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** **October 13, 2021**

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]

(a) [2 pts] Find the remainder of division of 7^{157} by 5.

Solution: By Fermat's little theorem $2^4 \equiv_5 1$ we get

$$7^{157} \equiv_5 2^{157} \equiv_5 2^{4\cdot 39+1} \equiv_5 \left(2^4\right)^{39} \cdot 2^1 \equiv_5 2.$$

(b) [2 pts] Find the remainder of division of 2^{119} by 6.

Solution: Fermat's little theorem is not applicable here, but computing several powers of 2 we observe the following:

$2^1 \equiv_6 2$ $2^2 \equiv_6 4$ $2^3 \equiv_6 2$ $2^4 \equiv_6 4$ $2^5 \equiv_6 2$ $2^6 \equiv_6 4$ etc.,

each odd power of two is 2 and each even power of two is 4. Thus, the answer is 2.

(c) [6 pts] Solve the following system of congruences:

$$\begin{cases} x \equiv_4 2 \\ x \equiv_5 2 \\ x \equiv_7 3 \end{cases}$$

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

$$\begin{cases} x \equiv_5 2 \\ x \equiv_7 3 \end{cases}$$

by enumerating solutions for the second congruence and choose one satisfying the first congruence. $x \equiv_{35} 17$ works. Then consider the system

$$\begin{cases} x \equiv_4 2 \\ x \equiv_{35} 17 \end{cases}$$

and a sequence $17, 52, 87, 122$. $x \equiv_{140} 122$ works for both congruences, which is the answer.

Please, write legibly.

(2) [10 pts] Consider a linear Diophantine equation $10x + 27y = 2$.

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

Solution: First, notice that $\gcd(10, 27) = 1$ that divides the right hand side. Hence, the equation has solutions. To find a particular solution we use the Euclidean algorithm

$$\begin{aligned} 27 &= 2 \cdot 10 + 7 && \Rightarrow \gcd(17, 10) &&= \gcd(7, 10) \\ 10 &= 1 \cdot 7 + 3 && &&= \gcd(7, 3) \\ 7 &= 2 \cdot 3 + 1 && &&= \gcd(1, 3). \end{aligned}$$

Hence

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 2 \cdot 10 \\ &= 3 \cdot (27 - 2 \cdot 10) - 2 \cdot 10 = 3 \cdot 27 - 8 \cdot 10. \end{aligned}$$

Therefore, $x = -8$ and $y = 3$ is a solution for $10x + 27y = 1$. Thus, $x = -16$ and $y = 6$ is a solution for $10x + 27y = 2$.

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

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

$$\begin{cases} x = -16 + 27n, \\ y = 6 - 10n, \end{cases} \qquad n \in \mathbb{Z}.$$

(c) [2 pts] Find the multiplicative inverse of 10 modulo 27.

Solution: Taking $3 \cdot 27 - 8 \cdot 10 = 1$ modulo 27 we get

$$-8 \cdot 10 \equiv_{27} 1$$

and, hence, $10^{-1} \equiv_{27} -8 \equiv_{27} 19$.

Did you write your name on the front page?

(3) [10 pts] Consider a set $G = \{x_1, x_2, \ldots, x_6\}$ of six elements equipped with a binary operation $\cdot$ defined by the multiplication table shown below. $(G, \cdot)$ is a group.

$\cdot$	x_1	x_2	x_3	x_4	x_5	x_6
x_1	x_3	x_5	x_1	x_6	x_2	x_4
x_2	x_4	x_6	x_2	x_5	x_1	x_3
x_3	x_1	x_2	x_3	x_4	x_5	x_6
x_4	x_2	x_1	x_4	x_3	x_6	x_5
x_5	x_6	x_4	x_5	x_2	x_3	x_1
x_6	x_5	x_3	x_6	x_1	x_4	x_2

(a) [2 pts] Which element is the identity of G? ***Solution***: x_3 is the identity element because it satisfies the group axiom (G1).

