# Homework 4

**ECE4802**

**Nam Tran Ngoc**

---

## 1. Consider the multiplicative group of ℤ*53

## a. What are the possible element orders? How many element exit for each order ?

*Z53 = {1,2,3,4,5,...,52}*

-> *The order of Z53* is 52.

**We have the element order of Z*53 to be 1,2,4,13,26,52 as they are divisors of 52.**

For each element orders we have:

ϕ(1) = {1} -> **1 element**

ϕ(2) = {1} -> **1 element**

ϕ(4) = {1,3} -> **2 elements**

ϕ(13) = {1,2,3,4,...,12} -> **12 elements**

ϕ(26) = {1,3,5,7,9,11,15,17,19,21,13,25} -> **12 elements**

ϕ(52) = {1,3,5,7,9,11,15,17,19,21,13,25,27,29,31,33,35,37,41,43,45,47,49,51} -> **24 elements**

## b. Determine the order of all elements of ℤ*53

We take 2 to be a generator of *Z53, since 2 and 53 are coprime, and 2 is an element of Z53*.

We have the following subgroups:

- **Subgroup of order 1: 2^(52/1) = 1.**
  - 1^1 = 1
- **Subgroup of order 2: 2^(52/2) = 2^26 = 52.**
  - 52^1 = 1
- **Subgroup of order 4: 2^(52/4) = 2^13 = 30.**

- 30^1 = 30
- 30^3 = 23

- **Subgroup of order 13: 2^(52/13) = 2^4 = 16.**
    - 16^1 = 16
    - 16^2 = 44
    - 16^3 = 15
    - 16^4 = 28
    - 16^5 = 24
    - 16^6 = 13
    - 16^7 = 49
    - 16^8 = 42
    - 16^9 = 36
    - 16^10 = 46
    - 16^11 = 47
    - 16^12 = 10
- **Subgroup of order 26: 2^(52/26) = 2^2 = 4.**
    - 4^1 = 11
    - 4^2 = 17
    - 4^3 = 7
    - 4^4 = 6
    - 4^5 = 43
    - 4^6 = 37
    - 4^7 = 9
    - 4^8 = 38
    - 4^9 = 25
    - 4^10 = 29
    - 4^11 = 40
- **Subgroup of order 52: 2^(52/52) = 2^1 = 2.**
    - 2^1 = 8
    - 2^2 = 32
    - 2^3 = 22
    - 2^4 = 35
    - 2^5 = 34
    - 2^6 = 14

- 2^7 = 3
- 2^8 = 12
- 2^9 = 48
- 2^10 = 33
- 2^11 = 26
- 2^13 = 51
- 2^14 = 45
- 2^15 = 21
- 2^16 = 31
- 2^17 = 18
- 2^18 = 19
- 2^19 = 39
- 2^20 = 50
- 2^21 = 41
- 2^22 = 5
- 2^23 = 20
- 2^24 = 27

### c. What are the generators of $\mathbb{Z}$*53 ?

The generators of Z*53 are {8,32,22,35,34,14,3,12,48,33,26,51,45,21,31,18,19,39,50,41,5,20,27}

---

## 2. Use Baby-step Giant-step Algorithm to compute following discrete logarithm problems:

### a. 5 = 3^x mod 59

q = 58

t = floor(sqrt(q)) = floor(sqrt(58)) = 7

**Giant step calculation:**

3^0t = 3^0 mod 59 = 1

3^1t = 3^7 mod 59 = 4

3^2t = 3^14 mod 59 = 16

3^3t = 3^21 mod 59 = 5

3^4t = 3^28 mod 59 = 20

3^5t = 3^35 mod 59 = 21

3^6t = 3^42 mod 59 = 25

3^7t = 3^49 mod 59 = 41

Sorting this we have the following pairs:

```
{
    1,  0,
    4,  7
    5,  14
    16, 21
    20, 28
    21, 35
    25, 42
    41, 49
}
```

**Baby step calculation**

5*3^1 mod 59 = 15

5*3^2 mod 59 = 45

5*3^3 mod 59 = 17

5*3^4 mod 59 = 51

5*3^5 mod 59 = 35

5*3^6 mod 59 = 46

**5*3^7 mod 59 = 20**

So we have (20,7) matches (20,28).

