1. [10]	2. [10]	3. [10]	4. [10]	5. [10]
6. [10]	7. [10]	8. [10]	9. [10]	10. [10]
Total. [100]				

MA 503 **Midterm** **March 2, 2022**

Name: ***Solutions***

No collaboration!	*One formula sheet is allowed.*
Cell phones out of sight.	*Answers must include supporting work.*
Basic calculators are allowed.	*Closed book and notes.*

(1) [10 pts] Solve the following system of linear congruences:

$$\begin{cases} x \equiv_2 1 \\ x \equiv_5 3 \\ x \equiv_9 1 \end{cases}$$

Solution: We can solve subsystems one by one. For instance, we can find a solution for a subsystem

$$\begin{cases} x \equiv_5 3 \\ x \equiv_9 1 \end{cases}$$

by enumerating solutions for the second congruence and choosing one satisfying the first congruence. $x \equiv_{45} 28$ works. Then consider the system

$$\begin{cases} x \equiv_2 1 \\ x \equiv_{45} 28 \end{cases}$$

and a sequence $28, 73$ of solutions for the second congruence. $x \equiv_{90} 73$ works for both congruences, which is the answer.

(2) [10 pts] Consider a linear Diophantine equation $12x + 29y = -1$.

(a) [6 pts] Find a particular solution, i.e., a pair of integers (x, y) satisfying the equation.

Solution: First, notice that $\gcd(12, 29) = 1$ which divides the right hand side, -1. Hence, the equation has solutions. To find a particular solution we use the Euclidean algorithm

$$\begin{aligned} 29 &= 2 \cdot 12 + 5 & \Rightarrow \gcd(29, 12) &= \gcd(5, 12) \\ 12 &= 2 \cdot 5 + 2 & &= \gcd(5, 2) \\ 5 &= 2 \cdot 2 + 1 & &= \gcd(1, 2). \end{aligned}$$

Hence

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 \\ &= 5 \cdot (29 - 2 \cdot 12) - 2 \cdot 12 = 5 \cdot 29 - 12 \cdot 12. \end{aligned}$$

Therefore, $x = -12$ and $y = 5$ is a solution for $12x + 29y = 1$. Multiply by -1 and get $x = 12$ and $y = -5$ is a solution for $12x + 29y = -1$.

(b) [2 pts] Write down a general solution of the equation.

Solution: Using the formula discussed in lecture 1, we get

$$\begin{cases} x = 12 + 29n, \\ y = -5 - 12n, \end{cases} \qquad n \in \mathbb{Z}.$$

(c) [2 pts] Find the multiplicative inverse of 12 modulo 29.

Solution: Taking $5 \cdot 29 - 12 \cdot 12 = 1$ modulo 29 we get

$$-12 \cdot 12 \equiv_{29} 1$$

and, hence, $12^{-1} \equiv_{29} -12 \equiv_{29} 17$.

(3) [10 pts] Let $G = \{a, b, c, d\}$. Let $+$ be a binary operation partially defined by the table shown below.

$+$	a	b	c	d
a	c			b
b			c	
c	d		b	
d				

Assuming that $(G, +)$ is an abelian group answer the following questions.

(a) [1 pt] What does it mean that $(G, +)$ is abelian? ***Solution***: It means that $x + y = y + x$ for any $x, y \in G$. (You can also say that $+$ is commutative.)

(b) [1 pt] $d + a =$ ***Solution***: $d + a = a + d = b$.

(c) [1 pt] $c + b =$ ***Solution***: $c + b = b + c = c$

(d) [1 pt] What property defines the identity element of $(G, +)$? ***Solution***: The identity is defined by $x + e = e + x = x$ for every $x \in G$.

(c) [2 pts] What element is the identity of G? ***Solution***: It is b. Indeed, subtracting c from both sides of $c + b = c$ we get $b = 0$.

(d) [4 pts] Fill in the addition table with ALL values. ***Solution***: Using (a), (b), (c) and the property that $+$ is commutative we get values

$+$	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	d	c	b	
d	b	d		

$c + d = (a + a) + d = a + (a + d) = a + b = a$ and
$d + d = d + (a + c) = (d + a) + c = b + c = c$ which adds the remaining values to the table.