(b) [2 pts] Is G abelian? Why? ***Solution***: G is not abelian because

$$x_2 \cdot x_1 = x_4 \neq x_5 = x_1 \cdot x_2.$$

(c) [2 pts] Find $|x_2|$. ***Solution***:

- $x_2^2 = x_6$
- $x_2^3 = x_3$ – the identity.

Hence, $|x_2| = 3$.

(d) [2 pts] Find $\langle x_6 \rangle$. ***Solution***:

- $x_6^2 = x_2$
- $x_6^3 = x_3$ – the identity.

Hence, $\langle x_6 \rangle = \{x_6, x_2, x_3\}$.

(e) [2 pts] Find x_5^{-1}. ***Solution***: $x_5^{-1} = x_5$ because $x_5 \cdot x_5 = x_3$.

(f) [+1 pt] Use the definition of the discrete logarithm to find $\log_{x_2}(x_6)$. ***Solution***: $\log_{x_2}(x_6) = 2$ because $x_6^2 = x_2$.

(4) [10 pts] $g = 13$ is a primitive root of $N = 31$. Use the index calculus method to compute $\log_{13}(2)$, $\log_{13}(3)$, and $\log_{13}(5)$ using the provided powers of 13 only

$$13^3 \equiv_{31} 27$$
$$13^4 \equiv_{31} 10$$
$$13^5 \equiv_{31} 6$$
$$13^6 \equiv_{31} 16$$
$$13^{15} \equiv_{31} 30.$$

Solution: Take $\log_{13}$ of the given congruences and denote $\log_{13}(2)$, $\log_{13}(3)$, and $\log_{13}(5)$ by l_2, l_3, l_5 to get

$13^3 \equiv_{31} 27$	$3 \equiv_{30} 3\log_{13} 3$	$3 \equiv_{30} 3l_3$
$13^4 \equiv_{31} 10$	$4 \equiv_{30} \log_{13} 2 + \log_{13} 5$	$4 \equiv_{30} l_2 + l_5$
$13^5 \equiv_{31} 6$	$5 \equiv_{30} \log_{13} 2 + \log_{13} 3$	$5 \equiv_{30} l_2 + l_3$
$13^6 \equiv_{31} 16$	$6 \equiv_{30} 4\log_{13} 2$	$6 \equiv_{30} 4l_2$
$13^{15} \equiv_{31} 30$	$15 \equiv_{30} \log_{13} 2 + \log_{13} 3 + \log_{13} 5$	$15 \equiv_{30} l_2 + l_3 + l_5$.

- Subtract congruence #2 from congruence #5 to obtain
$$11 \equiv_{30} l_3.$$
- Subtract congruence #3 from congruence #5 to obtain
$$10 \equiv_{30} l_5.$$
- Subtract congruence $11 \equiv_{30} l_3$ from from congruence #3 to get
$$-6 \equiv_{30} l_2.$$

Thus,

$$\log_{13} 2 \equiv_{30} 24, \quad \log_{13} 3 \equiv_{30} 11, \quad \log_{13} 5 \equiv_{30} 10.$$

(5) [10 pts]

(a) [2 pts] Can a quadratic residue of n be a primitive root of n? Explain.

Solution: It cannot. If r is a primitive root of n, then, clearly, $r = r^1$. As we proved in class, r^k is a quadratic residue if and only if k is even. Thus, every primitive root of n is a quadratic non-residue.

