Crypto HW1.2

Milena Gonzalez

September 2018

Q1.

a) a $\equiv$ b(mod n) implies b$\equiv$a(mod n)
Let n be a positive integer. For all $a, b, c \in Z$
a $\equiv$ b(mod n) means that $n|(b-a)$. This means that a-b = nk for some $k \in Z$.
Therefore,

$$\begin{aligned} b-a = -nk = n(-k) \\ (b-a = -nk)(-1) \\ -b+a = nk \\ a-b = nk \end{aligned}$$

Alternatively, $n|(b-a) = n|(-1)(b-a) = n|(a-b) = b \equiv a$ (mod n)

b) prove that a$\equiv$b(mod n) and b$\equiv$c(mod n) imply a$\equiv$c (mod n)
We have established that a $\equiv$ b(mod n) means that $n|(b-a)$. Therefore, b $\equiv$ c(mod n) means that $n|(c-b)$. Once combined linearly, we get the equation $n|(b-a+c-b) = n|(c-a)$, which can also be written as a$\equiv$c (mod n).

Alternatively,
$n|(b-a) \equiv a-b = nk$
$n|(c-b) \equiv b-c = nk'$

Once combined we get:

$$\begin{aligned} a-b+b-c = n(k+k') \\ a-c = n(k+k') \end{aligned}$$

which means $n|(c-a)$ and can also be written as a$\equiv$c (mod n).

Q2.

Using extended Euclidean algorithm find the multiplicative inverse of
a) 1234 mod 4321
First find the GCD to make sure a multiplicative inverse exists

$$1234x = 1(mod 4321)$$
$$4321 - 3(1234) = 619$$
$$1234 - 1(619) = 615$$
$$619 - 1(615) = 4$$
$$615 - 4(154) = 3$$
$$4 - 1(3) = 1$$

Now that we know an inverse exists...

$$1 = 4 - 1(3)$$
$$1 = 4(615 - 4(153))$$
$$1 = 4(154) - 615$$
$$1 = (619)(154) - 615(155)$$
$$1 = 309(619) - 155(-1234)1 \qquad = 309(4321) - 1082(1234)$$

(-1082 * 1234) mod 4321 = (-1 335 188) mod 4321 = 4321 * (-308) = -1330868 and 4321 * (-309) = -1335189
So -309 is the greatest multiple less than 1330868, so 4321*-309 = -1335189 and (-1 335 188) – (-1335189) = 1, showing it's a multiplicative inverse. b) 24140 mod 40902

$$24140x = 1(mod 40902)$$
$$40902 - 1(14140) = 16762$$
$$24140 - 1(16762) = 7378$$
$$16762 - 2(7378) = 2006$$
$$7378 - 3(2006) = 1360$$
$$2006 - 1(1360) = 646$$
$$1360 - 2(646) = 68$$
$$545 - 9(68) = 34$$
$$68 - 2(34) = 0$$

If the GCD is 0 there exists no such inverse.

c) 550 mod 1769

$$
\begin{aligned}
550x &= 1(mod 1769) \\
1769 - 3(550) &= 119 \\
550 - 4(119) &= 74 \\
119 - 1(74) &= 45 \\
74 - 1(45) &= 29 \\
45 - 1(29) &= 16 \\
29 - 1(16) &= 13 \\
16 - 1(13) &= 3 \\
13 - 4(3) &= 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 13 - 4(3) \\
1 &= 13 - 4(16 - 13) \\
1 &= 13 - 4(16) + 4(13) \\
1 &= 5(13) - 4(16) \\
1 &= 5(29 - 16) - 4(16) \\
&. \\
&. \\
&. \\
1 &= 550(550) - 171(1769)
\end{aligned}
$$

The multiplicative inverse of 550 mod 1769 = 550.
550 * 550 = 302500 mod 1769 = 1

Q3.

