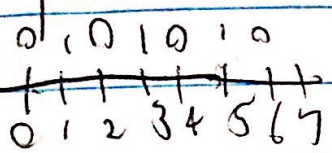
10/6/2018 HW2 Theory Pt. a.

$17 \bmod 5 = 2 / 7$ $5 = 3 \pmod 2$



① Prove that

a) $a \equiv b \pmod n$ implies $b \equiv a \pmod n$

b) prove that $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$

~~a) $17 \bmod 5 = 2$. So, $17 \equiv 2 \bmod 5$. When divided by n, a & b have same remainder. n divides a-b AKA $n \mid (a-b)$~~

(a) If $a \equiv b \bmod n$, this is equivalent to $n \mid (a-b)$. We can also write $n \mid (-1)(a-b)$, and this means $n \mid (b-a)$. $n \mid (b-a)$ is equivalent to $b \equiv a \pmod n$. Therefore, $a \equiv b \bmod n$ implies $b \equiv a \bmod n$.

(b) If $a \equiv b \bmod n$, then $n \mid (a-b)$ and $n \mid (b-a)$. If $b \equiv c \bmod n$, the $n \mid (c-b)$ and $n \mid (b-c)$. This can be used to show $a \equiv c \bmod n$ as this can be written as $n \mid (a-c)$ or $n \mid (c-a)$. We can combine these to have $n \mid (b-a+c-b)$. The b cancels out and we have $n \mid (c-a)$, which is equivalent to $a \equiv c \bmod n$.

① Using extended Euclidean Algorithm Find the multiplicative inverse of

(a) 1234 mod 4321

(b) 24140 mod 40902

(c) 550 mod 1769

$1234 \overline{)4321}^{3}$

-3702

619

(a) $4321 = 1234 \cdot 3 + 619$

$1234 = 619 \cdot 1 + 615$

$619 = 615 \cdot 1 + 4$

$615 = 4 \cdot 153 + 3$

$4 = 3 \cdot 1 + 1$

$1 = 4 - 3$

Sub. $3 = 615 - (4 \cdot 153)$

$1 = 4 - (615 - (4 \cdot 153))$

$1 = 4 - 615 + (4 \cdot 153)$

$1 = -615 + 4(154)$

$1 = -615 + (619 - 615(1))(154)$

$1 = -615 + 619(154) - 615(154)$

$1 = -615(155) + 619(154)$

$1 = -(1234 - 619)(155) + 619(154)$

$1 = -1234(155) + 619(155) + 619(154) = -1234(155) + 619(309)$

$1 = -1234(155) + (4321 - 1234 \cdot 3)(309)$

$1 = -1234(155) + 4321(309) - 1234(927)$

$1 = -1234(1082) + 4321(309)$

$1 = (309(4321) - 1082(1234))$

So $1234 \cdot x \bmod 4321 = 1$

$1234(1082) \bmod 4321 = 1$. So the multiplicative inverse is $\boxed{1082}$.

(b) $40902 = 24140(1) + 16762$

$24140 = 16762 + 7378$

$16762 = 7378 \cdot 2 + 2006$

$7378 = 2006 \cdot 3 + 1360$

$2006 = 1360(1) + 646$

$1360 = 646 \cdot 2 + 68$

$646 = 68 \cdot 9 + 34$

$68 = 34 \cdot 2 + 0$ Because the gcd is equal to 34, there is no multiplicative inverse.

(c) 550 mod 1769

$1769 = (550) \cdot 3 + 119$

$550 = 119 \cdot 4 + 74$

$119 = 74(1) + 45$

$74 = 45(1) + 29$

$45 = 29(1) + 16$

$29 = 16(1) + 13$

$16 = 13(1) + 3$

$13 = 3 \cdot 4 + 1$

$3 = 1 \cdot 3 + 0$

always expand the smallest thing you have. the big, a, R, always want to shift from Q, R, to new remainder

$1 = 13 - 3 \cdot 4$

$1 = 13 - 4 \cdot (16 - 13)$

$1 = 13 - 4(16) + 4(13)$

$1 = 5(13) - 4(16)$

$1 = 5(29 - 16) - 4(16)$

$1 = 5(29) - 5(16) - 4(16)$

$1 = 5(29) - 9(16)$

$1 = 5(29) - 9(45 - 29)$

$1 = 5(29) - 9(45) + 9(29)$

$1 = 14(29) - 9(45)$

$1 = 14(74 - 45) - 9(45)$

$1 = 14(74) - 23(45)$

$1 = 14(74) - 23(119 - 74)$

$1 = 37(74) - 23(119)$

$1 = 37(550 - 119(4)) - 23(119)$

$1 = 37(550) - 148(119) - 23(119)$

$1 = 37(550) - 171(119)$

$1 = 37(550) - 171(1769 - 3(550))$

$1 = 37(550) - 171(1769) + 513(550)$

$1 = 550(550) - 171(1769)$

So $550 \cdot x \bmod 1769 = 1$.

$x = 550$, and

$302500 \bmod 1769 = 1$

So the multiplicative inverse is $\boxed{550}$.

(3) (a) $x^3+1 = f(x)$

$f(0) = 0^3+1 = 1$

$f(1) = x \cdot x \cdot x \cdot +1 = 1 \cdot 1 \cdot 1 + 1 = 0.$

Since it is impossible to obtain 0 from x^3+1 when $f(1)$ from GF(2), then x^3+1 is reducible over GF(2), as you can have $x^3+1 = (x+1)(x^2-x+1)$

(b) $x^3 + x^2 + 1 = f(x)$

$f(0) = 0^3 + 0^2 + 1 = 1$

$f(1) = 1^3 + 1^2 + 1 = 3 \bmod 2 = 1.$

Since both cases equal 1, then it is not reducible.

