MATH 4440/5440 Assessment, Module 1

Katherine Stange, CU Boulder, Fall 2026

Name: _____

Note: There are mod 26 tables on the final page of this packet.

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 a has multiplicative order 4 modulo n, then $a^{10} \equiv a^2 \pmod{n}$.

   Solution. True. Since $a^4 \equiv 1$, we have $a^{10} = a^8 \cdot a^2 = (a^4)^2 a^2 \equiv a^2 \pmod{n}$. (Exponents can be reduced modulo the order of a.)

2. If $ab \equiv ac \pmod{n}$ and $a \not\equiv 0 \pmod{n}$, then $b \equiv c \pmod{n}$.

   Solution. False. Cancellation requires a to be invertible, i.e. $\gcd(a, n) = 1$. For example $2 \cdot 1 \equiv 2 \cdot 4 \pmod{6}$ but $1 \not\equiv 4 \pmod{6}$.

3. Diffie-Hellman key exchange is an example of a symmetric-key cryptosystem.

   Solution. False. It is public-key (asymmetric): each party keeps a private exponent and publishes g^a or g^b; the two parties share no secret in advance. (The key they produce is typically then used in a symmetric cipher, but the exchange itself is public-key.)

4. If g is a primitive root modulo a prime p, then every nonzero residue modulo p is a power of g.

   Solution. True. A primitive root has multiplicative order $p - 1$, so $g^0, g^1, \ldots, g^{p-2}$ are $p - 1$ distinct nonzero residues, i.e. all of $(\mathbb{Z}/p\mathbb{Z})^*$.

5. In a Vigenère cipher with a keyword of length 3, the plaintext letters in positions 2 and 5 are shifted by the same amount.

   Solution. True. The keyword repeats every 3 letters, so positions 2 and 5 (which differ by 3) are both encrypted with the second letter of the keyword.

1.2 Fill in the blank

(10 points) Only the answer matters.

1. (2 points) State Euler's Theorem (be precise, including hypotheses and conclusion).

   Solution. Let n be a positive integer and let a be an integer coprime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

2. (2 points) Encrypt CAT with the Vigenère cipher and keyword DOG: _____.

   Solution. $C + D = 2 + 3 = 5 = F$, $A + O = 0 + 14 = 14 = O$, $T + G = 19 + 6 = 25 = Z$: the ciphertext is FOZ.

3. (2 points) List the elements of $(\mathbb{Z}/10\mathbb{Z})^*$: _____.

   Solution. $\{1, 3, 7, 9\}$ (the residues coprime to 10). Note there are $\varphi(10) = 4$ of them.

4. (2 points) The Discrete Logarithm Problem modulo a prime p with primitive root g is: given _____, find _____. (Place the variables g, h, p, x into the blanks, where $h \equiv g^x \pmod{p}$; use all four.)

   Solution. Given p, g, h, find x.

5. (2 points) Circle the correct answers. In terms of the number of bits of p, the runtime of successive squaring modulo p is (polynomial / subexponential / exponential); the runtime of index calculus is (polynomial / subexponential / exponential); the runtime of exhaustive search for a discrete logarithm modulo p is (polynomial / subexponential / exponential).

   Solution. polynomial; subexponential; exponential.

2 Part B

(30 points)

Only three of the four problems count toward your grade. Please indicate which three you want me to count toward your grade:

Check **exactly 3**:

Problem 1 _____

Problem 2 _____

Problem 3 _____

Problem 4 _____

If you check fewer or more than three, I will count problems 1,2,3.

3 Question 1

(10 points)

Note: There are mod 26 tables on the final page of this packet.

1. (7 points) The plaintext IT was encrypted to WZ using an affine cipher whose key is unknown to you. Find the key (α, β). Explain your work.

2. (3 points) How many valid affine cipher keys are there in total? Explain how you compute this.

Solution.

