ECE 646 – Lecture 5A

Solving Equations in Modular Arithmetic

1

Solving equations of the form $a \cdot x \equiv b \bmod n$
(linear congruences)

The equation

$$a \cdot x \equiv b \bmod n$$

has

1. one solution iff $\gcd(a, n) = 1$
$x = a^{-1} \cdot b \pmod{n}$

2. no solutions iff $d = \gcd(a, n) \neq 1$, and $d \nmid b$

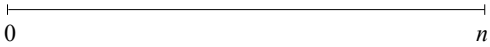
3. *d* solutions iff $d = \gcd(a, n) \neq 1$, and $d \mid b$
The solutions are
$x_0,\ x_0 + n/d,\ x_0 + 2 \cdot n/d,\ x_0 + 3 \cdot n/d,\ \ldots,\ x_0 + (d\text{-}1) \cdot n/d,$
where $x_0 = (a/d)^{-1} \cdot (b/d) \pmod{n/d}$

2

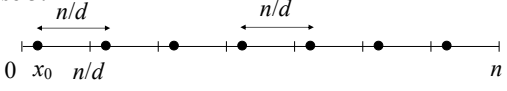
Solving equations of the form $a \cdot x \equiv b \bmod n$
(linear congruences)

Case 1:

Case 2:

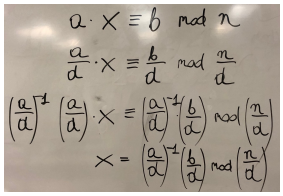


Case 3:



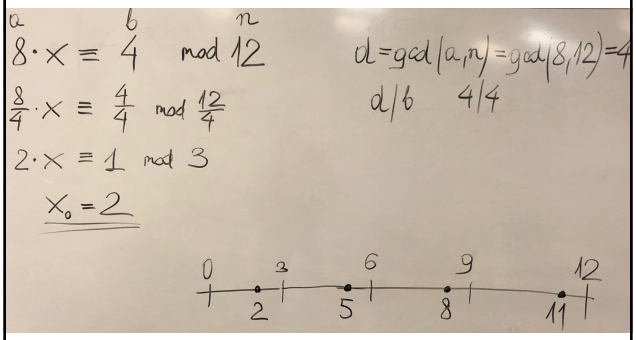
3

Solving equations of the form $a \cdot x \equiv b \bmod n$
Case 3: $d = \gcd(a, n) \neq 1$, and $d \mid b$



4

Solving equations of the form $a \cdot x \equiv b \bmod n$
Case 3: $d = \gcd(a, n) \neq 1$, and $d \mid b$
Example



5

Motivation

Breaking the affine ciphers

6

Coding characters into numbers

A ⇔ 0	N ⇔ 13
B ⇔ 1	O ⇔ 14
C ⇔ 2	P ⇔ 15
D ⇔ 3	Q ⇔ 16
E ⇔ 4	R ⇔ 17
F ⇔ 5	S ⇔ 18
G ⇔ 6	T ⇔ 19
H ⇔ 7	U ⇔ 20
I ⇔ 8	V ⇔ 21
J ⇔ 9	W ⇔ 22
K ⇔ 10	X ⇔ 23
L ⇔ 11	Y ⇔ 24
M ⇔ 12	Z ⇔ 25

7

Historical ciphers

Affine Cipher

Key:

Key = (k_1, k_2) $\quad k_1, k_2 \in [0, 25]$, $\quad \gcd(k_1, 26)=1$

Encryption transformation:

$$c_i = f(m_i) = k_1 \cdot m_i + k_2 \bmod 26$$

Decryption transformation:

$$m_i = f^{-1}(c_i) = k_1^{-1} \cdot (c_i - k_2) \bmod 26$$

8

Historical ciphers

Affine Cipher – Example (1)

Key:

Key = $(k_1, k_2) = (3, 11)$ $\quad 3, 11 \in [0, 25]$, $\quad \gcd(3, 26)=1$

Encryption transformation:

$$c_i = f(m_i) = 3 \cdot m_i + 11 \bmod 26$$

Decryption transformation:

$k_1^{-1} = 3^{-1} \bmod 26 = 9$ $\quad$ because $\quad 3 \cdot 9 \bmod 26 = 1$

$$m_i = f^{-1}(c_i) = 9 \cdot (c_i - 11) \bmod 26$$

9

Historical ciphers

Affine Cipher – Example (2)

coding		encryption		decoding
N	13	$3 \cdot 13 + 11 \bmod 26 = 24$		Y
S	18	$3 \cdot 18 + 11 \bmod 26 = 13$		N
A	0	$3 \cdot 0 + 11 \bmod 26 = 11$		L

10

Historical ciphers

Affine Cipher – Example (3)

coding		decryption		decoding
Y	24	$9 \cdot (24 - 11) \bmod 26 = 13$		N
N	13	$9 \cdot (13 - 11) \bmod 26 = 18$		S
L	11	$9 \cdot (11 - 11) \bmod 26 = 0$		A

11

Breaking the affine cipher (1)

Step 1: Establish a relative frequency of letters in the ciphertext

Ciphertext:

```
FMXVE DKAPH FERBN DKRXR SREFM ORUDS
DKDVS HVUFE DKAPR KDLYE VLRHH RH
```

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

R - 8
D - 7
E, H, K - 5

12

Most frequent single letters

Average frequency in a random string of letters:

$$\frac{1}{26} = 0.038 = 3.8\%$$

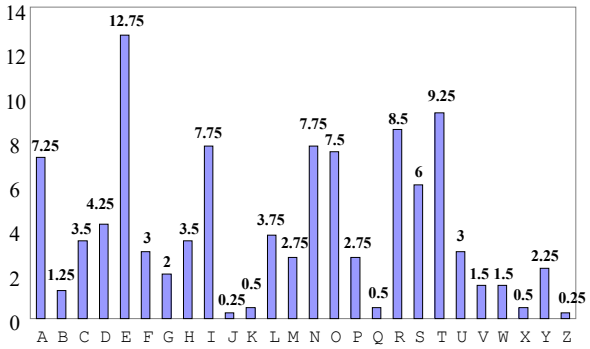
Average frequency in a long English text:

