BBM 205 Discrete Mathematics
Hacettepe University
http://web.cs.hacettepe.edu.tr/~bbm205

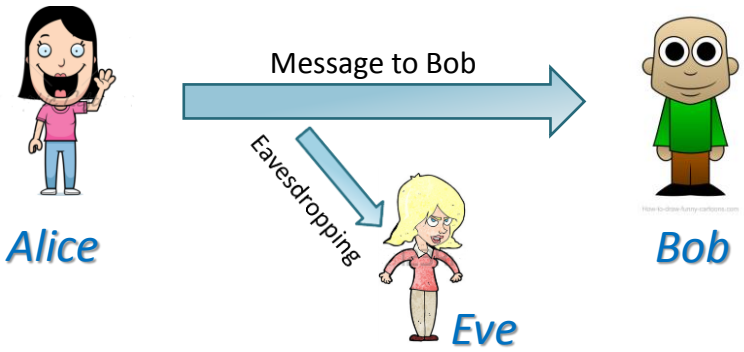
Lecture 5: Arithmetic Modulo m, Primes and Greatest Common Divisors

Lecturer: Lale Özkahya

Resources:
Kenneth Rosen, "Discrete Mathematics and App."
http://www.math.caltech.edu/ 2016-17/1term/ma006a/#notes

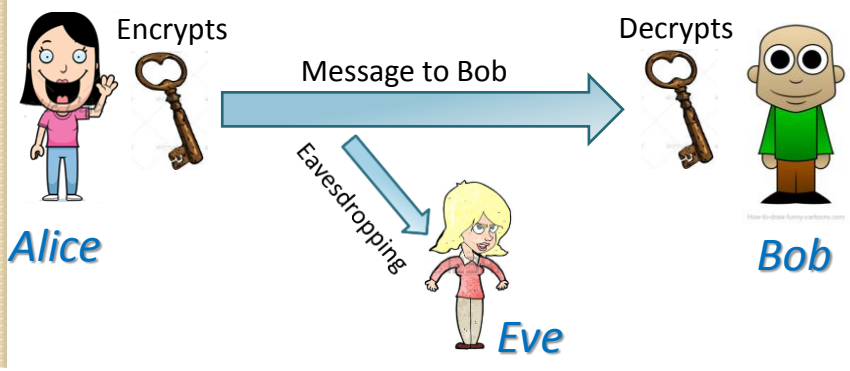
Our Problem: Encryption

- Alice needs to send bob a message.
- Eve can read the communications.
- Alice *encrypts* the message.



Classic Cryptography

- Alice and Bob exchange some information in advance, in a secure way.



Example: Atbash Cipher

- Replace each letter with a symbol, according to the sequence (*key*):

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

"My hovercraft is full of eels"

"Nb slevixizug rh ufoo lu vvoh"

Other Historical Ciphers

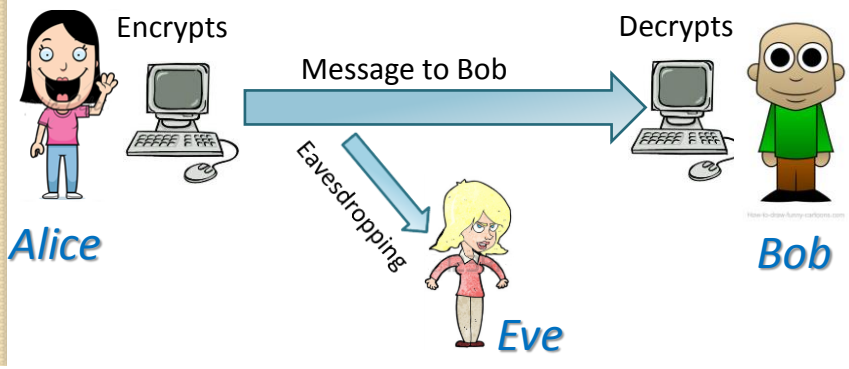
- Scytale transposition cipher, used by the Spartan military.

- The Enigma machine in World War II.

- Cipher runes.

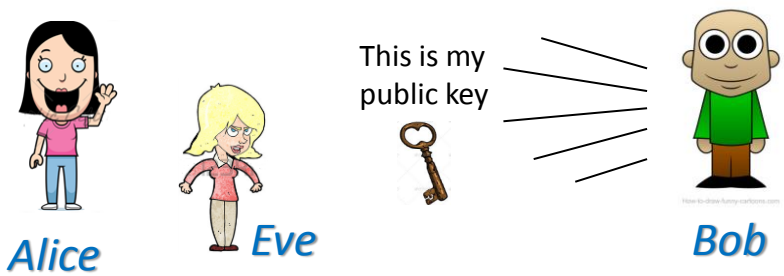
The Internet

- **Problem.** When performing a secret transaction over the internet, we cannot securely exchange information in advance.



