Number Theory & Cryptography

- Divisibility and Congruence
- Modular Arithmetic and its Applications
- GCD, (Extended) Euclidean Algorithm, Relative Prime
- The Caesar Cipher and Affine Cipher, Modular Inverse
- The Chinese Remainder Theorem
- Fermat's Little Theorem and Modular Exponentiation
- Private and Public Key Cryptography, The RSA Cryptosystem

Imdad ullah Khan

Solving System of Simultaneous Congruences

The Chinese remainder theorem characterizes solvable system of simultaneous congruences and derive a solution

The Chinese Remainder Theorem

- Make an $m \times n$ grid
- Start from lower left and move up and right
- Wrap around both from top to bottom and right to left
- At every step write integers starting from 0

0				

	1			
0				

		2		
	1			
0				

			3	
		2		
	1			
0				

			3	
		2		
	1			
0				4

			3	
		2		
5	1			
0				4

15	11	7	3	19
10	6	2	18	14
5	1	17	13	9
0	16	12	8	4

The Chinese Remainder Theorem

- Make an $m \times n$ grid
- Start from lower left and move up and right
- Wrap around both from top to bottom and right to left
- At every step write integers starting from 0

	7		3		11
6		2		10	
	1		9		5
0		8		4	

The Chinese Remainder Theorem

- Make an $m \times n$ grid
- Start from lower left and move up and right
- Wrap around both from top to bottom and right to left
- At every step write integers starting from 0
- For which m and n the grid gets completely filled in?

15	11	7	3	19
10	6	2	18	14
5	1	17	13	9
0	16	12	8	4

	7		3		11
6		2		10	
	1		9		5
0		8		4	

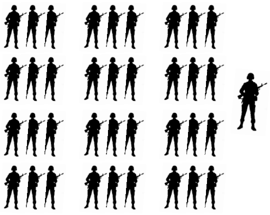
The Chinese Remainder Theorem

Anceint Tale: In a war some soldiers died, wanted to find how many soldiers (**x**) are left. The Chinese emperor ordered a series of tasks

The Chinese Remainder Theorem

Anceint Tale: In a war some soldiers died, wanted to find how many soldiers (**x**) are left. The Chinese emperor ordered a series of tasks

Task-1: Make groups of 3 and report how many couldn't $\triangleright\ x \,\%\, 3 = 1$

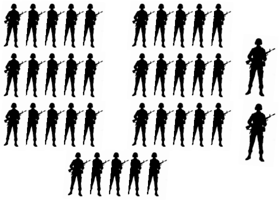


The Chinese Remainder Theorem

Anceint Tale: In a war some soldiers died, wanted to find how many soldiers (**x**) are left. The Chinese emperor ordered a series of tasks

Task-1: Make groups of 3 and report how many couldn't $\triangleright\ x \,\%\, 3 = 1$

Task-2: Make groups of 5 and report how many couldn't $\triangleright\ x \,\%\, 5 = 2$



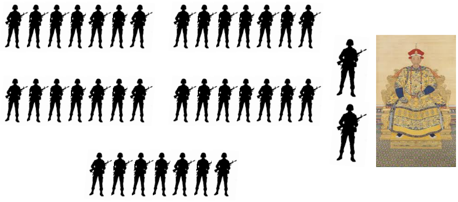
The Chinese Remainder Theorem

Anceint Tale: In a war some soldiers died, wanted to find how many soldiers (**x**) are left. The Chinese emperor ordered a series of tasks

Task-1: Make groups of 3 and report how many couldn't $\triangleright\ x \,\%\, 3 = 1$

Task-2: Make groups of 5 and report how many couldn't $\triangleright\ x \,\%\, 5 = 2$

Task-3: Make groups of 7 and report how many couldn't $\triangleright\ x \,\%\, 7 = 2$



The Chinese Remainder Theorem

Anceint Tale: In a war some soldiers died, wanted to find how many soldiers (**x**) are left. The Chinese emperor ordered a series of tasks

Task-1: Make groups of 3 and report how many couldn't ▷ $x \,\%\, 3 = 1$

Task-2: Make groups of 5 and report how many couldn't ▷ $x \,\%\, 5 = 2$

Task-3: Make groups of 7 and report how many couldn't ▷ $x \,\%\, 7 = 2$

Magically the emperor figured out their number ▷ $\mathbf{x = 37}$

The Chinese Remainder Theorem

Anceint Tale: In a war some soldiers died, wanted to find how many soldiers ($\mathbf{x}$) are left. The Chinese emperor ordered a series of tasks

Magically the emperor figured out their number ▷ $\mathbf{x = 37}$

Solve a system of modular congruences.

