CS 441: Solving Congruences

PhD. Nils Murrugarra-Llerena
nem177@pitt.edu



[Key CS Link] Congruences

Time on a Clock

Imagine it's 10 o'clock. What time will it be 5 hours from now?

The answer is not 15 o'clock; it's 3 o'clock ☺. A clock naturally "resets" after every 12 hours. This is the essence of modular arithmetic and congruences.



Today's topics

- Arithmetic modulo n (reminder)
- Solving linear congruences
  - Modular inverses
  - Extended Euclidean algorithm and Bézout numbers
- Solving systems of congruences
  - Chinese remainder theorem
- Primitive roots and discrete log



Defining arithmetic restricted to remainders when dividing by m

Recall

$\mathbf{Z}_m$ denotes the set of nonnegative integers less than m

- i.e., the remainders when dividing by m

Recall that **mod** "preserves" addition and multiplication

- (a+b) **mod** m = ((a **mod** m) + (b **mod** m)) **mod** m
- (ab) **mod** m = ((a **mod** m)(b **mod** m)) **mod** m

Thus, we can define versions of addition and multiplication restricted to this set

- $a +_m b = (a+b)$ **mod** m
- $a \cdot_m b = (a \cdot b)$ **mod** m
- These operations form arithmetic modulo m

Modular arithmetic behaves similarly to standard arithmetic: Recap properties from §4.1

Solving congruences via inverses

Consider the equation a + 8 ≡ 2 (mod 11)

- In standard arithmetic, we'd subtract 8 from both sides
  - i.e., utilize the additive inverse

In modular arithmetic, additive inverses are easy to compute!

- –8 ≡ 3 (mod 11)
  - -8 = 11*(-1) + 3
- Thus, we can add 3 to both sides:
  - a + 8 + 3 ≡ 2 + 3 (mod 11)
  - a + 11 ≡ 5 (mod 11)
  - a ≡ 5 (mod 11)
- Note that adding any multiple of m preserves the value (mod m)

Unfortunately, multiplicative inverses are not as simple

We cannot easily “divide by a” mod n

- What is the equivalent of 1/a mod n?

Linear congruences are of the form $ax \equiv b \pmod{m}$

- Given values for *a* and *b*, how do we solve for x?
- We need a value, say $\bar{a}$, where $a\bar{a} \equiv 1 \pmod{m}$
- If we had this, we could multiply on both sides, then simplify!

Good news: Bézout’s theorem says that there exist integers s and t such that gcd(a, m) = sa + tm

- Assume a and m are coprime: How does this help us?

Bézout numbers for modular inverses

If *a* and *m* are coprime, then gcd(a, m) = 1

The extended Euclidean algorithm yields:

- 1 = gcd(a, m) = sa + tm
- So sa = 1 – tm
- Rewrite sa = -tm + 1
- **sa ≡ 1 (mod m)**
  - Remember Since km ≡ 0 (mod m) for any k, this means…

This means that, when *a* and *m* are coprime, the Bézout numbers reveal a's (multiplicative) inverse mod m (!)

Extended Euclidean Algorithm

The extended Euclidean algorithm computes the GCD of a and b, **and** computes the Bézout numbers s and t which satisfy the Bézout identity:

$$\gcd(a, b) = sa + tb$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78					
2							
3							
4							
5							
6							

*Let this represent "a **div** b"*

*"a **mod** b"*

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1				
2							
3							
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2							
3							
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2							
3							
4							
5							
6							



Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21					
3							
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3				
3							
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3							
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15					
4							
5							
6							



Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1				
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4							
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6					
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2				
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5							
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5	6	3					
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5	6	3	2				
6							

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5	6	3	2	0			
6							

Find the Bézout numbers and GCD of 99 and 78

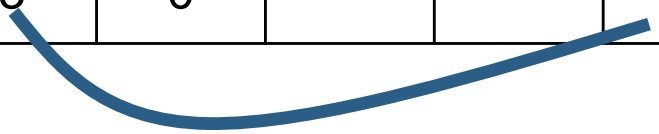
Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5	6	3	2	0			
6	3	0					