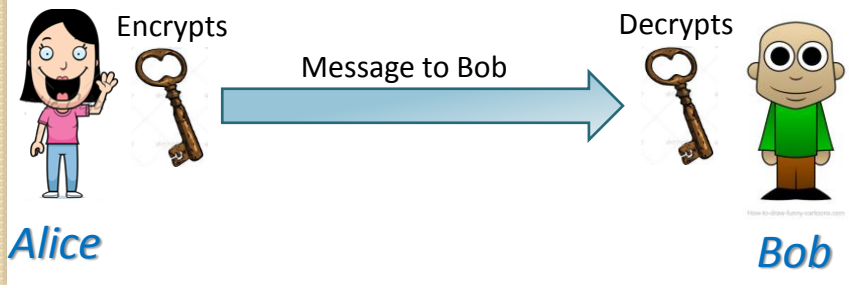
Public-key Cryptography

- **Idea.** Use a *public key* which is used for *encryption* and a *private key* used for *decryption*.
- Bob generates both keys. Keeps the private key and publishes the public one.



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.



Public-key Cryptography

- Eve has the public key and the encrypted message.
- We need an action that is easy to do (*encrypt* using a public key) but very difficult to reverse (*decrypt* using a public key).

Public-key Cryptography

- Eve has the public key and the encrypted message.
- We need an action that is easy to do (*encrypt* using a public key) but very difficult to reverse (*decrypt* using a public key).
- **Bad example.** The public key is the number k. We encrypt a number a as $a \cdot k$. The adversary can divide by k…

Public-key Cryptography

- Eve has the public key and the encrypted message.
- We need an action that is easy to do (*encrypt* using a public key) but very difficult to reverse (*decrypt* using a public key).

Prime factorization

Integers

- We consider the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

- The expression "$a \in \mathbb{Z}$" means that a is *in* the set $\mathbb{Z}$.
- For example, we have

$$1 \in \mathbb{Z}, \qquad 10^2 \in \mathbb{Z}.$$

- On the other hand

$$0.3 \notin \mathbb{Z}, \qquad \sqrt{2} \notin \mathbb{Z}.$$

Division

- Given two integers $a, b \in \mathbb{Z}$, we say that a divides b (or $a|b$) if there exists $s \in \mathbb{Z}$ such that $b = sa$.
- True or false:

$3|12$ ✓ $\quad 12|3$ ✗

$3|-15$ ✓ $\quad -3|3$ ✓

$-7|0$ ✓ $\quad 0|-7$ ✗

$0|0$ ✓

Our First Proof

- **Claim.** If $a|b$ an $b|c$ then $a|c$.
- **Proof.**
  - There exists $s \in \mathbb{Z}$ such that $b = as$.
  - There exists $t \in \mathbb{Z}$ such that $c = bt$.
  - Therefore, $c = ast$.
  - Setting $r = st$, we have $c = ar$.

Our Second Proof

- **Claim.** If $a|b$ and $b|a$ then $a = \pm b$.
- **Proof.**
  - There exists $s \in \mathbb{Z}$ such that $a = sb$.
  - There exists $t \in \mathbb{Z}$ such that $b = ta$.
  - That is, $a = sta$.
  - $st = 1$ so either $s = t = 1$ or $s = t = -1$.

Prime Numbers

- A *natural number* is an integer that is non-negaive. The set of natural numbers:
$$\mathbb{N} = \{0,1,2,3, \dots\}.$$
- A number of $\mathbb{N} \setminus \{0,1\}$ is said to be *prime* if its only positive divisors are one at itself.

Proof by Induction

- **Claim (Prime decomposition).** Every natural number $n \geq 2$ is either a prime or a product of primes.
- **Proof.**
  - Induction basis: The claim holds for 2.
  - Induction step: Assume that the claim holds for every natural number smaller than n.
  - If n is a prime, the claim holds for n.
  - Otherwise, we can write $n = ab$.
  - By the induction hypothesis, both a and b are either primes or a product of primes.
  - Thus, n is a product of primes.

Proof by Contradiction

- **Claim.** There exist infinitely many prime numbers.
  - **Proof.** Assume, for contradiction, that there exists a finite set of primes
    $$P = \{p_1, p_2, p_3, \dots, p_n\}.$$
  - The number $p_1 p_2 \cdots p_n + 1$ is not prime, since it is not in P.
  - The number $p_1 p_2 \cdots p_n + 1$ is prime, since it cannot be divided by any of the primes of P.
  - *Contradiction! So there must be infinitely many primes!*

More Division Properties

- **Claim.** Given two numbers $a, b \in \mathbb{N}$, there are unique $q, r \in \mathbb{N}$ such that $r < b$ and
  $$a = qb + r.$$
- We say that q and r are the *quotient* and the *remainder* of dividing a with b.
- We write $r = a \bmod b$.
- *Proof by algorithm!*

Our First Algorithm

- **Input.** Two numbers $a, b \in \mathbb{N}$.
- **Output.** Two number $q, r \in \mathbb{N}$ such that $a = qb + r$ and $r < b$.

