GEH1036/GEK1505 Tutorial 9(week 11)

Tsien Lilong

March 26, 2017

Department of Mathematics,NUS

Personal Information

- Tsien Lilong
  - Email: qian.lilong@u.nus.edu
  - Phone Number: 90874186
  - Website: tsien.farbox.com
    Go to the website, and scroll down, see the **Work** entry, in the "Tutor" project, click the link for more information. I will provide this slide and the source .tex file on that site.
- Course information
  - EVERY WEEK MONDAY 10:00-11:00 S16-0431

1. Encrypt the message

Encrypt the message

Question

Replace the letters in the following message by numbers according to the rule: A = 0,B = 1,...,Z = 25.

BE BACK BY ELEVEN

Hence encrypt the message using the shift transformation given by $y \equiv x + 15 \pmod{26}$.

- According to the coding rule, the message is converted to numbers as

  01 04 01 00 02 10 01 24 04 11 04 21 04 13

- Then shift by $15 \pmod{26}$,

  16 19 16 15 17 25 16 13 19 00 19 10 19 01

- Back to the ciphertext in letters: “QT QPRZ QN TAKTC”.

2. Frequency analysis

Frequency analysis

Question

The following message encrypted by a shift transformation was received "CXJFIFXOFQV YOBBAP ZLKQBJMQ". Use frequency analysis to decipher it.

- The most frequently occurring letters are F, Q and B, with the same count 3.
- The letter used most frequently in English language is E. Suppose the shift is k, i.e. $y = x + k$.
  - If F is encoded by E, then $5 = 4 + k \pmod{26}$. Then $k = 1$. The deciphering transformation is thus $x = y - 1$, which gives "BWIEHE⋯". Does not make sense.
  - If Q is E. Then $16 = 4 + k \pmod{26}$, i.e. $k = 12$. Decipher it by $x = y - 12 \pmod{26}$, which gives "QLXSWS⋯". Does not make sense.

Question

The following message encrypted by a shift transformation was received "CXJFIFXOFQV YOBBAP ZLKQBJMQ". Use frequency analysis to decipher it.

- If B is E, i.e., $1 = 4 + k \pmod{26}$ and $k = -3$. The deciphering transformation is $x = y + 3 \pmod{26}$. This gives: "FAMILIARITY BREEDS CONTEMPT".

3. Inverse of modulo

Inverse of modulo

Question

For each value of a between 1 and 26 inclusive, use trial and error to find the inverse of a modulo 27, if it exists, i.e., find an integer x between 1 and 26 inclusive such that $ax \equiv 1 (\text{mod} 27)$.

- Start from $a = 1$, that is $x \equiv 1 \pmod{27}$, then $x = 1$.
- As for $a = 2$, we have $2x \equiv 1 \pmod{27}$, then $x = \frac{1+27k}{2}, k = 0, 1, ...$ We get $x = 14$.
- $a = 3$, we have $3x \equiv 1 \pmod{27}$, then $x = \frac{1+27k}{3}, k = 0, 1, ...,$ which has no integer solution. i.e. Multiples of 3 don't have inverses modulo 27
- similarly, the rest inverse of a is given as
  $(a, x) = (4, 7), (5, 11), (7, 4), (8, 17), (10, 19), (13, 25), (16, 22),$
  $(20, 23), (26, 26).$

4. Enciphering function

Enciphering function

Question

The enciphering function on 27 symbols is given by the transformation $y = f(x) \equiv ax + b \pmod{27}$. Suppose that $f(1) = 2, f(2) = 6$, find the values of$a$ and b. Hence find the deciphering function in the form $x \equiv a'y + b' \pmod{27}$, where$a', b'$ are integers between 1 and 26 inclusive.

- Find enciphering function. It is in fact to solve a linear system. By $f(1) = 2, f(2) = 6$, we have

$$a + b \equiv 2 \pmod{27}$$
$$2a + b \equiv 6 \pmod{27}$$

Subtracting the first from the second, we get $a \equiv 4$. And $a+b \equiv 2 \pmod{27}$ gives that $b \equiv -2$.

- Deciphering function is

$$x \equiv a'y + b' \pmod{27}.$$

Already we have

$$y \equiv 4x - 2 \pmod{27}$$

then

$$4x \equiv y + 2 \pmod{27}$$

And

$$7 \times 4x \equiv 7y + 14 \pmod{27}.$$
$$\Rightarrow 27x + x \equiv 7y + 14 \pmod{27}$$

Hence

$$x \equiv 7y + 14 \pmod{27}.$$

5. cyphering guess

Cyphering guess

Question

A message in English contains only letters of the alphabet and is encrypted using an affine transformation (with the original spacing words left intact). It is guessed that the letters E,T in the original message have been substituted by I,N respectively. It is also found that the sequences “JI” and “EJI” occur in isolated blocks many times in the encrypted message. Do you think that the guess above is correct? Justify your answer.