(b) [8 pts] Find all solutions of the quadratic congruence $2x^2 - 4x + 9 \equiv_{13} 0$

Solution: One way to solve the given congruence is to compute the values of $f(x) = 2x^2 - 4x + 9$ modulo 13:

- $f(0) = 9 \equiv_{13} 9 \not\equiv_{13} 0$ is not a solution,
- $f(1) = 7 \equiv_{13} 7 \not\equiv_{13} 0$ is not a solution,
- $f(2) = 9 \equiv_{13} 9 \not\equiv_{13} 0$ is not a solution,
- $f(3) = 15 \equiv_{13} 2 \not\equiv_{13} 0$ is not a solution,
- $f(4) = 25 \equiv_{13} 0 \not\equiv_{13} 0$ is not a solution,
- $f(5) = 39 \equiv_{13} 0$ is a solution,
- $f(6) = 57 \equiv_{13} 5 \not\equiv_{13} 0$ is not a solution,
- $f(7) = 79 \equiv_{13} 1 \not\equiv_{13} 0$ is not a solution,
- $f(8) = 105 \equiv_{13} 1 \not\equiv_{13} 0$ is not a solution,
- $f(9) = 135 \equiv_{13} 5 \not\equiv_{13} 0$ is not a solution,
- $f(10) = 169 \equiv_{13} 0$ is a solution,
- $f(11) = 207 \equiv_{13} 12 \not\equiv_{13} 0$ is not a solution,
- $f(12) = 249 \equiv_{13} 2 \not\equiv_{13} 0$ is not a solution,

Hence, $x = 5$ and $x = 10$ are the solutions.

(c) [+2 pts] Find the number of quadratic residues of 41, i.e., find $|Q_{41}|$. Explain your answer.

Solution: This question is related to (a). 41 is prime and, hence, the following holds.

- There is a primitive root r of 41.
- $|U_{41}| = \varphi(41) = 40$.
- $U_{41} = \{r^0, r^1, \ldots, r^{39}\}$.
- $r^k \in Q_{41} \quad \Leftrightarrow \quad k$ is even.
- $Q_{41} = \{r^0, r^2, r^4, \ldots, r^{38}\}$.

Thus, $|Q_{41}| = 20$.

(6) [10 pts] Consider the group U_{18}.

(a) [2 pts] What elements does U_{18} contain?

For each $a \in U_{18}$ compute

(b) [4 pts] $\langle a \rangle$

(c) [2 pts] $|a|$

(d) [2 pts] a^{-1}

Using the obtained data, prove that U_{18} is not cyclic.

Solution:

(a) $U_{18} = \{1, 5, 7, 11, 13, 17\}$.

(b)

$$\langle 1 \rangle = \{1\} \qquad \langle 5 \rangle = \{1, 5, 7, 17, 13, 11\} \qquad \langle 7 \rangle = \{1, 7, 13\}$$
$$\langle 11 \rangle = \{1, 11, 13, 17, 7, 5\} \qquad \langle 13 \rangle = \{1, 13, 7\} \qquad \langle 17 \rangle = \{1, 17\}.$$

(c)

$$|1| = 1 \qquad |5| = 6 \qquad |7| = 3$$
$$|11| = 6 \qquad |13| = 3 \qquad |17| = 2.$$

(d)

$$1^{-1} = 1 \qquad 5^{-1} = 11 \qquad 7^{-1} = 13$$
$$11^{-1} = 5 \qquad 13^{-1} = 7 \qquad 17^{-1} = 17.$$

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

(a) [3 pts] Is $N = 143$ and $a = 5$ an appropriate Alice's public key for the Goldwasser–Micali public key cryptosystem? Explain!

Solution: $143 = 11 \cdot 13$ and

$$(5/11) = (11/5) = (1/5) = 1$$

$$(5/13) = (13/5) = (3/5) = (5/3) = (2/3) = -1.$$

The latter means that $a = 5$ cannot be used with $N = 143$.

(b) [3 pts] For the same Alice's public key $N = 143$ and $a = 2$. Bob generates a random number $r = 12$ and encrypts a message $m = 1$. What is the value of the ciphertext c?

Solution: For $m = 1$ Bob computes $2 \cdot 12^2 = 2 \cdot 144 \equiv_{143} 2 = c$.

(c) [4 pts] Alice's public key is the pair $N = 143$ and $a = 2$. Bob encrypts four bits and sends Alice the ciphertext blocks

$$3, 4, 5 \text{ and } 8.$$

Decrypt Bob's message.

