Primality Testing

Antonio Carzaniga

Faculty of Informatics
Università della Svizzera italiana

December 12, 2008

Outline

- Basic modular arithmetic
- Fermat’s little theorem
- Probabilistic primality testing

Primality Test

- **Problem:** given an ℓ-bit integer n, find whether n is *prime*

Primality Test

- **Problem:** given an ℓ-bit integer n, find whether n is *prime*

- Naïve solution

```
NAÏVE-PRIMALITY(n)
for i = 2 to ⌊√n⌋
    if n = 0 mod i                // i.e., i divides n
        return FALSE
return TRUE
```

Primality Test

- **Problem:** given an ℓ-bit integer n, find whether n is *prime*

- Naïve solution

```
NAÏVE-PRIMALITY(n)
for i = 2 to ⌊√n⌋
    if n = 0 mod i                // i.e., i divides n
        return FALSE
return TRUE
```

This algorithm is intractable because it has a running time

$$T(\ell) = \Theta(\sqrt{n}) = \Theta(2^{\ell/2})$$

- exactly $\sqrt{n}$ steps if n is prime

A *Randomized* Primality Test

A *Randomized* Primality Test

- Main idea: we use ***Fermat's little theorem*** as a "yes/no" test
  - more accurately, we have a ***"maybe/no" test***
  - ***"no"***—*n* is *composite*
  - ***"maybe"***—50/50 chance that *n* is *prime*

A *Randomized* Primality Test

- Main idea: we use ***Fermat's little theorem*** as a "yes/no" test
  - more accurately, we have a ***"maybe/no" test***
  - ***"no"***—*n* is *composite*
  - ***"maybe"***—50/50 chance that *n* is *prime*
  - we repeat the test *k* times, and if all the *k* tests say "maybe," then we conclude that *n* is *prime*

A *Randomized* Primality Test

- Main idea: we use ***Fermat's little theorem*** as a "yes/no" test
  - more accurately, we have a ***"maybe/no" test***
  - ***"no"***—n is *composite*
  - ***"maybe"***—50/50 chance that n is *prime*
  - we repeat the test k times, and if all the k tests say "maybe," then we conclude that n is *prime*
  - there is a chance that we are wrong, but that chance vanishes *exponentially* with k

A *Randomized* Primality Test

- Main idea: we use ***Fermat's little theorem*** as a "yes/no" test
  - more accurately, we have a ***"maybe/no" test***
  - ***"no"***—n is *composite*
  - ***"maybe"***—50/50 chance that n is *prime*
  - we repeat the test k times, and if all the k tests say "maybe," then we conclude that n is *prime*
  - there is a chance that we are wrong, but that chance vanishes *exponentially* with k

- Ingredients
  - simple *modular arithmetic*

- Last night I started working on my lecture at 20:00, and it took me 7 hours to finish it

  Question: at what time did I finish my lecture?

- Last night I started working on my lecture at 20:00, and it took me 7 hours to finish it

  Question: at what time did I finish my lecture?

$$\textit{finish-time} = 3$$

- Last night I started working on my lecture at 20:00, and it took me 7 hours to finish it

  Question: at what time did I finish my lecture?

$$\textit{finish-time} = 3 \equiv 20 + 7 \pmod{24}$$

- Last night I started working on my lecture at 20:00, and it took me 7 hours to finish it

  Question: at what time did I finish my lecture?

$$\textit{finish-time} = 3 \equiv 20 + 7 \pmod{24}$$

  Question: what if it took me 37 hours?

