Name:

COL202: Minor

Maximum marks: 34 Kerberos id:

Instructions.

1. For Questions 2-5, you will receive 10% marks for leaving it unattempted. Clearly mark that you are leaving it unattempted. However, there will be penalty for submitting bogus proofs.
2. Please write your proofs clearly (marks will be deducted for skipping steps, not mentioning which PMI you are using, etc).
3. There will be **no clarifications** during the exam. In case you feel a question is incorrect, clearly explain why it is incorrect. In case you are not sure if you can use a particular theorem/lemma, state it clearly, and your answer script will be graded accordingly.

Question 1: Short Answers (7 marks)

For each of the following questions, write the answer in the space provided.

1. (1 mark) Suppose we show that for all $n \in \mathbb{N}$, for all sets of size n, some property P holds. Can we conclude that the property P holds even for infinite sets? State yes/no, with a single-line explanation.

2. (1 marks) Let n be a composite number. Using Euler's theorem, we know that for all elements $a \in \mathbb{Z}_n^*$, $\exp_n(a, \phi(n)) = 1$. Using Fermat's theorem, we know that if p is a prime, then $\exp_p(a, p-1) = 1$. Finally, using Lagrange's theorem, can we conclude that for all $n \in \mathbb{N}$, $\phi(n)$ divides $n - 1$? State yes/no, with a single-line explanation.

3. (2 marks) Below you are given two statements. State whether it is true for all predicates $P : \mathbb{N} \times \mathbb{N} \to \{T, F\}$. If it is not true for some predicate, give an example.

$$\Big(\forall x \in \mathbb{N}, \exists y \in \mathbb{N} \text{ s.t. } P(x, y)\Big) \implies \Big(\exists x \in \mathbb{N} \text{ s.t. } \forall y \in \mathbb{N}, P(x, y)\Big)$$

4. (3 marks) Let $\mathbb{Z}[x]$ denote all polynomials with integer coefficients. Similarly, let $\mathbb{Z}_n[x]$ denote the set of all polynomials with coefficients in $\mathbb{Z}_n$. For each of the following statements, mention whether the statement is true for $\mathbb{Z}[x]$ and $\mathbb{Z}_n[x]$ (where n is composite). Give a one-line justification.

   (a) every degree d polynomial has at most d roots.

   (b) For every $d \in \mathbb{N}$, there is exactly one polynomial $f(x)$ such that $f(i) = i$ for all $i \in \{1, 2, \ldots, d+1\}$ and degree of f is at most d. You can assume that $n > d + 1$.

   - $\mathbb{Z}[x]$:

   - $\mathbb{Z}_n[x]$:

Question 2: Once in $\mathbb{N}$, always in $\mathbb{N}$. (5 marks)

Let $x \in \mathbb{R}$ such that $\left(x + \frac{1}{x}\right)$ is a natural number. Prove that for all $n \in \mathbb{N}$,

$$\left(x^n + \frac{1}{x^n}\right) \in \mathbb{N}.$$

You can use the following identity (although it is not mandatory to use it): for every $n \in \mathbb{N}$, there exist constants $c_0, c_1, \ldots, c_{n-1}, c_n \in \mathbb{N}$ such that for all $i \in \{0, 1, \ldots, n\}$, $c_i = c_{n-i}$ and for every $a \in \mathbb{R}$, $b \in \mathbb{R}$,

$$(a+b)^n = c_0 \cdot a^n + c_1 \cdot a^{n-1} \cdot b + \ldots + c_{n-1} \cdot a \cdot b^{n-1} + c_n \cdot b^n.$$

Question 3: Déjà tut - didn't we prove this in T3? (6 marks)

Let $m, n \in \mathbb{N}$ such that $\gcd(m, n) = d$, and let $a, b \in \mathbb{N}$ such that d divides $a - b$. Prove that there exists an $x \in \mathbb{N}$ such that

$$(x - a) \bmod m = (x - b) \bmod n = 0.$$

Question 4: Optimized RSA Setup (6 marks)

In RSA, it is important to sample the two primes p and q independently, at random from a large range. Consider the following approach for RSA setup (which is, unfortunately, often used in practice).

1. Sample a uniformly random large prime $p \leftarrow [2^{1000}]$.
2. Instead of sampling q uniformly, compute q as follows: for each $i \in [1000]$

   (a) check if $q = p + i$ is a prime. If so, set $N = p \cdot q$ and quit loop.

