DTTF/NB479: Dszquphsbqiz Day 9

- Announcements:
  - Homework 2 due now
  - Computer quiz Thursday on chapter 2
- Questions?
- Today:
  - Wrap up congruences
  - Fermat’s little theorem
  - Euler’s theorem
  - Both really important for RSA – pay careful attention!

The Chinese Remainder Theorem establishes an equivalence

- A single congruence mod a composite number is equivalent to a system of congruences mod its factors
- Two-factor form
  - Given gcd(m,n)=1. For integers a and b, there exists *exactly 1* solution (mod mn) to the system:

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

CRT Equivalences let us use systems of congruences to solve problems

- Solve the system:

$$x \equiv 3 \pmod{7}$$
$$x \equiv 5 \pmod{15}$$

- How many solutions?
  - Find them.

$$x^2 \equiv 1 \pmod{35}$$

Chinese Remainder Theorem

- n-factor form
  - Let m_1, m_2,… m_k be integers such that $\gcd(m_i, m_j)=1$ when $i \neq j$. For integers a_1, … a_k, there exists *exactly 1* solution (mod $m_1 m_2 \ldots m_k$) to the system:

$$
\begin{aligned}
&x \equiv a_1 \pmod{m_1} \\
&x \equiv a_2 \pmod{m_2} \\
&\ldots \\
&x \equiv a_k \pmod{m_k}
\end{aligned}
$$

Modular Exponentiation is extremely efficient since the partial results are always small

Q

- Compute the last digit of 3^{2000}

- Compute 3^{2000} (mod 19)
  Idea:
  - Get the powers of 3 by repeatedly squaring 3, BUT taking mod at each step.

Modular Exponentiation Technique and Example

- Compute 3^{2000} (mod 19)
- Technique:
  - Repeatedly square 3, but take mod ***at each step***.
  - Then multiply the terms you need to get the desired power.
- Book's powermod()

(All congruences are mod 19)

$$3^2 \equiv 9$$
$$3^4 = 9^2 \equiv 81 \equiv 5$$
$$3^8 = 5^2 \equiv 25 \equiv 6$$
$$3^{16} = 6^2 \equiv 36 \equiv 17 (or -2)$$
$$3^{32} = 17^2 \equiv 289 \equiv 4$$
$$3^{64} = 4^2 \equiv 16$$
$$3^{128} \equiv 16^2 \equiv 256 \equiv 9$$
$$3^{256} \equiv 5$$
$$3^{512} \equiv 6$$
$$3^{1024} \equiv 17$$

$$3^{2000} \equiv (3^{1024})(3^{512})(3^{256})(3^{128})(3^{64})(3^{16})$$
$$3^{2000} \equiv (17)(6)(5)(9)(16)(17)$$
$$3^{2000} \equiv (1248480)$$
$$3^{2000} \equiv 9 (\mathrm{mod} 19)$$

Modular Exponentiation Example

- Compute 3^{2000} (mod 152)

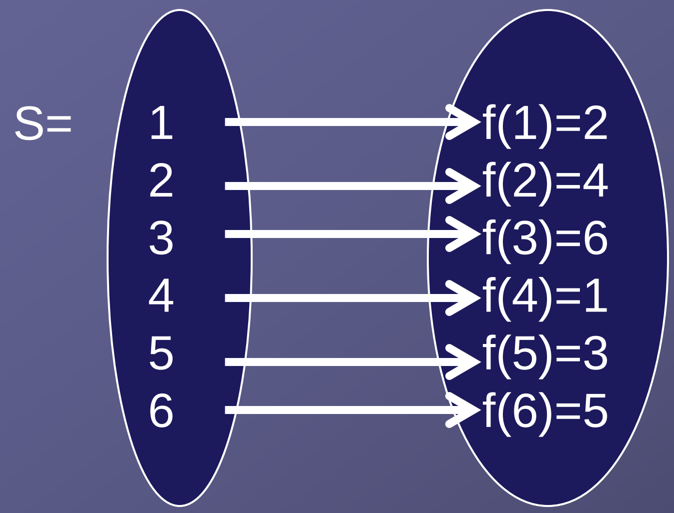
$$3^2 \equiv 9$$
$$3^4 = 9^2 \equiv 81$$
$$3^8 = 81^2 \equiv 6561 \equiv 25$$
$$3^{16} = 25^2 \equiv 625 \equiv 17$$
$$3^{32} = 17^2 \equiv 289 \equiv 137$$
$$3^{64} = 137^2 \equiv 18769 \equiv 73$$
$$3^{128} \equiv 9$$
$$3^{256} \equiv 81$$
$$3^{512} \equiv 25$$
$$3^{1024} \equiv 17$$

