Affine Cipher

Math 4175

§2.3.0. Some Number Theory

Recall that Shift Cipher is a special case of Substitution Cipher with only 26 possible keys.

Now we will consider another special case of Substitution Cipher which has larger key space, but still easy to remember.

For this purpose, we need to learn more about modular arithmetic, an area in number theory.

§2.3.0. Some Number Theory

Notations:

- Let $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ be the set of integers (both positive and negative).
- Let $m, n \in \mathbb{Z}$. If $m = nq$ for some $q \in \mathbb{Z}$, then we say that either n divides m, m is divisible by n, m is a multiple of n, n is a factor of m, or n is a divisor of m, and denote it by $n|m$.
- Division Algorithm: If a and b are integers with $b > 0$, then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$ and r is called the remainder and q is called the quotient.
- For any $a, b, c \in \mathbb{Z}$, we say that c is a common divisor of a and b if $c|a$ and $c|b$.

§2.3.0. Some Number Theory

- A positive number $p > 1$ is called a prime number if it has no positive divisors other than 1 and p.
- Every integer $m > 1$ can be factored into powers of primes in a unique way. For example, $120 = 2^3 \times 3 \times 5$ and $490 = 2 \times 5 \times 7^2$.

Theorem: Let $a, b \in \mathbb{Z}$, not both zero. Then there is a unique largest common divisor of a and b, that is, there is a unique positive integer d such that:

- $d|a$ and $d|b$.
- If $c \in \mathbb{Z}$, $c|a$ and $c|b$, then $c|d$.

This number d is called the greatest common divisor of a and b. It is denoted by $\gcd(a, b)$.

§2.3.0. Some Number Theory

- Find $\gcd(60, 490)$
- Find $\gcd(270, 192)$
- More generally, if $a = \pm p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ and $b = \pm p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$, then $d = \gcd(a, b) = p_1^{g_1} p_2^{g_2} \cdots p_n^{g_n}$ where $g_i = \min\{e_i, f_i\}$.

Theorem: Let $a, b \in \mathbb{Z}$, not both zero, and $d = \gcd(a, b)$. Then there exist integers x and y such that $d = ax + by$. In other words, d is a linear combination of x and y in $\mathbb{Z}$.

§2.3.0. Some Number Theory

Proof: Let $S = \{ax + by > 0 | x, y \in \mathbb{Z}\}$. Notice that S is non-empty.

Let $d = ax_0 + by_0$ be the minimum of the set S, that is, the smallest integer in S.

Claim: $d|a$, that is, d divides a. If not, then

$$\begin{aligned} a &= dq + r \text{ for some } 0 < r < d \\ a &= (ax_0 + by_0)q + r \\ r &= a(1 - x_0 q) - by_0 q \\ r &= ax' + by' \end{aligned}$$

which is a contradiction.

Similarly, one can show that d divides b.

§2.3.0. Some Number Theory

Suppose that $c|a$ and $c|b$. Then $c|(ax + by)$ and hence $c|d = ax_0 + by_0$. This proves that $d = \min\{S\} = \gcd(a, b)$.

We found earlier that $\gcd(270, 192) = 6$. So according to above theorem, there exists integers x and y such that $6 = 270x + 192y$.

Can you find such x and y and also the gcd more efficiently?

One may find them by trial and error.

Question: Is there any efficient algorithm to find them?

Yes, there are many of course! We will describe one of them, for the above example $\gcd(270, 192) = 6$ (Source: oxfordmathcenter.com).

§2.3.0. Some Number Theory

We write a table with 7 columns. In the first row, the first 4 numbers are always 1, 0, 0, 1 (in that order), while the 5th and 6th numbers are the two numbers for which one seeks the gcd, and the 7th is always zero.

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0

Then we add a new row using the following rules:

- The new q is the greatest integer less than or equal to the quotient of the old u_3 and v_3.
- The new u_i is the old v_i.
- The new $v_i =$ old $u_i -$ (current q)(old v_i)
- We do this multiple times, until we produce a row where $v_3 = 0$

§2.3.0. Division Algorithm

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0		1		192		1

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0	1	1		192		1

$$1 = 1 - 1 \cdot 0$$

§2.3.0. Division Algorithm

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0	1	1		192		1

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0	1	1	-1	192		1

$$-1 = 0 - 1 \cdot 1$$

§2.3.0. Division Algorithm

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0	1	1	-1	192		1

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0	1	1	-1	192	78	1

$$78 = 270 - 1 \cdot 192$$

§2.3.0. Some Number Theory

We get (Division Algorithm):

u_1	v_1	u_2	v_2	u_3	v_3	q
1	0	0	1	270	192	0
0	1	1	-1	192	78	1
1	-2	-1	3	78	36	2
-2	5	3	-7	36	6	2
5	-32	-7	45	6	0	6

Now $\gcd(270, 192) = 6$ and $(270)(5) + (192)(-7) = 6$.

