UW Math Circle

March 21, 2013

We can represent each letter in the alphabet as a number (mod 26): $A = 1, B = 2, C = 3, \ldots, Y = 25, Z = 0$.

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

Try to encrypt, send, and decrypt secret messages using the following rules.

1. To encrypt a message, replace x with $x + a$, where a is your secret key, and reduce mod 26.

   For example, I tell you that my secret key is 2 and send you the message "FQI" (6,17,9). You know that I must have meant "DOG" (4,15,7).

   Try this with different keys. Also see if your partner can decrypt your message without knowing the key! In general, do you think this is a very secure encryption method?

2. Now try encrypting by replacing x with $x \cdot a$, where a is your secret key.

   For example, if my key is 7 and I want to send "DOG" (4,15,7), I will multiply by 7 to get (28,105,49) and reduce mod 26 to get (2,1,23) – "BAW".

   Can you find a fast way to decrypt messages when you know the key is 7? Try using different keys, such as 4, 13, or 21. Can you always decrypt the messages? Do you think this is a very secure encryption method?

3. What if you replace x with $5x + 7$ and reduce mod 26? Have you added an extra layer of security by using ciphers of the form $x \mapsto ax + b$? Can your partner still easily decrypt the message without knowing a and b?

4. For fun: try to think of an English word...

   (a) containing the sequence of letters "CHB"

   (b) containing the sequence of letters "UND" twice

   (c) containing the sequence of letters "GGU" (only one such word!)