Solution:

- $(3/11) = -(11/3) = -(2/3) = 1$ and, hence, $m_1 = 0$.
- $(4/11) = 1$ and, hence, $m_2 = 0$.
- $(5/11) = (11/5) = (1/5) = 1$ and, hence, $m_3 = 0$.
- $(8/11) = (2/11) = -1$ and, hence, $m_4 = 1$.

The plaintext is 0001.

Remark: 5 is not actually a quadratic residue mod 143, so it cannot be used in encryption. This was a typo.

(8) [10 pts] Let $n = 33$.

(a) [2 pts] Is 33 a Fermat pseudoprime?

Solution: Not, it is not, because it is easy to check that $2^5 \equiv_{33} -1$ and so $2^{32} \equiv_{33} 2^2 = 4 \neq 1$

(b) [2 pts] Is $n = 33$ a Carmichael number?

Solution: No, it is not. 33 is composite, but, as we've seen above, for the base 2

$$2^{32} \equiv_{33} 2^2 = 4 \neq 1.$$

(c) [2 pts] Use Fermat primality test with base $a = 4$ to decide if $n = 15$ is prime or not.

Solution: Since $4^{14} \equiv_{15} 1$, Fermat test is inconclusive. It returns ProbablyYes, (or MaybePrime or DontKnow).

(d) [4 pts] Use Miller-Rabin test with base $a = 4$ to decide if $n = 15$ is prime or not.

Solution: Since $n - 1 = 2 \cdot 7$, we compute the following powers of 4:

- $4^{14} \equiv_{15} 1$
- $4^7 \equiv_{15} 4$

Hence, the test concludes that $n = 15$ is composite.

(9) [10 pts]

(a) [8 pts] For $N = 221$ **use the quadratic sieve algorithm** (aka factorization using difference of squares) and the following data:

$$16^2 \equiv_N 35 = 5 \cdot 7,$$
$$22^2 \equiv_N 42 = 2 \cdot 3 \cdot 7,$$
$$35^2 \equiv_N 120 = 2^2 \cdot 3 \cdot 5,$$
$$56^2 \equiv_N 42 = 2 \cdot 3 \cdot 7,$$
$$76^2 \equiv_N 30 = 2 \cdot 3 \cdot 5,$$

to find nontrivial factors of N.

Solution: We need to take an appropriate product of the given identities to have squares on the left and on the right. Here, the product of the second and fourth identities gives

$$(22 \cdot 56)^2 \equiv_N 2^2 3^2 7^2 = (42)^2$$

here $a = 1232$ and $b = 42$. Hence,

$$\gcd(221, 1232 - 42) = 17$$

which is one of the factors of N. The other factor is 17.

(b) [2 pts] Is there $x \in \mathbb{Z}$ satisfying $x^2 \equiv_N 2$?

Solution: No, such x does not exist, because

$$x^2 \equiv_{221} 2 \quad \Leftrightarrow \quad \begin{cases} x^2 \equiv_{13} 2 \\ x^2 \equiv_{17} 2 \end{cases}$$

because $(2/13) = -1$ and, hence, $x^2 \equiv_{13} 2$ has no solutions.

(10) [10 pts] Let $n = 23$.

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

Solution: $\varphi(23) = 22 = 2 \cdot 11$. If 5 is not a primitive root, then

$$2^{11} \equiv_{23} 1 \quad \text{or} \quad 2^2 \equiv_{23} 1.$$

But

$$5^{11} \equiv_{23} -1 \not\equiv_{23} 1 \quad \text{or} \quad 5^2 \equiv_{23} 2 \not\equiv_{23} 1.$$

Hence, is a primitive root.

(b) [5 pts] Find $|2|$ in U_n.

Solution: $|2|$ is a divisor of 22 and, hence, $|2| = 2, 11, 22$. Direct computation shows that

$$2^2 \equiv_{23} 4 \quad \text{and} \quad 2^{11} \equiv_{23} 1,$$

Therefore, $|2| = 11$.