Write a program to generate the above table to find gcd(1239, 168) and the corresponding linear combination.

§2.3.0. Modular Arithmetic

Definition: Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. If m divides $(a - b)$, then we write as $a \equiv b \pmod{m}$ or simply as $a \equiv b \mod m$ and read as a is congruent to b modulo m.

Examples:

$32 \equiv 7 \mod 5$ $\qquad -12 \equiv 37 \mod 7$ $\qquad 19 \equiv 19 \mod 12$

Recall that we dealt with modulo 26 in the Shift Cipher. For example,

$$29 \equiv 3 \mod 26$$

So in modulo 26 arithmetic 29 and 3 are equivalent and we will write as 29 mod 26 is 3. Compute 101 mod 7 and -101 mod 7.

§2.3.0. Modular Arithmetic

Properties:

- $a \equiv 0 \mod m$ if and only if $m|a$.
- $a \equiv a \mod m$.
- If $a \equiv b \mod m$ if and only if $b \equiv a \mod m$.
- If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.
- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then
  - $a + c \equiv b + d \mod m$ and
  - $ac \equiv bd \mod m$
- In particular, if $a \equiv b \mod m$, then for any x,
  - $a + x \equiv b + x \mod m$ and
  - $ax \equiv bx \mod m$

§2.3.0. Modular Arithmetic

Let $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$. For example, $\mathbb{Z}_{26} = \{0, 1, \cdots, 25\}$. One can define addition $+$ and multiplication $\times$ in $\mathbb{Z}_m$.

Both addition and multiplication are exactly same as real addition and multiplication except the results are reduced to modulo m.

For example, in $\mathbb{Z}_{26}$, one has $23 + 13 = 36$ which is 10 after reducing to modulo 26 and so we simply write it as $23 + 13 = 10 \mod 26$.

Similarly, $23 \times 13 = 299$ which is 13 after reducing to modulo 26, because $299 = (11)(26) + 13$. So $23 \times 13 = 13 \mod 26$!!

Notice that $1 \times 13 = 13 \mod 26$. So the equation $13x = 13$ has more than one solution in modulo 26. So one need to be bit careful in dealing with modular arithmetic.

§2.3.0. Multiplicative inverse

Consider $5 \in \mathbb{Z}_{26}$. Since $\gcd(5, 26) = 1$, one can find x and y (by division algorithm) such that $26x + 5y = 1$.

In this case, we obtain $26(1) + 5(-5) = 1$.

Now $-5 \equiv 21 \mod 26$.

Notice that $(5)(21) = 105 = 4(26) + 1 \equiv 1 \mod 26$.

That is, $(5)(21) \equiv 1 \mod 26$. So 21 is called the multiplicative inverse of 5 in $\mathbb{Z}_{26}$ and we denoted it by $5^{-1} = 21$.

Note: Here $\gcd(5, 26) = 1$ is a necessary condition. For example, $\gcd(10, 26) = 2 \neq 1$. So 10 has no multiplicative inverse in $\mathbb{Z}_{26}$. In other words, 10^{-1} does not exist in $\mathbb{Z}_{26}$, that is, $10x \equiv 1 \mod 26$ has no solution!!!

Notation: Let $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$ be the set of all elements of $\mathbb{Z}_m$ which have multiplicative inverse in $\mathbb{Z}_m$.

§2.3.0. Modular Equations

Solve: $5x + 4 = 20 \mod 26$.

Solution: Since $\gcd(5, 26) = 1$, this equation has unique solution.

$$\begin{aligned}
5x + 4 &= 20 \mod 26 \\
5x + 4 - 4 &= (20 - 4) \mod 26 \\
5x &= 16 \mod 26 \\
(5)^{-1}(5)x &= (5)^{-1}(16) \mod 26 \\
x &= (5)^{-1}(16) \mod 26 \\
x &= (21)(16) \mod 26 \\
x &= 336 \mod 26 \\
x &= (12)(26) + 24 \mod 26 \\
x &= 24 \mod 26
\end{aligned}$$

§2.3.0. Modular Equations

Solve: $20x + 6 = 22 \mod 26$.

Solution: Since $\gcd(20, 26) \neq 1$, this equation may have no solution or more than one solution.

The above equation is equivalent to $20x = 16 \mod 26$.

