Math373 **Quiz 5** **Fri. Feb 18, 2022**

Name: Solutions

Directions: Show all work. No credit for answers without work.

1. Recall the affine cipher with $\mathcal{K} = \mathbb{F}_p^* \times \mathbb{F}_p$, $\mathcal{M} = \mathcal{C} = \mathbb{F}_p$, encryption function $e_k(m) = \alpha m + \beta$, and decryption function $d_k(c) = \alpha^{-1}(c - \beta)$, where the key k is the pair (α, β).

   (a) [**3 points**] Alice and Bob choose $p = 149$ and key $k = (43, 16)$. Alice wishes to send Bob the message $m = 101$. What ciphertext should she send?

$e_k(101) = \alpha(101) + \beta = (43)(101) + 16 = 4343 + 16 = 4359 = (29)(149) + 38 = \boxed{38}$

$149 \overline{)4359}$ quotient 29; 298; 1379; 134; 38

$(150-1)(10-1) = 1500 - 160 + 1$

$= 1341$

   (b) [**4 points**] Alice receives the ciphertext $c = 20$ from Bob. What is the corresponding plaintext message?

Need $\alpha^{-1} \pmod p$:

$149 = (3)(43) + 20$

$43 = (2)(20) + 3$

$20 = (6)(3) + 2$

$3 = (1)(2) + 1$

$1 = 3 - (1)(2)$

$= 3 - (1)[20 - (6)(3)]$

$= (7)(3) - (1)(20)$

$= (7)[43 - (2)(20)] - (1)(20)$

$= (7)(43) - (15)(20)$

$= (7)(43) - (15)[149 - (3)(43)]$

$= (52)(43) - (15)(149)$

So $(43)^{-1} \equiv 52 \pmod{149}$.

Check: $(40+3)(50+2) = 2000 + 150 + 80 + 6$

$= 2236 = 746 = (5)(149) + 1$ ✓

$d_k(c) = (c - \beta)\alpha^{-1}$

$= (20 - 16)(43)^{-1} = (4)(52)$

$= 208 = 208 - 149 = \boxed{59}$

Check: $e_k(59) \doteq (43)(59) + 16$

$= (43)(60-1) + 16 = 2580 - 43 + 16$

$= 2580 - 27 = 2553 = (17)(149) + 20$

$149 \overline{)2533}$ quotient 17; 1043

$= 20$ ✓

2. [**3 points**] Alice and Bob still use the affine cipher with $p = 149$ but start using a new key (α, β). Eve obtains two plaintext/ciphertext pairs: $(m_1, c_1) = (32, 81)$ and $(m_2, c_2) = (33, 123)$. Help Eve obtain the secret key (α, β).

(m_1, c_1): $81 = \alpha \cdot 32 + \beta$ (Eq 1)

(m_2, c_2): $123 = \alpha \cdot 33 + \beta$ (Eq 2)

$123 - 81 = \alpha(33 - 32)$ (Eq 2) − (Eq 1)

$\underline{42 = \alpha}$

$81 = (42)(32) + \beta$

$\beta = 81 - [(40+2)(30+2)]$

$= 81 - [1200 + 60 + 80 + 4]$

$= 81 - [1344] = -1263$

$= -1263 + 1490 = 227 = 227 - 149$

$= \underline{78}$

So the key is $(\alpha, \beta) = \boxed{(42, 78)}$