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5	6	3	2	0			
6	3	0	—	—			

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21			
2	78	21	3	15			
3	21	15	1	6			
4	15	6	2	3			
5	6	3	2	0			
6	3	0	—	—	3	1	0

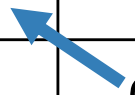


Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3		
5	6	3	2	0	3		
6	3	0	—	—	3	1	0

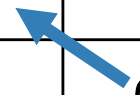
Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3		
5	6	3	2	0	3		
6	3	0	—	—	3	1	0



Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3		
5	6	3	2	0	3	0	
6	3	0	—	—	3	1	0



Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3		
5	6	3	2	0	3	0	
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

= 1 – 2 * 0 = 1

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3		
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3		
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0



$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3	1	
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

= 0 – 2 * 1 = -2

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3		
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3	-2	
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

= 1 – 1 * (-2) = 3

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3		
3	21	15	1	6	3	-2	3
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3	3	
3	21	15	1	6	3	-2	3
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3		
2	78	21	3	15	3	3	-11
3	21	15	1	6	3	-2	3
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3	-11	
2	78	21	3	15	3	3	-11
3	21	15	1	6	3	-2	3
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3	-11	14
2	78	21	3	15	3	3	-11
3	21	15	1	6	3	-2	3
4	15	6	2	3	3	1	-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

Find the Bézout numbers and GCD of 99 and 78

Row	a	b	a/b	a%b	d	s	t
1	99	78	1	21	3	-11	14
2	78	21	3	15	3	3	-11
3							3
4							-2
5	6	3	2	0	3	0	1
6	3	0	—	—	3	1	0

To check your work, verify:

$$99 * (-11) + 78 * 14 = 3$$

$$t = s_{previous} - \left(\frac{a}{b}\right) * t_{previous}$$

An example

Solve the following linear congruence:

$$57x \equiv 5 \pmod{98}$$

Using the extended Euclidean algorithm on 98 and 57, we can show that 98 * (-25) + 57 * 43 = 1, so 43 is the inverse of 57 (mod 98)

Multiply by 43 on both sides

- 57x * 43 ≡ 5 * 43 (mod 98)
- x ≡ 215 (mod 98)
- x ≡ 19 (mod 98)

Solving systems of congruences

The Chinese Remainder Theorem: Let $m_1, m_2, \ldots, m_n$ be pairwise coprime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system:

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

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

1

Let m be the product of the moduli, and let M_k be the product of all but the kth modulus

3 2

- Let y_k be the inverse of $M_k \pmod{m_k}$
- Now, compute $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$

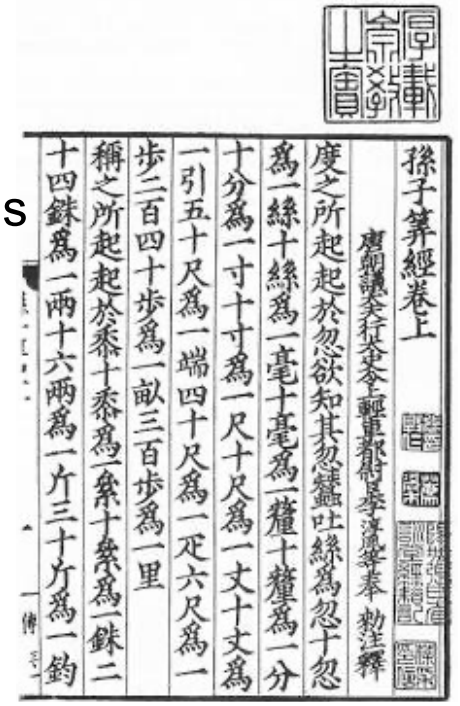
4

Solving systems of congruences

In *Sunzi Suanjing*, the first known example of such problems was posed:

