

**Math 373 Exam 1**

**Instructions** No credit for solutions (even correct solutions) without supporting computations/arguments. Not full credit will be granted if the supporting materials are not sufficient. For all classical cryptosystem problems, we use the English alphabet with  $A - Z$  represented by the mod 26 numbers 0 - 25, respectively, as shown below.

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

- (10 %) Find  $\gcd(132, 156)$  by using Euclidean algorithm, and find integers  $u$  and  $v$  such that  $\gcd(132, 156) = 132u + 156v$ .
- (5 %) Suppose that  $a, b, c \in \mathbf{Z}$ . Show that if  $a|b$  and  $a|c$ , then  $a|(b + c)$ .
- (10 %) Solve the equation  $3x \equiv 7 \pmod{13}$
- (10 %) Compute  $3^{1001} \pmod{11}$ .
- (10 %) Find the  $\text{ord}_7(2)$  and  $\text{ord}_7(3)$ . Which one is a primitive root modulo 7? Explain why the one in your answer is a primitive root.
- (10 %) Find a solution  $x$  for the system

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} .$$

and check your solution.

- (10 %) Find all solutions of  $x^2 \equiv 1 \pmod{15}$ .
- (10 %) Encrypt *how* using the affine function  $E_{3,1}(x) = 3x + 1 \pmod{26}$ . Write down the ciphertext. What is the decryption function? (Check your answer to see it works).
- (10 %) Consider an affine cypher  $E_{a,b}(x) = ax + b \pmod{26}$ . Suppose you use this cipher to encrypt a plaintext *hahaha* to NONONO, find  $a$  and  $b$ .
- Solve the system of equations in  $\mathbf{Z}_{26}$

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

by doing the following two steps: (No credit for solutions not doing these two steps).

- (10 %) Let  $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ . Find  $A^{-1}$  in  $\mathbf{Z}_{26}$ .
- (5 %) Multiply both sides of the equations by  $A^{-1}$  from the left to get the solutions of system of equations.

**Math 373 Exam 1 Solutions**

1. (10 %) Find  $\gcd(132, 156)$  by using Euclidean algorithm, and find integers  $u$  and  $v$  such that  $\gcd(132, 156) = 132u + 156v$ .

**Solution:** Apply Euclidean Algorithm,

$$\begin{aligned} 156 &= 1(132) + 24 & 12 &= 132 - 5(24) \\ 132 &= 5(24) + 12 & 12 &= 132 - 5(156 - 132) \\ 24 &= 2(12) + 0 & 12 &= 6(132) + (-5)(156) \end{aligned}$$

Thus  $\gcd(132, 156) = 12$ , and  $12 = 6(132) + (-5)(156)$ .

2. (5 %) Suppose that  $a, b, c \in \mathbf{Z}$ . Show that if  $a|b$  and  $a|c$ , then  $a|(b + c)$ .

**Proof:**

Claim	Statement	Reason
1	$\exists u_1, u_2 \in \mathbf{Z}, b = au_1 \ \& \ c = au_2$	Definition of $a b \ \& \ a c$
2	$b + c = au_1 + au_2$	add $b = au_1 \ \& \ c = au_2$
3	$b + c = au, u \in \mathbf{Z}$	use substitution $u = u_1 + u_2$ .
4	$a (b + c)$	Definition of $a (b + c)$

3. (10 %) Solve the equation  $3x \equiv 7 \pmod{13}$

**Solution:** First compute  $\gcd(3, 13)$ . We have  $1 = \gcd(3, 13) = (-4)(3) + (1)(13)$ . Thus  $3^{-1} \equiv -4 \pmod{13}$ . It follows that

$$x \equiv (-4)(3x) \equiv (-4)(7) \equiv -28 \equiv -2 \equiv 11 \pmod{13} .$$

4. (10 %) Compute  $3^{1001} \pmod{11}$ .

**Solution:** By Fermat's Little Theorem,  $3^{10} \equiv 1 \pmod{11}$ . Since  $1001 = 10 \cdot 100 + 1$ , we have

$$3^{1001} \equiv 3^{10 \cdot 100 + 1} \equiv (3^{10})^{100} \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{11} .$$

5. (10 %) Find the  $\text{ord}_7(2)$  and  $\text{ord}_7(3)$ . Which one is a primitive root modulo 7? Explain why the one in your answer is a primitive root.

**Solution:** Note that  $\phi(7) = 6 = 2 \cdot 3$ . It suffices to compute  $2^2 \equiv 4, 2^3 \equiv 1 \pmod{7}$  to determine that  $\text{ord}_7(2) = 3$ , and  $3^2 \equiv 2, 3^3 \equiv -1 \pmod{7}$  to determine that  $\text{ord}_7(3) = 6$ . As  $\text{ord}_7(3) = 6 = \phi(7)$ , 3 is a primitive root modulo 7, but 2 is not.

6. (10 %) Find a solution  $x$  for the system

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} .$$

and check your solution.

**Solution:** Then  $m_1 = 5, m_2 = 7$  and  $m = 35$ . Since  $1 = \gcd(5, 7) = (3)(5) + (-2)(7)$ , we have  $7^{-1} \equiv -2 \pmod{5}$  and  $5^{-1} \equiv 3 \pmod{7}$ . Therefore, the answer is

$$x = (3)(7)(-2) + (2)(5)(3) = (-42) + 30 = -12 \equiv 23 \pmod{35}.$$

**Checking the solution:** Direct computation yields  $23 \equiv 3 \pmod{5}$  and  $23 \equiv 2 \pmod{7}$ . Therefore,  $x = 23$  is a solution of the system with  $0 \leq x < 35$ .