$$3^{2000} \equiv (3^{1024})(3^{512})(3^{256})(3^{128})(3^{64})(3^{16})$$
$$3^{2000} \equiv (17)(25)(81)(9)(73)(17)$$
$$3^{2000} \equiv (384492875)$$
$$3^{2000} \equiv 9 (\text{mod} 152)$$

Fermat's Little Theorem:

If p is prime and gcd(a,p)=1, then $a^{(p-1)} \equiv 1 \pmod{p}$

Fermat's Little Theorem:
If p is prime and gcd(a,p)=1, then $a^{(p-1)} \equiv 1 \pmod{p}$



Example: a=2, p=7

Examples:

- $2^2=1 \pmod{3}$
- $6^4 = 1$(mod ???)
- $(3^{2000}) \pmod{19}$

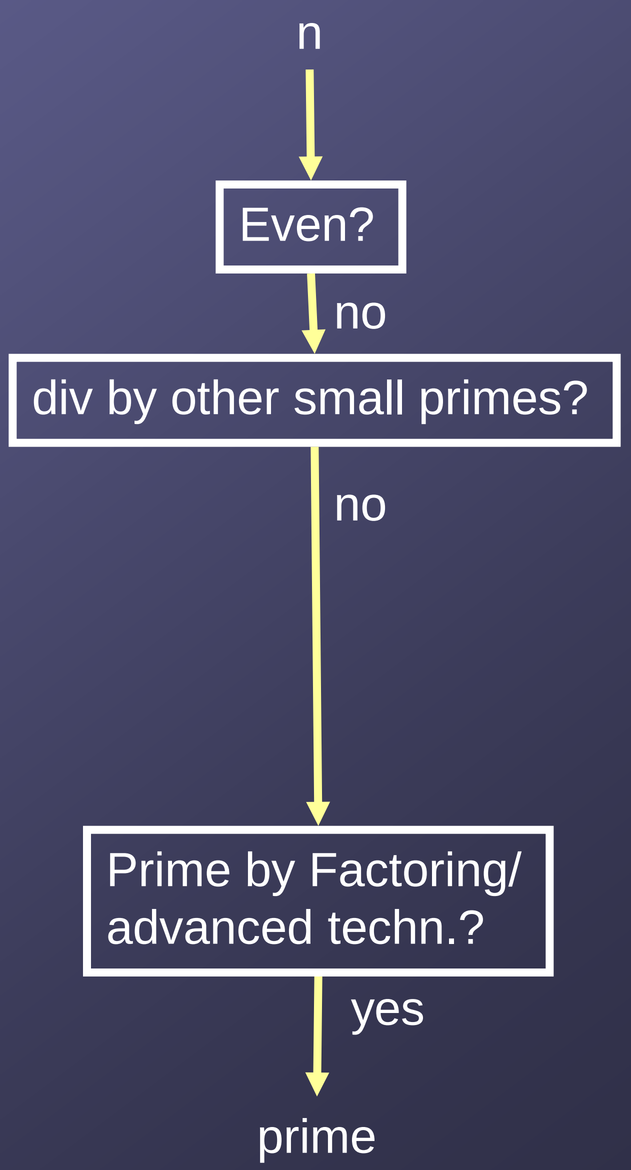
The converse when a=2 usually holds

- Fermat:
  If p is prime and doesn't divide a, $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$