- $q \leftarrow 0$ and $n \leftarrow a$.
- While $n \geq b$:
  - $n \leftarrow n - b$.
  - $q \leftarrow q + 1$.
- $r \leftarrow n$

$a = 12 \quad b = 5$

$q = 0$	$n = 12$	$r =?$
$q = 1$	$n = 7$	$r =?$
$q = 2$	$n = 2$	$r =?$
	$r = 2$	

Greatest Common Divisor

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

Examples: GCD

- What is $\mathrm{GCD}(18,42)$? *6*
- What is $\mathrm{GCD}(50,100)$? *50*
- What is $\mathrm{GCD}(6364800, 1491534000)$?
  - $\mathrm{GCD}(2^7 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 17, 2^4 \cdot 3^7 \cdot 5^3 \cdot 11 \cdot 31)$?

    $= 2^4 \cdot 3^2 \cdot 5^2 = 3600.$
- What can we do when dealing with numbers that are too large to factor?

GCD Property

- **Claim.** If $a = bq + r$ then

  $$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$$
- **Example.**

  $$66 = 21 \cdot 3 + 3$$

  $$GCD(66,21) = GCD(21,3) = 3.$$

Computing GCD: General approach

- **Problem.** Compute $\mathrm{GCD}(a, b)$.
  - Find $q_1, r_1 \in \mathbb{Z}$ such that $a = q_1 b + r_1$.
  - Since $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r_1)$, it suffices to compute the latter.
  - Find $q_2, r_2 \in \mathbb{Z}$ such that $b = q_2 r_1 + r_2$.
  - Since $\mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, r_2)$, it suffices to compute the latter.
  - …
  - Continue until obtaining a zero remainder (then the divider is the required GCD).

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.

$a = 78 \quad b = 45$

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

Proof of GCD Property

- **Claim.** If $a = bq + r$ then

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$$

- **Proof.**
  - Since $r = a - bq$, every common divisor of a and b is also a divisor of r. Thus,
    $$\mathrm{GCD}(a, b) | \mathrm{GCD}(b, r)$$
  - Since $a = bq + r$, every common divisor of b and r is also a common divisor of a. Thus,
    $$\mathrm{GCD}(b, r) | \mathrm{GCD}(a, b).$$

The End

- The Voynich manuscript:

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.

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

$a = 78 \quad b = 45$

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

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.

$$\left(\begin{array}{ccc} 78 & 1 & 0 \\ 45 & 0 & 1 \\ 33 & 1 & -1 \\ 12 & -1 & 2 \\ 9 & 3 & -5 \\ 3 & -4 & 7 \end{array}\right)$$

$33 = 2 \cdot 12 + 9$
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
$$as + bt = c.$$

$$\left(\begin{array}{ccc} 78 & 1 & 0 \\ 45 & 0 & 1 \\ 33 & 1 & -1 \\ 12 & -1 & 2 \\ 9 & 3 & -5 \\ 3 & -4 & 7 \end{array}\right)$$

$$78 = 1 \cdot 78 + 0 \cdot 45$$
$$45 = 0 \cdot 78 + 1 \cdot 45$$
$$33 = 1 \cdot 78 - 1 \cdot 45$$
$$12 = -1 \cdot 78 + 2 \cdot 45$$
$$9 = 3 \cdot 78 - 5 \cdot 45$$
$$3 = -4 \cdot 78 + 7 \cdot 45$$

Algorithm Correctness

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

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

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

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

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

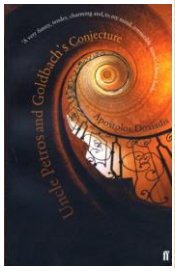
Number Theory

- **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

$$r = a \bmod m.$$

- If also $r = b \bmod m$, we say that "a is *congruent* to b modulo m", and write

$$a \equiv b \bmod m.$$

  - 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

$$0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots \bmod 3$$
$$1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots \bmod 3$$
$$2 \equiv 5 \equiv 8 \equiv 11 \equiv \cdots \bmod 3$$

- 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 $a \equiv c \ mod \ m$.

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

$$5 \equiv 95 \ mod \ 10$$

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
$$a + c \equiv b + d \; mod \; m.$$

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

$$3 + 2 \equiv 15 + 26 \bmod 12$$

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 $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then
$$ac \equiv bd \bmod m.$$

$$3 \equiv 15 \bmod 12$$
$$2 \equiv 26 \bmod 12$$

$$3 \cdot 2 \equiv 15 \cdot 26 \bmod 12$$

Congruency and Multiplication

- **Claim 3.** If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then
$$ac \equiv bd \bmod m.$$
- **Proof.** We have
$$ac - bd = (ac - cb) + (cb - bd)$$
$$= c(a - b) + b(c - d).$$
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 $a \equiv b \ mod \ m$.

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

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
$$ak \equiv bk \ mod \ m,$$
then $a \equiv b \ mod \ m$.