   You can assume that for every prime $p \in [2^{1000}]$, there exists a prime q in the set $\{p+1, \ldots, p+1000\}$. The above loop finds the first such prime q and uses it to set $N = p \cdot q$.
3. Sample e uniformly at random from $\mathbb{Z}_N$ such that $\gcd(e, \phi(N)) = 1$ where $\phi(N) = (p-1) \cdot (q-1)$.
4. Using Extended Euclid's Algorithm, find $d \in \mathbb{N}$ such that $e \cdot d \bmod \phi(N) = 1$. Set the public key $\mathsf{pk} = (N, e)$ and the secret key $\mathsf{sk} = d$.

What is the flaw in this approach? Prove that if the RSA public/secret keys are sampled in this manner, then an adversary, given (N, e), can efficiently compute a secret key that will allow it to decrypt ciphertexts.

You can assume that the following can be performed efficiently:

- given two numbers n, m, $n + m$, $n \cdot m$, $\lfloor n/m \rfloor$ and $n \bmod m$ can be computed efficiently (in $\log(m) \cdot \log(n)$ time)
- given two numbers n, m, computing integer coefficients s, t such that $s \cdot n + t \cdot m = \gcd(n, m)$ can be performed efficiently (in $\log(m) \cdot \log(n)$ time)
- checking if a number n is prime can be performed in $\mathrm{polylog}(n)$ time

[Hint: Suppose we use twin primes (that is, primes p, q such that $q = p+2$). Then, given $N = p \cdot q$ and e, the adversary can efficiently find a $d \in \mathbb{N}$ such that $e \cdot d \bmod \phi(N) = 1$.]

ATTEMPTED

NOT ATTEMPTED

Question 5: Order, Order! (10 marks)

Let p be a prime. Recall, in Quiz 2, we defined the order of an element $a \in \mathbb{Z}_p^*$, represented by $\mathsf{ord}(a)$, as the smallest positive integer z such that $\exp_p(a, z) = 1$.
We also saw that when $p = 2q + 1$ for some prime q, there is exactly one element with order 1 (that is 1), exactly one element with order 2 (that is, $p - 1$), and exactly $q - 1$ elements with order $(p-1)/2$. Therefore, the remaining elements must have order $p-1$.

We will generalize this for any prime p such that $p - 1 = 2^s \cdot q_1 \cdot q_2$ where q_1, q_2 are odd primes and $s \geq 1$.

1. (5 marks) Suppose there exists an element $y_1 \in \mathbb{Z}_p^*$ of order q_1 and an element $y_2 \in \mathbb{Z}_p^*$ of order q_2. Show that there exists an element $z \in \mathbb{Z}_p^*$ of order $q_1 \cdot q_2$. Note that when you need to prove that an element a has order θ, you need to prove that $\exp_p(a, \theta) = 1$, and for all $0 < \theta' < \theta$, $\exp_p(a, \theta') \neq 1$.

2. (5 marks) Prove that there exists an element $y_1 \in \mathbb{Z}_p^*$ of order q_1, and an element $y_2 \in \mathbb{Z}_p^*$ of order q_2.

Notations. The set of natural numbers is denoted by $\mathbb{N}$,[1] and for any natural number n, $[n] = \{1, 2, \ldots, n\}$ and $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. The set $\mathbb{Z}_n$ set has two associated operations : addition modulo n (denoted by $+_n$) and multiplication modulo n (denoted by $\times_n$).

1 Properties of $\mathbb{N}$

Theorem 1. *Every natural number greater than 1 is either prime, or can be expressed as a product of primes.*

Theorem 2 (Euclid's Lemma)**.** *Let p be a prime. If p divides $a \cdot b$, then p either divides a or p divides b.*

Theorem 3. *Let $a \in \mathbb{Z}, b \in \mathbb{N}$ be two numbers. There exist unique numbers $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, b-1\}$ such that $a = b \cdot q + r$.*

Theorem 4 (Fundamental Theorem of Arithmetic)**.** *For all $n > 1$, there exists $k \in \mathbb{N}$ and unique non-decreasing sequence of primes $(p_1, p_2, \ldots, p_k)$ such that $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.*

Given two natural numbers m, n, the greatest common divisor of m and n, denoted by $\gcd(m, n)$, is the largest natural number that divides both m and n. $\gcd(n, 0) = n$.