7. (10 %) Find all solutions of  $x^2 \equiv 1 \pmod{15}$ .

**Solution:** Note that  $15 = (3)(5)$ . As  $x^2 - 1 \equiv 0 \pmod{15} \iff (3)(5)|(x^2 - 1)$  (either  $3|(x^2 - 1)$  or  $5|(x^2 - 1)$ ), the equation  $x^2 \equiv 1 \pmod{15}$  is equivalent to the system

$$x^2 \equiv 1 \pmod{3} \text{ and } x^2 \equiv 1 \pmod{5}$$

Since both 3 and 5 are primes,  $x^2 \equiv 1 \pmod{3}$  has solutions  $x = \pm 1$  and  $x^2 \equiv 1 \pmod{5}$  has solutions  $x = \pm 1$ . Apply the Chinese Remainder Theorem (Algorithm) and consider all 4 possible combinations of solutions:

$$\begin{aligned} x \equiv 1 \pmod{3} \text{ and } x \equiv 1 \pmod{5} &\implies x \equiv 1 \pmod{15} \\ x \equiv -1 \pmod{3} \text{ and } x \equiv 1 \pmod{5} &\implies x \equiv 11 \pmod{15} \\ x \equiv 1 \pmod{3} \text{ and } x \equiv -1 \pmod{5} &\implies x \equiv 4 \pmod{15} \\ x \equiv -1 \pmod{3} \text{ and } x \equiv -1 \pmod{5} &\implies x \equiv 14 \pmod{15} \end{aligned}$$

Therefore, the solutions for the equation are 1, 4, 11 and 14 (modulo 15). To check the solutions, we compute

$$1^2 \equiv 1, 4^2 \equiv 16 \equiv 1, 11^2 \equiv 121 \equiv 1, 14^2 \equiv 144 \equiv 1 \pmod{15}.$$

8. (10 %) Encrypt *how* using the affine function  $E_{3,1}(x) = 3x + 1 \pmod{26}$ . Write down the ciphertext. What is the decryption function? (Check your answer to see it works).

**Solution:** Convert *how* to mod 26 numerical equivalence 7, 14, 22. Then

$$E_{3,1}(7) = 3 \cdot 7 + 1 \equiv 22, E_{3,1}(14) = 3 \cdot 14 + 1 = 43 \equiv 17, E_{3,1}(22) = 3 \cdot 22 + 1 = 67 \equiv 15 \pmod{26}$$

Thus the ciphertext is *wrp*.

To find the decryption function, we solve  $x$  from  $y = 3x + 1$  to get  $x = (y - 1)/3$ . To compute  $3^{-1} \pmod{26}$ , we first compute the  $\gcd(3, 26) = (3)(9) + (-1)(26) = 1$ , and so  $3^{-1} \equiv 9 \pmod{26}$ . Thus the decryption function is  $x = f(y) = 9(y - 1) = 9y - 9$ .

Checking the correctness:

$$f(22) = 9(22 - 1) \equiv 9(-5) \equiv 7, f(17) = 9(17 - 1) \equiv 9(-10) \equiv 14, f(15) = 9(15 - 1) \equiv 9(14) \equiv 22 \pmod{26}$$

9. (10 %) Consider an affine cypher  $E_{a,b}(x) = ax + b \pmod{26}$ . Suppose you use this cipher to encrypt a plaintext *hahaha* to NONONO, find  $a$  and  $b$ .

**Solution:** As  $h = 7, a = 0, n = 13$  and  $o = 14$ , we have

$$7 \cdot a + b \equiv 13 \text{ and } 0 \cdot a + b \equiv 14 \pmod{26}.$$

Thus  $b \equiv 14 \pmod{26}$ . Substituting  $b = 14$  in  $7a + b = 13 \pmod{26}$ , we have  $7a \equiv -1 \pmod{26}$ . Since  $\gcd(7, 26) = (-11)(7) + (3)(26) = 1$ ,  $7^{-1} \equiv -11 \pmod{26}$ , and so  $a \equiv (-11)(-1) = 11 \pmod{26}$ .

Check the correctness: Let  $f(x) = 11x + 14$ . Then  $f(7) = 77 + 14 = 91 \equiv 13 \pmod{26}$ , and  $f(0) \equiv 14 \pmod{26}$ .

10. Solve the system of equations in  $\mathbf{Z}_{26}$

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

by doing the following two steps: (No credit for solutions not doing these two steps).

(i) (10 %) Let  $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ . Find  $A^{-1}$  in  $\mathbf{Z}_{26}$ .

(ii) (5 %) Multiply both sides of the equations by  $A^{-1}$  from the left to get the solutions of system of equations.

**Solution:** The determinant of  $A$  is  $\det(A) = 16 - 21 = -5 \pmod{26}$ . Since  $5(-5) = -25 \equiv 1 \pmod{26}$ ,

$$A^{-1} = 5 \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \pmod{26}.$$

It follows that the solution is

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 7 \end{pmatrix} \pmod{26}.$$