1. $I = 8 \mapsto W = 22$ and $T = 19 \mapsto Z = 25$ gives

$$22 \equiv 8\alpha + \beta, \qquad 25 \equiv 19\alpha + \beta \pmod{26}.$$

   Subtracting, $11\alpha \equiv 3 \pmod{26}$. From the table $11^{-1} \equiv 19$ ($11 \cdot 19 = 209 = 8 \cdot 26 + 1$), so $\alpha \equiv 3 \cdot 19 = 57 \equiv 5$. Then $\beta \equiv 22 - 8 \cdot 5 = -18 \equiv 8$. The key is $(\alpha, \beta) = (5, 8)$. (Check: $5 \cdot 19 + 8 = 103 = 3 \cdot 26 + 25$.)

2. A key (α, β) is valid exactly when α is invertible modulo 26, so α must be a unit modulo 26. There are

$$\varphi(26) = 26\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{13}\right) = 12$$

   of these, namely

$$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25,$$

   while β can be any of the 26 residues. So there are $12 \cdot 26 = 312$ keys.

4 Question 2

(10 points) Compute the following expression by hand. Please show your work neatly and **show all steps**.

$$3302^{1003^{4003}} \pmod{33}.$$

Hint: Done thoughtfully, this should not be at all computationally intensive. Start by considering the correct modulus for the base and each level of exponents.

Solution. Each level of the tower has its own modulus, provided the relevant coprimality holds:

1. The base is taken modulo 33: $3302 = 100 \cdot 33 + 2$, so $3302 \equiv 2 \pmod{33}$. Note $\gcd(2, 33) = 1$, so Euler's theorem applies to the first exponent.
2. The first exponent is taken modulo $\varphi(33) = 33\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = 20$. We have $1003 \equiv 3 \pmod{20}$. Note $\gcd(3, 20) = 1$, so Euler's theorem applies again.
3. The second exponent is taken modulo $\varphi(20) = 20\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 8$. We have $4003 \equiv 3 \pmod{8}$.

Therefore

$$3302^{1003^{4003}} \equiv 2^{3^3} \pmod{33}.$$

Now $3^3 = 27 \equiv 7 \pmod{20}$, so this is $2^7 \pmod{33}$. By successive squaring,

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^4 \equiv 16 \pmod{33},$$

and $7 = 4 + 2 + 1$, so

$$2^7 \equiv 16 \cdot 4 \cdot 2 = 128 = 3 \cdot 33 + 29 \equiv 29 \pmod{33}.$$

The answer is 29.

5 Question 3

(10 points) Let $p = 43$ and $g = 3$, a primitive root. You wish to find $x = L_3(11)$, i.e. x with $3^x \equiv 11 \pmod{43}$, using index calculus with factor base $\{2, 3, 5\}$. You have computed the following (all congruences modulo 43):

$$\begin{aligned} 3^9 &\equiv 32, \\ 3^{26} &\equiv 15, \\ 3^{28} &\equiv 6, \\ 11 \cdot 3^7 &\equiv 20. \end{aligned}$$

1. (6 points) Use these relations to find $L_3(2)$, $L_3(3)$ and $L_3(5)$. Be careful about which modulus you are working in, and be careful about when dividing is safe.

2. (4 points) Find $x = L_3(11)$.

Solution.

1. Discrete logs live modulo $p - 1 = 42$. Since $g = 3$, $L_3(3) = 1$ immediately. Factoring: $32 = 2^5$, $15 = 3 \cdot 5$, $6 = 2 \cdot 3$. So

$$\begin{aligned} 9 &\equiv 5L_3(2), \\ 26 &\equiv L_3(3) + L_3(5) = 1 + L_3(5), \\ 28 &\equiv L_3(2) + L_3(3) = L_3(2) + 1 \pmod{42}. \end{aligned}$$

   From the third, $L_3(2) \equiv 27$. From the second, $L_3(5) \equiv 25$. The first equation can now serve as a check: $5 \cdot 27 = 135 = 3 \cdot 42 + 9 \equiv 9$. Good. (Alternatively one may solve the first equation directly: dividing by 5 is safe here because $\gcd(5, 42) = 1$, and $5^{-1} \equiv 17 \pmod{42}$ gives $L_3(2) \equiv 9 \cdot 17 = 153 \equiv 27$. Dividing by 2, 3, or 7 would *not* be safe modulo 42.)