P1.1 Suppose $m \geq n$, then $\gcd(m, n) = \gcd(n, m \bmod n)$.

P1.2 The gcd of two consecutive numbers is 1.

P1.3 The gcd can be computed efficiently (in time $O((\log m) \cdot (\log n))$) using Euclid's Algorithm.

Theorem 5 (Bézout's Identity)**.** *For any natural numbers n, m, there exist integers s, t such that $s \cdot m + t \cdot n = \gcd(m, n)$. The coefficients s and t can be computed efficiently (in time $O(\text{polylog}(m) + \text{polylog}(n))$ using Extended Euclid's Algorithm). However, these coefficients are not unique.*

P1.4 If a natural number d divides both m and n, then it divides $\gcd(m, n)$.

Theorem 6. *Let m, n be natural numbers such that $\gcd(m, n) = d$. Then if m and n both divide some natural number z, then $m \cdot n/d$ also divides z.*

[1] $\mathbb{N} = \{1, 2, 3, \ldots\}$

2 Modular Arithmetic

P2.1 $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

P2.2 $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$

P2.3 For all $k \in \mathbb{N}$, $a^k \bmod n = (a \bmod n)^k \bmod n$

P2.3 For any $c \in \mathbb{Z}$, $((a \bmod n = b \bmod n) \implies ((a \cdot c) \bmod n = (b \cdot c) \bmod n))$

Theorem 7. *For all $c \in \mathbb{Z}$ such that $\gcd(c, n) = 1$,*

$$((a \cdot c) \bmod n = (b \cdot c) \bmod n) \implies (a \bmod n = b \bmod n)\,.$$

Theorem 8 (Chinese Remainder Theorem)**.** *Let m, n be natural numbers such that $\gcd(m, n) = 1$. For every $a \in \{0, 1, \ldots, m-1\}$ and $b \in \{0, 1, \ldots, n-1\}$, there exists a unique $x \in \{0, 1, \ldots, m \cdot n - 1\}$ such that*

$$x \bmod m = a \textbf{ and } x \bmod n = b.$$

3 $\mathbb{Z}_p$ with operations $+_p$, $\times_p$

Next, we defined the set $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, together with operations $+_p \equiv$ addition modulo p, and $\times_p \equiv$ multiplication modulo p. If p is a prime, we have the following properties.

P3.1 For all $a, b \in \mathbb{Z}_p$, $a +_p b \in \mathbb{Z}_p$, and $a \times_p b \in \mathbb{Z}_p$.

P3.2 For all $a, b, c \in \mathbb{Z}_p$, $a +_p b = b +_p a$, $a \times_p b = b \times_p a$, $a +_p (b +_p c) = (a +_p b) +_p c$ and $a \times_p (b \times_p c) = (a \times_p b) \times_p c$.

P3.3 For all $a, b, c \in \mathbb{Z}_p$, $a \times_p (b +_p c) = (a \times_p b) +_p (a \times_p c)$.

P3.4 For all $a \in \mathbb{Z}_p$, there exists a $b \in \mathbb{Z}_p$ such that $a +_p b = 0$. We will refer to b as the additive inverse of a.

P3.5 For all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists a unique $b \in \mathbb{Z}_p \setminus \{0\}$ such that $a \times_p b = 1$. We will refer to b as the multiplicative inverse of a. Also, $a \times_p 0 = 0$ for all $a \in \mathbb{Z}_p$.

P3.6 If $a, b \in \mathbb{Z}_p$ and $a \times_p b = 0$, then either $a = 0$ or $b = 0$.

P3.7 If $a, b \in \mathbb{Z}_p$, $c \in \mathbb{Z}_p \setminus \{0\}$, and $a \times_p c = b \times_p c$, then $a = b$.

P3.8 If $f(x) \in \mathbb{Z}_p[x]$ is a degree d polynomial, then $f(x)$ has at most d distinct roots in $\mathbb{Z}_p$.

P3.9 If $\{(x_i, y_i) \in \mathbb{Z}_p^2\}_{i \in [d+1]}$ such that all x_i are distinct, then there exists exactly one polynomial $f(x)$ of degree at most d such that $f(x_i) = y_i$ for all $i \in [d+1]$. This polynomial can be found efficiently (that is, in time $\mathsf{poly}(d \cdot \log p)$).