Determine which of the following are reducible over GF(2)
$a)x^3 + 1$
$GF(2) = (x + 1)(x^2 + x + 1)$
$b)x^3 + x^2 + 1$
$GF(2)DNE, irreducible$
$c)x^4 + 1$
$GF(2) = (x + 1)^4$

Q4.

Determine the GCD of following pair of polynomials:
a) $x^3–x+1$ and x^2+1 over GF(2)

$$\begin{aligned} x^3–x+1 &= x^3+x+1 \\ x^3–x+1-(x+1)(x^2+x+1) &= x^2+x \\ x^2+x+1-(1)(x^2+x) &= 1 \\ x^2+x-(x^2+x)(1) &= 0 \\ gcd &= 1 \end{aligned}$$

b) $x^5+x^4+x^3–x^2–x+1$ and x^3+x^2+x+1 over GF(3)
$\frac{x^5+x^4+x^3-x^2-x+1}{x^3+x^2+x+1} = x^2, r = x^2-x+1$
$\frac{x^3+x^2+x+1}{x^2-x+1} = x+2$
$\frac{x+2}{x+2} = 1(GCD)$

Q5.

For a cryptosystem P,K,C,E,D where P=a,b,c with
PP(a)=1/4
PP(b)=1/4
PP(c)=1/2

K = (k1,k2,k3) with
PK(k1)=1/2
PK(k2)=1/4
PK(k3)=1/4
C = 1,2,3,4
Encryption table:

Ek(P)	a	b	c
k1	1	2	1
k2	2	3	1
k3	3	2	4
k4	3	4	4

Calculate H($K|C$)
I did not include k4 below because there is no p for k4.
Pr(1): $\frac{1}{2}*(\frac{1}{4}+\frac{1}{2})+\frac{1}{4}(\frac{1}{2})+\frac{1}{4}(0) = \frac{3}{8}+\frac{1}{8} = \frac{1}{2}$
Pr(2): $\frac{1}{2}*(\frac{1}{4})+\frac{1}{4}(\frac{1}{4})+\frac{1}{4}(\frac{1}{4}) = \frac{1}{8}+\frac{1}{16}+\frac{1}{16} = \frac{1}{4}$
Pr(3): $\frac{1}{2}*(0)+\frac{1}{4}(\frac{1}{4})+\frac{1}{4}(\frac{1}{4}) = \frac{1}{16}+\frac{1}{16} = \frac{1}{8}$

Pr(4): $\frac{1}{2} * (0) + \frac{1}{4}(0) + \frac{1}{4}(\frac{1}{2}) + 0 = \frac{1}{8}$

Using Bayes Theorem....
$Pr(k|c) = \frac{Pr(c|k)Pr(k|c)}{Pr(c)}$

$$Pr(1|k1) = \frac{3}{4}$$
$$Pr(2|k1) = \frac{1}{4}$$
$$Pr(3|k1) = 0$$
$$Pr(4|k1) = 0$$

$$Pr(1|k2) = \frac{1}{2}$$
$$Pr(2|k2) = \frac{1}{4}$$
$$Pr(3|k2) = \frac{1}{4}$$
$$Pr(4|k2) = 0$$

$$Pr(1|k3) = 0$$
$$Pr(2|k3) = \frac{1}{4}$$
$$Pr(3|k3) = \frac{1}{4}$$
$$Pr(4|k3) = \frac{1}{2}$$

$$Pr(1|k4) = 0$$
$$Pr(2|k4) = 0$$
$$Pr(3|k4) = \frac{1}{4}$$
$$Pr(4|k4) = \frac{3}{4}$$

$H(k|c) = -\sum Pr(c) * Pr(k|c) log_2(Pr(k|c))$
$H(k|c) = -(\frac{1}{2}(\frac{3}{4} * log_2(\frac{3}{4}) + \frac{1}{4} * log_2(\frac{1}{4}) + 0 + 0)) = -0.09$