2007 CTY Summer Program
Introduction to Cryptology
Midterm Examination
Instructor: Také Nakama
July 4, 2007
© All rights reserved.

6. Please compute the following.
   ① 4 mod 11
   ② 11 mod 4
   ③ -11 mod 3
   ④ 3 mod -11
   ⑤ 14 mod 2
   ⑥ 2 mod 14
   ⑦ 115 mod 200
   ⑧ 200 mod 115
   ⑨ 1 mod 415
   ⑩ 415 mod 1
   ⑪ -1 mod 5
   ⑫ 5 mod -1

6. For each of the following, please change the symbol \( \equiv \) to \( \neq \) if and only if it is false.
   ① 4 \( \equiv \) 6 (mod 10) ② 7 \( \equiv \) 3 (mod 10)
   ③ 0 \( \equiv \) 3 (mod 6) ④ 4 \( \equiv \) 4 (mod 9)
   ⑤ 497 \( \equiv \) 506 (mod 3) ⑥ 3 \( \equiv \) 3 (mod 94321)
   ⑦ -18 \( \equiv \) -6 (mod 9) ⑧ -6 \( \equiv \) -18 (mod 9)
① In the context of $\mathbb{Z}_{12}$, please compute the following:

1. $1 \circledast 11$
2. $0 \circledast 0$
3. $9 \circledast 11$
4. $7 \circledast 6$
5. $0 \circledast 12$
6. $4 \circledast 4$

④ Please solve the following equations for $x$ in the $\mathbb{Z}_n$ specified.

Note: $\circledast$ is performed before $\circledast$ or $\oplus$.

1. $4 \circledast x \oplus 8 = 9$ in $\mathbb{Z}_{11}$
2. $4 \circledast 4 \oplus x = 5$ in $\mathbb{Z}_{10}$
3. $4 \circledast 4 \oplus x = 4$ in $\mathbb{Z}_4$

⑦ Please solve the following equations for $x$ in the $\mathbb{Z}_n$ specified. Please find all solutions.

1. $2 \circledast x = 4$ in $\mathbb{Z}_{10}$
2. $2 \circledast x = 3$ in $\mathbb{Z}_{10}$
3. $9 \circledast x = 4$ in $\mathbb{Z}_{12}$

⑥ In $\mathbb{Z}_8$, please compute the following:

1. $7 \oplus 8$
2. $2 \oplus 6$
3. $(3 \oplus 7) \oplus (7 \oplus 3)$
4. $(4 \oplus 6) \oplus (6 \oplus 4)$
1. Suppose that \( b \mod n = r \). Show that \((b + nk) \mod n = r \) for any integer \( k \), i.e., \( b \mod n = (b + nk) \mod n \).

Let's check if this is plausible. We have \( 3 \mod 10 = 3 \), and \((3 + 10) \mod 10 = 13 \mod 10 = 3 \), i.e., \( 3 \mod 10 = (3 + 10) \mod 10 \). Thus, the statement holds for \( b = 3 \), \( n = 10 \), and \( k = 1 \).

2. Suppose \( a \equiv b \pmod{n} \). Show that \( a \mod n = b \mod n \). (You may use 1.)

Let's check if this is plausible. We have \( 3 \equiv 13 \mod 10 \), and \( 3 \mod 10 = 3, \ 13 \mod 10 = 3 \), i.e., \( 3 \mod 10 = 13 \mod 10 \). Thus, the statement holds for \( a = 3, b = 13, \) and \( n = 10 \).

Note: 2) and 3) show that \( a \equiv b \pmod{n} \) if and only if \( a \mod n = b \mod n \).
1. Please solve the following problems.
   1. How many different arrangements can be formed from MISSISSIPPI if the first and last letters must be M and I, respectively?

2. How many different arrangements can be formed from MARVELOUS given that the four vowels must remain in alphabetical order?

3. You wish to make a symmetrical necklace with 15 different beads. In how many different ways can you do this?

4. We want to prove the following formula.
   \[ k \binom{n}{k} = n \binom{n-1}{k-1} \quad (1) \]
   However, to simplify it, you may consider
   \[ 10 \binom{20}{10} = 20 \binom{20-1}{10-1} \quad (2) \]
   1. Please prove (2) (or (1)) using the definition of \( \binom{n}{k} \).

2. Please prove the identity (2) (or (1)) combinatorially, i.e. please develop a question that both sides of the equation answer.
3. Suppose that you have a language with only three letters: a, b, and c and that they occur with frequencies 0.7, 0.2, and 0.1, respectively. The following ciphertext was encrypted by the Vigenère cipher (shifts are mod 3 instead of mod 26, of course):

   C A A A B B C A C B C A B A C A A B C C C A C A

Please find the most probable key.

4. The plugboard in the Enigma machine significantly increases the number of possible keys by swapping pairs of letters. In how many ways can we form 10 pairs of letters from 26 letters?
1. Please describe the algorithm of the Caesar cipher.

2. Please describe the key of the Caesar cipher. What is the number of possible keys?

3. Caesar wants to arrange a meeting with Marc either at an "arena" or at a "river." Caesar sends the ciphertext EVIRE. However, Marc does not know the key, so he tried all possibilities. Where will they meet?