- Let the affine transformation be $y = f(x) \equiv\equiv ax + b \pmod{26}$.
- The guess is $f(4) = 8$ and $f(19) = 13$. Hence

$$4a + b \equiv 8, \qquad 19a + b \equiv 13.$$

- Subtract the two congruence equations, we have $15a \equiv 5$, i.e. $15a - 5 = 5(3a - 1) = 26k$. Note that 26 is not divisible by 5, hence 26 must be divisible by $3a - 1$. Then $a = \frac{1+26k}{3}, k = 0, 1, 2, \ldots$,, which gives $a = 9$.
- Then $b \equiv 8 - 4 \times 9 \equiv -2 \pmod{26}$.
- Thus we have

$$y \equiv 9x - 2 \Rightarrow 9x \equiv y + 2 \Rightarrow x \equiv 3y + 6$$

The last equation is obtained for the fact the inverse of 9 mod 26 is 3.

- Using this deciphering formula, note that $E = 4, I = 8, J = 9$,

$$y = 4, x \equiv 3 \times 4 + 6 \equiv 18 = S$$

$$y = 8, x \equiv 3 \times 8 + 6 \equiv 4 = E$$

$$y = 9, x \equiv 3 \times 9 + 6 \equiv 7 = H$$

- Thus "JI" and "EJI" are "HE" and "SHE" respectively. It is likely that the guess is correct.

6. Modulo exponentiation

Modulo exponentiation

Question

Find the remainder when 1243 is divided by 713 using modular exponentiation.

- Write exponent as sum of powers of 2: $43 = 2^5 + 2^3 + 2 + 1 = 32 + 8 + 2 + 1$.
- Compute 12 raised to powers which are powers of 2 mod 713:

$$\begin{aligned} 12^2 &\equiv 144 \\ 12^4 \equiv 144^2 &\equiv 59 \\ 12^8 \equiv 59^2 &\equiv 629 \\ 12^16 \equiv 629^2 &\equiv 639 \\ 12^32 \equiv 639^2 &\equiv 458 \end{aligned}$$

Modulo exponentiation

Question

Find the remainder when 1243 is divided by 713 using modular exponentiation.

- Finally

$$12^{43} = 12^{13} \times 12^{8} \times 12^{2} \times 12^{1} \equiv 458 \times 629 \times 144 \times 12 \equiv 48 \pmod{713}$$

7. Inverse for 43 modulo 600

Inverse for 43 modulo 600

Question

Find an inverse for 43 modulo 600 that lies between 1 and 600, i.e., find an integer $1 \leqslant t \leqslant 600$ such that $43t \equiv 1 \pmod{600}$.

- For such question, first apply Euclidean algorithm, the write the GCD (1 in fact) in terms of two numbers.
- Apply Euclidean algorithm:

$$600 = 43 \cdot 15 + 15$$

$$43 = 15 \cdot 2 + 13$$

$$15 = 13 \cdot 1 + 2$$

$$13 = 2 \cdot 6 + 1$$

Inverse for 43 modulo 600

- Then work backwards:

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 \\ &= 13 - (15 - 13 \cdot 1)6 = 13 \cdot 7 - 15 \cdot 6 \\ &= (43 - 15 \cdot 2)7 - 15 \cdot 6 = 43 \cdot 7 - 15 \cdot 20 \\ &= 43 \cdot 7 - (600 - 43 \cdot 15)20 = 43 \cdot 307 - 600 \cdot 20 \end{aligned}$$

- Taking modulo 600, we have $1 \equiv 43 \cdot 307 \pmod{600}$.
- Thus $t = 307$ is an inverse.

8. RSA

Question

Consider the RSA cryptosystem with $p = 11, q = 17$, so that $n = pq = 187$ and with $k = 7$.

(a) Encrypt the message HI.

(b) Decrypt the encrypted message found in (a).

- H is 08 and I is 09.
- Encrypt each of H,I.
  - Compute the remainder of M^k on division by n. $8^7 \equiv 134 \pmod{187}$ and $9^7 \equiv 70 \pmod{187}$.
  - The ciphertext is the string of digits of the remainders: 134 70.

To decrypt the message 134 70.

- $(p-1)(q-1) = 160$.
- Find a inverse j of k mod 160. Using Euclidean algorithm

$$\begin{aligned} 160 &= 7 \cdot 22 + 67 = 6 \cdot 1 + 1 \\ 1 &= 7 - 6 \cdot 1 = 7 - (160 - 7 \cdot 22) \\ &= 7 \cdot 23 - 160 \cdot 1 \end{aligned}$$

  Hence the $j = 23$.

- To decrypt:

$$134^j \equiv 134^{23} \equiv 8 \qquad 70^j \equiv 70^{23} \equiv 9 \pmod{187}.$$

- Thus the message is HI.

Thank you for listening!