University College London
Department of Computer Science

Cryptanalysis Exercises Lab 01

**P. Spacek, N. Courtois,
J. Bootle**

January 23, 2019

peter.spacek@stuba.sk
Version 1.0

1. Basic Algebra Quiz

1.1. DONE WITHOUT a computer initially

Try to answer the following questions initially with paper and pen. For checking, use SAGE.

You can write the answer in the large box and press enter.

Click on the "Ans" button to get a hint.

Shift-click on "Ans" buttons that have a green boundary to get a full solution.

Click on the green square to go back to the questions.

The last white box shows the number of incorrect answers.

Quiz Answer each of the following.

1. $3 - 6 \mod 5 =$ [ ] Ans [ ]

2. $7 \times -1 \mod 11 =$ [ ] Ans [ ]

3. In SAGE maths type:
F9.< c >=GF(9);list(F9); F9.characteristic(); c+c+c;
What is the characteristic of GF(9)?

Ans

4. What is the characteristic of GF(7)?

Ans

5. What is the characteristic of GF(256)?

Ans

6. What is the characteristic of GF(3^2)?

Ans

7. What is the characteristic of GF(16)?

Ans

8. Recall the Fermat-Euler theorem (this is also related to the next exercise INDIRECTLY through the concept of cyclic groups with study of elements of type g^k, but first we study the standard version). In which multiplicative structure this theorem works?

9. How many elements in $(\mathbb{Z}/11\mathbb{Z})^*$?
$=$ [ ] Ans

10. Find a single element that generates $(\mathbb{Z}/11\mathbb{Z})^*$.
$=$ [ ] Ans

11. What is the order of 5 in $(\mathbb{Z}/11\mathbb{Z})^*$?
$=$ [ ] Ans

12. What is the Discrete Logarithm of 5 in basis 2 in $(\mathbb{Z}/11\mathbb{Z})^*$?
$=$ [ ] Ans

13. Type the following code:

```
[(i,GCD(i,8)) for i in range(0,8)]
```

What is the value of $\phi(8)$?

14. GF(q) denotes a finite field, where $q = p^n$. What is the size of the multiplicative group inside GF(9)?

Ans

15. In SAGE maths write the following lines:
F9.< c >=GF(9); c^8; (c+1).multiplicative_order(); How many distinct elements of the form c^k exist inside GF(9)? What are the possible values for $GCD(k, 8)$ in all these cases?

16. Does $c + 1$ belong to the cyclic subgroup generated by c?

17. What is the discrete logarithm of $c + 1$ in the basis c?

Ans

18. How many out of these c^k are generators of GF(9)*?
How many elements are (multiplicative) generators of GF(9)*?

Ans

19. Is $\mathbb{Z}_{10}$ a field?

☐ True ☐ False

1.2. Basic Maths in SAGE

Find Sage commands to answer the following questions, and copy the answers into the boxes.

Click on the "Ans" button to get a hint.

Shift-click on "Ans" buttons that have a green boundary to get a full solution. Click on the green square to go back to the questions.

Quiz Answer each of the following.

1. What are the factors of 12345678? Ans

2. What is the gcd of 3579609 and 890387967? Ans

3. Is 478 invertible mod 1329? Hint: 1329=3*443.

4. What is 478^{-1} mod 1329? Ans

5. Is there a practical method to know if 478^{-1} mod N is defined

when we do not know the factors?

Ans

6. Is there a practical method to find an element a such that a^{-1} mod N is NOT defined when we do not know the factors?

Ans

7. Is 25364772882647739926677265277281665356972 1 a prime number?

Ans

8. What are the prime divisors of 2266719?

Ans

9. What is the next prime number after 1 million?

Ans

10. Create two (2 x 2) vectors, and two matrices with sizes (3 x 1) and (1 x 3). Multiply the first pair together, and the second pair together (Leave answer box blank).

Ans

Clear

Solutions to Quizzes

Solution to Quiz: When working mod 5, we can add and subtract multiples of 5 freely.

$$3 - 6 = 8 - 6 \mod 5 = \boxed{2}$$

Solution to Quiz: Working modulo 11.

$$7 \times -1 = -7 \mod 11 = \boxed{4}$$

Solution to Quiz: The number of elements in $(\mathbb{Z}/N\mathbb{Z})^*$ is $\phi(N)$, so in this case, the answer is $\phi(11) = 10$. In SAGE we can type:

```
euler_phi(11)
```

Solution to Quiz: If we compute the powers of 2 modulo 11, we get $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$, so 2 is a generator. Alternatively, by Lagrange's Theorem, the order of an element divides the size of the group. The size of the group is 10, so the only possibilities for the order of an element are 1, 2, 5, and 10. A group generator should have order 10 to generate every group element, so to check that 2 is a generator, we just have to check that $2^2 \neq 1 \mod 11$, and $2^5 \neq 1 \mod 11$, implying that 2 has order 10. We can also try this: primitive_root(11)

Solution to Quiz: The smallest n such that $5^n = 1 \mod 11$ is $n = 5$.Alternatively, by Lagrange's Theorem, the order of an element divides the size of the group. The size of the group is 10, so the only possibilities for the order of an element are 1, 2, 5, and 10. Therefore, it is enough to check that $5^2 \neq 1 \mod 11$, and $5^5 = 1 \mod 11$. We can also type this:

```
R = Integers(11)
a = R(5)
a.multiplicative_order()
```

Solution to Quiz: Can be done by brute force. We can type this:
R = Integers(11); R(5).log(R(2))

Solution to Quiz: False, $\mathbb{Z}_{10}$ is not a field, because 2 and 5 are not invertible. ■

Solution to Quiz: $A = matrix([[2,3],[3,2]])$
$B = matrix([[3,4],[1,1]])$
$A * B$

$A = matrix([[2,3,1]])$
$B = matrix([[3],[1],[2]])$
$A * B$