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

$$k = 4 \qquad m = 8$$
$$2 \cdot k \equiv 4 \cdot k \equiv 0 \ mod \ 8$$

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 $ax \equiv b \ mod \ m$.

$$m = 11, \qquad a = 5, \qquad b = 6$$
$$5 \cdot x \equiv 6 \ mod \ 11$$
$$\Downarrow$$
$$x = 10.$$

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.**

$$3^1 \equiv 3\ mod\ 7$$
$$3^2 \equiv 3 \cdot 3^1 \equiv 2\ mod\ 7$$
$$3^3 \equiv 3 \cdot 3^2 \equiv 6\ mod\ 7$$
$$3^4 \equiv 3 \cdot 3^3 \equiv 4\ mod\ 7$$
$$3^5 \equiv 3 \cdot 3^4 \equiv 5\ mod\ 7$$
$$3^6 \equiv 3 \cdot 3^5 \equiv 1\ mod\ 7$$
$$3^7 \equiv 3 \cdot 3^6 \equiv 3\ mod\ 7$$

Problem: Large Powers

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

Reminder: Some Congruent Properties

- **Addition.** If $a \equiv b \ mod \ m$ and $c \equiv d \ mod \ m$, then $a + c \equiv b + d \ mod \ m$.
- **Products.** If $a \equiv b \ mod \ m$ and $c \equiv d \ mod \ m$, then $ac \equiv bd \ mod \ m$.
- **Cancellation.** If $\mathrm{GCD}(k, m) = 1$ and $ak \equiv bk \ mod \ m$, then $a \equiv b \ mod \ m$.
- **Inverse.** If $\mathrm{GCD}(a, m) = 1$, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \ mod \ m$.

Warm-up: Division by Nine

- **Claim.** A number $a \in \mathbb{N}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
- Is 123456789 divisible by 9?

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$$
$$4 + 5 = 9$$

✓

Warm-up: Division by Nine (2)

- **Claim.** A number $a \in \mathbb{N}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
  - **Proof.** Write a as $a_k a_{k-1} \cdots a_1 a_0$ where a_i is the $(i+1)$'th rightmost digit of a.

$$a - (a_0 + a_1 + \cdots + a_k) =$$
$$(a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots) - (a_0 + \cdots + a_k)$$
$$= a_1 \cdot 9 + a_2 \cdot 99 + a_3 \cdot 999 + \cdots$$

  - That is, $9 | a - (a_0 + a_1 + \cdots + a_k)$

Warm-up: Division by Nine (3)

- **Claim.** A number $a \in \mathbb{N}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
  - **Proof.** Write a as $a_k a_{k-1} \cdots a_1 a_0$ where a_i is the $(i-1)$'th rightmost digit of a.
  - We have: $9 | a - (a_0 + a_1 + \cdots + a_k)$.
  - Equivalently,
    $a \equiv (a_0 + a_1 + \cdots + a_k) \; mod \; 9.$

Casting Out Nines

- **Problem.** Is the following correct?
  $54{,}321 \cdot 98{,}765 = 5{,}363{,}013{,}565.$
- If this is correct, then
$54{,}321 \cdot 98{,}765 \equiv 5{,}363{,}013{,}565 \ mod\ 9.$

$$5 + 4 + 3 + 2 + 1 \equiv 6 \ mod\ 9$$
$$9 + 8 + 7 + 6 + 5 \equiv 2 \ mod\ 9$$
$$5 + 3 + 6 + 3 + 0 + 1 + 3 + 5 + 6 + 5 \equiv 1 \ mod\ 9.$$

$$6 \cdot 2 \not\equiv 1 \ mod\ 9$$

X

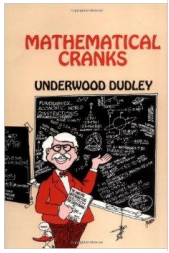
Casting Out Nines (cont.)

- Is the ***casting out nines*** technique always correct in verifying whether $a \cdot b = c$?
  - If the calculation $mod\ 9$ is wrong, the original calculation must be wrong.
  - If the calculation $mod\ 9$ is correct, the original calculation might still be wrong!

$$1 \cdot 2 \equiv 11 \ mod\ 9.$$

Casting Out Nines Crank

- In the 1980's, a crank wrote a 124-page book explaining *the law of conservations of numbers* that he "developed for 24 years".
- This law "was perfected with 100% effectiveness".
- The book is basically 124 pages about the casting out nines trick. It does not mention that the method can sometimes fail.