Now one can reduce the equation to $10x = 8 \mod 13$

Since $\gcd(10, 13) = 1$, one can see by division algorithm that
$(13)(-3) + (10)(4) = 1$, and so $10^{-1} = 4$ in $\mathbb{Z}_{13}$ (NOT in $\mathbb{Z}_{26}$)
or $(10)(-9) + (13)(7) = 1$, and so $10^{-1} = -9 = 4$ in $\mathbb{Z}_{13}$ (NOT in $\mathbb{Z}_{26}$).

By multiplying on both sides of the equation by $10^{-1} = 4$ one gets the solution $x = 6$ in $\mathbb{Z}_{13}$ for the equation $10x = 8 \mod 13$.

So the original equation has solution $x = 6$ and $x = 6 + 13 = 19$ in $\mathbb{Z}_{26}$.

§2.3.0. Modular Arithmetic

Properties (without proof):

1. For any $a, b \in \mathbb{Z}_m,\ a + b \in \mathbb{Z}_m$ (addition is closed)
2. For any $a, b \in \mathbb{Z}_m,\ a + b = b + a$ (addition is commutative)
3. For any $a, b, c \in \mathbb{Z}_m,\ (a + b) + c = a + (b + c)$ (associative)
4. For any $a \in \mathbb{Z}_m,\ a + 0 = a$ (0 is an additive identity)
5. For any $a \in \mathbb{Z}_m,\ a + (m - a) = (m - a) + a = 0$ (additive inverse)
6. For any $a, b \in \mathbb{Z}_m,\ ab \in \mathbb{Z}_m$ (multiplication is closed)
7. For any $a, b \in \mathbb{Z}_m,\ ab = ba$ (multiplication is commutative)
8. For any $a, b, c \in \mathbb{Z}_m,\ (ab)c = a(bc)$ (associative)
9. For any $a \in \mathbb{Z}_m,\ a1 = 1a = a$ (1 is a multiplicative identity)
10. For any $a, b, c \in \mathbb{Z}_m,\ (a + b)c = (ac) + (bc)$ and $a(b + c) = (ab) + (ac)$ (distributive)

§2.3.0. Modular Arithmetic

Remark:

- A group is any set S with an operation that satisfies properties 1, 3-5.
- It is called an abelian group if property 2 also holds.
- A (commutative) ring is any set S with two operations satisfying properties 1-10.
- A field is a commutative ring in which every non-zero element has a multiplicative inverse.

$\mathbb{Z}_m$ is an additive abelian group, and more generally, it is a ring with addition and multiplication. For any prime number p, $\mathbb{Z}_p$ is a (finite) field.

§2.3.1. Affine Cipher

Now we are in a position to describe Affine Cipher, which is a special case of Substitution Cipher where the encryption function is defined by

$$e(x) = (ax + b) \mod 26$$

In order for this encryption makes sense, we need to make sure that it is an injective function (Why?)

Recall that a function $f(x)$ is injective (or 1-1) if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$. In other words, $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.

So we need to know the condition that makes above function $e(x)$ injective. Since there is nothing special with number 26 regarding this argument, we state more general theorem.

§2.3.1. Affine Cipher

Theorem: The function $f(x) = ax + b \mod m$ defined for $a, b, x \in \mathbb{Z}_m$ with $m \geq 2$ is injective if and only if $\gcd(a, m) = 1$.

Proof: First notice that

$$\begin{aligned} f(x_1) = f(x_2) &\iff ax_1 + b \equiv ax_2 + b \mod m \\ &\iff ax_1 \equiv ax_2 \mod m \end{aligned}$$

$(\Rightarrow)$: Suppose that $f(x)$ is injective and $\gcd(a, m) = d > 1$.
Then let $x_2 = \dfrac{m}{d} + x_1$.

Now $ax_2 = \dfrac{a}{d}m + ax_1$ which implies that $ax_1 \equiv ax_2 \mod m$.

So $f(x)$ is not injective which is a contradiction.

§2.3.1. Affine Cipher

($\Leftarrow$): Suppose that $\gcd(a, m) = 1$.

Then there exists s and t such that $sa + tm = 1$ and hence $sa \equiv 1 \mod m$.

Now

$$\begin{aligned} f(x_1) &= f(x_2) \\ \implies ax_1 &\equiv ax_2 \mod m \\ \implies sax_1 &\equiv sax_2 \mod m \\ \implies x_1 &\equiv x_2 \mod m \end{aligned}$$

which implies that $f(x)$ is injective.

Note: In this case, s above is called the multiplicative inverse of a and is denoted by a^{-1}.

§2.3.1. Affine Cipher

If $\gcd(a, m) = 1$, then we say that a and m are relatively prime. The number of integers in $\mathbb{Z}_m$ that are relatively prime to m is denoted by $\phi(m)$. This function is called the Euler phi function.

Example: Since $26 = 2 \times 13$, a is relatively prime to 26 if $a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23,$ and 25. Therefore $\phi(26) = 12$.

