**CMPT 335 Discrete Structures**

Homework 8

**1**. Evaluate the following quantities

1. -17 mod 2

**1**

1. 144 mod 7

**4**

1. 13 mod 3

**1**

1. -97 mod 11

**2**

**2**. Which of the following are true and why?

1. 

-303 (mod101)

**True** because -303 is divisible by 101

1. 

-22 (mod11)

**True** because -22 is divisible by 11

1. 

82 (mod5)

**False** because 82 isn’t divisible by 5

1. 

-14 (mod8)

**False** because -14 isn’t divisible by 8

**3**. Evaluate the following (show your solution explicitly)

1.  in 

[10]…-2,1,4,7,10,13,16…

[7]…-2,1,4,7,10,13,16…

[10]+[7]=[7]+[10]

1.  in 

[10]…-2,1,4,7,10,13,16…

[7]…-2,1,4,7,10,13,16…

[10]\*[7]=[7]\*[10]

1.  in 

[3]…-4,3,10,17…

[6]…-1,6,13,20…

[3]\*[6]=[10]\*[13]

1.  in 

[39]^(17)=[-1]^(17)=[-1]=[39]

**4**. Find the greatest common divisor using the Euclidian algorithm

1. of 88 and 33

88mod33=22

33mod22=11

22mod11=0

**GCD=11**

1. of 84 and 56

84mod56=28

56mod28=0

**GCD=28**

**5**. Encrypt the message “Do not pass go” using a simple encryption method with the encryption function  and then decrypt the obtained cipher checking your solution.

DO NOT PASS GO

Encryption using f(p)=(9p+13)mod26

D

p=3

r=(9p+13)mod26

r=(9\*3+13)mod26

r=40mod26

r=14

O

O

p=14

r=(9p+13)mod26

r=(9\*14+13)mod26

r=139mod26

r=9

J

N

p=13

r=(9p+13)mod26

r=(9\*13+13)mod26

r=130mod26

r=0

A

T

p=19

r=(9p+13)mod26

r=(9\*19+13)mod26

r=184mod26

r=2

C

P

p=15

r=(9p+13)mod26

r=(9\*15+13)mod26

r=148mod26

r=18

S

A

p=0

r=(9p+13)mod26

r=(9\*0+13)mod26

r=13mod26

r=13

N

S

p=18

r=(9p+13)mod26

r=(9\*18+13)mod26

r=175mod26

r=19

T

G

p=6

r=(9p+13)mod26

r=(9\*6+13)mod26

r=67mod26

r=15

P

Ciphertext: OJ AJC SNTT PJ

Decryption using p=3(r-13)mod26

O

r=14

p=3(r-13)mod26

p=3(14-13)mod26

p=3mod26

p=3

D

J

r=9

p=3(r-13)mod26

p=3(9-13)mod26

p=-12mod26

p=14

O

A

r=0

p=3(r-13)mod26

p=3(0-13)mod26

p=-39mod26

p=13

N

C

r=2

p=3(r-13)mod26

p=3(2-13)mod26

p=-33mod26

p=19

T

S

r=18

p=3(r-13)mod26

p=3(18-13)mod26

p=15mod26

p=15

P

N

r=13

p=3(r-13)mod26

p=3(13-13)mod26

p=0mod26

p=0

A

T

r=19

p=3(r-13)mod26

p=3(19-13)mod26

p=18mod26

p=18

S

P

r=15

p=3(r-13)mod26

p=3(15-13)mod26

p=6mod26

p=6

G

Plaintext: DO NOT PASS GO