NAME: (print!) Josefina Mansour

E-Mail address: [redacted]@gmail.com.

MATH 356, Dr. Z. , Exam II, Tue., Nov. 26, 2013, 10:20-11:40am, SEC-218

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 8)
2. (out of 8)
3. (out of 8)
4. (out of 8)
5. (out of 8)
6. (out of 8)
7. (out of 8)
8. (out of 8)
9. (out of 9)
10. (out of 9)
11. (out of 9)
12. (out of 9)

tot.: (out of 100)

100

Exc!

1. Using the **formula** (no credit for other methods!) to find the unique x between 0 and 34 such that

a.

$$x \equiv 2 \pmod 5 \quad , \quad x \equiv 1 \pmod 7 \quad .$$

Reminder: The unique solution of the system $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}$ in $0 \le x < m_1 m_2$, when m_1 and m_2 are relatively prime

$$x \equiv a_1 m_2 [m_2^{-1}]_{m_1} + a_2 m_1 [m_1^{-1}]_{m_2} \pmod{m_1 m_2} \quad .$$

(Note: you may find the modular inverse by trial-and-error rather than by the 'official' way, using the Extended Euclidean Algorithm.)

Ans.: $x =$ 22

Find $5^{-1} \bmod 7 = 3$ $\quad 7^{-1} \bmod 5 = \underline{-2} = 3$

$\gcd(7,5) = \gcd(5,2) = \gcd(2,1)$

$2 = \boxed{7} - \boxed{5}$

$1 = \boxed{5} - 2\boxed{2}$

$= \boxed{5} - 2\boxed{7} + 2\boxed{5} \Leftarrow 3\boxed{5} - 2\boxed{7}$

$x = (2(7^{-1})(7^{-1} \bmod 5) + 1(5)(5^{-1} \bmod 7)) \bmod 35$

$= (2 \cdot 7 \cdot 3 + 1 \cdot 5 \cdot 3) \bmod 35$

$= (42 + 15) \bmod 35$

$= 22 \bmod 35 = 22$

$14 \times 3 = 42$

$57 - 35 = 22$

check

$22 \equiv 2 \bmod 5$ ✓

$22 \equiv 1 \bmod 7$ ✓

2. (8 pts.) Using a suitable divisibility test, determine which of the following integers is divisible by 7

a. 357707147287798

b. 357707147287799

Ans.: a. is/is not divisible by 7

b. is/is not divisible by 7 .

8

(a) 35 7 | 70 7 | 14 7 | 28 7 | 79 8

+ − + − +

$$\begin{array}{r} 114 \\ 7\overline{)798} \\ 7 \\ \hline 98 \\ 7 \\ \hline 28 \\ 28 \\ \hline 0 \end{array}$$

all blocks of 3 are divisible by 7

$(357 - 707 + 147 - 287 + 798) \bmod 7$

$= 0 \bmod 7$

(b) 357 | 707 | 147 | 287 | 799

not divisible by 7

$0 + 0 + 0 + 0 + 799 \bmod 7$

$1 \bmod 7 = 1$

not divisible

3. (8 pts.) Illustrate the proof of Wilson's theorem for $p = 7$.

Wilson's Proof

$(n-1)! \equiv -1 \bmod n$

Find

$[2^{-1}]_7 = 4$

$[3^{-1}]_7 = 5$

$[4^{-1}]_7 = 2$

$[5^{-1}]_7 = 3$

8

$7 - 2(3) = 1$

$4 = -3 = 2^{-1} \bmod 7$

then $(-4) = (-2)^{-1} \bmod 7$

$3 = 5^{-1} \bmod 7$

Illustrating:

$(7-1)! \bmod 7 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \bmod 7$

$1 \cdot (2 \cdot 4)(5 \cdot 3)(-1) \bmod 7$

$1 \cdot (1)(1)(-1) \bmod 7 \equiv -1$

4. (8 pts.) Use the Miller-Rabin primality test to investigate whether 15 is prime or composite by picking one random a between 2 and 14

$15-1 = 14 = 7 \cdot 2^1$

$d = 7$

Find $2^7 \bmod 15 = ?$ $s = 1$

$\underline{a=2}$

$2^2 \bmod 15 = 4$

$2^4 = (2^2)^2 \bmod 15 = 16 = 1$

$2^7 = 2^4 \cdot 2^2 \cdot 2^1 \bmod 15 = (1 \cdot 4 \cdot 2) \bmod 15$

$\equiv 8 \bmod 15 \neq 1$ or 14

$2^{14} \equiv 64 \bmod 15$

$\equiv 4 \bmod 15 \equiv 4$

15 is a composite.