Fermat's Little Theorem

- **Theorem.** For any prime p and integer a,

$$a^p \equiv a \bmod p.$$

- Examples:

$$15^7 \equiv 15 \equiv 1 \bmod 7$$

$$20^{53} \equiv 20 \bmod 53$$

$$2^{1009} \equiv 2 \bmod 1009$$

Pierre de Fermat

Fermat's Little Theorem

- **Theorem.** For any prime p and integer a,

$$a^p \equiv a \bmod p.$$

- **Proof.** By induction on a:
  - We now prove only the case of $a \geq 0$.
  - Induction basis: Obviously holds for $a = 0$.
  - Induction step: Assume that the claim holds for a. In a later lecture we prove
    $$(a+b)^p \equiv a^p + b^p \bmod p.$$
  - Thus:
    $$(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p.$$

A Corollary

- **Corollary.** If $a \in \mathbb{N}$ is not divisible by a prime p then $a^{p-1} \equiv 1 \bmod p$.
- **Proof.**
  - We have $\mathrm{GCD}(a, p) = 1$.
  - Fermat's little theorem: $a^p \equiv a \bmod p$.
  - Combine with cancelation property: If $\mathrm{GCD}(k, m) = 1$ and $ak \equiv bk \bmod m$, then $a \equiv b \bmod m$.

Euler's Totient Function

- *Euler's totient* $\varphi(n)$ is defined as follows: Given $n \in \mathbb{N} \setminus \{0\}$, then

$$\varphi(n) = |\{x \mid 1 \leq x < n \text{ and } \mathrm{GCD}(x, n) = 1\}|.$$

- In more words: $\varphi(n)$ is the number of natural numbers $1 \leq x \leq n$ such that x and n are relatively prime.

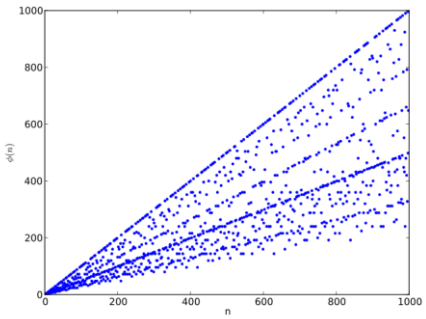
$$\varphi(12) = |\{1,5,7,11\}| = 4$$

Leonhard Euler

The Totient of a Prime

- **Observation.** If p is a prime number, then $\varphi(p) = p - 1$.

The first thousand values of $\varphi(n)$:



Euler's Theorem

- **Theorem.** For any pair $a, n \in \mathbb{N}$ such that $GCD(a, n) = 1$, we have
$$a^{\varphi(n)} \equiv 1 \; mod \; n.$$

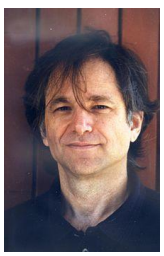
- This is a generalization of the claim $a^{p-1} \equiv 1 \; mod \; p$ (when p is prime).

The RSA Algorithm

- Public key cryptosystem.
- Discovered in 1977 by *R*ivest, *S*hamir, and *A*dleman.
- Still extremely common!

Ron Rivest

Adi Shamir



Leonard Adleman

RSA Public and Private Keys

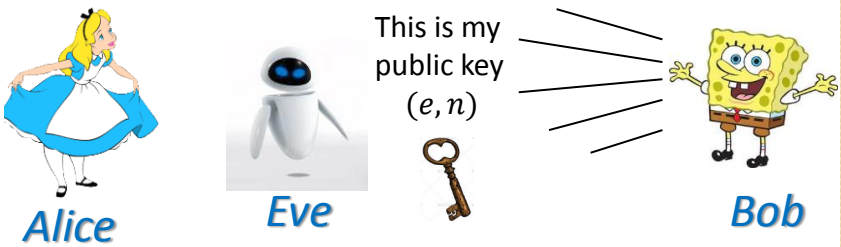
1. Choose two LARGE primes p, q (say, 500 digits).
2. Set $n = pq$.
3. Compute $\varphi(n)$, and choose $1 < e < \varphi(n)$ such that $\mathrm{GCD}(e, \varphi(n)) = 1$.
4. Find d such that $de \equiv 1 \ mod \ \varphi(n)$.

Public key. n and e.

Private information. p, q, and d.

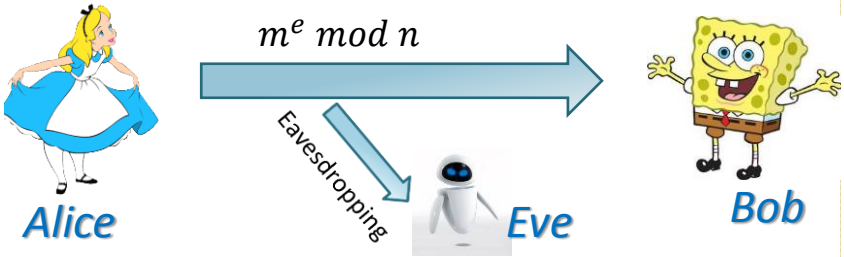
Preparing for Secure Communication

- Bob generates p, q, n, d, e, and transmits only e and n.



Encrypting a Message

- Alice wants to send Bob the number $m < n$ without Eve deciphering it.
- Alice uses n, e to calculate $X = m^e \ mod \ n$, and sends X to Bob.



