University of Colorado **Boulder**

Department of Computer Science

CSCI 2824: Discrete Structures

Chris Ketelsen

Lecture 21: Systems of Congruences, Fermat's Little Theorem, and Intro to Crypto

Midterm Exam Tonight

- **Midterm Exam**:
  - **When**: **TONIGHT** 7-8:30pm
  - **Where**: DUAN G1B30

- **Bring**:
  - Your **handwritten** cheat sheet
  - Your CU ID Card
  - A calculator that cannot access the internet
  - Pencil
  - Your A Game

Linear Congruence Refresher

Last time we solved congruences of the form $ax \equiv b \pmod{m}$

Warm-Up: Solve the congruence $5x \equiv 4 \pmod{17}$

Linear Congruence Refresher

Last time we solved congruences of the form $ax \equiv b \pmod{m}$

Warm-Up: Solve the congruence $5x \equiv 4 \pmod{17}$

First we check that 5 and 17 are relatively prime using the EA

$$17 = 3 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1$$

$\gcd(5, 17) = 1$ so 5 has an inverse mod 17. Working backwards

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17$$

Thus the inverse of 5 modulo 17 is 7, so

$$x \equiv 7 \cdot 4 \pmod{17} \equiv 28 \pmod{17} \equiv 11 \pmod{17}$$

Systems of Congruences

Puzzle: Find a number that when divided by 3, the remainder is 2; and when divided by 5, the remainder is 3.

Systems of Congruences

Puzzle: Find a number that when divided by 3, the remainder is 2; and when divided by 5, the remainder is 3.

Equivalent Problem: Find x such that

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$

This is called a **system** of linear congruences

Note that the divisors 3 and 5 are relatively prime

When this happens we have a couple of ways to solve the system

Back Substitution

Example: Find x such that $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$

Back Substitution

Example: Find x such that $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$

Since $x \equiv 2 \pmod{3}$ we know that x can be written as

$$x = 3t + 2 \quad \text{for some integer } t$$

Plug into second congruence

$$3t + 2 \equiv 3 \pmod{5} \quad \Rightarrow \quad 3t \equiv 1 \pmod{5}$$

The inverse of 3 modulo 5 is 2, so $t \equiv 2 \cdot 1 \pmod{5} \equiv 2 \pmod{5}$

which implies that $t = 5u + 2$ for some integer u. Plug back in to x

$$x = 3t + 2 = 3(5u + 2) + 2 = 15u + 8$$

Which tells us that $x \equiv 8 \pmod{15}$

Back Substitution

EFY: Find x such that $x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{7}$ using Back Substitution

Chinese Remainder Theorem

The Chinese Remainder Theorem: Let $m_1, m_2, \ldots, m_n$ be positive integers that are **pairwise** relatively prime and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot m_n$

Let $M_k = \dfrac{m}{m_k}$ and let y_k be the inverse of M_k modulo m_k

Solution is $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \pmod{m}$

Chinese Remainder Theorem

Example: Find x such that $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$

Chinese Remainder Theorem

Example: Find x such that $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$

First note that 3 and 5 are relatively prime, and let $m = 3 \cdot 5 = 15$

We have $M_1 = \dfrac{m}{m_1} = \dfrac{15}{3} = 5$ and $M_2 = \dfrac{m}{m_2} = \dfrac{15}{5} = 3$

The inverse of $M_1 = 5$ modulo 3 is 2

The inverse of $M_2 = 3$ modulo 5 is also 2

Thus the solution is

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 \pmod{15} \\ &\equiv 2 \cdot 5 \cdot 2 + 3 \cdot 3 \cdot 2 \pmod{15} \\ &\equiv 20 + 18 \pmod{15} \equiv 8 \pmod{15} \end{aligned}$$

Chinese Remainder Theorem

EFY: Find x s.t. $x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{7}$ using the CRT

Party Trick

Pick an integer k and I'll tell you what $2^k \bmod 11$ is

Fermat's Little Theorem

The following theorem shows that in special cases we can compute modular exponentials extremely fast

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p then

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

Fermat's Little Theorem

The following theorem shows that in special cases we can compute modular exponentials extremely fast

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p then

$$a^{p-1} \equiv 1 \ (\mathbf{mod}\ p)$$

$$\begin{aligned} \textbf{Example}: \quad 5^6 \ (\mathbf{mod}\ 7) &\equiv 15625 \ (\mathbf{mod}\ 7) \\ &\equiv 2232 \cdot 7 + 1 \ (\mathbf{mod}\ 7) \\ &\equiv 1 \ (\mathbf{mod}\ 7) \end{aligned}$$

Fermat's Little Theorem

Example: Use Fermat's Little Theorem to compute $7^{222} \pmod{11}$

From FLT we know that $7^{10} \equiv 1 \pmod{11}$

And furthermore $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k

What value of k would be helpful?

