AMSI Summer School 2022
Cryptography for Cybersecurity
Pre-course Quiz

1 Quiz questions

1. Using the Euclidean algorithm, find the gcd of 235 and 115. Express this gcd as a linear combination of the two integers.

2. Reduce the following integers

   (a) $103 \pmod{12}$

   (b) $97 \pmod{9}$

   (c) $229 \times 223 \pmod{23}$

   (d) $7001 \pmod{2}$

   (e) $45^2 \pmod{101}$

   (f) $45^{17} \pmod{101}$ (Hint: Compute large exponents by repeated squaring)

3. This question is on the concept of Cayley Tables

   (a) Compute the addition and multiplication Cayley Table of $\mathbf{Z}_{11}$.

   (b) Does the set of elements $\mathbf{Z}_{11}$ under the addition operation form an Algebraic Group? Why or why not?

   (c) Using the table compute $(3^{-1} + 4^{-1}) * 7$

4. This question is about the arithmetic for real polynomials, $\mathbf{R}[x]$

   (a) Reduce the polynomial $x^5 + 2x^4 - x^3 - 2x^2 - 3x - 1 \pmod{x^3 - 2x^2 + 8x - 3}$.

   (b) Find by trial and error a root of the polynomial $f(x) = x^3 + 4x^2 + 2x - 69$. Using this root find the corresponding linear factor. Hence find a non trivial factorization of $f(x)$.

5. This question is about the arithmetic for binary polynomials, $\mathbf{Z_2}[x]$

   (a) Given two polynomials $a(x) = x^5 + x^3 + x + 1$ and $b(x) = x^2 + 1$, find the gcd, $g(x)$ of these two polynomials.

(b) Using the extended Euclidean algorithm find two polynomials $s(x)$ and $t(x)$ such that $g(x) = s(x)a(x) + t(x)b(x)$

(c) Find $b^{-1}(x) \pmod{a(x)}$

6. This question is about the construction of Finite Fields.

   Consider the Field $GF(2^8)$ defined by the polynomial $f(x) = x^4 + x + 1$ where $f(x) \in \mathbf{Z_2[x]}$. Let α be the root of $f(x)$. Then $GF(2^8) = \{b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0, b_i \in \mathbf{Z_2} \forall\ 0 \leq i \leq 3, \alpha^4 = \alpha + 1\ \}$

   (a) Write α^{13} as an element of $GF(2^8)$.

   (b) Find $(\alpha^3 + \alpha)^{-1}$ as an element of $GF(2^8)$.

2 Solutions

1. Divide the bigger number by the smaller number. If the remainder is not 0, repeat the division by taking the previous divisor as the new dividend and the previous remainder as the new divisor. Continue until the remainder is 0. The last non-zero remainder is the gcd.

   $$\begin{aligned} 235 &= 2 \times 115 + 5 \\ 115 &= 23 \times 5 + 0. \end{aligned}$$

   In this example, the gcd is 5.
   Using the expression that has the gcd, work backwards, continuously replacing the remainder until we get the gcd as a linear combination of the two given numbers. In this example, it is very straightforward.

   $$5 = 235 - 2 \times 115$$

   The coefficients of the two given numbers in the linear expression are 1 and -2.

2. This is an example of modular arithmetic. Divide the given number by the modulus to find the remainder of the division.

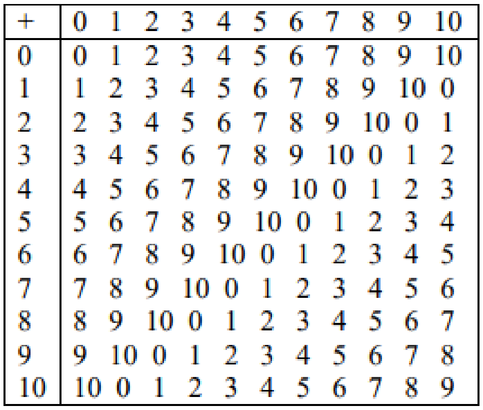
   (a) 7
   (b) 7
   (c) 7
   (d) 1
   (e) 5
   (f) $45^{17} \pmod{101}$ This requires repeated squaring. It is easier to do if we observe the binary expansion of the modulus $17 = 2^4 + 1$

   $$\begin{aligned} 45^17 &= 45^{2^4}.45 \pmod{()}101 \\ &= 45^{2^4}.45 \pmod{()}101 \\ &= 45^{2^{2^2}}.45 \pmod{()}101 \\ &= 5^{2^2}.45 \pmod{()}101 (\textit{Recall that } 45^2 \pmod{101} = 5) \\ &= 25^2.45 \pmod{()}101 \\ &= 19.45 \pmod{()}101 \\ &= 47 \end{aligned}$$

3. The Cayley table is a table that shows the result of pairwise operations on a set. $\mathbf{Z}_{11}$ represents the set of numbers from 0 till 10.