- Last night I started working on my lecture at 20:00, and it took me 7 hours to finish it

  Question: at what time did I finish my lecture?

$$\textit{finish-time} = 3 \equiv 20 + 7 \pmod{24}$$

  Question: what if it took me 37 hours?

$$9 \equiv 20 + 37 \pmod{24}$$

- **Definition:** “x is equivalent to y, modulo *N*”

$$x \equiv y \pmod{N} \quad \Leftrightarrow \quad N \text{ divides } (x - y) \text{ or } (y - x)$$

- Simple exercises
  - $? \equiv 45 + 45 \pmod{60}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $? \equiv 201 \pmod{60}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $? \equiv 4717382910421 \pmod{10}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $1 \equiv 4717382910421 \pmod{10}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $1 \equiv 4717382910421 \pmod{10}$
  - $? \equiv 4717382910421 \pmod{9}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $1 \equiv 4717382910421 \pmod{10}$
  - $4 \equiv 4717382910421 \pmod{9}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $1 \equiv 4717382910421 \pmod{10}$
  - $4 \equiv 4717382910421 \pmod{9}$
  - $? \equiv 4717382910421 \pmod{3}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $1 \equiv 4717382910421 \pmod{10}$
  - $4 \equiv 4717382910421 \pmod{9}$
  - $1 \equiv 4717382910421 \pmod{3}$

Modular Arithmetic (2)

- Simple exercises
  - $30 \equiv 45 + 45 \pmod{60}$
  - $21 \equiv 201 \pmod{60}$
  - $1 \equiv 4717382910421 \pmod{10}$
  - $4 \equiv 4717382910421 \pmod{9}$
  - $1 \equiv 4717382910421 \pmod{3}$
  - $? \equiv 2976146201360 + 10436201964293 \pmod{3}$

Equivalence Classes

- An equivalence relation

$$x \equiv y \pmod{m}$$

Equivalence Classes

- An equivalence relation

$$x \equiv y \pmod{m}$$

- In the modulo-m world, all integers are in *m equivalence classes*
  - e.g.,

$$2 \equiv 5 \equiv 8 \cdots \equiv -1 \equiv -4 \equiv \cdots \pmod{3}$$

Equivalence Classes

- An equivalence relation

$$x \equiv y \pmod{m}$$

- In the modulo-m world, all integers are in *m equivalence classes*
  - e.g.,

$$2 \equiv 5 \equiv 8 \cdots \equiv -1 \equiv -4 \equiv \cdots \pmod{3}$$

- Values in the same equivalence classes are *interchangeable* in arithmetic operations
  - $x \equiv x' \pmod{m} \wedge y \equiv y' \pmod{m} \Rightarrow x + y \equiv x' + y' \pmod{m}$
  - $x \equiv x' \pmod{m} \wedge y \equiv y' \pmod{m} \Rightarrow xy \equiv x'y' \pmod{m}$

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y$

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:
  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

- $x \equiv r_x \pmod{m} \land 0 \leq r_x < m \quad \Rightarrow \quad xy \equiv r_x y \pmod{m}$

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:
  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

- $x \equiv r_x \pmod{m} \wedge 0 \leq r_x < m \quad \Rightarrow \quad xy \equiv r_x y \pmod{m}$

  Proof:

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

- $x \equiv r_x \pmod{m} \wedge 0 \leq r_x < m \quad \Rightarrow \quad xy \equiv r_x y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:
  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

- $x \equiv r_x \pmod{m} \wedge 0 \leq r_x < m \quad \Rightarrow \quad xy \equiv r_x y \pmod{m}$

  Proof:
  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$

Equivalence Classes (2)

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

- $x \equiv r_x \pmod{m} \wedge 0 \leq r_x < m \quad \Rightarrow \quad xy \equiv r_x y \pmod{m}$

  Proof:

  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $xy = (q_x m + r_x)(q_y m + r_y) = (q_x q_y)m^2 + (q_x r_y + q_y r_x)m + r_x r_y$

- $x \equiv r_x \pmod{m} \quad \Rightarrow \quad x + y \equiv r_x + y \pmod{m}$

  Proof:
  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $x + y = q_x m + r_x + q_y m + r_y = (q_x + q_y)m + r_x + r_y \equiv r_x + r_y \pmod{m}$

- $x \equiv r_x \pmod{m} \wedge 0 \leq r_x < m \quad \Rightarrow \quad xy \equiv r_x y \pmod{m}$

  Proof:
  - $x = q_x m + r_x$, from the hypothesis
  - let $y = q_y m + r_y$
  - $xy = (q_x m + r_x)(q_y m + r_y) = (q_x q_y)m^2 + (q_x r_y + q_y r_x)m + r_x r_y \equiv r_x r_y \pmod{m}$