Fermat's Little Theorem

Example: Use Fermat's Little Theorem to compute $7^{222} \pmod{11}$

From FLT we know that $7^{10} \equiv 1 \pmod{11}$

And furthermore $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k

Note that $222 = 10 \cdot 22 + 2$, so

$$\begin{aligned} 7^{222} &= 7^{10 \cdot 22+2} \\ &= (7^{10})^{22} \cdot 7^2 \\ &\equiv (1)^{22} \cdot 49 \pmod{11} \\ &\equiv 4 \cdot 11 + 5 \pmod{11} \\ &\equiv 5 \pmod{11} \end{aligned}$$

Fermat's Little Theorem

From Sp17 Final: Compute $3^{160000000000000000000000001} \pmod{17}$

Fermat's Little Theorem

From Sp17 Final: Compute $3^{160000000000000000000000001} \pmod{17}$

From FLT we have $3^{16} \equiv 1 \pmod{17}$

and $160000000000000000000000001 = 16 \times 10^{\text{something}} + 1$

Thus $3^{160000000000000000000000001} \equiv 3^{1} \pmod{17} \equiv 3 \pmod{17}$

EFYs: Compute $5^{2003} \pmod{7}$ and $5^{2003} \pmod{11}$

Proof of Fermat's Little Theorem

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p then $a^{p-1} \equiv 1 \ (\mathbf{mod}\ p)$

Proof:

Proof of Fermat's Little Theorem

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$

Proof:

Proof of Fermat's Little Theorem

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$

Proof:

Let $S = \{1, 2, \ldots, p-1\}$ and $a \cdot S = \{a, 2a, \ldots, (p-1)a\}$

Claim: $a \cdot S \equiv S \pmod{p}$

In other words, if you mod out elements of $a \cdot S$ by p you get elements of S back (in some order)

Assume False: S'pose $ra \equiv sa \pmod{p}$ for some $r \neq s$ both $< p$

$\gcd(a, p) = 1$, so $r \equiv s \pmod{p}$, which is a contradiction

Proof of Fermat's Little Theorem

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$

Proof Continued: Thus

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

which we can rearrange to

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

Since p is prime $(p-1)! \nmid p$ and we can cancel to get

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

Intro to Crypto

One of the earliest known cryptographic ciphers was used by Julius Caesar. His strategy was to simply shift each letter of the alphabet forward 3 places (wrapping around when you get to the end). In this scheme:

$$A \to D \qquad K \to N \qquad Y \to B$$

This is often called a **Caesar Cipher** or a **Shift Cipher**

Mathematically, we can accomplish this by assigning to each letter a number between 0 and 25

$$A \to 0 \qquad K \to 10 \qquad Y \to 24$$

The encoding can be done by passing the value through a shift function modulo 26, i.e. $f(p) = (p + 3) \bmod 26$

Intro to Crypto

In general, for a shift k we use the function

$$f(p) = (\, p + k) \bmod 26$$

To encode a message

- Convert letters to numbers between 0 and 25
- Pass each value through $f(p)$

Example: Encode *HELLO WORLD* using shift $k = 5$

HELLO WORLD is 7 4 11 11 14 22 14 17 11 3

Shifting gives 12 9 16 16 19 1 19 22 16 8

The encoded message is then *MJQQT BTWQI*

Intro to Crypto

How do we decode a message like *MJQQT BTWQI* ?

If we know the shift then it's easy, we just run it through the inverse

$$f^{-1}(p) = (p - k) \bmod 26$$

Why is this a very unsecure cipher?

The Affine Cipher

Instead of just shifting, multiply and then shift

$$f(p) = (ap + b) \bmod 26$$

where a and b are integers and $\gcd(a, 26) = 1$

Intro to Crypto

Suppose we know a and b, how could we decode a message?

Suppose we have an encrypted character c which we know satisfies

$$c \equiv ap + b \ (\mathbf{mod}\ 26)$$

We need to solve this congruence for p. Subtract b from both sides

$$c - b \equiv ap \ (\mathbf{mod}\ 26)$$

To solve for p we need the inverse of a (which we know exists because $\gcd(a, 26) = 1$). Call this inverse $\bar{a}$, then

$$p \equiv \bar{a}(c - b) \ (\mathbf{mod}\ 26)$$

Example: Use an affine cipher with $a = 7$ and $b = 13$ to encrypt the letter K

The numerical value of K is 10, so we have

$$K \to a \cdot 10 + b = 7 \cdot 10 + 13 = 83 \equiv 5 \ (\mathbf{mod}\ 26) \to F$$