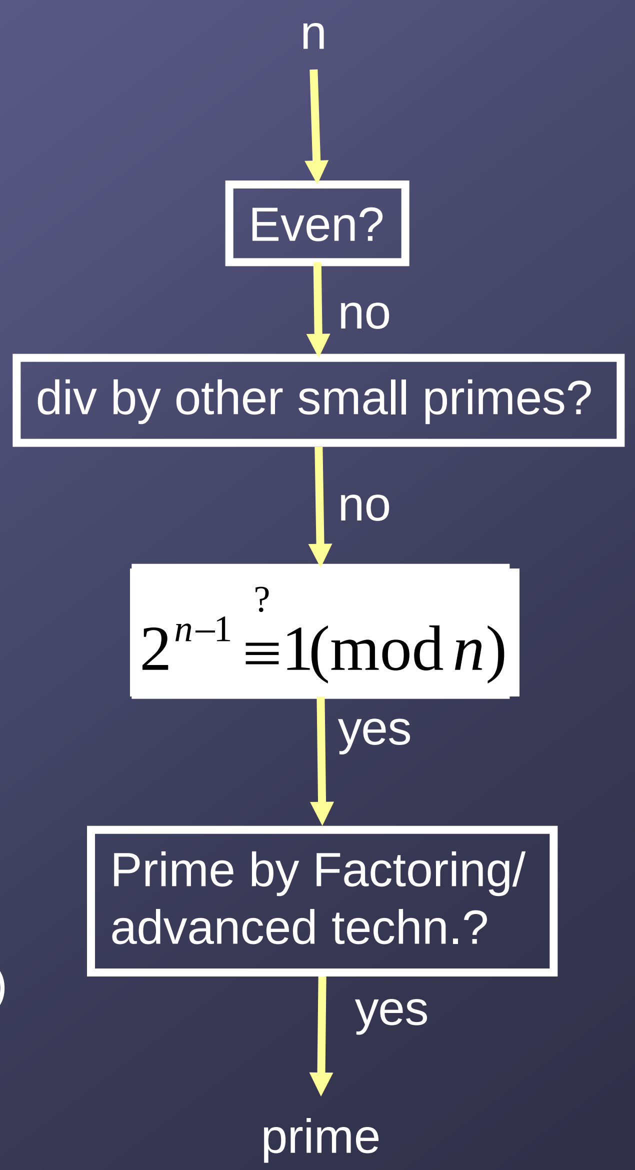
- Converse:
- If $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$, then p is prime and doesn't divide a.

- This is **almost** always true when a = 2. Rare counterexamples:
  - n = 561 =3*11*17, but $2^{560} \equiv 1 (\mathrm{mod}\ 561)$
  - n = 1729 = 7*13*19
  - Can do first one by hand if use Fermat and combine results with Chinese Remainder Theorem

Primality testing schemes typically use the contrapositive of Fermat



Primality testing schemes typically use the contrapositive of Fermat



Use Fermat as a filter since it's faster than factoring (if calculated using the powermod method).

Fermat: p prime→ $2^{p-1} \equiv 1 \pmod{p}$

Contrapositive?

Why can't we just compute $2^{n-1} \pmod{n}$ using Fermat if it's so much faster?

Euler's Theorem is like Fermat's, but for composite moduli

If gcd(a,n)=1, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

So what's $\phi(n)$?

$\phi(n)$ is the number of integers a,
such that $1 \le a \le n$ and $\gcd(a,n) = 1$.

Examples:

1. $\phi(10) = 4$.

2. When p is prime, $\phi(p)$ = ____

3. When n =pq (product of 2 primes), $\phi(n)$ = ____

The general formula for $\phi(n)$

$$\phi(n) = n\prod_{p|n}\left(\frac{p-1}{p}\right)$$

p are distinct primes

Example: $\phi(12)=4$

Euler's Theorem can also lead to computations that are more efficient than modular exponentiation

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

as long as gcd(a,n) = 1

Basic
Principle: when working mod n, view the exponents mod ϕ(n).

Examples:

1. Find last 3 digits of 7^{803}
2. Find 3^{2007} (mod 12)
3. Find 2^{6004} (mod 99)
4. Find 2^{6004} (mod 101)