E	—	13%
T, N, R, I, O, A, S	—	6%-9%
D, H, L	—	3.5%-4.5%
C, F, P, U, M, Y, G, W, V	—	1.5%-3%
B, X, K, Q, J, Z	—	< 1%

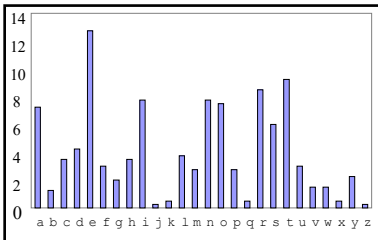
13

Relative frequency of letters in a long English text

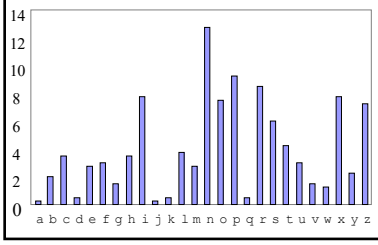
by Stallings



14



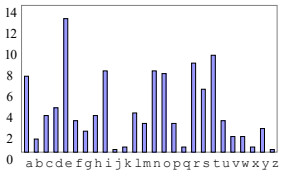
Character frequency in a long English plaintext



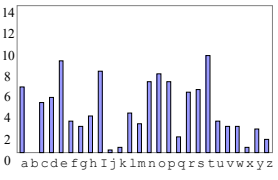
Character frequency in the corresponding ciphertext for the affine cipher

15

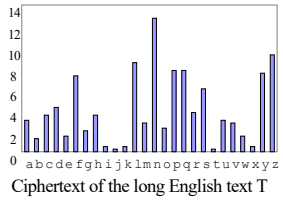
Frequency analysis attack: relevant frequencies



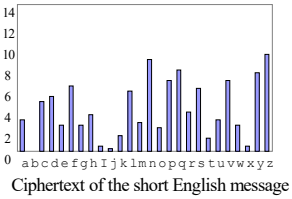
Long English text T



Short English message M



Ciphertext of the long English text T



Ciphertext of the short English message M

16

Breaking the affine cipher (2)

Step 2: Assuming the relative frequency of letters in the corresponding message, derive the corresponding equations

Assumption: Most frequent letters in the message: E and T

Corresponding equations:

$E \rightarrow R$	$f(E) = R$
$T \rightarrow D$	$f(T) = D$
$4 \rightarrow 17$	$f(4) = 17$
$19 \rightarrow 3$	$f(19) = 3$

17

Breaking the affine cipher (3)

Step 3: Solving a set of equations for unknowns k_1 and k_2

$f(4) = 17$
$f(19) = 3$

$\Downarrow$

$4 \cdot k_1 + k_2 \equiv 17 \pmod{26}$
$19 \cdot k_1 + k_2 \equiv 3 \pmod{26}$

$\Downarrow$

$15 \cdot k_1 \equiv -14 \pmod{26}$

$\Downarrow$

$15 \cdot k_1 \equiv 12 \pmod{26}$

18

Solving equations of the form $a \cdot x \equiv b \bmod n$ (linear congruences)

The equation

$$a \cdot x \equiv b \bmod n$$

has

1. one solution iff $\gcd(a, n) = 1$
$x = a^{-1} \cdot b \pmod{n}$

2. no solutions iff $d = \gcd(a, n) \neq 1$, and $d \nmid b$

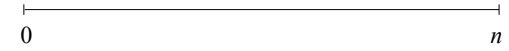
3. *d* solutions iff $d = \gcd(a, n) \neq 1$, and $d \mid b$
The solutions are
$x_0,\ x_0 + n/d,\ x_0 + 2 \cdot n/d,\ x_0 + 3 \cdot n/d,\ \ldots,\ x_0 + (d\text{-}1) \cdot n/d,$
where $x_0 = (a/d)^{-1} \cdot (b/d) \pmod{n/d}$

19

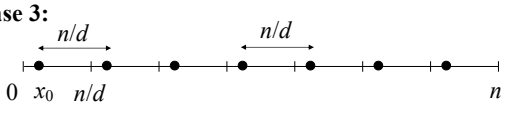
Solving equations of the form $a \cdot x \equiv b \bmod n$ (linear congruences)

Case 1:

Case 2:



Case 3:



20

Breaking the affine cipher (4)

Step 4: Solving the equation of the form
$a \cdot x \equiv b \; mod \; n$ for x = k_1

$$15 \cdot k_1 \equiv 12 \pmod{26}$$

gcd(15, 26) = 1

Thus, one solution

$k_1 = (15^{-1}) \cdot 12 \bmod 26 = 7 \cdot 12 \bmod 26 = 6$

However, gcd(k1, 26) = $2 \neq 1$
Thus, our initial assumption incorrect.

21

Historical ciphers

Affine Cipher

Key:

Key = (k_1, k_2) $\quad k_1, k_2 \in [0, 25]$, $\quad \gcd(k_1, 26)=1$

Encryption transformation:

$$c_i = f(m_i) = k_1 \cdot m_i + k_2 \bmod 26$$

Decryption transformation:

$$m_i = f^{-1}(c_i) = k_1^{-1} \cdot (c_i - k_2) \bmod 26$$

22