Find $x \leq 3 \cdot 5 \cdot 7$ satisfying

$$\begin{aligned} x &\equiv_3 1 \\ x &\equiv_5 2 \\ x &\equiv_7 2 \end{aligned}$$

The Chinese Remainder Theorem

Theorem

If m_1, m_2, m_3 are relatively prime and a_1, a_2, a_3 are integers, then

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ x &\equiv_{m_3} a_3 \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 m_3$

Proof by construction:

1. $n_1 = m/m_1$
2. $y_1 = n_1^{-1} \% m_1$

1. $n_2 = m/m_2$
2. $y_2 = n_2^{-1} \% m_2$

1. $n_3 = m/m_3$
2. $y_3 = n_3^{-1} \% m_3$

▷ y_k always exists as $\mathrm{GCD}(n_k, m_k) = 1$

$x = a_1 n_1 y_1 + a_2 n_2 y_2 + a_3 n_3 y_3$

x satisfies all congruences. Uniqueness!

The Chinese Remainder Theorem

Solve the system of modular congruences

$$x \equiv_3 1$$
$$x \equiv_5 2$$
$$x \equiv_7 2$$

Find $n_1, y_1, n_2, y_2, n_3, y_3$ as follows

$$n_1 = 5 \times 7 = 35 \qquad y_1 = 35^{-1} \text{ modulo } 3 = 2$$
$$n_2 = 3 \times 7 = 21 \qquad y_2 = 21^{-1} \text{ modulo } 5 = 1$$
$$n_3 = 3 \times 5 = 15 \qquad y_3 = 15^{-1} \text{ modulo } 7 = 1$$

Note that by construction

$$n_1 y_1 \equiv_3 1, \quad n_1 y_1 \equiv_5 0, \quad n_1 y_1 \equiv_7 0$$
$$n_2 y_2 \equiv_3 0, \quad n_2 y_2 \equiv_5 1, \quad n_2 y_2 \equiv_7 0$$
$$n_3 y_3 \equiv_3 0, \quad n_3 y_3 \equiv_5 0, \quad n_3 y_3 \equiv_7 1$$

$$x = a_1 n_1 y_1 + a_2 n_2 y_2 + a_3 n_3 y_3 = 1 \cdot 70 + 2 \cdot 21 + 2 \cdot 15 = 142 \equiv_{105} 37$$

Verify that $37 \equiv_3 1, \quad 37 \equiv_5 2, \quad 37 \equiv_7 2$

The Chinese Remainder Theorem

Theorem

If $m_1, m_2, \ldots, m_n$ are relatively prime and $a_1, a_2, \ldots, a_n$ are integers, then

$$\begin{aligned} x &\equiv_{m_1} a_1 \\ x &\equiv_{m_2} a_2 \\ &\vdots \\ x &\equiv_{m_n} a_n \end{aligned}$$

has a unique solution modulo $m = \prod_{i=1}^{n} m_i$

Proof by construction is the same

The Chinese Remainder Theorem

Using CRT we can uniquely represent any integer with remainders when moduli are relatively prime

▷ The integer has to be less than the product of moduli

Any integer $0 \leq x < 15$ can be represented by $(x \;\%\; 3, x \;\%\; 5)$

$$\begin{aligned} 12 &= (0,2) \\ 11 &= (2,1) \end{aligned}$$

How many ordered pairs are possible? ▷ Will the grid fill?

Used two smaller integers to represent a big integer!

To perform arithmetic upon large integers, we can instead perform arithmetic on these small remainders

The Chinese Remainder Theorem

Compute $123684 + 413456$

By CRT any $0 \leq x < 99 \cdot 98 \cdot 97 \cdot 95 = 89,403,930$ can be represented by its remainders modulo these moduli

$$123684 + 413456 \; = \; (33, 8, 9, 89) + (32, 92, 42, 16)$$

$$123684 + 413456 \; = \; (65, 2, 51, 10)$$

To convert back, Solve

$$\begin{aligned} x &\equiv_{99} 65 \\ x &\equiv_{98} 2 \\ x &\equiv_{97} 51 \\ x &\equiv_{95} 10 \end{aligned}$$

We get

$$x \; = \; 123684 + 413456 \; = \; 537140$$

The Chinese Remainder Theorem

Compute 1345×2368

By CRT any $0 \leq x < 99 \cdot 98 \cdot 97 \cdot 95 = 89,403,930$ can be represented by its remainders modulo these moduli

1345×2368

$= (58, 71, 84, 15) * (91, 16, 40, 88)$ $\quad \triangleright$ coordinate-wise products

$= (5278, 1136, 3360, 1320) \; = \; (31, 58, 62, 85)$ $\quad \triangleright$ Took mod

To convert back, Solve

$$x \equiv_{99} 31$$
$$x \equiv_{98} 58$$
$$x \equiv_{97} 62$$
$$x \equiv_{95} 85$$

We get

$$x = 1345 \times 2368 = 3184960$$