Ma/CS 6a

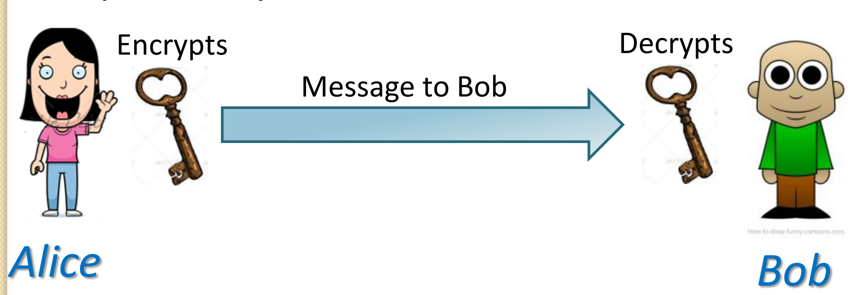
Class 2: Congruences

$$1 + 1 \equiv 5 \ _{(mod\ 3)}$$

By Adam Sheffer

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: The Euclidean Algorithm

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

- $r \leftarrow a \bmod b$.
- While $r \neq 0$:
  - $a \leftarrow b$.
  - $b \leftarrow r$.
  - $r \leftarrow a \bmod b$.
- Output b.

$a = 78 \qquad b = 45$

$a = 78$	$b = 45$	$r = 33$
$a = 45$	$b = 33$	$r = 12$
$a = 33$	$b = 12$	$r = 9$
$a = 12$	$b = 9$	$r = 3$
$a = 9$	$b = 3$	$r = 0$

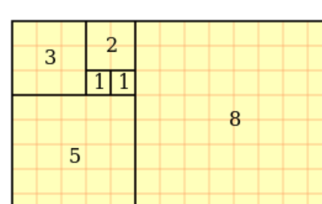
Warm-up: The Fibonacci Numbers

- *Fibonacci numbers*:

$$F_0 = F_1 = 1 \qquad F_i = F_{i-1} + F_{i-2}.$$

$$1,1,2,3,5,8,13,21,34,\ldots$$

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



Warm-up: The Fibonacci Numbers

- *Fibonacci numbers*:

$$F_0 = F_1 = 1 \qquad F_i = F_{i-1} + F_{i-2}.$$

$$1,1,2,3,5,8,13,21,34, \ldots$$

- 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

$$\mathrm{GCD}(a, b) = as + bt.$$

$\mathrm{GCD}(18,27) = 9 \qquad -1 \cdot 18 + 1 \cdot 27 = 9$

$\mathrm{GCD}(25,65) = 5 \qquad 8 \cdot 25 - 3 \cdot 65 = 5$

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.

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

$a = 78 \qquad b = 45$

$$\begin{array}{ccc} a = 78 & b = 45 & r = 33 \\ a = 45 & b = 33 & r = 12 \\ a = 33 & b = 12 & r = 9 \\ a = 12 & b = 9 & r = 3 \\ a = 9 & b = 3 & r = 0 \end{array}$$

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

$$a \leftarrow b, \qquad b \leftarrow r.$$

If R_i denotes the i'th row:

$$R_i = R_{i-2} - qR_{i-1}.$$

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.

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

$33 = 2 \cdot 12 + 9$
so $R_5 = R_3 - 2R_4$

Proof by Algorithm!

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

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

$$\begin{aligned} 78 &= 1 \cdot 78 + 0 \cdot 45 \\ 45 &= 0 \cdot 78 + 1 \cdot 45 \\ 33 &= 1 \cdot 78 - 1 \cdot 45 \\ 12 &= -1 \cdot 78 + 2 \cdot 45 \\ 9 &= 3 \cdot 78 - 5 \cdot 45 \\ 3 &= -4 \cdot 78 + 7 \cdot 45 \end{aligned}$$

Algorithm Correctness

- **Proof Sketch.**
  - Induction basis. Trivial for the first two rows.
  - Induction step.

$$\begin{array}{c} R_i \\ R_{i+1} \\ R_{i+2} \end{array} = \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix}$$

$$s_1 = a \cdot s_2 + b \cdot s_3,$$
$$t_1 = a \cdot t_2 + b \cdot t_3,$$

Induction hypothesis

$$u_1 = s_1 - qt_1 = a(s_2 - qt_2) + b(s_3 - qt_3)$$
$$= a \cdot u_2 + b \cdot u_3.$$

Scales Problem

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

$$GCD(a, b) = 1.$$

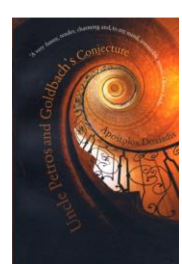
Number Theory

- **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.



Congruences

- **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
$$0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots mod \ 3$$
$$1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots mod \ 3$$
$$2 \equiv 5 \equiv 8 \equiv 11 \equiv \cdots mod \ 3$$
- In general, we have exactly m *equivalence classes* of numbers.