Decrypting a Message

- Bob receives message $X = m^e \ mod \ n$ from Alice. Then he calculates:

$$X^d \ mod \ n \equiv m^{ed} \ mod \ n$$
$$\equiv m^{1+k\cdot\varphi(n)} mod \ n \equiv m \ mod \ n.$$

$de \equiv 1 \ mod \ \varphi(n)$

Euler's Theorem: $m^{\varphi(n)} \equiv 1 \ mod \ n$

Slightly cheating since the theorem requires $GCD(m, n) = 1$

RSA in One Slide

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q. sets $n = pq$ and finds $\varphi(n)$.
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$.
  - Find d such that $de \equiv 1 \; mod \; \varphi(n)$.
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \; mod \; n$.
- Bob receives X.

  Calculates $X^d \; mod \; n$.

Example: RSA (with small numbers)

- Bob wants to generate keys:
  - Arbitrarily chooses primes $p = 61$ and $q = 53$. $n = 61 \cdot 52 = 3233$. $\varphi(3233) = 3120$.
  - Chooses $e = 17$ ($GCD(3120,17) = 1$).
  - For $de \equiv 1 \; mod \; 3120$, we have $d = 2753$.
- Alice wants to pass bob $m = 65$.
  - Receives n, e from Bob. Returns $m^e = 65^{17} \equiv 2790 \; mod \; 3233$.
- Bob receives $X \equiv 2790 \; mod \; 3233$.

  Calculates $X^d = 2790^{3233} \equiv 65 \; mod \; 3233$.

Some Details

- Bob needs to:
  - Find two large primes p, q.
  - Calculate n, d, e.
- Alice needs to
  - Use n, e to calculate $X = m^e \ mod \ n$.
- Eve must not be able to
  - Use n, e, X to find m.
- Bob needs to:
  - Use n, d, X to find m.

That is: Easy to compute a large power $mod \ n$. Hard to compute a large "root" $mod \ n$.

Taking Large Roots

- Eve has n, e, and Alice's message $X \equiv m^e \ mod \ n$.
- If Eve can compute $X^{1/e} \ mod \ n$, she can read the message! (i.e., if she can factor n).
- So far nobody knows how to compute this in a reasonable time.
- Or do they?

Computing a Large Power

- **Problem.** How can we compute

$$65^{2^{4000}} \; mod \; 9721?$$

- A naïve approach:

$$65^2 \equiv 4225 \; mod \; 9721$$
$$65^3 \equiv 65 \cdot 65^2 \equiv 2437 \; mod \; 9721$$
$$65^4 \equiv 65 \cdot 65^3 \equiv 2869 \; mod \; 9721$$
$$\ldots$$

- This approach requires 2^{4000} (about $1.3 \cdot 10^{1204}$) steps. *Impossible!*

Computing a Large Power – Fast!

- **Problem.** How can we compute

$$65^{2^{4000}} \; mod \; 9721?$$

$$65^2 \equiv 4225 \; mod \; 9721$$
$$65^4 \equiv 65^2 \cdot 65^2 \equiv 2869 \; mod \; 9721$$
$$65^8 \equiv 65^4 \cdot 65^4 \equiv 7195 \; mod \; 9721$$
$$65^{16} \equiv 65^8 \cdot 65^8 \equiv 3700 \; mod \; 9721$$
$$\ldots$$

Only 4000 steps. *Easy!*

A Small Technical Issue

- What if we calculate a^b where b is not a power of two?
- We calculate $a, a^2, a^4, a^8, a^{16}, a^{32}, \ldots$
- Every number can be expressed as a sum of distinct powers of 2.

$$57 = 32 + 16 + 8 + 1$$

$$a^{57} = a^{32}a^{16}a^8a$$

What is Left to Do?

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q. ? $n = pq$ ✓ find $\varphi(n)$. ?
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$.
  - Find d such that $de \equiv 1 \ mod \ \varphi(n)$. ?
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \ mod \ n$. ✓
- Bob receives X.

  Calculates $X^d \ mod \ n$. ✓

Reminder: Euler's Totient Function

- *Euler's totient $\varphi(n)$* is defined as follows: Given $n \in \mathbb{N}$, then

$$\varphi(n) = |\{x \mid 1 \leq x < n \text{ and } \mathrm{GCD}(x, n) = 1\}|.$$

- In more words: $\varphi(n)$ is the number of natural numbers $1 \leq x \leq n$ such that x and n are coprime.

$$\varphi(12) = |\{1,5,7,11\}| = 4.$$

Reminder #2: The RSA Algorithm

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q. ? $n = pq$ ✓ find $\varphi(n)$. ?
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$. ?
  - Find d such that $de \equiv 1 \ mod \ \varphi(n)$. ?
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \ mod \ n$. ✓
- Bob receives X.

