Math 139
Quiz 2

Solution
21 February 2003

Multiplicative inverses modulo 26

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

	0	1	2	3	4	5	6	7	8	9
0	A	B	C	D	E	F	G	H	I	J
1	K	L	M	N	O	P	Q	R	S	T
2	U	V	W	X	Y	Z				

1. Let f map $\{0, 1, 2, \ldots, 25\}$ to $\{0, 1, 2, \ldots, 25\}$ by $f(x) = (11x + 10) \bmod 26$. Find a function g such that $g \circ f(x) = x$ for all x. Also find $g(0)$.

   Solution: We need $g(x) = 11^{-1}(x - 10)$. From the table above, we find that 11^{-1} is 19, so our function is

   $$\begin{aligned} g(x) &= 19(x - 10) \bmod 26 \\ &= (19x - 190) \bmod 26 \\ &= (19x + 18) \bmod 26. \end{aligned}$$

   Thus $g(0) = 18$.

2. Suppose we have an affine cipher $f_{a,b} : \mathbb{A} \to \mathbb{A}$, and we guess that f sends plaintext e to ciphertext U and plaintext t to B. Find a and b. (Find values for a and b that are in the set $\{0, 1, 2, \ldots, 25\}$).

   Solution: The two mappings give us the congruences

   $$\begin{aligned} 4a + b &\equiv 20 \pmod{26} \\ 19a + b &\equiv 1 \pmod{26}. \end{aligned}$$

   We subtract the first from the second to get

   $$\begin{aligned} 15a &\equiv -19 \pmod{26} \\ &\equiv 7 \pmod{26}. \end{aligned}$$

   From the table above, we find that 15^{-1} is 7, so we get

   $$\begin{aligned} a &\equiv 7 \times 7 \pmod{26} \\ &\equiv 23 \pmod{26}. \end{aligned}$$

   To find b, we substitute 23 for a in the first congruence above, getting

   $$\begin{aligned} 4 \times 23 + b &\equiv 20 \pmod{26} \\ 92 + b &\equiv 20 \pmod{26} \\ b &\equiv -72 \pmod{26} \\ &\equiv 6 \pmod{26}. \end{aligned}$$

   The solution is $a = 23$, $b = 6$.