MATH 4440/5440 Assessment, Module 2

(More Modular Arithmetic, RSA)

Katherine Stange, CU Boulder, Fall 2026

Name: _____

1 Part A (20 points)

On this page of the exam, complete all problems.

1.1 True/False Questions

(10 points) Please indicate, for each statement, whether it is true or false.

1. If $2^{n-1} \equiv 1 \pmod{n}$, then n is prime.

   Solution. False. This is the converse of Fermat's Little Theorem, and it fails: for example $2^{340} \equiv 1 \pmod{341}$ but $341 = 11 \cdot 31$. The Fermat test can only ever say "probably prime."

2. In RSA with public key (n, e), the private decryption exponent d satisfies $ed \equiv 1 \pmod{n}$.

   Solution. False. The exponent lives modulo $\varphi(n)$: we need $ed \equiv 1 \pmod{\varphi(n)}$, so that $m^{ed} \equiv m \pmod{n}$ by Euler's theorem.

3. Let $n = pq$ with p, q distinct odd primes and let $\gcd(a, n) = 1$. Then $x^2 \equiv a \pmod{n}$ has either 0 or 4 solutions.

   Solution. True. Modulo each prime, a has either 0 or 2 square roots, and Sunzi's theorem combines each pair of choices into a unique root modulo n: $0 \cdot (*) = 0$ or $2 \cdot 2 = 4$.

4. For a cryptographic hash function h, it is impossible for two different messages to have the same hash.

   Solution. False. Collisions must exist, since there are infinitely many messages and finitely many hash values (e.g. 2^{256} of them). The requirement is that collisions be computationally *hard to find*.

5. Fermat factoring is most effective when the two prime factors of $n = pq$ are close together.

   Solution. True. Writing $n = x^2 - y^2$ with $x = (p+q)/2$ and $y = (q-p)/2$, the search starting from $\lceil \sqrt{n} \rceil$ finds x after about $x - \sqrt{n}$ steps, which is tiny when $p \approx q$.

1.2 Fill in the blank

(10 points) Only the answer matters.

1. (2 points) The equation $12x + 20y = c$ has a solution in integers x, y exactly when c is a multiple of _____.

   Solution. $4 = \gcd(12, 20)$.

2. (2 points) In RSA with $n = pq$, we have $\varphi(n) =$ _____ (a formula in p and q).

   Solution. $(p-1)(q-1)$.

3. (2 points) Let $p = 23$ and suppose a is a square modulo 23. A square root of a modulo 23 is given by a^k with $k =$ _____.

   Solution. $k = (23 + 1)/4 = 6$, since $23 \equiv 3 \pmod 4$.

4. (2 points) Bob's RSA public key is (n, e). Eve has intercepted a ciphertext c, which is the encryption of a message m that she wants to learn. Bob refuses to decrypt c itself, but he will decrypt any other ciphertext Eve sends him. Eve asks Bob to decrypt _____ (give an expression in terms of c, e and n); his reply is $2m$, and she divides by 2.

   Solution. $2^e c \bmod n$. Bob computes $(2^e c)^d \equiv 2^{ed} m^{ed} \equiv 2m \pmod n$.

5. (2 points) Circle the correct answers. In terms of the number of bits of the input, the runtime of the Euclidean algorithm is (polynomial / subexponential / exponential); the runtime of the quadratic sieve is (polynomial / subexponential / exponential); the runtime of Pollard's rho factoring method is (polynomial / subexponential / exponential).

   Solution. polynomial; subexponential; exponential (about $\sqrt{p} \leq n^{1/4}$ steps, which is $2^{k/4}$ for a k-bit n).

2 Part B (30 points)

Only three of the four problems count toward your grade. Check **exactly 3** to indicate which (if you check fewer or more than three, I will count problems 1, 2, 3):

Problem 1 _____ Problem 2 _____ Problem 3 _____ Problem 4 _____

3 Question 1

(10 points) Solve the system

$$x \equiv 4 \pmod{15},$$
$$x \equiv 7 \pmod{22}.$$

Give your answer as a residue modulo 330. Please show your work neatly and **show all steps**, including the extended Euclidean algorithm. When you are done, check your answer against both congruences.

Solution. First solve $22u + 15v = 1$ with recipe cards: each number d in the rows gets a card (u, v) meaning $22u + 15v = d$. The first row's cards are $(1, 0)$ for 22 and $(0, 1)$ for 15, and each remainder's card is the left card minus q times the middle card.

row		cards		check
$22 = 1 \cdot 15 + 7$	$(1, 0)$	$(0, 1)$	$(1, -1)$	$22 \cdot 1 + 15 \cdot (-1) = 7$
$15 = 2 \cdot 7 + 1$	$(0, 1)$	$(1, -1)$	$(-2, 3)$	$22 \cdot (-2) + 15 \cdot 3 = 1$
$7 = 7 \cdot 1 + 0$	$(1, -1)$	$(-2, 3)$	$(15, -22)$	$22 \cdot 15 + 15 \cdot (-22) = 0$

For example, the card for 1 is $(0, 1) - 2 \cdot (1, -1) = (-2, 3)$. The card above the gcd is the answer: $22 \cdot (-2) + 15 \cdot 3 = -44 + 45 = 1$. (The last card is the free check: $22 \cdot 15 = 15 \cdot 22$.)

Now read this off as building blocks: $45 = 3 \cdot 15$ is $\equiv 0 \pmod{15}$ and $\equiv 1 \pmod{22}$, while $-44 = -2 \cdot 22$ is $\equiv 1 \pmod{15}$ and $\equiv 0 \pmod{22}$. Hence

$$x \equiv 4 \cdot (-44) + 7 \cdot 45 = -176 + 315 = 139 \pmod{330}.$$

Check: $139 = 9 \cdot 15 + 4$ and $139 = 6 \cdot 22 + 7$.