Therefore **x = 28 - 7 = 21.**

# b. 9 = 11^x mod 79

q = 78

t = floor(sqrt(q)) = floor(sqrt(78)) = **8**

**Giant step calculation:**

11^0t = 11^0 mod 79 = 1

11^1t = 11^8 mod 79 = 44

11^2t = 11^16 mod 79 = 40

11^3t = 11^24 mod 79 = 22

11^4t = 11^32 mod 79 = 20

11^5t = 11^40 mod 79 = 11

11^6t = 11^48 mod 79 = 10

11^7t = 11^56 mod 79 = 45

11^8t = 11^64 mod 79 = 5

Sorting this we have the following pairs:

```
{
    1, 0
    5, 64
    10,48
    11, 40
    20, 32
    22, 24
    40, 16
    44, 8
    45, 56
}
```

**Baby step calculation**

**9*11^1 mod 79 = 20**

So we have (20,32) matches (20,1).

Therefore **x = 32 - 1 = 31.**

## c. 47 = 3^x mod 103

q = 102

t = floor(sqrt(q)) = floor(sqrt(78)) = **8**

**Giant step calculation:**

11^0t = 11^0 mod 79 = 1

11^1t = 11^8 mod 79 = 44

11^2t = 11^16 mod 79 = 40

11^3t = 11^24 mod 79 = 22

11^4t = 11^32 mod 79 = 20

11^5t = 11^40 mod 79 = 11

11^6t = 11^48 mod 79 = 10

11^7t = 11^56 mod 79 = 45

11^8t = 11^64 mod 79 = 5

Sorting this we have the following pairs:

```
{
    1, 0
    5, 64
    10,48
    11, 40
    20, 32
    22, 24
    40, 16
    44, 8
    45, 56
}
```

**Baby step calculation**

**9*11^1 mod 79 = 20**

So we have (20,32) matches (20,1).

Therefore **x = 32 - 1 = 31.**

# c. 47 = 3^x mod 103

q = 102

t = floor(sqrt(q)) = floor(sqrt(102)) = **10**

**Giant step calculation:**

3^0t = 3^0 mod 103 = 1

3^1t = 3^10 mod 103 = 30

3^2t = 3^20 mod 103 = 76

3^3t = 3^30 mod 103 = 14

3^4t = 3^40 mod 103 = 8

3^5t = 3^50 mod 103 = 34

3^6t = 3^60 mod 103 = 93

3^7t = 3^70 mod 103 = 9

3^8t = 3^80 mod 103 = 64

3^9t = 3^90 mod 103 = 66

3^10t = 3^100 mod 103 = 23

Sorting this we have the following pairs:

```
{
    1, 0
    8, 40
    9, 70
    14, 30
    23, 100
    30, 10
    34, 50
    64, 80
    66, 90
    76, 20
    93, 60
}
```