Intro to Crypto

Example: Find a decryption formula for the affine cipher in the previous example and use it to decrypt the character F

We need to compute the inverse of 7 modulo 26

$$26 = 3 \cdot 7 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$

$$\text{Then} \quad 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$$
$$= 3 \cdot (26 - 3 \cdot 7) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7$$

So the inverse of 7 modulo 26 is -11

Intro to Crypto

Example: Find a decryption formula for the affine cipher in the previous example and use it to decrypt the character F

So a decryption formula is given by

$$f^{-1}(c) = -11(c - 13) \bmod 26$$

To decrypt *F* we then have

$$F \to -11(5 - 13) \bmod 26 = 88 \bmod 26 = 10 \to K$$

EFY: Encrypt *HELLO WORLD* with an affine cipher with $a = 5$ and $b = 17$. Derive the decryption formula and check that your encrypted message decrypts back to *HELLO WORLD*.

Chinese Remainder Theorem Proof

Existence Proof: We'll show that a solution exists by construction

Let $M_k = \dfrac{m}{m_k}$ for $k = 1, 2, \ldots, n$

Note that M_k is the product of all m_i's *except* m_k

Since the m_i's are all relatively prime, so are M_k and m_k

Since $\gcd(m_k, M_k) = 1$ there exists an inverse, y_k, s.t.

$$M_k y_k \equiv 1 \ (\mathbf{mod}\ m_k)$$

Find inverses for each M_k, then solution is

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

Chinese Remainder Theorem Proof

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

To see that this is a sol., note that $M_i \equiv 0 \pmod{m_k}$ when $i \neq k$

Since all of the terms in the sum except M_k are congruent to 0 modulo m_k, we have, for any $k = 1, 2, \ldots, n$

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + \cdots + a_k M_k y_k + \cdots + a_n M_n y_n \pmod{m_k} \\ &\equiv a_k M_k y_k \equiv a_k \pmod{m_k} \end{aligned}$$

Thus x solves each congruence in the system

The uniqueness proof can be found in Exercises 29-30 in Section 4.4 of the textbook

EFYs

Back Substitution

EFY: Find x such that $x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{7}$

Since $x \equiv 1 \pmod{5}$ we know that x can be written as

$$x = 5t + 1 \quad \text{for some integer } t$$

Plug into second congruence

$$5t + 1 \equiv 3 \pmod{7} \quad \Rightarrow \quad 5t \equiv 2 \pmod{7}$$

The inverse of 5 modulo 7 is 3, so $t \equiv 3 \cdot 2 \pmod{7} \equiv 6 \pmod{7}$

which implies that $t = 7u + 6$ for some integer u. Plug back in to x

$$x = 5t + 1 = 5(7u + 6) + 1 = 35u + 31$$

Which tells us that $x \equiv 31 \pmod{35}$

Chinese Remainder Theorem

EFY: Find x s.t. $x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{7}$ using the CRT

First note that 5 and 7 are relatively prime, and let $m = 5 \cdot 7 = 35$

We have $M_1 = \dfrac{m}{m_1} = \dfrac{35}{5} = 7$ and $M_2 = \dfrac{m}{m_2} = \dfrac{35}{7} = 5$

The inverse of $M_1 = 7$ modulo 5 is 3

The inverse of $M_2 = 5$ modulo 7 is also 3

Thus the solution is

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 \pmod{35} \\ &\equiv 1 \cdot 7 \cdot 3 + 5 \cdot 3 \cdot 2 \pmod{35} \\ &\equiv 21 + 45 \pmod{35} \equiv 31 \pmod{35} \end{aligned}$$

Fermat's Little Theorem

EFYs: Compute $5^{2003} \pmod 7$

Solution: Note that $2003 = 333 \cdot 6 + 5$, so

$$\begin{aligned} 5^{2003} &\equiv (5^6)^{333} \cdot 5^5 \pmod 7 \\ &\equiv 1 \cdot 5^5 \pmod 7 \\ &\equiv 3125 \pmod 7 \\ &\equiv 446 \cdot 7 + 3 \pmod 7 \\ &\equiv 3 \pmod 7 \end{aligned}$$

Fermat's Little Theorem

EFYs: Compute $5^{2003} \pmod{11}$

Solution: Note that $2003 = 200 \cdot 10 + 3$, so

$$\begin{aligned} 5^{2003} &\equiv (5^{10})^{200} \cdot 5^3 \pmod{11} \\ &\equiv 1 \cdot 5^3 \pmod{11} \\ &\equiv 125 \pmod{11} \\ &\equiv 11 \cdot 11 + 4 \pmod{11} \\ &\equiv 4 \pmod{11} \end{aligned}$$