COMP5631: Cryptography and Security
2024 Spring – Written Assignment Number 1
Sample solutions

Q1. Solve the equation $1111 \otimes_{121111} x = 3$ to find the unique solution $x \in Z_{121111}$. Please use the extended Euclidean algorithm, and write down all the details of your computation. $\boxed{\text{20 marks}}$

Solution: We first compute the multiplicative inverse of 1111 modulo 121111 with the extended Euclidean algorithm. Running the Euclidean algorithm, we obtain

$$\begin{aligned} 121111 &= 109 \times 1111 + 12; \\ 1111 &= 92 \times 12 + 7; \\ 12 &= 1 \times 7 + 5; \\ 7 &= 1 \times 5 + 2; \\ 5 &= 2 \times 2 + 1. \end{aligned}$$

Hence, $\gcd(1111, 121111) = 1$. Backtracking, we have

$$\begin{aligned} 1 &= 5 - 2 \times 2, \\ 1 &= -2 \times 7 + 3 \times 5, \\ 1 &= 3 \times 12 - 5 \times 7, \\ 1 &= -5 \times 1111 + 463 \times 12, \\ 1 &= 463 \times 121111 - 50472 \times 1111. \end{aligned}$$

Hence the multiplicative inverse of 1111 modulo 121111 is $121111 - 50472 = 70639$. It then follows that

$$x = 3 \times 70639 \bmod 121111 = 90806.$$

Q2. This problem is about modular arithmetic.

1. How many elements in $\mathbf{Z}_{1025}$ have the multiplicative inverse modulo 1025? (10 marks)
   Solution: Note that $1025 = 5^2 \times 41$. The total number of invertible elements $\mathbf{Z}_{1025}$ is equal to $5(5-1)(41-1) = 800$.
2. Let a and b be two integers and $n \geq 2$ be an integer. Prove that the following equality holds: (10 marks)

   $$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n.$$

   Proof: Let $a = q_a n + r_a$ and $b = q_b n + r_b$, where $0 \leq r_a \leq n-1$ and $0 \leq r_b \leq n-1$. Then

   $$(ab) \bmod n = (q_a q_b n^2 + (q_a r_b + q_b r_a)n + r_a r_b) \bmod n = (r_a r_b) \bmod n$$

   and

   $$((a \bmod n)(b \bmod n)) \bmod n = (r_a r_b) \bmod n.$$

   The desired conclusion then follows.

Q3. For each positive integer n, let $\phi(n)$ be the total number of integers i with $1 \leq i \leq n-1$ and $\gcd(i, n) = 1$. This function $\phi(n)$ is called the *Euler totient function*. Prove that

$$\phi(pq) = (p-1)(q-1)$$

for a pair of distinct primes p and q. $\boxed{\text{20 marks}}$

Proof. Note that p ad q are distinct primes. The integers i with $1 \leq i \leq pq-1$ and $\gcd(i, pq) \neq 1$ are listed below:

$$p, 2p, \ldots, (q-1)p; q, 2q, \cdots, (p-1)q.$$

The total number of integers in the list above is $(q-1)+(p-1)$. Hence,

$$\phi(pq) = pq - 1 - (p+q-2) = (p-1)(q-1).$$

This completes the proof. □

Q4. Euler's Theorem: For any positive integer a and n with $\gcd(a, n) = 1$, we have

$$a^{\phi(n)} \bmod n = 1.$$

If $n = p$ is prime, we have **Fermat's Theorem**:

$$a^{p-1} \bmod p = 1.$$

Prove Euler's theorem above in detail. (20 marks)

Proof. Define $R = \{1 \leq i < n \mid \gcd(i, n) = 1\}$. By definition, $|R| = \phi(n)$. Since $\gcd(a, n) = 1$, the sets $aR := \{ar \bmod n \mid r \in R\}$ and R are equal. It then follows that

$$\left(\prod_{x \in R} x\right) \bmod n = \left(a^{\phi(n)} \prod_{x \in R} x\right) \bmod n.$$

Note that the integer $\prod_{x \in R}$ is relatively prime to n. Multiplying the multiplicative inverse of $\prod_{x \in R}$ modulo n on both sides of the equality above yields the desired equality. □

Q5. Let p be a prime. A positive integer α is called a *primitive root* of p if ever integer a with $1 \leq a \leq p-1$ can be expressed as

$$a = \alpha^i \bmod p$$

for a unique i with $0 \leq i \leq p-2$. It is known that every prime has at least one primitive root.

The exponent i is referred to as the **discrete logarithm**, or **index**, of a for the base α, and is denoted $\log_\alpha(a)$ or $\mathrm{index}(a)$. The *discrete logarithm problem* is to compute the unique exponent i (i.e., $\log_\alpha(a)$), given p, α and a. If p is large (say, p has 130 digits), people believe that it is computationally very hard to solve the discrete logarithm problem.

Prove that 2 is a primitive root of 11. Find out $\log_2(9)$. (10 marks)

Show that it is easy to compute a, given p, α and i. To this end, you need to describe an efficient algorithm for computing a. (10 marks)

Proof. We compute the values of $2^i \bmod 11$ for all i with $0 \leq i \leq 9$, which are listed in the table below. As seen, each integer a with $1 \leq a \leq 10$ can be uniquely expressed as $a = 2^i \bmod 11$ for some i with $0 \leq i \leq 9$. By definition, 2 is a primitive root of 11.

i	0	1	2	3	4	5	6	7	8	9
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6

We now describe an efficient algorithm for computing a, given p, α and i. Let

$$i = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_t}$$

where $0 \leq i_1 < i_2 < \cdots < i_t$ for some positive integer t. Then

$$a \quad = \quad \alpha^{2^{i_1}} \times \alpha^{2^{i_2}} \times \cdots \times \alpha^{2^{i_t}} \bmod p.$$

The algorithm is to compute each $\alpha^{2^{i_j}}$ first. Then compute their product.

Note that

$$\alpha^{2^{i_j}} = (\cdots((\alpha^2))^2 \cdots)^2$$

Computing each $a^{2^{i_j}}$ takes i_j multiplications. Hence, the algorithm takes

$$i_1 + i_2 + \cdots + i_t + t - 1$$

modulo-p multiplications, which is very efficient.

$\square$