Congruency is Transitive

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

$$5 \equiv 55 \ mod \ 10.$$
$$55 \equiv 95 \ mod \ 10$$
$$\Downarrow$$
$$5 \equiv 95 \ mod \ 10$$

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
$$a-c=(a-b)+(b-c).$$

Congruency and Addition

- **Claim 2.** If $a \equiv b \mod m$ and $c \equiv d \mod m$, then
$$a + c \equiv b + d \mod m.$$

$$3 \equiv 15 \mod 12$$
$$2 \equiv 26 \mod 12$$
$$3 + 2 \equiv 15 + 26 \text{ mod } 12$$

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 $m|(\mathrm{c} - \mathrm{d})$ then $m|\big((a + c) - (b + d)\big)$.

Congruency and Multiplication

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

$$3 \equiv 15 \; mod \; 12$$
$$2 \equiv 26 \; mod \; 12$$
$$\Downarrow$$
$$3 \cdot 2 \equiv 15 \cdot 26 \bmod 12$$

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
$$\begin{aligned} ac - bd &= (ac - cb) + (cb - bd) \\ &= c(a - b) + b(c - d). \end{aligned}$$
That is, $m|(ac - bd)$.

Relatively Prime Numbers

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

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

$$6 \cdot 3 = 1 \; mod \; 17$$

Relatively Prime Numbers

- Two integers $m, n \in \mathbb{Z}$ are ***relatively prime*** if $\mathrm{GCD}(m, n) = 1$.
- **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
$$m | (ab + mt - 1) \quad \Rightarrow \quad m | (ab - 1).$$

A Cancellation Law

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

$$\text{GCD}(5,9) = 1$$
$$1 \cdot 5 \equiv 10 \cdot 5 \ mod \ 9$$
$$\Downarrow$$
$$1 \equiv 10 \ mod \ 9$$

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 exist $s \in \mathbb{Z}$ such that $ks \equiv 1 \ mod \ m$.

$$a \equiv a \cdot 1 \equiv aks \equiv bks \equiv b \cdot 1 \equiv b \ mod \ m.$$

A Cancellation Law

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

- What happens when $\mathrm{GCD}(k, m) \neq 1$?

$$k = 4 \qquad m = 8$$

$$2 \cdot k \equiv 4 \cdot k \equiv 0 \bmod 8$$

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 $ax \equiv b \bmod m$.

$$m = 11, \qquad a = 5, \qquad b = 6$$

$$5 \cdot x \equiv 6 \bmod 11$$

$$\Downarrow$$

$$x = 10.$$

Latin Squares

- **Claim 6.** Let $a, b, m \in \mathbb{Z}$ and let a, m be relatively prime. Then there is a ***unique*** x $(mod\ m)$ such that $ax \equiv b\ mod\ m$.
- **Proof.** By Claim 4 there exists $s \in \mathbb{Z}$ such that $as \equiv 1\ mod\ m$.
- Thus, $x = sb$ is one valid solution.
- Assume, for contradiction, that there are two distinct solutions x, x'.
  - Then $ax \equiv ax'\ mod\ m$.

$$x = sax = sax' = x'.$$

Problem: Large Powers

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

Problem: Large Powers

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

$$
\begin{gathered}
3^1 \equiv 3\ mod\ 7 \\
3^2 \equiv 3 \cdot 3^1 \equiv 2\ mod\ 7 \\
3^3 \equiv 3 \cdot 3^2 \equiv 6\ mod\ 7 \\
3^4 \equiv 3 \cdot 3^3 \equiv 4\ mod\ 7 \\
3^5 \equiv 3 \cdot 3^4 \equiv 5\ mod\ 7 \\
3^6 \equiv 3 \cdot 3^5 \equiv 1\ mod\ 7 \\
3^7 \equiv 3 \cdot 3^6 \equiv 3\ mod\ 7
\end{gathered}
$$

Problem: Large Powers

$$
\begin{gathered}
3^1 \equiv 3\ mod\ 7 \\
3^2 \equiv 3 \cdot 3^1 \equiv 2\ mod\ 7 \\
3^3 \equiv 3 \cdot 3^2 \equiv 6\ mod\ 7 \\
3^4 \equiv 3 \cdot 3^3 \equiv 4\ mod\ 7 \\
3^5 \equiv 3 \cdot 3^4 \equiv 5\ mod\ 7 \\
3^6 \equiv 3 \cdot 3^5 \equiv 1\ mod\ 7 \\
3^7 \equiv 3 \cdot 3^6 \equiv 3\ mod\ 7 \\
3^8 \equiv 3 \cdot 3^7 \equiv 2\ mod\ 7 \\
\dots \\
3^{100} \equiv 3^{4+6\cdot 16} \equiv 3^4 \cdot 1 \equiv 4\ mod\ 7
\end{gathered}
$$

The End

- 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 main tool of modern cryptography.