Midterm 2 Review Sheet

Disclaimer: This study sheet is intended for practice and is not necessarily exhaustive. It does not necessarily reflect the final difficulty of the exam, as actual exam problems may be harder or easier than those presented here. Please use this at your own risk, I have not checked every solution so there may be errors (please point out any that you find!).

The Euler Phi Function $\varphi(n)$ counts integers $1 \leq k \leq n$ such that $\gcd(k, n) = 1$. If $n = p_1^{a_1} \dots p_k^{a_k}$, then $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$.

1. Calculate $\varphi(72)$, $\varphi(125)$, and $\varphi(1001)$.
2. If $n > 2$, prove that $\varphi(n)$ is always even.

Fermat's Little Theorem (FLT) & Euler's Theorem $a^p \equiv a \pmod{p}$ for prime p. $a^{\varphi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$.

1. Compute $5^{2026} \pmod{7}$ and $3^{162} \pmod{100}$.
2. Find the last two digits of 7^{402}.
3. Provide an example where $a^{n-1} \equiv 1 \pmod{n}$ holds but n is not prime.

Congruences and the Chinese Remainder Theorem (CRT) If $m_1, \dots, m_k$ are pairwise relatively prime, the system $x \equiv a_i \pmod{m_i}$ has a unique solution modulo $M = m_1 \dots m_k$.

1. Solve the linear congruence $12x \equiv 18 \pmod{30}$. List all distinct solutions modulo 30.
2. Find the smallest positive integer x such that $x \equiv 3 \pmod{11}$, $x \equiv 2 \pmod{5}$.
3. Find all integers x such that $x^2 \equiv 1 \pmod{15}$ using CRT.

Order Modulo n & Primitive Roots $\mathrm{ord}_n(a)$ is the smallest $k > 0$ such that $a^k \equiv 1 \pmod{n}$.

1. Find $\mathrm{ord}_{17}(3)$. Use this to determine if 3 is a primitive root modulo 17.
2. Find the number of primitive roots modulo 19.
3. Let $\mathrm{ord}_n(a) = d$. Prove that $\mathrm{ord}_n(a^j) = d/\gcd(j, d)$.

Binary Exponentiation Computing $a^k \pmod{n}$ in $O(\log k)$ steps by repeatedly squaring the base.

1. Compute $2^{25} \pmod{11}$ using the square-and-multiply algorithm. Track each squaring and multiplication step.
2. How many total multiplications (including squarings) are required to compute $a^{255} \pmod{n}$?

Primality Testing For $n-1 = 2^s \cdot t$, n passes the Miller-Rabin test for base a if $a^t \equiv 1 \pmod{n}$ or $a^{2^r t} \equiv -1 \pmod{n}$ for some $0 \leq r < s$. If n passes MR for base a, we say that n is a probable prime. If n fails MR for base a, we say n is composite.

1. Use the Miller-Rabin test on $n = 21$ with base $a = 8$.
2. Use the Miller-Rabin test on $n = 13$ with base $a = 2$.
3. If the Miller-Rabin test returns that n is composite for a specific base a, is n definitely composite? If the test returns that n is probably prime, is n definitely prime? Explain.
4. Define a Carmichael number and explain why the Fermat primality test fails to identify them as composite.

RSA Cryptosystem $n = pq$, $ed \equiv 1 \pmod{\varphi(n)}$. Encryption: $E(m) = m^e \pmod{n}$. Decryption: $D(c) = c^d \pmod{n}$.

1. Let $p = 7, q = 11$, and $e = 7$. Find the private key d. Encrypt the message $m = 2$.
2. Let $n = 35$ and $e = 5$. If you intercept the ciphertext $c = 10$, determine the original message m.
3. Given $(n, e) = (91, 5)$, find the decryption exponent d.
4. Suppose you know $n = pq$ and $\varphi(n)$. Describe how to recover the specific primes p and q.

Algorithmic Runtime Efficiency of operations as the input size (number of digits or bits) increases.

1. Computing $\gcd(a, b)$ using the Euclidean Algorithm, in terms of the number of digits in a and b.
2. Factoring an integer n into primes, in terms of n.
3. Computing the order $\text{ord}_n(a)$, in terms of n.
4. Computing $a^k \pmod{n}$ for very large k, in terms of the number of bits in k.
5. Computing $\varphi(n)$ given the prime factorization of n, versus computing $\varphi(n)$ without the factorization.