Brendan Forbes

Cryptography

Homework 2 Part a

1. a ≡ b (mod n) ->

a = kn + b (a equals some integer k times n plus b)

b = (-k)n + a -> let j = (-k)

b = jn +a (Therefore b equals some integer j times n plus a)

b ≡ a (mod n)

a ≡ b (mod n) b ≡ c (mod n)

a = pn + b b = qn + c

a = pn + qn + c

a = (p+q)n + c let r = p + 1

a = rn + c (Therefore a equals some integer r times n plus c

a ≡ c (mod n)

1. a) 1234 mod 4321

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | Ot | R | Or | Q |
| 1 | 0 | 1234 | 4321 | 3 |
| -3 | 1 | 619 | 1234 | 1 |
| 4 | -3 | 615 | 619 | 1 |
| -7 | 4 | 4 | 615 | 153 |
| 1075 | -7 | 3 | 4 | 1 |
| -1082 | 1075 | 1 | 3 | 3 |
| 4321 | -1082 | 0 | 1 |  |

4321 – 1082 = **3239** = Multiplicative Inverse

b) 24140 mod 40902 has no Multiplicative inverse because their GCD is not 1

c) 550 mod 1769

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | Ot | R | Or | Q |
| 1 | 0 | 550 | 1769 | 3 |
| -3 | 1 | 119 | 550 | 4 |
| 13 | -3 | 74 | 119 | 1 |
| -16 | 13 | 45 | 74 | 1 |
| 29 | -16 | 29 | 45 | 1 |
| -45 | 29 | 16 | 29 | 1 |
| 74 | -45 | 13 | 16 | 1 |
| -119 | 74 | 3 | 13 | 4 |
| 550 | -119 | 1 | 3 | 3 |
|  | 550 | 0 | 1 |  |

**550** = Multiplicative Inverse

1. x^3 + 1 = (x+1)(x^2+x+1) = reducible

x^3+x^2+1 = irreducible

x^4+1 = (x^3+x^2+x+1)(x+1) = reducible

1. GCD(x^3 + x + 1, x^2 + 1) in GF(2) = GCD(x^2+1, 1) = **1**

GCD(x^5 + x^4 + x^3 – x^2 – x + 1, x^3+x^2+x+1) in GF(3) =

GCD(x^3+x^2+x+1, x^2-x+1) = GCD (x^2-x+1, -x-1) = **-x-1**

1. H(K| C) = H(K) + H(P) – H(C)

H(K) =

H(P) =

Pc(1) = (.5\*.25 + .5\*.5 + .5\*.25) = .5

Pc(2) = (.25\*.25 + .25\*.5 + .25\*.25) = .25

Pc(3) = (.25\*.25 + .25\*.25) = .125

Pc(4) = (.25\*.5) =.125

H(C)=

H(K) + H(P) – H(C) = 1.5+1.5 -1.75 = 1.25