Mathematics 124 (Winter 2009)
Affine Ciphers, Decimation Ciphers, and Modular Arithmetic

Affine Ciphers

An encipherment scheme (or algorithm) of the form

$$E(x) = (ax + b) \,\mathrm{MOD}\, 26$$

is called an **affine cipher**. Here x is the numerical equivalent of the given plaintext letter, and a and b are (appropriately chosen) integers.

Recall that the numerical equivalents of the letters are as follows:

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

Example: Encipher `ITS COOL` with

$$E(x) = (5x + 8) \,\mathrm{MOD}\, 26.$$

Solution: Filling in the following table gives

plain	I	T	S	C	O	O	L
x							
$5x+8$							
$(5x+8)\,\mathrm{MOD}\,26$							
cipher							

If $y = E(x) = (ax+b) \,\mathrm{MOD}\, 26$, then we can "solve for x in terms of y" and so determine $E^{-1}(y)$. That is, if $y \equiv (ax+b) \pmod{26}$, then $y - b \equiv ax \pmod{26}$, or equivalently $ax \equiv (y-b) \pmod{26}$. Using our earlier results, we see that if we multiply both sides by $a^{-1} \pmod{26}$, then $x \equiv a^{-1}(y-b) \pmod{26}$ and so our decipherment function is

$$E^{-1}(y) = a^{-1}(y-b) \,\mathrm{MOD}\, 26.$$

Example: Decipher `HPCCXAQ` if the encipherment function is $E(x) = (5x+8) \,\mathrm{MOD}\, 26$.

Solution: We begin by finding the decipherment function. Since $5x \equiv 1 \pmod{26}$ is solved with $x \equiv 21 \pmod{26}$ we see $5^{-1} \pmod{26} = 21$. Therefore,

$$E^{-1}(y) = 21(y-8) \,\mathrm{MOD}\, 26$$

and so filling in our table gives

cipher	H	P	C	C	X	A	Q
y							
$y-8$							
$21(y-8)$							
$21(y-8)\,\mathrm{MOD}\,26$							
plain							

Example: Suppose that an affine cipher $E(x) = (ax + b)\,\mathrm{MOD}\,26$ enciphers `H` as `X` and `Q` as `Y`. Find the cipher (that is, determine a and b).

Solution: We see that `H` $\mapsto$ `X` means $E(7) = 23$ and `Q` $\mapsto$ `Y` means $E(16) = 24$. That is,

$$a \cdot 7 + b \equiv 23 \pmod{26} \text{ and } a \cdot 16 + b \equiv 24 \pmod{26}.$$

Subtracting gives $16a - 7a \equiv 1 \pmod{26}$ so that $9a \equiv 1 \pmod{26}$. Therefore, $a = 9^{-1} \pmod{26} = 3$. Finally, we substitute $a = 3$ into either of the earlier equations and solve for b,

$$\text{i.e., } 3 \cdot 7 + b \equiv 23 \pmod{26} \text{ implies } b = 2.$$

In summary,

$$E(x) = (3x + 2)\,\mathrm{MOD}\,26.$$

Remark: (The "Mod-mod Connection")
The least non-negative solution of the congruence $x \equiv b \pmod{m}$ is $x = b\,\mathrm{MOD}\,m$.

Decimation Ciphers

In the special case where $b = 0$, the affine cipher $E(x) = ax\,\mathrm{MOD}\,m$ is called a **decimation cipher**. This is discussed in detail on pages 70–73. The key idea in this subsection is that certain choices of a and m do not lead to valid substitutions.

Example: Suppose that $E(x) = 4x\,\mathrm{MOD}\,26$. Determine the ciphertext alphabet.

Solution: We begin with our table of numerical equivalents, and then determine $4x\,\mathrm{MOD}\,26$.

plain	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
$4x$													
$4x\,\mathrm{MOD}\,26$													
cipher													
plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25
$4x$													
$4x\,\mathrm{MOD}\,26$													
cipher													

The problem, of course, is that 4 and 26 are *not* relatively prime, and so this cyclic phenomenon occurs in the cipher alphabet. Since the numbers $0, 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24$ are not relatively prime with respect to the 26, the only possible choices for the decimation cipher $E(x) = ax\,\mathrm{MOD}\,26$ are $a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$. Therefore, we conclude that the decimation cipher is weaker than the simple shift cipher. If the cryptanalyst knows that a shift cipher has been used, then there are 25 possible shifts that need to be checked. However, if it is known that a decimation cipher has been used, then there are only 12 possible ciphers that need to be checked.

Summary of Valid Affine Ciphers

The function $E(x) = (ax + b)\,\mathrm{MOD}\,26$ defines a valid affine cipher if a is relatively prime to 26, and b is an integer between 0 and 25, inclusive. If $b = 0$, then we refer to this cipher as a decimation cipher. (Note that since there are 12 valid choices of a and 26 valid choices of b, there are $12 \times 26 = 312$ possible valid affine ciphers.)

Also note that if $a = 1$, then $E(x) = (x + b)\,\mathrm{MOD}\,26$ is simply a Caesar $(+b)$ shift cipher.