4 Question 2

(10 points) Perform the Miller-Rabin primality test on $n = 1105$ with base $a = 2$. To save you some time, you may use the fact that $2^{69} \equiv 967 \pmod{1105}$. For full credit, explain what you are doing, make clear what output/computation determines the answer, and if n is composite, find a nontrivial factor.

Solution. $1104 = 2^4 \cdot 69$. Starting from $2^{69} \equiv 967$ and squaring modulo 1105:

$$967^2 = 935089 \equiv 259, \quad 259^2 = 67081 \equiv 781, \quad 781^2 = 609961 \equiv 1, \quad 1^2 = 1.$$

The chain is $967 \to 259 \to 781 \to 1 \to 1$. Since $781^2 \equiv 1$ with $781 \not\equiv \pm 1$, this is a surprise square root of 1, so 1105 is composite. A factor: $\gcd(781 - 1, 1105) = \gcd(780, 1105)$: $1105 = 780 + 325$, $780 = 2 \cdot 325 + 130$, $325 = 2 \cdot 130 + 65$, $130 = 2 \cdot 65$, so 65. (Also $\gcd(782, 1105) = 17$.) In fact $1105 = 5 \cdot 13 \cdot 17$. Note the chain ends in 1, so $2^{1104} \equiv 1$: the Fermat test is fooled (1105 is a Carmichael number) but Miller-Rabin is not.

5 Question 3

(10 points) Alice's RSA key is $n = 33$, $e = 3$, with private exponent $d = 7$.

1. (3 points) Alice signs the message $m = 4$. Compute her signature s.
2. (2 points) Bob receives $(m, s) = (4, s)$. Show the computation Bob does to verify the signature.
3. (3 points) Eve sees Alice's signatures $s_1 = 16$ on $m_1 = 4$ and $s_2 = 14$ on $m_2 = 5$. Without knowing d, produce a valid signature on the message 20, and explain why it verifies.
4. (2 points) Explain how signing $h(m)$ for a cryptographic hash function h, rather than m itself, defeats Eve's trick.

Solution.

1. $s \equiv 4^7 \pmod{33}$: $4^2 = 16$, $4^4 = 256 = 7 \cdot 33 + 25 \equiv 25$, $4^7 \equiv 25 \cdot 16 \cdot 4 = 1600 = 48 \cdot 33 + 16 \equiv 16$. So $s = 16$.
2. Bob computes $s^e = 16^3 = 4096 = 124 \cdot 33 + 4 \equiv 4 = m$. It matches, so the signature is valid.
3. $s = s_1 s_2 = 16 \cdot 14 = 224 = 6 \cdot 33 + 26 \equiv 26$. It verifies because $s^e \equiv s_1^e s_2^e \equiv m_1 m_2 = 20$. (Indeed $20^7 \equiv 26 \pmod{33}$.)
4. Eve's forged $s_1 s_2$ now verifies to $h(m_1)h(m_2) \bmod n$, and to exploit it she would need a message m with $h(m) \equiv h(m_1)h(m_2)$, i.e. a preimage of a specified hash value, which preimage resistance makes infeasible.

6 Question 4

(10 points) Let $n = 7739$. You wish to factor n. Using the quadratic sieve with factor base $\{2, 5, 7, 13, 19\}$, you obtain the following facts (all congruences modulo n):

$$\begin{aligned} 89^2 &\equiv 2 \cdot 7 \cdot 13, \\ 93^2 &\equiv 2 \cdot 5 \cdot 7 \cdot 13, \\ 119^2 &\equiv 2 \cdot 13^2 \cdot 19, \\ 336^2 &\equiv 2 \cdot 5^2 \cdot 7 \cdot 13. \end{aligned}$$

Use this information to complete the quadratic sieve procedure and find a nontrivial factor of n. Show your work, including your reasoning for which relations to combine and your gcd computation.

Solution. Multiplying relations adds exponents, so we want a subset of the relations in which every prime of the factor base appears to an *even* total exponent. Recording the exponents modulo 2 as vectors over $(2, 5, 7, 13, 19)$:

$$\begin{aligned} 89: &\quad (1,0,1,1,0) \\ 93: &\quad (1,1,1,1,0) \\ 119: &\quad (1,0,0,0,1) \\ 336: &\quad (1,0,1,1,0) \end{aligned}$$

The rows for 89 and 336 are identical, so they sum to $(0, 0, 0, 0, 0)$ modulo 2. (The pair $89, 93$ is tempting but leaves 5 to an odd power; any subset using 119 leaves 19 to an odd power, since 19 appears nowhere else.) Multiplying those two relations,

$$(89 \cdot 336)^2 \equiv 2^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \pmod{n}.$$

So $X = 89 \cdot 336 = 29904 = 3 \cdot 7739 + 6687 \equiv 6687$, and $Y = 2 \cdot 5 \cdot 7 \cdot 13 = 910$. Then $\gcd(X - Y, n) = \gcd(5777, 7739)$:

$$7739 = 5777 + 1962, \quad 5777 = 2 \cdot 1962 + 1853, \quad 1962 = 1853 + 109, \quad 1853 = 17 \cdot 109,$$

so the gcd is 109, and $7739 = 71 \cdot 109$. (Alternatively $\gcd(X + Y, n) = \gcd(7597, 7739)$: $7739 = 7597 + 142$, $7597 = 53 \cdot 142 + 71$, $142 = 2 \cdot 71$, giving 71.) The factor is nontrivial because $X \not\equiv \pm Y \pmod{n}$.