  Calculates $X^d \ mod \ n$. ✓

Finding $\varphi(n)$

- **Problem.** Given $n = pq$, where p, q are large primes, find $\varphi(n)$.
  - We need the number of elements in $\{1,2, \dots, n\}$ that are not multiplies of p or q.
  - There are $\frac{n}{p} = q$ numbers are divisible by p.
  - There are $\frac{n}{q} = p$ numbers are divisible by q.
  - Only $n = pq$ is divided by both.
  - Thus: $\varphi(n) = n - p - q + 1$.

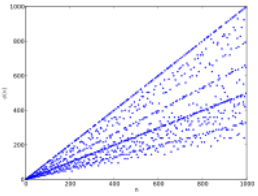
The RSA Algorithm

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q. ? $n = pq$ ✓ find $\varphi(n)$. ✓
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$. ?
  - Find d such that $de \equiv 1 \ mod \ \varphi(n)$. ?
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \ mod \ n$. ✓
- Bob receives X.

  Calculates $X^d \ mod \ n$. ✓

Choose e s.t. $\mathrm{GCD}(\varphi(n), e) = 1$

- **Problem.** Given $n = pq$, where p, q are large primes, find $e \in \mathbb{N}$ such that $\mathrm{GCD}(\varphi(n), e) = 1$.
  - We can choose arbitrary numbers until we find one that is relatively prime to $\varphi(n)$.
  - For the "worst" values of $\varphi(n)$, a random number is good with probability $1/\log\log n$.



The RSA Algorithm

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q. ? find $\varphi(n)$. ✓ $n = pq$ ✓
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$. ✓
  - Find d such that $de \equiv 1 \ mod \ \varphi(n)$. ?
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \ mod \ n$. ✓
- Bob receives X.

  Calculates $X^d \ mod \ n$. ✓

Find d such that $de \equiv 1 \; mod \; \varphi(n)$

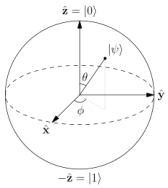
- **Recall.** Since $\mathrm{GCD}(e, \varphi(n)) = 1$ then there exist $s, t \in \mathbb{Z}$ such that
$$se + t\varphi(n) = 1.$$
- That is, $se \equiv 1 \; mod \; \varphi(n)$.
- We can find s, t by the ***extended Euclidean algorithm*** from lecture 2.

The RSA Algorithm

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q. ? find $\varphi(n)$. ✓
    $n = pq$ ✓
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$. ✓
  - Find d such that $de \equiv 1 \; mod \; \varphi(n)$. ✓
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \; mod \; n$. ✓
- Bob receives X.
  Calculates $X^d \; mod \; n$. ✓

Quantum Computing

- A *bit* of a computer contains a value of either 0 or 1.
- A quantum computer contains *qubits*, which can be in superpositions of states.
- Theoretically, a quantum computer can easily factor numbers and decipher almost any known encryption.



Should We Stop Ordering Things Online?

SEARCH The New York Times

TECHNOLOGY

Microsoft Makes Bet Quantum Computing Is Next Breakthrough

By JOHN MARKOFF JUNE 23, 2014

The Washington Post Search MERRILL EDGE

NSA seeks to build quantum computer that could crack most types of encryption

Finding Large Primes

- Let n be a LARGE integer (e.g., 2^{4000}).
- *The prime number theorem.* The probability of a random $p \in \{1, \dots, n\}$ being prime is about $1/\log n$.
- If we randomly choose numbers from $\{1, \dots, n\}$, we expect to have about $\log n$ iterations before finding a prime.
  - *But how can we check whether our choice is a prime or not?!*

Primality Testing

- Given a LARGE $q \in \mathbb{Z}$, how can we check whether q is prime?
- **The naïve approach.** Go over every number in $\{2, \dots, \sqrt{q}\}$ and check whether it divides q.
  - *But we chose our numbers to be too large for a computer to go over all of them!*

Recall: Fermat's Little Theorem

- For any prime p and integer a relatively prime to p, we have

$$a^p \equiv a \bmod p.$$

- Pick a random integer a and check whether $a^q \equiv a \bmod q$.
  - If not, q is not a prime!
  - If yes, ***???***

Pierre de Fermat

Example: Fermat Primality Testing

- Is $n = 355207$ prime?

$$2^{355207} \equiv 84927 \bmod 355207.$$

- n is not prime since $2^n \not\equiv 2 \bmod n$.

- We can try 1000 different values of a and see if $a^n \equiv a \bmod n$ for each of them.

Carmichael Numbers

- A number $q \in \mathbb{N}$ is said to be a *Carmichael number* if it is not prime, but still satisfies $a^q \equiv a \, mod \, q$ for every a that is relatively prime to q.
  - The smallest such number is 561.
  - Very rare – about one in 50 trillion in the range 1 – 10^{21}.

R. D. Carmichael

Example: Carmichael Numbers

- **Claim.** Let $k \in \mathbb{N} \setminus \{0\}$ such that $6k + 1, 12k + 1$, and $18k + 1$ are primes. Then
  $$n = (6k + 1)(12k + 1)(18k + 1)$$
  is a Carmichael number.