**Baby step calculation**

47*3^1 mod 103 = 38

47*3^2 mod 103 = 11

47*3^3 mod 103 = 33

47*3^4 mod 103 = 99

47*3^5 mod 103 = 91

47*3^6 mod 103 = 67

47*3^7 mod 103 = 98

47*3^8 mod 103 = 88

47*3^9 mod 103 = 58

47*3^10 mod 103 = 71

Since we don't have a match, **there is no solutions for this**

# d. 5 = 31^x mod 141

q = 140

t = floor(sqrt(q)) = floor(sqrt(140)) = **11**

**Giant step calculation:**

31^0t = 3^0 mod 103 = 1

3^1t = 3^11 mod 141 = 51

3^2t = 3^22 mod 141 = 63

3^3t = 3^33 mod 141 = 111

3^4t = 3^44 mod 141 = 52

3^5t = 3^55 mod 141 = 75

3^6t = 3^66 mod 141 = 109

3^7t = 3^77 mod 141 = 95

3^8t = 3^88 mod 141 = 9

3^9t = 3^99 mod 141 = 111

3^10t = 3^101 mod 141 = 103

3^11t = 3^121 mod 141 = 10

Sorting this we have the following pairs:

```
{
    1, 0
    9, 88
    10, 121
    51, 11
    52, 44
    63, 22
    75, 55
    95, 77,
    103, 110
    109, 66
    111, 33
    111, 99
}
```

**Baby step calculation**

5*31^1 mod 141 = 14

5*31^2 mod 141 = 11

5*31^3 mod 141 = 59

5*31^4 mod 141 = 137

5*31^5 mod 141 = 17

5*31^6 mod 141 = 104

5*31^7 mod 141 = 122

5*31^8 mod 141 = 116

5*31^9 mod 141 = 71

5*31^10 mod 141 = 14

Since we don't have a match, **there is no solutions for this**

---

## 3. D-H Key Exchange: Alice and Bob want to generate a common key. They agreed to use prime number p = 709 and generator $\alpha$ =

# 2. Alice's private key= 17, Bob's private key= 41. Find the the followings and show every intermediate step:

## a. Alice's public key

A = g^a mod p = 2^17 mod 709 = 616

## b. Bob's public key

B = g^b mod p = 2^41 mod 709 = 323

## c. Common key generated by Alice and Bob.

s = 323^17 mod 709 = 35,

or

s = 616^41 mod 709 = 350

## d. Explain how Alice and Bob establish the key.

- Alice and Bob first starts out by calculating their public keys - which are known to each others.
- They then generate the common key by taking the other person's public key, bring it to the power of their own private key in the modular space p.
- The result is the common key which is shared between the two.

---

# 4. ElGamal Encryption: Encrypt and decrypt the following messages using ElGamal Encryption for $\mathbb{Z}*$971 and g = 314 (generator r = 8 and a = 10, q = 97) and show every intermediate step:

## a. Private key = 23, random parameter = 21, message = 49.

**Key generation**

h = g^x mod 971 = 314^23 mod 971

```
23 = 0b10111

1   314
0   525
1   49
1   418
1   865
```

*h = 865*

**Encryption**

c1 = g^k = 314^21

```
21 = 0b10101

1   314
0   525
1   49
0   459
1   575
```

*c1 = 575*

c2 = m* h^k = 49 * 865^21

```
1   865
0   555
1   196
0   547
1   590
```

*c2 = 590 * 49 mod 971 = 751*

Therefore **c = (575, 751)**

**Decryption**

s = c1^x = 575^23

```
23 = 0b10111

1   575
0   485
1   872
1   862
1   590
```

*s = 590*

M = (s^-1 mod 971) * c2 mod 971

= (590^-1 mod 971) * 751 mod 971

= 525 * 751 mod 971

= **49**

# b. Private key = 23, random parameter = 51, message = 49.

**Key generation**

h = g^x mod 971 = 314^23 mod 971

= 865 (same as part a.)

**Encryption**

c1 = g^k = 314^51

```
51 = 0b110011

1   314
1   751
0   821
0   167
1   668
1   7
```

*c1 = 7*

c2 = m* h^k = 49 * 865^51

```
1   865
1   401
0   586
0   633
1   448
1   957
```

*c2 = 957 * 49 mod 971 = 285*

Therefore **c = (7, 285)**

**Decryption**

s = c1^x = 7^23

```
23 = 0b10111

1   7
0   49
1   300
1   792
1   957
```

*s = 957*

M = (s^-1 mod 971) * c2 mod 971

= (957^-1 mod 971) * 285 mod 971

= 208 * 285 mod 971

= **49**

(Yay!)

* This homework was brought to you by: tedious hand calculations and hacky Javascript code to verify result.