NAME: (print!) ____

E-Mail address: ____

MATH 356, Dr. Z. , Exam 2, Tue., Nov. 26, 2024 8:30-9:50am SEC-204

No Calculators! No Cheatsheets!
Write the final answer to each problem in the space provided. Incorrect answers (even due to minor errors) can receive at most one half partial credit, so please check and double-check your answers.

Do not write below this line (office use only)

---

1. (out of 10)

2. (out of 10)

3. (out of 10)

4. (out of 10)

5. (out of 10)

6. (out of 10)

7. (out of 10)

8. (out of 10)

9. (out of 10)

10. (out of 10)

---

tot.: (out of 100)

1. (10 pts.)
Using the formula, find the unique x between 0 and 2001 such that

$$x \equiv 1 \pmod 2 \quad , \quad x \equiv 5 \pmod 7 \quad , \quad x \equiv 6 \pmod{11} \quad , \quad x \equiv 4 \pmod{13} \quad .$$

Reminder (Chinese Remainder Theorem, General Version) If $n_1, n_2, \ldots, n_k$ are pairwise relatively prime (i.e. $gcd(n_i, n_j) = 1$, $1 \leq i < j \leq k$), then the unique x , $0 \leq x < n_1 \cdots n_k$ satisfying

$$x \equiv a_i \pmod{n_i} \quad , \quad 1 \leq i \leq k$$

is (letting $N = n_1 \cdots n_k$)

$$x = \sum_{i=1}^{k} a_i \frac{N}{n_i} \cdot \left((\frac{N}{n_i})^{-1} \pmod{n_i} \right)$$

Ans.:

---

2. (10 pts.) What is the day of the week of Nov. 26, 3024.
Reminders: Every year that is a multiple of 4 is a leap year, with the exception that every year that is a multiple of 100 is **not** a leap year, with the exception to the exception that if the year is a multiple of 400 it **is** a leap year.

Ans.:

---

3. **a** (5 pts.) What is is the remainder when you divide 102! by 103? Explain! What theorem are you using?

Ans.:

---

b (5 pts.) What is is the remainder when you divide 11^{1002} by 1003? What theorem are you using?

Ans.:

---

4. **a** (3 pts.) Define Euler's Toitent function $\phi(n)$.

b (7 pts. altogether)
State (2 pts.) and prove (5 pts), Euler's Classical Formula for Euler's Toitent function $\phi(n)$.

5. (10 pts.)
Using the RSA encrypton method, with $p = 5$, $q = 11$, $e = 7$, Alice sent you the encripted message $c = 2$ what was her original message m?

Ans.: $m =$

---

6. (10 pts., 2 pts. each) What are $\sigma(105)$, $\sigma_2(105)$, $\sigma_3(105)$, $\sigma_4(105)$, $\sigma_5(105)$?

Ans.: $\sigma(105) =$

$\sigma_2(105) =$,

$\sigma_3(105) =$

$\sigma_4(105) =$

$\sigma_5(105) =$

---

7. (10 pts., 5 pts. each) Find **(a):** $\mu(2002)$ **(b):** $\mu(4004)$. Explain!

Ans.:

a:

b:

---

8. (10 pts.) Is 17 a quadratic residue modulo 281? Explain!

Reminders:
Rule 1: If p is an odd prime and a and b are not multiples of p, then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Rule 2: If p is an odd prime then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \quad .$$

Rule 3: If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \quad .$$

Rule 4: (**THE QUADRATIC-RECIPROCITY LAW**)
If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \quad .$$

Ans.:

---

9. (10 pts.) For the following partitions λ, (i) Draw the Ferrers graph (ii) Find the conjugate partition λ'.

$$\lambda = (7, 5, 5, 3, 2, 1, 1, 1)$$

10. (10 pts. altogether)

i. (5 pts) Apply Glashier's bijection (in the distinct $\rightarrow$ odd direction) to the distinct partition $(8, 6, 3, 2, 1)$ to get an partition, call it μ

ii. (5 pts.) Apply Glashier's bijection (in the odd $\rightarrow$ distinct direction) to the partition μ and show that you get $(8, 6, 3, 2, 1)$ back, as you should.