Equivalence Classes (3)

- Simple exercises

Equivalence Classes (3)

- Simple exercises
  - $? \equiv 483921097 \times 891720476436 \pmod{10}$

Equivalence Classes (3)

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $? \equiv 483921097 + 891720476436 \pmod{5}$

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $3 \equiv 2 + 1 \equiv 483921097 + 891720476436 \pmod{5}$

Equivalence Classes (3)

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $3 \equiv 2 + 1 \equiv 483921097 + 891720476436 \pmod{5}$
  - $? \equiv 483921097 \times 891720476436 \pmod{9}$

Equivalence Classes (3)

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $3 \equiv 2 + 1 \equiv 483921097 + 891720476436 \pmod{5}$
  - $3 \equiv 7 \times 3 \equiv 483921097 \times 891720476436 \pmod{9}$

Equivalence Classes (3)

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $3 \equiv 2 + 1 \equiv 483921097 + 891720476436 \pmod{5}$
  - $3 \equiv 7 \times 3 \equiv 483921097 \times 891720476436 \pmod{9}$
  - $? \equiv 86544127367 \times 61922483628096 \pmod{3}$

Equivalence Classes (3)

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $3 \equiv 2 + 1 \equiv 483921097 + 891720476436 \pmod{5}$
  - $3 \equiv 7 \times 3 \equiv 483921097 \times 891720476436 \pmod{9}$
  - $0 \equiv 86544127367 \times 0 \equiv 86544127367 \times 61922483628096 \pmod{3}$

Equivalence Classes (3)

- Simple exercises
  - $2 \equiv 7 \times 6 \equiv 483921097 \times 891720476436 \pmod{10}$
  - $3 \equiv 2 + 1 \equiv 483921097 + 891720476436 \pmod{5}$
  - $3 \equiv 7 \times 3 \equiv 483921097 \times 891720476436 \pmod{9}$
  - $0 \equiv 86544127367 \times 0 \equiv 86544127367 \times 61922483628096 \pmod{3}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times ? \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times ? \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$
  - $3 \times ? \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$
  - $3 \times 7 \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$
  - $3 \times 7 \equiv 1 \pmod{10}$
  - $9 \times ? \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$
  - $3 \times 7 \equiv 1 \pmod{10}$
  - $9 \times 9 \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$
  - $3 \times 7 \equiv 1 \pmod{10}$
  - $9 \times 9 \equiv 1 \pmod{10}$
  - $4 \times ? \equiv 1 \pmod{10}$

Multiplicative Inverse (Modulo N)

- The *multiplicative inverse* (mod N) of a is an integer x such that

$$ax \equiv 1 \pmod{N}$$

- Examples
  - $1 \times 1 \equiv 1 \pmod{10}$
  - $7 \times 3 \equiv 1 \pmod{10}$
  - $3 \times 7 \equiv 1 \pmod{10}$
  - $9 \times 9 \equiv 1 \pmod{10}$
  - $4 \times ? \equiv 1 \pmod{10}$

    4 does not have an inverse (modulo 10)

Multiplicative Inverse (Modulo N) (2)

- For all a, a has a multiplicative inverse (modulo N) if and only if $\gcd(a, N) = 1$

  Proof:

  - let a^{-1} denote a's inverse (modulo N), then there is an integer q such that

$$aa^{-1} = qN + 1$$

Multiplicative Inverse (Modulo N) (2)

- For all a, a has a multiplicative inverse (modulo N) if and only if $\gcd(a, N) = 1$

  Proof:

  - let a^{-1} denote a's inverse (modulo N), then there is an integer q such that
  $$aa^{-1} = qN + 1$$
  - dividing both sides by $\gcd(a, N)$, we get
  $$\frac{aa^{-1}}{\gcd(a, N)} = \frac{qN}{\gcd(a, N)} + \frac{1}{\gcd(a, N)}$$

Multiplicative Inverse (Modulo N) (2)

- For all a, a has a multiplicative inverse (modulo N) if and only if $\gcd(a, N) = 1$