- $x \equiv 2 \pmod 3$ $\quad m_1 = 3, a_1 = 2$
- $x \equiv 3 \pmod 5$ $\quad m_2 = 5, a_2 = 3$
- $x \equiv 2 \pmod 7$ $\quad m_3 = 7, a_3 = 2$

1. $m = 3*5*7 = 105$, and M_k is the product of all but the kth modulus
   2. - $M_1 = 5*7 = 35$, $M_2 = 3*7 = 21$, $M_3 = 3*5 = 15$
      - y_k is the inverse of $M_k \pmod{m_k}$
        - $y_1 = 2$ since $35*2 = 70 \equiv 1 \pmod 3$
        3. - $y_2 = 1$ since $21*1 = 21 \equiv 1 \pmod 5$
           - $y_3 = 1$ since $15*1 = 15 \equiv 1 \pmod 7$
      - Then, $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$
        4. - $x = 2*35*2 + 3*21*1 + 2*15*1 = 233 \equiv 23 \pmod{105}$


孫子算經卷上

唐朝議大夫行太常少卿直弘文館上柱國李淳風奉 勅注釋

度之所起起於忽欲知其忽纖吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

In-class Activities

Activity 1: Find x where 8x ≡ 3 (mod 13) [miro]

Activity 2: Find x where: [miro]

- x ≡ 1 (mod 2)
- x ≡ 2 (mod 3)
- x ≡ 3 (mod 5)

Submit on



Steps:

1. Introduce to a classmate
2. Work in pairs on the exercise
3. Submit answers on miro
4. Volunteers to share answers

Fermat's Little Theorem

Theorem: If *p* is prime and *a* is an integer not divisible by *p*, then $a^{p-1} \equiv 1 \pmod{p}$

- This also means that $a^{p} \equiv a \pmod{p}$

Examples:

- Find 7^{222} **mod** 11
  - Since 11 is prime, $7^{10} \equiv 1 \pmod{11}$
  - Thus, $7^{10k} \equiv 1 \pmod{11}$ for any integer k
  - So $7^{220} \equiv 1 \pmod{11}$, and $7^{222} \equiv 7^{2} \equiv 5 \pmod{11}$
  - 7^{222} **mod** 11 = 5
- Find 5^{147} **mod** 13
  - Since 13 is prime, $5^{12} \equiv 1 \pmod{13}$
  - $5^{144} \equiv 1 \pmod{13}$ so $5^{147} \equiv 5^{3} \equiv 8 \bmod 13$
  - 5^{147} **mod** 13 = 8

The discrete logarithm problem

Given a prime p, a primitive root r modulo p, and a positive integer $b \in \mathbf{Z}_p$, find a value e such that

$$r^e \textbf{ mod } p = b$$

How would you solve this?

- No known algorithm in polynomial time

Takeaways for solving congruences:

- We can invert addition with subtraction
- We can invert multiplication with modular inverses
- **Inverting exponentiation is more difficult than it appears**

Final thoughts

- We can solve congruences by inverting operations, similar to standard algebra
  - To do so with multiplication, we use Euclid's algorithm and Bézout numbers to calculate multiplicative modular inverses
- The Chinese Remainder Theorem allows us to solve systems of congruences with coprime moduli
- Fermat's Little Theorem and primitive roots will come up again in cryptography
  - Section 4.5–4.6, next time!

Extra

Primitive roots

Definition: A primitive root modulo a prime p is an integer r in $\mathbf{Z}_p$ such that every nonzero element of $\mathbf{Z}_p$ is a power of r

- We sometimes call r a generator, since multiplying r by itself repeatedly can generate every element of $\mathbf{Z}_p$
- There is a primitive root in $\mathbf{Z}_p$ for every prime p

Corollary: If b is an integer in $\mathbf{Z}_p$ and r is a primitive root modulo p, then there exists a unique exponent e in $\mathbf{Z}_p$ such that $r^e = b$

- i.e., r^e **mod** $p = b$
- Here, e is called the discrete log of b modulo p with base r
  - $\log_r b = e$ (where the prime p is understood from context)