

Math 55 — Discrete Mathematics — Spring 2003

Quiz 2 Solutions

Both versions had the same cipher with different messages.

Consider the cipher in which the letters A through Z are represented by congruence classes 0 through 25 (mod 26), and encrypted using the function that sends p to

$$f(p) = 17p + 10 \pmod{26}$$

Find the decryption function $g(p)$, and decrypt this message:

CAKZ

or

ZAC!

Hint: $17 \cdot (-3) = -52 + 1$.

We need to solve

$$q \equiv 17p + 10 \pmod{26}$$

for p in terms of q . The hint shows that $17(-3) \equiv 1 \pmod{26}$. So subtract 10 and multiply by -3 to get

$$p \equiv -3(q - 10) \equiv 4 - 3q \pmod{26},$$

that is,

$$g(p) = 4 - 3p \pmod{26}.$$

The letters in the messages are $A = 0$, $C = 2$, $K = 10$, $Z = 25 \equiv -1$. Applying the decryption function g , we get $A \rightarrow 4 = E$, $C \rightarrow -2 \equiv 24 = Y$, $K \rightarrow 0 = A$, $Z \rightarrow 7 = H$. So

CAKZ \rightarrow YEAH,

ZAC! \rightarrow HEY!