- **Example.**
  - For $k = 1$, we have that $7, 13, 19$ are primes.
  - $7 \cdot 13 \cdot 19 = 1729$ is a Carmichael number.

Proof

- We need to prove that for any a that is relatively prime to n, we have
$$a^n \equiv a \bmod n.$$
- **Recall.** Since $GCD(a, n) = 1$, this is equivalent to $a^{n-1} \equiv 1 \bmod n$.
- We rewrite $n = 1296k^3 + 396k^2 + 36k + 1$.
- For any such a, we have
$$a^{n-1} = a^{1296k^3+396k^2+36k}$$
$$= \left(a^{6k}\right)^{216k^2+66k+6}.$$

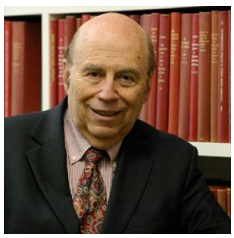
Proof (cont.)

- For any a relatively prime to n, we have
$$a^{n-1} = \left(a^{6k}\right)^{216k^2+66k+6}.$$
- **Recall.** If $a \in \mathbb{N}$ is not divisible by a prime p then $a^{p-1} \equiv 1 \bmod p$.
- Since a and $6k - 1$ are relatively prime
$$a^{n-1} \equiv 1^{216k^2+66k+6} \equiv 1 \bmod 6k + 1.$$
- Similarly, we have $a^{n-1} \equiv 1 \bmod 12k + 1$ and $a^{n-1} \equiv 1 \bmod 18k + 1$.
- Since $a^{n-1} - 1$ is divisible by the three pairwise coprime integers $6k + 1, 12k + 1$, and $18k + 1$, it is also divisible by their product n. That is, $a^{n-1} \equiv 1 \bmod n$.

Miller–Rabin Primality Test

- The *Miller–Rabin primality test* works on *every number*.

Gary Miller



Michael Rabin

Root of Unity

- **Claim.** For any prime p, the only numbers $a \in \{1, \dots, p\}$ such that $a^2 \equiv 1 \; mod \; p$ are 1 and $p - 1$.

- **Example.** The solutions to
$$a^2 \equiv 1 \; mod \; 1009$$
are exactly the numbers satisfying
$$a \equiv 1 \text{ or } 1008 \; mod \; 1009.$$

Root of Unity

- **Claim.** For any prime p, the only numbers $a \in \{1, \dots, p\}$ such that $a^2 \equiv 1 \; mod \; p$ are 1 and $p - 1$.
- **Proof.**

$$a^2 \equiv 1 \; mod \; p$$

$$a^2 - 1 \equiv 0 \; mod \; p$$

$$(a + 1)(a - 1) \equiv 0 \; mod \; p$$

- That is, either $p|(a + 1)$ or $p|(a - 1)$.

Roots of Unity Properties

- Given a prime $p > 2$, we write

$$p - 1 = 2^s d$$

  where d is odd and $s \geq 1$.
- **Claim.** For any *odd* prime p and any $1 < a < p$, one of the following holds.
  - $a^d \equiv 1 \; mod \; p$.
  - There exists $0 \leq r < s$ such that

$$a^{2^r d} \equiv -1 \; mod \; p.$$

Roots of Unity Properties (2)

- **Claim.** For any ***odd*** prime p and any $1 < a < p$, one of the following holds.
  - $a^d \equiv 1 \; mod \; p$.
  - There exists $0 \leq r < s$ such that $a^{2^r d} \equiv -1 \; mod \; p$.
- **Proof.**
  - By Fermat's little theorem $a^{p-1} \equiv 1 \; mod \; p$.
  - Consider $a^{(n-1)/2}, a^{(n-1)/4}, \ldots, a^{(n-1)/2^s}$. By the previous claim, each such root is $\pm 1 \; mod \; n$.
  - If all of these roots equal 1, we are in the first case. Otherwise, we are in the second.

Composite Witnesses

- Given a composite (non-prime) ***odd*** number n, we again write $n - 1 = 2^s d$ where d is odd and $s \geq 1$.
- We say that $a \in \{2,3,4, \ldots, n-2\}$ is a ***witness*** for n if
  - $a^d \not\equiv 1 \; mod \; n$.
  - For every $0 \leq r < s$, we have $a^{2^r d} \not\equiv -1 \; mod \; n$.

Example: Composite Witness

- **Problem.** Prove that 91 is not a prime.

$$90 = 2 \cdot 45.$$

$$2^{45} \equiv 57 \; mod \; 91.$$

- 2 is a witness that 91 is not a prime.

There are Many Witnsses

- Given an odd composite n, the probability of a number $\{2, \dots, n-2\}$ being a witness is at least ¾.
- Given an odd $n \in \mathbb{N}$, take i numbers and check if they are witnesses.
  - If we found a witness, n is composite.
  - If we did not find a witness, n is prime with probability at least

The End


ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?
I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.