  Proof:

  - let a^{-1} denote a's inverse (modulo N), then there is an integer q such that
  $$aa^{-1} = qN + 1$$
  - dividing both sides by $\gcd(a, N)$, we get
  $$\frac{aa^{-1}}{\gcd(a, N)} = \frac{qN}{\gcd(a, N)} + \frac{1}{\gcd(a, N)}$$
  - since $\gcd(a, N)$ divides both a and N, then the first two fractions are integers, so the last fraction, $1/\gcd(a, N)$, must also be an integer, which requires that $\gcd(a, N) = 1$

Summary on Modulo Arithmetic

- In additions and multiplications (modulo N) we can *always* replace x with r if $x \equiv r \pmod{N}$

Summary on Modulo Arithmetic

- In additions and multiplications (modulo N) we can *always* replace x with r if $x \equiv r \pmod{N}$
  - for simplicity, we always use the (unique) $r < N$ as the representative of its equivalence class

Summary on Modulo Arithmetic

- In additions and multiplications (modulo N) we can *always* replace x with r if $x \equiv r \pmod{N}$
  - for simplicity, we always use the (unique) $r < N$ as the representative of its equivalence class

- Each a relatively prime to N has a *multiplicative inverse* (modulo N) that we denote as a^{-1}

$$aa^{-1} \equiv 1 \pmod{N} \qquad \text{if } \gcd(a, N) = 1$$

Fermat’s Little Theorem

Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof:

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof:

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S;

- If P is *prime*, then for all $1 \le a \le P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof:

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof:

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

  Proof:

  - by contradiction, suppose $\exists x' \neq x$ such that $ax \equiv y \pmod{P}$ and $ax' \equiv y \pmod{P}$

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof:

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

  Proof:

  - by contradiction, suppose $\exists x' \neq x$ such that $ax \equiv y \pmod{P}$ and $ax' \equiv y \pmod{P}$
  - since P is prime, then $\gcd(a, N) = 1$, therefore a has a multiplicative inverse a^{-1} (modulo P)

Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

  Proof:

  - let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
  - multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

    Proof:

    - by contradiction, suppose $\exists x' \neq x$ such that $ax \equiv y \pmod{P}$ and $ax' \equiv y \pmod{P}$
    - since P is prime, then $\gcd(a, N) = 1$, therefore a has a multiplicative inverse a^{-1} (modulo P)
    - so, multiplying $ax \equiv y \pmod{P}$ and $ax' \equiv y \pmod{P}$ by a^{-1}, we have $x \equiv y \pmod{P}$ and $x' \equiv y \pmod{P}$, which means that $x \equiv x' \pmod{P}$, which is a contradiction

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof: (continued)

  - let $S = \{1, 2, \ldots, P - 1\}$ and $0 < a < P$
  - multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

Fermat's Little Theorem (2)

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof: (continued)

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

$$\{1, 2, \ldots, P-1\} = \{a, 2a, \ldots, (P-1)a\} \pmod{P}$$

- If P is *prime*, then for all $1 \le a \le P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof: (continued)

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

$$\{1, 2, \ldots, P-1\} = \{a, 2a, \ldots, (P-1)a\} \pmod{P}$$

- multiplying together all the elements on each side, we get

$$(P-1)! \equiv a^{P-1}(P-1)! \pmod{P}$$

Fermat's Little Theorem (2)

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Proof: (continued)

- let $S = \{1, 2, \ldots, P-1\}$ and $0 < a < P$
- multiplying the elements of S by $a \pmod{P}$ yields a *permutation* of S; i.e., for each $y \in S$ there is exactly one element $x \in S$ such that $ax \equiv y \pmod{P}$

$$\{1, 2, \ldots, P-1\} = \{a, 2a, \ldots, (P-1)a\} \pmod{P}$$

- multiplying together all the elements on each side, we get

$$(P-1)! \equiv a^{P-1}(P-1)! \pmod{P}$$

- $(P-1)!$ also has a multiplicative inverse, so

$$1 \equiv a^{P-1} \pmod{P}$$

Using Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

Using Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

- This suggests a test: given N
  - $a^{N-1} \not\equiv 1 \pmod{N}$

Using Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

- This suggests a test: given N
  - $a^{N-1} \not\equiv 1 \pmod{N}$, then we must conclude that N is *composite*

