Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 8

1. The following are equivalent (TFAE)
2. Inverses
3. More on Multiplicative Inverses
4. Linear Congruence Theorem 2 [LCT2]
5. Fermat's Little Theorem [FℓT]
6. Example of Fermat's Little Theorem
7. Important Corollaries to FℓT
8. Chinese Remainder Theorem [CRT]
9. Chinese Remainder Theorem Example
10. Splitting the Modulus [SM]
11. Introduction to Cryptography
12. Public Key Cryptography
13. Square and Multiply Algorithm

The following are equivalent (TFAE)

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- a and b have the same remainder when divided by m
- $[a] = [b]$ in $\mathbb{Z}_m$.

The following are equivalent (TFAE)

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- a and b have the same remainder when divided by m
- $[a] = [b]$ in $\mathbb{Z}_m$.

For example, solving $[10][x] = [1]$ is the exact same as solving $10x \equiv 1 \pmod{m}$.

Inverses

1. $[-a]$ is the additive inverse of $[a]$, that is, $[a] + [-a] = [0]$.
2. If there exists an element $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1] = [b][a]$, we call $[b]$ the multiplicative inverse of $[a]$ and write $[b] = [a]^{-1}$ or $b \equiv a^{-1} \mod m$.

More on Multiplicative Inverses

Proposition: Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$.

1. $[a]^{-1}$ exists in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.
2. $[a]^{-1}$ is unique if it exists.

Proof:

1. $$\begin{aligned} [a]^{-1} \text{ exists} &\Leftrightarrow [a][x] = [1] \text{ is solvable in } \mathbb{Z}_m \\ &\Leftrightarrow ax + my = 1 \text{ is a solvable [LDE]} \\ &\Leftrightarrow \gcd(a, m) = 1 \text{ [GCDOO]} \end{aligned}$$

   completing the proof. ■

2. Assume $[a]^{-1}$ exists. Suppose there exists a $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1] = [b][a]$. Then

$$\begin{aligned} [a]^{-1}[a][b] &= [a]^{-1}[1] \\ [1][b] &= [a]^{-1} \\ [b] &= [a]^{-1} \end{aligned}$$

Linear Congruence Theorem 2 [LCT2]

Theorem: Let $a, c \in \mathbb{Z}$ and let $m \in \mathbb{N}$. Let $\gcd(a, m) = d$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x] = [x_0]$ is one particular solution, then the complete solution is

$$\left\{[x_0], [x_0 + \tfrac{m}{d}], [x_0 + 2\tfrac{m}{d}], \ldots, [x_0 + (d-1)\tfrac{m}{d}]\right\}$$

Fermat's Little Theorem [FℓT]

Theorem: If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$.
Equivalently, $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$.
Proof: Major Ideas:

- **Lemma:** Let $\gcd(a, p) = 1$. Let

$$S = \{a, 2a, ..., (p-1)a\} \qquad T = \{1, 2, ..., p-1\}.$$

  Then the elements of S are unique modulo p and for all $s \in S$, there exists a unique element $t \in T$ such that $s \equiv t \mod p$.

-

$$\prod_{x \in S} x \equiv \prod_{y \in T} y \mod p \iff \prod_{k=1}^{p-1} ka \equiv \prod_{j=1}^{p-1} j \mod p$$

$$\iff a^{p-1} \prod_{k=1}^{p-1} k \equiv \prod_{j=1}^{p-1} j \mod p \iff a^{p-1} \equiv 1 \mod p$$

Example of Fermat's Little Theorem

Find the remainder when 7^{92} is divided by 11.

Example of Fermat's Little Theorem

Find the remainder when 7^{92} is divided by 11.

$$\begin{aligned} 7^{92} &\equiv 7^{9(10)+2} \mod 11 \\ &\equiv (7^{10})^9 7^2 \mod 11 \\ &\equiv 1^9 \cdot 7^2 \mod 11 \qquad \text{By F}\ell\text{T since } 11 \nmid 7 \\ &\equiv 49 \mod 11 \\ &\equiv 5 \mod 11 \end{aligned}$$

Important Corollaries to FℓT

- **Corollary:** If p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.
- **Corollary:** If p is a prime number and $[a] \neq [0]$ in $\mathbb{Z}_p$, then there exists a $[b] \in \mathbb{Z}_p$ such that $[a][b] = [1]$, namely $[b] = [a^{p-2}] = [a]^{p-2}$.
- **Corollary:** If $r = s + kp$, then $a^r \equiv a^{s+k} \mod p$ where p is a prime and $a \in \mathbb{Z}$ and $r, s, k \in \mathbb{N}$.
- **Corollary:** Prove that if $p \nmid a$ and $r \equiv s \mod (p-1)$, then $a^r \equiv a^s \mod p$.