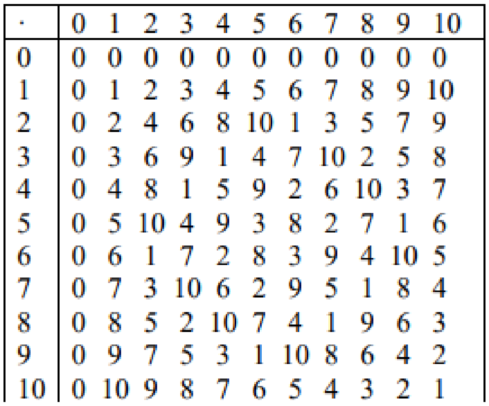
   (a) Computing the operations of addition and multiplication mod 11 on pairs of elements gives the following two tables.

Figure 1: The Cayley Table showing $\mathbf{Z}_{11}$ under addition with modulus 11



+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Figure 2: The Cayley Table showing $\mathbf{Z}_{11}$ under multiplication with modulus 11



·	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

(b) The set of elements under $(\mathbf{Z}_{11}, +)$ form a Group as they satisfy the four properties of closure, associativity, identity and inverse.
Closure is easy to check as every element in the table is an element of $\mathbf{Z}_{11}$.
Associativity means that given three elements a, b and c in $\mathbf{Z}_{11}$, $(a+b)+c = a+(b+c)$ i.e. it doesn't matter which pair of elements you add first, you will get the same result.
The identity element $e = 0$ as the row (or column) indexed by 0 gives the entire set $\mathbf{Z}_{11}$ in the same order. It demonstrates that $a + e = e + a = a$ for any element $a \in \mathbf{Z}_{11}$.
Every element a has an inverse $-a$ as every row has the identity element 0 as one of the entries. The corresponding element of the column will be the inverse of the row index. For example, $-2 = 9$ in the Cayley Table under addition.

A similar argument can be made for $\mathbf{Z}^*{}_{11}$, the set of non-zero elements, under multiplication ($*$). In the figure, we ignore the row and column of all zeros to get $\mathbf{Z}^*{}_{11}$.

(c) From the multiplication table, we can see that $3^{-1} = 4$ and $4^{-1} = 3$

$$\begin{aligned} 3^{-1} + 4^{-1} &= 4 + 3 \\ &= 7 \ (\textit{addition table}) \\ (3^{-1} + 4^{-1}) * 7 &= 7 * 7 \\ &= 5 \ (\textit{multiplication table}) \end{aligned}$$

4. (a) Long division will give you a quotient of $x^2 + 4x - 1$ and a remainder of $-33x^2 + 17x - 4$. The remainder will be the reduced form.

   (b) $x = 3$ is a root. So $x - 3$ is a factor. Using polynomial division we find that the other factor is $x^2 + 7x + 23$

5. (a) Dividing $a(x)$ by $b(x)$ using the Euclidean algorithm, the gcd is $x + 1$.

   (b) Using the extended Euclidean algorithm $s(x) = 1$ and $t(x) = x^3$

   (c) $b^{-1}(x)$ does not exist as the gcd is $\neq 1$.

6. (a) $\alpha^{13} = \alpha^4.\alpha^4.\alpha^4.\alpha = (\alpha + 1)(\alpha + 1)(\alpha + 1).\alpha = \alpha^3 + \alpha^2 + 1$

   (b) The easy way to do it is to write out all the 16 elements of the Field to get a correspondence between their exponential and polynomial form. This shows us that $\alpha^3 + \alpha = \alpha^9$. So $(\alpha^3 + \alpha)^{-1} = \alpha^{-9}$.
   We also know that $\alpha^{15} = 1 \implies \alpha^9\alpha^6 = 1$. So $\alpha^{-9} = \alpha^6 = \alpha^3 + \alpha^2$.