$+$	a	b	c	d
a	c	a	d	b
b	a	b	c	d
c	d	c	b	a
d	b	d	a	c

(4) [10 pts] $g = 11$ is a primitive root of $N = 47$. Use the index calculus method to compute $\log_{11}(2)$, $\log_{11}(3)$, and $\log_{11}(5)$ using the provided powers of 11 only

$$11^2 \equiv_{47} 27$$
$$11^3 \equiv_{47} 15$$
$$11^{29} \equiv_{47} 10.$$

Solution: Take $\log_{11}$ of the given congruences and denote $\log_{11}(2)$, $\log_{11}(3)$, and $\log_{11}(5)$ by l_2, l_3, l_5 to get

$$\begin{array}{lll} 11^2 \equiv_{47} 3^3 & 2 \equiv_{46} 3\log_{11} 3 & 2 \equiv_{46} 3l_3 \\ 11^3 \equiv_{47} 15 & 3 \equiv_{46} \log_{11} 3 + \log_{11} 5 & 3 \equiv_{46} l_3 + l_5 \\ 11^{29} \equiv_{47} 10 & 29 \equiv_{46} \log_{11} 2 + \log_{11} 5 & 29 \equiv_{46} l_2 + l_5. \end{array}$$

- Divide congruence #1 by 3 (we can do that because 3 is a unit modulo 46) to obtain
$$l_3 \equiv_{46} \frac{2}{3} \equiv_{46} \frac{2+46}{3} = 16.$$
- Using congruence #2 we get
$$3 \equiv_{46} 16 + l_5 \quad \Rightarrow \quad l_5 \equiv_{46} 3 - 16 = -13 \equiv_{46} 33.$$
- Using congruence #3 we get
$$29 \equiv_{46} l_2 + 33 \quad \Rightarrow \quad l_2 \equiv_{46} 29 - 33 = -4 \equiv_{46} 42.$$

(5) [10 pts]

(a) [5 pts] Does $x^2 \equiv_{79} 2$ have a solution? If yes, then find all solutions. If no, explain why.

Solution: $(2/79) = 1$ and, hence, the congruence has a solution. Since $79 \equiv_4 3$, solutions can be found as

$$a^{(p+1)/4} = \pm 2^{20} \equiv_{79} \pm 9.$$

(b) [5 pts] (Remote coin flipping protocol) Alice sends the number $n = 11 \cdot 19 = 209$ to Bob. Bob sends $a = 15^2 \ \% \ 209 = 16$ to Alice. Which of the following numbers can Alice send back to Bob:

$$0, 3, -3, 4, -4, 5, -5, 6, -6, 15, -15, 11, -11, 19, -19, 209?$$

Which of those numbers represent winning calls for Alice?

Solution: Alice finds solutions of $x^2 \equiv_{209} 16$ which are

- ± 4 – obvious square roots of $x^2 \equiv_{209} 16$, and
- ± 15 because 16 was generated as $15^2 \mod 209$.

± 15 represent winning calls for Alice.

(6) [10 pts]

(a) [5 pts] (RSA encryption) Let $n = 323 = 17 \cdot 19$ be Alice's public modulus and $e = 7$ her public exponent. What is the value of her private exponent d?

Solution: $\varphi(323) = 16 \cdot 18 = 288$. Hence, d must satisfy $7d \equiv_{288} 1$ which can be computed as follows:

$$d = \frac{1}{7} \equiv_{288} \frac{1-288}{7} = -41 \equiv_{288} 247.$$

(b) [5 pts] (ElGamal encryption) Let $(p = 37, g = 2, A = 17)$ be Alice's public key for ElGamal encryption. Decrypt a ciphertext $(5, 3)$. Use the table of powers of 2 modulo 37 shown below.

$2^0 \equiv 1$	$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 8$	$2^4 \equiv 16$	$2^5 \equiv 32$	$2^6 \equiv 27$	$2^7 \equiv 17$	$2^8 \equiv 34$
$2^9 \equiv 31$	$2^{10} \equiv 25$	$2^{11} \equiv 13$	$2^{12} \equiv 26$	$2^{13} \equiv 15$	$2^{14} \equiv 30$	$2^{15} \equiv 23$	$2^{16} \equiv 9$	$2^{17} \equiv 18$
$2^{18} \equiv 36$	$2^{19} \equiv 35$	$2^{20} \equiv 33$	$2^{21} \equiv 29$	$2^{22} \equiv 21$	$2^{23} \equiv 5$	$2^{24} \equiv 10$	$2^{25} \equiv 20$	$2^{26} \equiv 3$
$2^{27} \equiv 6$	$2^{28} \equiv 12$	$2^{29} \equiv 24$	$2^{30} \equiv 11$	$2^{31} \equiv 22$	$2^{32} \equiv 7$	$2^{33} \equiv 14$	$2^{34} \equiv 28$	$2^{35} \equiv 19$

Solution: Using the table we immediately find Alice's private key $a = 7$. Then we compute $c_1^a = 5^7 \equiv_{37} 18$ and decrypt the message

$$m = \frac{c_2}{c_1^a} = \frac{3}{18} = \frac{1}{6} \equiv_{37} \frac{1-37}{6} = -6 \equiv_{37} 31.$$

(7) [10 pts] Perform the following encryptions and decryptions using the Goldwasser–Micali public key cryptosystem.

(a) [3 pts] Is $N = 253$ and $a = 7$ an appropriate Alice's public key for the Goldwasser–Micali public key cryptosystem? Explain!