(c) $x^4 + 1 = f(x)$

$f(0) = 0^4 + 1 = 1$

$f(1) = 1 \cdot 1 \cdot 1 \cdot 1 + 1 = 0$

However, $x^4+1 = (x+1)^4$ in GF(2) because

$(x+1)^2 = x^2 + 2x + 1 = x^2+1$ because $\cdot 2 = 0$ in GF(2), so

$(x^2+1)^2 = x^4 + 2x^2 + 1 = x^4+1$ and

$(x+1)^4 = x^4+1$ so x^4+1 is reducible.

(4) (a) Determine GCD of pair of polynomials $x^3 - x + 1$ and $x^2 + 1$ over GF(2).

They will only have a gcd in GF(2) if they are both reducible.

$f(0) = 0^3 - 0 + 1 = 1$

$f(1) = 1^3 - 1 + 1 = 0 + 1 = 1.$

As 0 is not obtainable, $f(x) = x^3 - x + 1$ is irreducible, so a gcd over GF(2) cannot be found, unless you want a gcd of 1 because x^2+1 does not have real roots.

(b) $f_1(x): X^5 + X^4 + X^3 - X^2 - X + 1$ and $f_2(x) = X^3 + X^2 + X + 1$ over GF(3)

We first check to see if both equations are reducible over GF(3)

$f_1(0): 0^5 + 0^4 + 0^3 - 0^2 - 0 + 1 = 1$

$f_1(1): 1^5 + 1^4 + 1^3 - 1^2 - 1 + 1 = 2 \bmod 3 = 1$

$f_1(2): 2^5 + 2^4 + 2^3 - 2^2 - 2 + 1 = 51 \bmod 3 = 0$ ✓

$f_2(0): 0^3 + 0^2 + 0 + 1 = 1$

$f_2(1): 1^3 + 1^2 + 1 + 1 = 4 \bmod 3 = 1$

$f_3(2): 2^3 + 2^2 + 2 + 1 = 15 \bmod 3 = 0$ ✓

Based on this, we can see $X - 2 = 0$ is a root and $x - 2$ is equal to $x + 1$ in GF(3). We can factor this out of each to get:

$f_1(x): x^5 + x^4 + x^3 - x^2 + x + 1$

$f_1(x): (x+1)(X^4 + X^3 + x^2 + 1x - 1)$

and

$f_2(x): (X^3 + X^2 + x + 1) = (x+1)(x^2 + 1)$, so. we know this is right.

(5) It is not a valid cryptosystem, so

We use $H(K|C) = -\sum_{c \in C} \sum_{k \in K} Pr(c) Pr(k|c) \log_2(Pr(k|c))$

We first calculate $Pr(C)$.

$Pr(1) = \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8} + \frac{2}{8} + \frac{1}{8} = \frac{4}{8} = \frac{1}{2}$

$Pr(2) = \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{8} + \frac{1}{8} = \frac{2}{8} = \frac{1}{4}$

$Pr(3) = \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} + 0 = \frac{1}{8}$

$Pr(4) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

$Pr(k|c) = \frac{Pr(c|k) Pr(k)}{Pr(c)}$ & $E_k(p) \cdot c = \sum_i Pr(p)$

$Pr(1|k_1) = Pr(a) + Pr(c) = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$

$Pr(1|k_2) = Pr(c) = \frac{1}{2}$, $Pr(1|k_3) = 0$, $Pr(1|k_4) = 0$.

$Pr(2|k_1) = Pr(b) = \frac{1}{4}$, $Pr(2|k_2) = Pr(a) = \frac{1}{4}$

$Pr(2|k_3) = \frac{1}{4}$, $Pr(2|k_4) = 0$, $Pr(3|k_1) = 0$, $Pr(3|k_2) = \frac{1}{4}$

$Pr(3|k_3) = \frac{1}{4}$, $Pr(3|k_4) = \frac{1}{4}$, $Pr(4|k_1) = 0$, $Pr(4|k_2) = 0$

$Pr(4|k_3) = \frac{1}{2}$, $Pr(4|k_4) = Pr(b) + Pr(c) = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$

—

$Pr(k_1|1) = (Pr(1|k_1) \cdot Pr(k_1)) / Pr(1) = (\frac{3}{4} \cdot \frac{1}{2}) / \frac{1}{2} = 0.75$

In a similar fashion, $P(k_1|2) = 0.125$, $Pr(k_1|3) = 0$,

$Pr(k_1|4) = 0$, $Pr(k_2|1) = 0.5$, $Pr(k_2|2) = 0.25$,

$Pr(k_2|3) = 0.5$, $Pr(k_2|4) = 0$, $Pr(k_3|1) = 0$, $Pr(k_3|2) = 0.25$

$Pr(k_3|3) = 0.5$, $Pr(k_3|4) = 1$, $Pr(k_4|1) = 0$, $Pr(k_4|2) = 0$,

$Pr(k_4|3) = 0$, $Pr(k_4|4) = 0$.

We can use the $H(K|C)$ formula from above to get

$-(\frac{1}{2} * ((0.75 \log_2 0.75) + (0.5 \log_2 0.5)) + (\frac{1}{4} * (0.125 \log_2 0.125) + (0.25 \log 0.25) + (0.25 \log 0.25)) +$

$(\frac{1}{8} \cdot (0.5 \log 0.5) + (0.5 \log 0.5)) + (\frac{1}{8} * (1 \log_2 1)) =$ **0.874**