Using Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

- This suggests a test: given N
  - $a^{N-1} \not\equiv 1 \pmod{N}$, then we must conclude that N is *composite*
  - $a^{N-1} \equiv 1 \pmod{N}$

Using Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P-1$

$$a^{P-1} \equiv 1 \pmod{P}$$

- This suggests a test: given N
  - $a^{N-1} \not\equiv 1 \pmod{N}$, then we must conclude that N is *composite*
  - $a^{N-1} \equiv 1 \pmod{N}$, we can not say much

Using Fermat's Little Theorem

- If P is *prime*, then for all $1 \leq a \leq P - 1$

$$a^{P-1} \equiv 1 \pmod{P}$$

- This suggests a test: given N
  - $a^{N-1} \not\equiv 1 \pmod{N}$, then we must conclude that N is *composite*
  - $a^{N-1} \equiv 1 \pmod{N}$, we can not say much
- However, another lemma gives us a way to measure the probability that a *composite* N passes the test

How Many False Positives?

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

- I.e., if there is one a that "exposes" N as a composite, by failing the test of Fermat's little theorem, then at least half of the choices of a expose N as a composite

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

- I.e., if there is one a that “exposes” N as a composite, by failing the test of Fermat’s little theorem, then at least half of the choices of a expose N as a composite

  Proof:

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

- I.e., if there is one a that "exposes" N as a composite, by failing the test of Fermat's little theorem, then at least half of the choices of a expose N as a composite

  Proof:

  - fix a such that $a^{N-1} \not\equiv 1 \pmod{N}$ (hypothesis)
  - for each $b < N$ that passes the test $b^{N-1} \equiv 1 \pmod{N}$, there is a "twin" value $c = ab$, that fails the test

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

- I.e., if there is one a that "exposes" N as a composite, by failing the test of Fermat's little theorem, then at least half of the choices of a expose N as a composite

  Proof:

  - fix a such that $a^{N-1} \not\equiv 1 \pmod{N}$ (hypothesis)
  - for each $b < N$ that passes the test $b^{N-1} \equiv 1 \pmod{N}$, there is a "twin" value $c = ab$, that fails the test. In fact,

$$c^{N-1} = (ab)^{N-1} = a^{N-1}b^{N-1} \not\equiv 1 \pmod{N}$$

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

- I.e., if there is one a that "exposes" N as a composite, by failing the test of Fermat's little theorem, then at least half of the choices of a expose N as a composite

  Proof:

  - fix a such that $a^{N-1} \not\equiv 1 \pmod{N}$ (hypothesis)
  - for each $b < N$ that passes the test $b^{N-1} \equiv 1 \pmod{N}$, there is a "twin" value $c = ab$, that fails the test. In fact,

$$c^{N-1} = (ab)^{N-1} = a^{N-1}b^{N-1} \not\equiv 1 \pmod{N}$$

  - two distinct $b < N$ and $b' < N$, with $b \neq b'$, that pass the test have distinct "twins" ab and ab'

How Many False Positives?

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then $a^{N-1} \not\equiv 1 \pmod{N}$ holds for *at least half* the choices of a

- I.e., if there is one a that "exposes" N as a composite, by failing the test of Fermat's little theorem, then at least half of the choices of a expose N as a composite

  Proof:

  - fix a such that $a^{N-1} \not\equiv 1 \pmod{N}$ (hypothesis)
  - for each $b < N$ that passes the test $b^{N-1} \equiv 1 \pmod{N}$, there is a "twin" value $c = ab$, that fails the test. In fact,

  $$c^{N-1} = (ab)^{N-1} = a^{N-1}b^{N-1} \not\equiv 1 \pmod{N}$$

  - two distinct $b < N$ and $b' < N$, with $b \neq b'$, that pass the test have distinct "twins" ab and ab'; **proof:** by contradiction, assume $ab \equiv ab'$, then multiply by $a^{-1} \pmod{N}$, you immediately get a contradiction