8

5. (8 pts.) Compute $\phi(9)$ **a.** Using the definition ; **b.** Using the formula (in terms of the factorization into prime powers) Explain!

Ans.: $\phi(9) =$ 6

8

$\phi(9)$

By definition,

$\gcd(9,1) = 1$

$\gcd(9,2) = 1$

$\gcd(9,3) = 3$

$\gcd(9,4) = 1$

$\gcd(9,5) = 1$

$\gcd(9,6) = 3$

$\gcd(9,7) = 1$

$\gcd(9,8) = 1$

$\gcd(9,9) = 9$

Therefore $\phi(9) = 6$

There are 6 numbers coprime to 9

By formula

$n = 9 = 3^2$ $\quad p = 3$

$$\phi(n) = 9\left(1 - \frac{1}{3}\right) = 3(2) = 6$$

6. (8 pts.) Suppose Alice used RSA to send you the encrypted message c, using the public key e that you gave her. Check that this is an OK message (coprime to $n = pq$). Also check that the key is a valid key. If they are both OK, find her original message?, m.

$p = 7$, $q = 5$, $e = 11$, $c = 18$

Ans.: $m =$ 2 ✓ 8

$pq = 7 \cdot 5 = 35$

$\phi(35) = 35\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{5}\right) = (6)(4) = \boxed{24 = \phi(35)}$

$\gcd(\phi(35), e) = \gcd(24, 11) = \gcd((2^3 \cdot 3), 11) = 1$

$\therefore \gcd(\phi(35), e) = 1$ This is an ok key.

$d = e^{-1} \bmod (\phi(n))$

$= 11^{-1} \bmod 24$

$\gcd(24, 11) = \gcd(11, 2) = \gcd(2, 1)$

$2 = \boxed{24} - 2\boxed{11}$

$1 = \boxed{11} - 2(5)$

$= \boxed{11} - 5\boxed{24} + 10\boxed{11} = 11\boxed{11} - 5\boxed{24}$

check: $121 - 120 = 1$ ✓ $11 \cdot 11$ $\quad 24 \times 5 = 120$

$11 = 11^{-1} \bmod 24$

$\boxed{d = 11}$

$\gcd(35, 18) = \gcd(5 \cdot 7, 2 \cdot 3^2) = 1$

This is OK message

$m = c^d \bmod n = 18^{11} \bmod 35 = ?$

$m = 2$

$18^2 \bmod 35 = 324 = 9$

$18^4 = 81 \bmod 35 = 11 \bmod 35$

$18^8 = 121 \bmod 35 = 14$

$18^{10} = 18^8 \cdot 18^2 = 14 \cdot 9 \bmod 35 = 144$

$= 4$

$18^{11} = 4 \cdot 18 \bmod 35 = 72$

$\boxed{18^{11} \bmod 35 = 2 = m}$

$4 \times 18 = 72$

$35 \overline{)324}$ 9, 315, 9

$4 \times 18 = 144$

$35 \overline{)144}$ 4, 140, 4

$5 \times 14 = 144$

$35 \overline{)121}$ 3, 105, 16

$35 \overline{)144}$ 4, 140, 4

7. (8 pts.) Prove that for every integer n

$$n = \sum_{d|n} \phi(d) \quad ;$$

where $\phi(n)$ is Euler's totient formula.

8

Proof:

Write down fraction $\frac{i}{n}$, where $i = 1, 2, 3, \ldots n$. Reduce the terms. The number of fractions whose denominators are n are those with the numerator that is coprime to n. That is is $\phi(n)$. The denominator, d_i, are those that are not coprime to n. But its numerator is coprime to d_i. The number of fractions with d_i as denominator $= \phi(d_i)$. This is for all divisors, d_i, of n. The total of all

$$\sum_{d|n} \phi(d) \quad \text{is equal to } n.$$

√ (8)

8. (8 pts.) Prove that if p and q are distinct odd primes, then pq can **not** be a perfect number.

p and q are distinct odd primes. Then

~~Let~~ $3 \le p < q$

$\sigma(pq) = (p+1)(q+1)$

$$2pq - \sigma(pq) = 2pq - pq - p - q - 1$$
$$= pq - p - q - 1$$
$$= (p-1)(q-1) - 1 - 1$$
$$= (p-1)(q-1) - 2$$

Since the smallest value p and q can be ~~are~~ 3 and 5, respectively than

$$2pq - \sigma(pq) = (p-1)(q-1) - 2$$
$$\ge (2)(4) - 2$$
$$\ge 6$$

Therefore $2pq - \sigma(pq)$ can never be zero. pq can not be a perfect number, if p and q are distinct odd primes

9. (9 pts.) Compute

$$\sum_{n=1}^{8} \mu(n) \quad ,$$

where $\mu(n)$ is the Möbius function .