In $\mathbb{Z}_{26}$, we have

a	1	3	5	7	11	17	25
a^{-1}	1	9	21	15	19	23	25

§2.3.1. Affine Cipher

More generally, if $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$, then

$$\phi(m) = (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \cdots (p_n^{e_n} - p_n^{e_n - 1})$$

or equivalently,

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_n})$$

If $m = p$, a prime number, then $\phi(p) = p - 1$ and hence every non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse.

Any ring with this property is called field. Hence $\mathbb{Z}_p$ is a field.

§2.3.1. Affine Cipher

An Affine Cipher is a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}$. For each $k = (a, b) \in \mathcal{K}$, define

$$e_k(x) = (ax + b) \mod 26$$

$$d_k(y) = a^{-1}(y - b) \mod 26$$

Remark: A key for Affine Cipher is a pair $(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ with $\gcd(a, 26) = 1$. Using the Euler-phi function, there are 12 possible choices for a and there are 26 choices for b. Therefore, $|\mathcal{K}| = (12)(26) = 312$.

§2.3.1. Affine Cipher

Example: Let $k = (9, 5)$ and so $e_k(x) = 9x + 5 \mod 26$. We want to encrypt the word "hokies".

$$\begin{array}{cccccc} \text{h} & \text{o} & \text{k} & \text{i} & \text{e} & \text{s} \\ 7 & 14 & 10 & 8 & 4 & 18 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 68 & 131 & 95 & 77 & 41 & 167 \\ 16 & 1 & 17 & 25 & 15 & 11 \\ \text{Q} & \text{B} & \text{R} & \text{Z} & \text{P} & \text{L} \end{array}$$

Affine Cipher is used with the key $k = (7, 3)$ to encrypt the following message. Decrypt the message:

`AXG`

§2.3.2. Cryptanalysis of Affine Cipher

Suppose that Oscar received the following message which is encrypted by using Affine Cipher. Decrypt the message.

```
NVKEFFQRKUQHVKXISKSBQRKEXUM
RAXIKRUKSNMKRUXHONHBEQRNKTN
```

The frequency analysis of alphabets yilelds:

letter	A	B	C	D	E	F	G	H	I	J	K	L	M
frequency	1	2	0	0	3	2	0	3	2	0	9	0	2

letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
frequency	5	1	0	4	6	3	1	4	2	0	4	0	0

From the frequency of K we might conjecture that $d_k(\mathrm{K}) = \mathrm{e}$.

§2.3.2. Cryptanalysis of Affine Cipher

The letter R is second most common letter in the text. So we conjecture that $d_k(\mathrm{R}) = \mathrm{t}$.

By encoding the letters, this yields: $e_k(4) = 10$ and $e_k(19) = 17$.

So we get the system of equations in $\mathbb{Z}_{26}$:

$$4a + b = 10$$

$$19a + b = 17$$

This system has unique solution $(a, b) = (23, 22)$ and $\gcd(a, 26) = 1$. How?

§2.3.2. Cryptanalysis of Affine Cipher

So we could guess that the key $k = (23, 22)$ and

- $e_k(x) = 23x + 22 \mod 26$
- $d_k(y) = 23^{-1}(y - 22) = 17(y - 22) = 17y + 16 \mod 26$

But when we decrypt the given message, letter by letter, by using this key, we obtain:

```
djegxxctescfjerwkekhctegrsm
tqrwetsekdmetsrfudfhgctdebd
```

So our conjecture is incorrect!!
We need to modify our conjecture.

§2.3.2. Cryptanalysis of Affine Cipher

- We are still confident that 'e 'corresponds to 'K ', that is, $e_k(4) = 10$.
- So let us revise our conjecture for 't '.
- Since 'N' is almost as common as 'R' in the cipher text, let's assume that 't' corresponds to 'N', that $e_k(19) = 13$.
- So we get a new set of congruences: $e_k(4) = 10$ and $e_k(19) = 13$.

So we get the system of equations in $\mathbb{Z}_{26}$:

$$4a + b = 10$$
$$19a + b = 13$$

This system has unique solution $(a, b) = (21, 4)$ and $\gcd(a, 26) = 1$. How?

§2.3.2. Cryptanalysis of Affine Cipher

So we try the key $k = (21, 4)$ and

- $e_k(x) = 21x + 4 \mod 26$
- $d_k(y) = 21^{-1}(y - 4) = 5(y - 4) = 5y + 6 \mod 26$

By repeating the process of decryption with the new key, we obtain:

```
theaffinecipheruseslinearco
ngruencestoencryptplaintext
```

```
the affine cipher uses linear congruences
to encrypt plaintext
```

So we can conclude that we have determined the key!!