A Probabilistic Test

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

- Probabilistic test

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

- Probabilistic test
  - choose $a < N$ and relatively prime to N (easy)

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

- Probabilistic test
  - choose $a < N$ and relatively prime to N (easy)
  - if $a^{N-1} \not\equiv 1 \pmod{N}$

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

- Probabilistic test
  - choose $a < N$ and relatively prime to N (easy)
  - if $a^{N-1} \not\equiv 1 \pmod{N}$, then we conclude that N is *composite*

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod N$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod N$.

- Probabilistic test
  - choose $a < N$ and relatively prime to N (easy)
  - if $a^{N-1} \not\equiv 1 \pmod N$, then we conclude that N is *composite*
  - if $a^{N-1} \equiv 1 \pmod N$

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

- Probabilistic test
  - choose $a < N$ and relatively prime to N (easy)
  - if $a^{N-1} \not\equiv 1 \pmod{N}$, then we conclude that N is *composite*
  - if $a^{N-1} \equiv 1 \pmod{N}$, N is *prime* with probability $1/2$

A Probabilistic Test

- If $a^{N-1} \not\equiv 1 \pmod N$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod N$.

- Probabilistic test
  - choose $a < N$ and relatively prime to N (easy)
  - if $a^{N-1} \not\equiv 1 \pmod N$, then we conclude that N is *composite*
  - if $a^{N-1} \equiv 1 \pmod N$, N is *prime* with probability 1/2

- Repeat the test k times, with different choices of a, and if N passes all k tests, then we can say that N is *prime* with probability $1 - 2^{-k}$

Modular Exponentiation

Modular Exponentiation

- How do we compute $a^N \pmod{M}$?
  - remember that N may be a huge number here

- How do we compute $a^N \pmod{M}$?
  - remember that N may be a huge number here

- ***Idea:*** think of the binary representation of N. E.g.,

$$N = 1189 = 2^{10} + 2^7 + 2^5 + 2^2 + 1 = 10010100101_{\text{two}}$$

- How do we compute $a^N \pmod{M}$?
  - remember that N may be a huge number here

- ***Idea:*** think of the binary representation of N. E.g.,

$$N = 1189 = 2^{10} + 2^7 + 2^5 + 2^2 + 1 = 10010100101_{\text{two}}$$

  so $a^N = a^{2^{10}} \cdot a^{2^7} \cdot a^{2^5} \cdot a^{2^2} \cdot a^1$

Modular Exponentiation

- How do we compute $a^N \pmod{M}$?
  - remember that N may be a huge number here

- ***Idea:*** think of the binary representation of N. E.g.,

$$N = 1189 = 2^{10} + 2^7 + 2^5 + 2^2 + 1 = 10010100101_{\text{two}}$$

so $a^N = a^{2^{10}} \cdot a^{2^7} \cdot a^{2^5} \cdot a^{2^2} \cdot a^1$

```
EXP-MOD(a, N, M) // computes a^N mod M
x = 1
while N > 0
    if N ≡ 1 mod 2
        x = xa mod M
    a = a^2 mod M
    N = ⌊N/2⌋
return x
```

One Last Problem

One Last Problem

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.

One Last Problem

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.
  - i.e., ***if there is at least one "witness" then…***

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.
  - i.e., ***if there is at least one "witness" then…***

- There may be *composites* N such that *no* a *would fail the test*

One Last Problem

- If $a^{N-1} \not\equiv 1 \pmod{N}$ for *some* $a < N$ relatively prime to N, then *at least half* the choices of a are such that $a^{N-1} \not\equiv 1 \pmod{N}$.
  - i.e., ***if there is at least one "witness" then…***

- There may be *composites* N such that *no a would fail the test*

- Indeed, there are such numbers (e.g., $N = 561$)
  - called Carmichael numbers
  - infinitely many, but extremely rare
    - their prevalence within the first N integers vanishes with $N \to \infty$
  - there is a more refined test that detects Carmichael (composite) numbers