9

Ans.: $\sum_{n=1}^{8} \mu(n) =$ -2

$\mu(1) = 1,$
$\mu(2) = -1$
$\mu(3) = -1$
$\mu(4) = 0$
$\mu(5) = (-1)$
$\mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1$
$\mu(7) = (-1)$
$\mu(8) = 0$

$$\sum_{n=1}^{8} \mu(n) = \cancel{1} - \cancel{1} - 1 - \cancel{1} + \cancel{1} - 1 = -2$$

10. (9 pts.) By 'brute force', find the set of quadratic residues, and the set of quadratic non-residues, for the prime $p = 11$.

Ans.: $QR(11) =$ $\{0, 1, 3, 4, 5, 9\}$

$QNR(11) =$ $\{2, 6, 7, 8, 10\}$

9

$\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2\}$ mod 11

$= \{0, 1, 4, 9, 16, 25\}$ mod 11

$= \{0, 1, 4, 5, 9, 25\}$ mod 11

$= \{0, 1, 3, 4, 5, 9\}$

10 pts

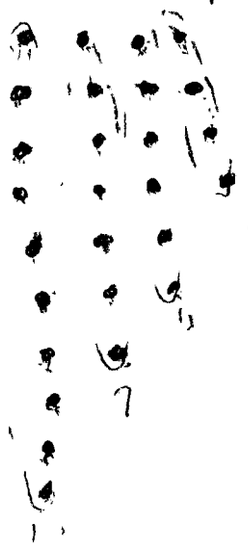
11. (9 pts. altogether) For the integer partition

$$\lambda = (4, 4, 4, 4, 3, 3, 2, 1, 1, 1)$$

(i) Draw the Ferrers graph (4 pts.)
(ii) Find the conjugate partition λ' (5 pts.)

Ans.: $\lambda' =$ (10, 7, 6, 4)

Ferrers Graph



$17 + 6 = 23 + 4 = 27$

$23 + 4 = 27$

$(10 + 7 + 6 + 4) = 27$ ✓

$4^4 3^2 2 \cdot 1^3$

$16 + 6 + 2 + 3 = 27$ ✓

~~$25 + 2 + 3 = 30$~~

$22 + 5 = 27$

9

12. (9 pts.)
i. Apply Glashier's bijection (in the odd To distinct direction) to the odd partition $(5,5,5,3,3,3,3,3,1,1,1)$ to get a distinct partition, call it λ
ii. Apply Glashier's bijection (in the distinct To odd direction) to the partition λ and show that you get $(5,5,5,3,3,3,3,3,1,1,1)$ back, as you should!

Ans.: $\lambda = (12, 10, 5, 3, 2, 1)$

---

odd → dis

$5^3 3^5 1^3$

$5^3 = 5^{2+1}$ — $5 \cdot 2 = 10$, $5 \cdot 1 = 5$

$3^5 = 3^{4+1}$ — $3 \cdot 4 = 12$, $3 \cdot 1 = 3$

$1^3 = 1^{2+1}$ — $2 \cdot 1 = 2$, $1 \cdot 1 = 1$

$$\boxed{\lambda = (12, 10, 5, 3, 2, 1)}$$

15
15
30
+3
33

22
27
+6
33

---

dis → odd

$12 = 3 \cdot 4 \rightarrow 3^4$
$10 = 5 \cdot 2 \rightarrow 5^2$
$5 = 5 \cdot 1 \rightarrow 5^1$
$3 = 3 \cdot 1 \rightarrow 3^1$
$2 = 1 \cdot 2 \rightarrow 1^2$
$1 = 1 \cdot 1 \rightarrow 1^1$

15
15
+3
33

$(3^4 5^2 5^1 3^1 1^2 1^1) = 5^3 3^5 1^3$

get back → $(5,5,5,3,3,3,3,3,1,1,1)$