Theorem 9 (Fermat's Little Theorem). *Let $a \in \mathbb{Z}_p \setminus \{0\}$. Then $\mathsf{exp}_p(a, p-1) = 1$.*

Theorem 10 (Lagrange's Theorem). *Let $a \in \mathbb{Z}_p \setminus \{0\}$, and let z be the smallest positive integer such that $\mathsf{exp}_p(a, z) = 1$. Then z divides $(p-1)$.*

4 $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$: Properties and Applications

For any $n \in \mathbb{N}$, let $\mathbb{Z}_n^*$ denote the set of all numbers less than n that are co-prime to n. The size of this set is denoted by $\phi(n)$. If n is prime, then $\phi(n) = (p-1)$. In the tutorial, we saw the following properties of $\phi(n)$.

Lemma 1. *Properties of $\phi(n)$:*

1. *If n, m are co-prime, then $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.*
2. *If p is prime, then $\phi(p^k) = p^{k-1}(p-1)$.*
3. *If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, then*

$$\phi(n) = p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot p_2^{\alpha_2 - 1} \cdot (p_2 - 1) \cdot \ldots \cdot p_k^{\alpha_k - 1} \cdot (p_k - 1).$$

The set $\mathbb{Z}_n^*$, together with the operation $\times_n$ forms a multiplicative group. That is, it satisfies the following properties:

1. $1 \in \mathbb{Z}_n^*$, $\times_n$ is associative and commutative.
2. If $a, b \in \mathbb{Z}_n^*$, then $a \times_n b \in \mathbb{Z}_n^*$.
3. For every $a \in \mathbb{Z}_n^*$, there exists a unique $b \in \mathbb{Z}_n^*$ such that $a \times_n b = 1$.

In the tutorial, we saw that Fermat's Little Theorem and Lagrange's theorem also hold for composite numbers.

Theorem 11 (Euler's Theorem). *For every $n \in \mathbb{N}$, every $a \in \mathbb{Z}_n^*$, $\exp_n(a, \phi(n)) = 1$. Moreover, if z is the smallest positive integer such that $\exp_n(a, z) = 1$, then z divides $\phi(n)$.*

Using Euler's theorem, we can make the following observation (which will be very useful for our main application of $\mathbb{Z}_n^*$):

Observation 1. *For any natural number $n \in \mathbb{N}$, any $a \in \mathbb{Z}_n^*$, any integers e, d such that $e \cdot d \bmod \phi(n) = 1$,*

$$\exp_n(\exp_n(a, e), d) = a.$$

This is the first key observation in the design on a public key encryption scheme. The above observation also holds if $a \in \mathbb{Z}_n$ and n is square-free. The second main observation is that, for certain natural numbers n, computing $\phi(n)$ is as hard as factoring n. Factoring is believed to be a computationally hard problem, and therefore so is computing $\phi(n)$ for such numbers.

Observation 2. *Let $n = p \cdot q$ where p and q are large primes. There exists an efficient algorithm for computing $\phi(n)$ (given n as input) if and only if there exists an efficient algorithm for computing the factors of n (given n as input). Note that the input is given in binary, and therefore, by efficient, we mean that the running time of the algorithm should be at most* $\mathrm{polylog}(n)$.

Public Key Encryption (PKE). In a public key encryption scheme, there is a setup algorithm that samples a public key pk together with a secret key sk. The public key is used to encrypt messages, and the secret key is used to decrypt ciphertexts. Rivest, Shamir and Adleman gave the first PKE scheme, which we describe below.

Setup: The setup algorithm samples two large primes p, q. It sets $n = p \cdot q$. Next, it samples a uniformly random exponent $e \in \mathbb{Z}_n$ such that $\gcd(e, \phi(n)) = 1$. Using Extended Euclid's Algorithm, the setup algorithm finds a number $d \in \mathbb{Z}_n$ such that $e \cdot d \bmod \phi(n) = 1$. The public key is (n, e), and the secret key is (n, d).

Encryption: Let $m \in \mathbb{Z}_n$ be the message. The encryption algorithm outputs $\exp_n(m, e)$.

Decryption: The decryption algorithm takes as input $\mathsf{sk} = (n, d)$ and ct. It outputs $\exp_n(\mathsf{ct}, d)$.

Correctness of this scheme follows from Observation 1, while our belief in security comes from Observation 2.