Solution: $253 = 11 \cdot 23$ and

$$(7/11) = -(11/7) = -(4/3) = -1$$
$$(7/23) = -(23/7) = -(2/7) = -1.$$

Hence $a = 7$ can be used with $N = 253$.

(b) [3 pts] For the same Alice's public key $N = 299$ and $a = 7$, Bob generates a random number $r = 20$ and encrypts a message $m = 0$. What is the value of the ciphertext c?

Solution: For $m = 0$ Bob computes $20^2 = 400 \equiv_{299} 101 = c$.

(c) [4 pts] Alice's public key is $N = 299$ and $a = 7$. Bob encrypts four bits and sends Alice the ciphertext blocks

$$2, 9, \text{ and } 11.$$

Decrypt Bob's message.

Solution:
- $(2/13) = -1$ and, hence, $m_1 = 1$.
- $(9/13) = 1$ and, hence, $m_2 = 0$.
- $(11/13) = (13/11) = (2/11) = -1$ and, hence, $m_3 = 1$.

The plaintext is 101.

(8) [10 pts]

(a) [2 pts] Is 25 a Fermat pseudoprime?

Solution: No, it is not, because $2^{24} \equiv_{25} 16$ which is not 1.

(b) [2 pts] Prove that $n = 2821$ is a Carmichael number. [Hint. $2821 = 7 \cdot 13 \cdot 31$.]

Solution: A Carmichael number is a composite number that fails Fermat test to any base a, i.e.

$$a^{n-1} \equiv_{2821} 1.$$

which translates into a system

$$a^{n-1} \equiv_{2821} 1 \quad \Leftrightarrow \quad \begin{cases} a^{2820} \equiv_7 1 \\ a^{2820} \equiv_{13} 1 \\ a^{2820} \equiv_{31} 1. \end{cases}$$

We claim that the system holds. By Fermat's little theorem we have $a^6 \equiv_7 1$, $a^{12} \equiv_{13} 1$, and $a^{30} \equiv_{31} 1$ and hence

$$\begin{aligned} a^{2820} &= \left(a^6\right)^{470} \equiv_7 1 \\ a^{2820} &= \left(a^{12}\right)^{235} \equiv_{13} 1 \\ a^{2820} &= \left(a^{30}\right)^{94} \equiv_{31} 1 \end{aligned}$$

(c) [2 pts] Use Fermat primality test with base $a = 3$ to decide if $n = 20$ is prime or not. Does it recognize 20 as composite?

Solution: Since $3^{19} \equiv_{20} 7$ which is not 1, Fermat primality test concludes that 20 is composite.

(d) [4 pts] Use Miller-Rabin test with base $a = 13$ to decide if $n = 21$ is prime or not. Does it recognize 21 as composite?

Solution: Notice that $13^2 \equiv_{21} 1$. Since $n - 1 = 20 = 2^2 \cdot 5$, we compute the following powers of 2:

- $13^5 \equiv_{21} 13$
- $13^{10} \equiv_{21} 1$
- $13^{20} \equiv_{21} 1$.

Hence, the test concludes that $n = 21$ is composite.

(9) [10 pts] For $N = 299$ **use the quadratic sieve algorithm** (aka factorization using difference of squares) and the following data:

$$30^2 \equiv_N 3$$
$$40^2 \equiv_N 3 \cdot 5 \cdot 7$$
$$55^2 \equiv_N 5 \cdot 7$$
$$125^2 \equiv_N 7 \cdot 11$$

to find nontrivial factors of N.

Solution: Take the product of these identities to get

$$(30 \cdot 40 \cdot 55)^2 \equiv_N 3^2 5^2 7^2 = (105)^2$$

here $a = 30 \cdot 40 \cdot 55 = 66000 \equiv_{299} 220$ and $b = 105$. Compute

$$\gcd(299, 220 - 105) = \gcd(299, 115) = 23$$

which is a factor for N. The other factor is $\frac{299}{23} = 13$.

(10) [10 pts] Let $n = 25$.

(a) [5 pts] Is 2 a primitive root modulo 25?

Solution: $\varphi(25) = \varphi(5^2) = 5 \cdot 4 = 20 = 2^2 \cdot 5$. Compute

$$2^{\frac{20}{2}} = 2^{10} = 1024 \equiv_{25} -1 \quad \text{and} \quad 2^{\frac{20}{5}} = 2^4 \equiv_{25} 16.$$

Hence, 2 is a primitive root.

(b) [5 pts] Find $|7|$ in U_{25}.

Solution: $|7|$ is a divisor of $\varphi(25) = 20$ and, hence, $|7| = 2, 4, 5, 10, 20$. Direct computation shows that

$$7^2 = 49 \equiv_{25} -1, \quad 7^4 \equiv_{25} 1,$$

Therefore, $|7| = 4$.