Chinese Remainder Theorem [CRT]

Theorem: If $\gcd(m_1, m_2) = 1$, then for any choice of integers a_1 and a_2, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2}$.

Chinese Remainder Theorem Example

Solve the simultaneous congruence

$$x \equiv 2 \mod 7 \qquad x \equiv 7 \mod 11$$

Chinese Remainder Theorem Example

Solve the simultaneous congruence

$$x \equiv 2 \mod 7 \qquad x \equiv 7 \mod 11$$

Solution: Write $x = 2 + 7k$ for some $k \in \mathbb{Z}$. Into the second eqn:

$$\begin{aligned} 2 + 7k &\equiv 7 \mod 11 \\ 7k &\equiv 5 \mod 11 \end{aligned}$$

Multiplying both sides by 3 gives

$$\begin{aligned} 3 \cdot 7k \equiv 15 \mod 11 &\iff 21k \equiv 4 \mod 11 \\ \iff -k \equiv 4 \mod 11 &\iff k \equiv 7 \mod 11 \end{aligned}$$

Therefore, $k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$. Thus, since $x = 2 + 7k$ and $k = 7 + 11\ell$, we have

$$x = 2 + 7k = 2 + 7(7 + 11\ell) = 51 + 77\ell$$

Therefore, $x \equiv 51 \mod 77$ is the solution. ■

Splitting the Modulus [SM]

Theorem: Let m and n be coprime positive integers. Then, for any integers x and a, we have

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

simultaneously if and only if $x \equiv a \mod mn$.

Introduction to Cryptography

- What is Cryptography?
- Private vs Public Key Cryptography (Pad Lock analogy)

Public Key Cryptography

1. Alice produces a private key d and a public key e.
2. Bob uses the public key e to take a message M and encrypt it to some ciphertext C
3. Bob then sends C over an insecure channel to Alice.
4. Alice decrypts C to M using d.

- Encryption and decryption are inverses to each other.
- d and e are different,
- Only d is secret.

Square and Multiply Algorithm

Example: Compute $5^{99} \mod 101$

Square and Multiply Algorithm

Example: Compute $5^{99} \mod 101$

Solution: First, we compute successive square powers of 5:

$$5^1 \equiv 5 \mod 101$$
$$5^2 \equiv 25 \mod 101$$
$$5^4 \equiv (25)^2 \equiv 625 \equiv 19 \mod 101$$
$$5^8 \equiv (19)^2 \equiv 361 \equiv 58 \mod 101$$
$$5^{16} \equiv (58)^2 \equiv 31 \mod 101$$
$$5^{32} \equiv (31)^2 \equiv 52 \mod 101$$
$$5^{64} \equiv (52)^2 \equiv 78 \mod 101$$

Square and Multiply Algorithm

Example: Compute $5^{99} \mod 101$

Solution: First, we compute successive square powers of 5:

$$5^1 \equiv 5 \mod 101$$
$$5^2 \equiv 25 \mod 101$$
$$5^4 \equiv (25)^2 \equiv 625 \equiv 19 \mod 101$$
$$5^8 \equiv (19)^2 \equiv 361 \equiv 58 \mod 101$$
$$5^{16} \equiv (58)^2 \equiv 31 \mod 101$$
$$5^{32} \equiv (31)^2 \equiv 52 \mod 101$$
$$5^{64} \equiv (52)^2 \equiv 78 \mod 101$$

Now, in binary, $99 = 64 + 32 + 2 + 1 = 2^6 + 2^5 + 2^1 + 2^0$. Hence,

$$\begin{aligned} 5^{99} &\equiv 5^{64} \cdot 5^{32} \cdot 5^2 \cdot 5^1 \mod 11 \\ &\equiv 78 \cdot 52 \cdot 25 \cdot 5 \mod 11 \\ &\equiv 81 \mod 11 \end{aligned}$$