4400-001 - SPRING 2022 - MIDTERM

Exam instructions. You have **one hour** to complete the exam. You may use any resource linked to from the class website, including the book and notes/whiteboards. You may also use your personal notes and your personal homeworks. You may use a calculator, including an online calculator or spreadsheet, to do computations, but you may not use a calculator that shows work (e.g., that carries out the Euclidean algorithm automatically and shows you the steps that it took). Your work should be your own, and you may not discuss the exam with anyone else until it is finished.

$\frac{10}{10}$

Exercise 0. Name and signed statement of academic integrity (10 points).
I certify that the work on this exam is my own, that I have not discussed any of the problems with my classmates or other people, and that I have followed the rules as explained in the exam instructions.

Name: Instructor Signature: Answers.

$\frac{30}{30}$

Exercise 1. True or False (30 points)
No justification is required for your true or false answer.

(1) 17 has a multiplicative inverse in $\mathbb{Z}/51\mathbb{Z}$. **True** / **False**

$\gcd(17, 51) = 17 \neq 1$

(2) $12,654,999,999,999,999,999,999,999,999$ is divisible by 9. **True** / **False**

Sum of digits is divisible by 9.

(3) $p = 11$, $g = 10$ is a valid set-up for Diffie-Hellman. **True** / **False**

$(10)^2 = 100 \equiv 1 \bmod 11$ so g is not a primitive root mod

(4) There are integers a and b such that $11a + 33b = 6$. **True** / **False**

$\gcd(11, 33) = 11$ so $11 \mid 11a + 33b$ for any a, b.

(5) The polynomial $x^3 + 1$ is irreducible/prime in $\mathbb{F}_5[x]$. **True** / **False**

$4 \equiv -1 \bmod 5$ is a root.

(6) There is a field with 81 elements. **True** / **False**

Week 5, Exercise 2-(4).

Exercise 2. Computation 1 (20 points)
Show your work – an answer alone will not receive credit.

Solve the system of congruences

$$x \equiv 3 \mod 13$$
$$x \equiv 10 \mod 11$$

Express your answer using an integer $0 \le x \le 142$.

$x = 10 \mod 11 \Rightarrow x = 11q + 10$

substitute into

$x \equiv 3 \mod 13$ to get

$11q + 10 \equiv 3 \mod 13$

$11q \equiv 6 \mod 13$ mult. inverse of 11 mod 13

$\cdot 6 \quad \cdot 6$ is 6

$q \equiv 10 \mod 13$

so

$x = 11 \cdot \underbrace{10}_{q} + 10 = 120$ is a solution.

There is ~~a~~ exactly one solution by the Chinese Remainder Theorem.

$\boxed{x = 120}$

Exercise 3. Computation 2 (20 points)
Show your work – an answer alone will not receive credit.

Solve the equation $(3-4i)x = 1$ in $\mathbb{Z}[i]/(17)$.
Express your answer in the form $a + bi$ where a and b are integers, $0 \le a, b \le 16$.

Note $(3-4i)x = 1$ in $\mathbb{Z}[i]/(17)$

means $x = \frac{1}{3-4i}$, the mult. inverse of $3-4i$ mod 17.

$$x = \frac{3+4i}{(3-4i)(3+4i)} = \frac{3+4i}{9+16} = \frac{3+4i}{25} = \frac{1}{25}(3+4i)$$

need to compute $\frac{1}{25}$ mod 17.

$$\frac{1}{25} = \frac{1}{8}.$$

Euclidean alg: $17 = 2 \cdot 8 + 1 \Rightarrow 1 = 17 + (-2) \cdot 8$.
so inverse is -2 ($= 15$ mod 17).

so $\frac{1}{25}(3+4i) \equiv -2(3+4i) \equiv -6-8i$
$\equiv 11 + 9i$ mod 17

$$\boxed{x = 11 + 9i}$$

Exercise 4. Computation 3 (20 points)
Show your work – an answer alone will not receive credit.

E	A	O	H	L	M	N	K	I
1	2	3	4	5	6	7	8	9

(1) My RSA public key is $m = 187$, $e = 3$. Use this and the encoding of the Hawaiian alphabet in the table above to send me the encrypted message "HAHA"

$\underbrace{HA}_{42}\underbrace{HA}_{42}$

$(42)^3 = 36 \bmod 187$

So I send $\boxed{36 \quad 36.}$

(2) My RSA public key is $m = 187$, $e = 3$. Using that $187 = 11 \cdot 17$, what is my decryption key d?

$d =$ mult. inverse of e mod $\phi(m)$

$\phi(187) = \phi(11)\phi(17) = 10 \cdot 16 = 160$

need mult. inverse of 3 mod 160.

Euclidean alg: $160 = 53 \cdot 3 + 1$

$1 = 160 + (-53) \cdot 3$

$d \equiv -53 \equiv 107 \bmod 160.$

$\boxed{107}$