Cryptography - Homework 2a

Samuel Breese

October 8, 2018

1 Prove that congruence modulo some $m : \mathbb{N}$ is symmetric and transitive:

Consider a function

$$f_m : \mathbb{N} \to \{x : \mathbb{N} \mid x < m\}$$

mapping the natural numbers to the residue set for the modulus m. We know that such a function exists, as it is simply defined in terms of the integer remainder function

$$\text{rem} : \mathbb{N} \to \Pi d : \mathbb{N}. \{x : \mathbb{N} \mid x < n\}$$

by $f_m(x) = x \text{ rem } m$.

We can consider a statement of congruence modulo m of naturals a and b as a simple statement of equality of the images of a and b under f_m; i.e., $a \equiv b \pmod{m}$ is (definitionally) $f_m(a) = f_m(b)$. By reducing congruence to equality in this way, our task becomes trivial: we know that equality is an equivalence relation, and so therefore it is both symmetric and transitive, and therefore congruence is both symmetric and transitive.

Aside: Note that this proof, along with the trivial observation that congruence is reflexive, demonstrates that congruence is an equivalence relation. We can therefore define the objects of the finite field of naturals defined by a modulus m as the quotient set $\mathbb{N} / \equiv \pmod{m}$ of the natural numbers under congruence modulo m. A bijection

$$g : \{x : \mathbb{N} \mid x < m\} \to \mathbb{N} / \equiv \pmod{m}$$

exists between this quotient and the naturals less than m (g is trivially defined, simply take the least element of each equivalence class). Alternatively worded, there is an isomorphism in **Set** between $\mathbb{N} / \equiv \pmod{m}$ and

$\{x : \mathbb{N} \mid x < m\}$. With this in mind, the function f_m is exactly the canonical projection of congruence modulo m (up to isomorphism). This justifies our definition of congruence modulo m as equality under f_m: assuming congruence is an equivalence relation and searching for a canonical projection leads us straight to f_m!

2 Find the multiplicative inverse (using the extended Euclidean algorithm):

2.1 1234 (mod 4321)

$$r_0 = 4321,\ s_0 = 1,\ t_0 = 0$$

$$r_1 = 1234,\ s_1 = 0,\ t_1 = 1$$

$q_2 = 4321 \operatorname{div} 1234 = 3$, $r_2 = 4321 \operatorname{rem} 1234 = 619$, $s_2 = 1{-}3{\times}0 = 1$, $t_2 = 0{-}3{\times}1 = -3$

$q_3 = 1234 \operatorname{div} 619 = 1$, $r_3 = 1234 \operatorname{rem} 619 = 615$, $s_3 = 0{-}1{\times}1 = -1$, $t_3 = 1{-}1{\times}{-3} = 4$

$q_4 = 619 \operatorname{div} 615 = 1$, $r_4 = 619 \operatorname{rem} 615 = 4$, $s_4 = 1{-}1{\times}{-1} = 2$, $t_4 = -3{-}1{\times}4 = -7$

$q_5 = 615 \operatorname{div} 4 = 153$, $r_5 = 615 \operatorname{rem} 4 = 3$, $s_5 = -1{-}153{\times}2 = -307$, $t_5 = 4{-}153{\times}{-7} = 1075$

$q_6 = 4 \operatorname{div} 3 = 1$, $r_6 = 4 \operatorname{rem} 3 = 1$, $s_6 = 2{-}1{\times}{-307} = 309$, $t_6 = -7{-}1{\times}1075 = -1082$

$q_7 = 3 \operatorname{div} 1 = 3$, $r_7 = 3 \operatorname{rem} 1 = 0$, $s_7 = -307{-}3{\times}309 = -1234$, $t_7 = 1075{-}3{\times}{-1082} = 4321$

Considering $t_6 = -1082$, we see that $1234 \times -1082 \equiv 1 \pmod{4321}$. Thus, the inverse is $-1082 \equiv 3239 \pmod{4321}$.

2.2 24140 (mod 40902)

24140 and 40902 are not relatively prime (both are even), so therefore no inverse exists.

2.3 550 (mod 1769)

$$r_0 = 1769,\ s_0 = 1,\ t_0 = 0$$

$$r_1 = 550,\ s_1 = 0,\ t_1 = 1$$

$q_2 = 1769 \operatorname{div} 550 = 3$, $r_2 = 1769 \operatorname{div} 550 = 119$, $s_2 = 1{-}3{\times}0 = 1$, $t_2 = 0{-}3{\times}1 = -3$

$q_3 = 550 \operatorname{div} 119 = 4$, $r_3 = 550 \operatorname{div} 119 = 74$, $s_3 = 1{-}4{\times}1 = -3$, $t_3 = 1{-}4{\times}{-3} = 13$

$q_4 = 119 \operatorname{div} 74 = 1$, $r_4 = 119 \operatorname{div} 74 = 45$, $s_4 = 1{-}1{\times}{-3} = 4$, $t_4 = -3{-}1{\times}13 = -16$

$q_5 = 74 \text{ div } 45 = 1$, $r_5 = 74 \text{ div } 45 = 29$, $s_5 = -3 - 1 \times 4 = -7$, $t_5 = 13 - 1 \times -16 = 29$

$q_6 = 45 \text{ div } 29 = 1$, $r_6 = 45 \text{ div } 29 = 16$, $s_6 = 4 - 1 \times -7 = 11$, $t_6 = -16 - 1 \times 29 = -45$

$q_7 = 29 \text{ div } 16 = 1$, $r_7 = 29 \text{ div } 16 = 13$, $s_7 = -7 - 1 \times 11 = -18$, $t_7 = 29 - 1 \times -45 = 74$

$q_8 = 16 \text{ div } 13 = 1$, $r_8 = 16 \text{ div } 13 = 3$, $s_8 = 11 - 1 \times -18 = 29$, $t_8 = -45 - 1 \times 74 = -119$

$q_9 = 13 \text{ div } 3 = 4$, $r_9 = 13 \text{ div } 3 = 1$, $s_9 = -18 - 4 \times 29 = -134$, $t_9 = 74 - 4 \times -119 = 550$

$q_{10} = 3 \text{ div } 1 = 3$, $r_{10} = 3 \text{ div } 1 = 0$, $s_{10} = 29 - 3 \times -134 = 431$, $t_9 = -119 - 3 \times 550 = 1769$

Considering $t_6 = 550$, we see that $550 \times 550 \equiv 1 \pmod{1769}$. Thus, the inverse is 550.