2. $20 = 2^2 \cdot 5$, so $x + 7 \equiv 2L_3(2) + L_3(5) = 54 + 25 = 79 \equiv 37 \pmod{42}$, giving $x \equiv 30$. So $L_3(11) = 30$. (Check by computer: $3^{30} \equiv 11 \pmod{43}$.)

6 Question 4

(10 points)

Bob sets up El Gamal encryption with the prime $p = 23$ and primitive root $g = 5$. His private key is $b = 6$.

1. (3 points) Compute Bob's public key B. Show your work.
2. (5 points) Alice, a hamster breeder, sends Bob the ciphertext $(K, c) = (10, 19)$, which encrypts the number of hamsters she is willing to part with. Decrypt it. Explain your work.
3. (2 points) Eve intercepts Alice's ciphertext $(10, 19)$ before it reaches Bob. She does not know the message, but she wants Bob to decrypt to *double* the number of hamsters Alice offered. How should Eve alter the ciphertext before sending it on to Bob? Explain why it works.

Solution.

1. $B = g^b = 5^6 \pmod{23}$. By successive squaring, $5^2 = 25 \equiv 2$, $5^4 \equiv 2^2 = 4$, so $5^6 \equiv 5^4 \cdot 5^2 \equiv 4 \cdot 2 = 8$. Bob's public key is $B = 8$.
2. Bob computes the shared mask $K^b = 10^6 \pmod{23}$: $10^2 = 100 \equiv 8$, $10^4 \equiv 64 \equiv 18$, so $10^6 \equiv 18 \cdot 8 = 144 \equiv 6 \pmod{23}$. The message is $m \equiv c \cdot (K^b)^{-1} \equiv 19 \cdot 6^{-1}$. Since $6 \cdot 4 = 24 \equiv 1$, we have $6^{-1} \equiv 4$, so

   $$m \equiv 19 \cdot 4 = 76 \equiv 7 \pmod{23}.$$

   Alice will part with 7 hamsters. (Check: Alice used $k = 3$: $K = 5^3 = 125 \equiv 10$ and $B^k = 8^3 = 512 \equiv 6$, so $c = 7 \cdot 6 = 42 \equiv 19$.)
3. Eve sends $(K, 2c) = (10, 2 \cdot 19) = (10, 38) \equiv (10, 15)$. Bob computes the same mask $K^b \equiv 6$ (since K is unchanged) and decrypts to $2c \cdot (K^b)^{-1} = 2m = 14$. It works because the ciphertext is the message *multiplied* by the mask, so multiplying the ciphertext by 2 multiplies the hidden message by 2; Eve never needs to know m or the mask. (Check: $15 \cdot 4 = 60 \equiv 14 \pmod{23}$.)

Standard english letter frequencies in percentage.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	4.0	2.4	6.7	7.5	1.9	0.1	6.0	6.3	9.1	2.8	1.0	2.3	0.1	2.0	0.1

Vigenère Square (addition table modulo 26).

	+	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	**0**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
B	**1**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0
C	**2**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1
D	**3**	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
E	**4**	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3
F	**5**	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4
G	**6**	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5
H	**7**	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6
I	**8**	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7
J	**9**	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8
K	**10**	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9
L	**11**	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10
M	**12**	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11
N	**13**	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12
O	**14**	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13
P	**15**	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Q	**16**	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
R	**17**	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
S	**18**	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
T	**19**	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
U	**20**	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
V	**21**	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
W	**22**	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
X	**23**	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Y	**24**	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Z	**25**	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Multiplication table modulo 26.

	×	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
B	**1**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	**2**	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
D	**3**	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
E	**4**	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
F	**5**	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
G	**6**	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
H	**7**	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
I	**8**	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
J	**9**	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
K	**10**	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
L	**11**	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
M	**12**	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
N	**13**	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
O	**14**	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
P	**15**	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
Q	**16**	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
R	**17**	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
S	**18**	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
T	**19**	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
U	**20**	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
V	**21**	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
W	**22**	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
X	**23**	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
Y	**24**	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
Z	**25**	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1