + (b - c)$.

---

Test Your Intuition

- If $a \equiv b \mod m$ and $c \equiv d \mod m$, do we necessarily have 
  
  $a + c \equiv b + d \mod m$ ?

  - $3 \equiv 15 \mod 12$
  - $2 \equiv 26 \mod 12$

  $3 + 2 \equiv 15 + 26 \mod 12$
Congruency and Addition

• Claim 2. If \( a \equiv b \mod m \) and \( c \equiv d \mod m \), then
  \[ a + c \equiv b + d \mod m. \]

• Proof. If \( m | (a - b) \) and \( m | (c - d) \) then
  \[ m | ((a + c) - (b + d)). \]

Test Your Intuition #2

• If \( a \equiv b \mod m \) and \( c \equiv d \mod m \), is it necessarily true that
  \[ ac \equiv bd \mod m \]?

\[
\begin{align*}
3 &\equiv 15 \mod 12 \\
2 &\equiv 26 \mod 12 \\
3 \cdot 2 &\equiv 15 \cdot 26 \mod 12
\end{align*}
\]
Congruency and Multiplication

- **Claim 3.** If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.

- **Proof.** We have
  
  $$ac - bd = (ac - cb) + (cb - bd) = c(a - b) + b(c - d).$$

- That is, $m|(ac - bd)$.

Test Your Intuition #3

- Is it true that for every $a$ and $m$ there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod m$?
  
  - $6 \cdot 3 \equiv 1 \mod 17$.

  - **No!**

  - For example, consider $a = 2$ and $m = 6$. $2x \equiv 1 \mod 6$?
Relatively Prime Numbers

- Two integers $m, n \in \mathbb{Z}$ are relatively prime if $\text{GCD}(m, n) = 1$.
- **Claim 4.** If $a$ and $m$ are relatively prime, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod m$.

$\text{GCD}(6, 17) = 1$

$6 \cdot 3 \equiv 1 \mod 17.$

Relatively Prime Numbers

- Two integers $m, n \in \mathbb{Z}$ are relatively prime if $\text{GCD}(m, n) = 1$.
- **Claim 4.** If $a$ and $m$ are relatively prime, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \mod m$.
- **Proof.** There exist $s, t \in \mathbb{Z}$ such that $as + mt = 1$. Taking $b = s$, we have $m|(ab + mt - 1) \Rightarrow m|(ab - 1)$. 


Test Your Intuition #4

- If \( ak \equiv bk \mod m \), do we necessarily have \( a \equiv b \mod m \)?
  - Obviously false when \( k \equiv 0 \mod m \).
  - What if \( k \) is not congruent to \( 0 \)?
  - Still false! For example, \( 1 \cdot 4 \equiv 4 \cdot 4 \mod 8 \).

A Cancellation Law

- **Claim 5.** If \( k, m \) are relatively prime, and \( ak \equiv bk \mod m \), then \( a \equiv b \mod m \).

  \[
  \text{GCD}(5,9) = 1 \\
  1 \cdot 5 \equiv 10 \cdot 5 \mod 9 \\
  1 \equiv 10 \mod 9
  \]
A Cancellation Law

• Claim 5. If \( k, m \) are relatively prime and \( ak \equiv bk \mod m \),
then \( a \equiv b \mod m \).

• Proof.
  ◦ By Claim 4 there exists \( s \in \mathbb{Z} \) such that \( ks \equiv 1 \mod m \).
  \[
  a \equiv a \cdot 1 \equiv aks \equiv bks \equiv b \cdot 1 \equiv b \mod m.
  \]

Latin Squares

• Claim 6. Let \( a, b, m \in \mathbb{Z} \) and let \( a, m \) be relatively prime. Then there is a unique \( x \) (mod \( m \)) such that \( ax \equiv b \mod m \).

\[
m = 11, \quad a = 5, \quad b = 6
\]
\[
5 \cdot x \equiv 6 \mod 11
\]
\[
x \equiv 10.
\]
Latin Squares

- **Claim 6.** Let $a, b, m \in \mathbb{Z}$ and let $a, m$ be relatively prime. Then there is a unique $x \pmod{m}$ such that $ax \equiv b \pmod{m}$.

- **Proof.** By Claim 4 there exists $s \in \mathbb{Z}$ such that $as \equiv 1 \pmod{m}$.

- Thus, $x = sb$ is one valid solution.

- Assume, for contradiction, that there are two distinct solutions $x, x'$.
  - Then $ax \equiv ax' \pmod{m}$.
  - $x \equiv sax \equiv sax' \equiv x' \pmod{m}$.

Problem: Large Powers

- **Problem.** Compute $3^{100} \pmod{7}$. 
Problem: Large Powers

- Problem. Compute $3^{100} \mod 7$.
- Modest beginning.

\[
3^1 \equiv 3 \mod 7 \\
3^2 \equiv 3 \cdot 3^1 \equiv 2 \mod 7 \\
3^3 \equiv 3 \cdot 3^2 \equiv 6 \mod 7 \\
3^4 \equiv 3 \cdot 3^3 \equiv 4 \mod 7 \\
3^5 \equiv 3 \cdot 3^4 \equiv 5 \mod 7 \\
3^6 \equiv 3 \cdot 3^5 \equiv 1 \mod 7 \\
3^7 \equiv 3 \cdot 3^6 \equiv 3 \mod 7 \\
3^8 \equiv 3 \cdot 3^7 \equiv 2 \mod 7
\]

\[
3^{100} \equiv 3^{4+6\cdot16} \equiv 3^4 \cdot 1 \equiv 4 \mod 7
\]
The famous number theorist G. H. Hardy in 1941:

“Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers ... and it seems unlikely that anyone will do so for many years.”

1970’s: number theory becomes the basis of modern cryptography.