3 Determine which of the following are reducible over GF(2):

3.1 $x^3 + 1$

Reducible:

$(x^2 + x + 1) \times (x + 1) \equiv x^3 + x^2 + x + x^2 + x + 1 \equiv x^3 + 2x^2 + 2x + 1 \equiv x^3 + 1$

3.2 $x^3 + x^2 + 1$

Irreducible.

3.3 $x^4 + 1$

Reducible:

$$(x^2 + 1) \times (x^2 + 1) \equiv x^4 + 2x^2 + 1 \equiv x^4 + 1$$

4 Determine the GCD of the following pairs of polynomials:

4.1 $x^3 - x + 1$ and $x^2 + 1$ over GF(2)

$x^3 - x + 1 \equiv x^3 + x + 1$ is irreducible.

$x^2 + 1 \equiv (x + 1) \times (x + 1)$

The only shared irreducible factor is therefore 1, and therefore the GCD is also 1.

4.2 $x^5+x^4+x^3-x^2-x+1$ and x^3+x^2+x+1 over GF(3)

$$x^5+x^4+x^3-x^2-x+1 \equiv x^5+x^4+x^3+2x^2+2x+1$$

Using the Euclidean algorithm for polynomials:

$$(x^5+x^4+x^3+2x^2+2x+1) \equiv x^2 \times (x^3+x^2+x+1)+(x^2+2x+1)$$

$$(x^3+x^2+x+1) \equiv x \times (x^2+2x+1)+(2x^2+1)$$

$$(x^2+2x+1) \equiv 1 \times (2x^2+1)+(2x^2+2x)$$

$$(2x^2+1) \equiv 1 \times (2x^2+2x)+(x+1)$$

$$(2x^2+x) \equiv x \times (x+1)+0$$

The GCD is $x+1$.

5 For the following cryptosystem $\{P, K, C, E, D\}$, calculate $H(K|C)$:

$P=\{a,b,c\}$ with $P_P(a)=\frac{1}{4}$, $P_P(b)=\frac{1}{4}$, and $P_P(c)=\frac{1}{2}$.

$K=\{k_1,k_2,k_3\}$ with $P_K(k_1)=\frac{1}{2}$, $P_K(k_2)=\frac{1}{4}$ and $P_K(k_3)=\frac{1}{4}$.

$C=\{1,2,3,4\}$

$E_{k_1}(a)=1$, $E_{k_1}(b)=2$, and $E_{k_1}(c)=1$ $E_{k_2}(a)=2$, $E_{k_2}(b)=3$, and $E_{k_2}(c)=1$ $E_{k_3}(a)=3$, $E_{k_3}(b)=2$, and $E_{k_3}(c)=4$ $E_{k_4}(a)=3$, $E_{k_4}(b)=4$, and $E_{k_4}(c)=4$

We must find $H(K|C)=H(K)+H(P)-H(C)$.

Assuming X is a random variable which takes on a finite set of n values according to some distribution $p(X)$, then

$$H(X)=-\sum_{i=1}^{n} p_i \log_2(p_i)$$

Therefore $H(P)=-\left(-\frac{2}{4}-\frac{2}{4}-\frac{1}{2}\right)=\frac{3}{2}$.

Similarly, $H(K)=-\left(-\frac{1}{2}-\frac{2}{4}-\frac{2}{4}\right)=\frac{3}{2}$.

Computing $H(C)$ requires us to find a probability distribution P_C for the ciphertext. To do this, we look at values of K and P that can lead to a given ciphertext C:

$$P_C(1)=P_P(a)P_K(k_1)+P_P(c)P_K(k_1)+P_P(c)P_K(k_2)=\frac{1}{4}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times\frac{1}{4}=\frac{1}{2}$$

$$P_C(2) = P_P(b)P_K(k_1)+P_P(a)P_K(k_2)+P_P(b)P_K(k_3) = \frac{1}{4}\times\frac{1}{2}+\frac{1}{4}\times\frac{1}{4}+\frac{1}{4}\times\frac{1}{4} = \frac{1}{4}$$

$$P_C(3) = P_P(b)P_K(k_2)+P_P(a)P_K(k_3)+P_P(a)P_K(k_4) = \frac{1}{4}\times\frac{1}{4}+\frac{1}{4}\times\frac{1}{4}+\frac{1}{4}\times 0 = \frac{1}{8}$$

$$P_C(4) = P_P(c)P_K(k_3)+P_P(b)P_K(k_4)+P_P(c)P_K(k_4) = \frac{1}{2}\times\frac{1}{4}+\frac{1}{4}\times 0+\frac{1}{2}\times 0 = \frac{1}{8}$$

Thus, $H(C) = -\left(-\frac{1}{2} - \frac{2}{4} - \frac{3}{8} - \frac{3}{8}\right) = \frac{11}{8}$.

Therefore, $H(K|C) = H(K) + H(P) - H(C) = \frac{3}{2} + \frac{3}{2} - \frac{11}{8} = \frac{13}{8} = 1.625$.