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

No Calculators! No Cheatsheets!

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 $n_1, n_2, \dots, n_k$ 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.: 1447

We have

$$x = 1 \cdot (7 \cdot 11 \cdot 13) \cdot \big((7 \cdot 11 \cdot 13)^{-1} \pmod{2}\big) + 5 \cdot (2 \cdot 11 \cdot 13) \cdot \big((2 \cdot 11 \cdot 13)^{-1} \pmod{7}\big)$$
$$+6 \cdot (2 \cdot 7 \cdot 13) \cdot \big((2 \cdot 7 \cdot 13)^{-1} \pmod{11}\big) + 4 \cdot (2 \cdot 7 \cdot 11) \cdot \big((2 \cdot 7 \cdot 11)^{-1} \pmod{13}\big)$$

$$= 1 \cdot (1001) \cdot \big((1001)^{-1} \pmod{2}\big) + 5 \cdot (286)) \cdot \big(286^{-1} \pmod{7}\big)$$
$$+6 \cdot (182) \cdot \big((182)^{-1} \pmod{11}\big) + 4 \cdot (154) \cdot \big((154)^{-1} \pmod{13}\big)$$
$$= 1 \cdot (1001) \cdot \big((1)^{-1} \pmod{2}\big) + 5 \cdot (286)) \cdot \big((-1)^{-1} \pmod{7}\big)$$
$$+6 \cdot (182) \cdot \big(6^{-1} \pmod{11}\big) + 4 \cdot (154) \cdot \big((-2)^{-1} \pmod{13}\big)$$

By inspection

$$6^{-1} \pmod{11} = 2 \quad , \quad 2^{-1} \pmod{13} = 7 \quad ,$$

Hence

$$x = 1 \cdot (1001) \cdot (-1) + 5 \cdot (286) \cdot (-1) + 6 \cdot (182) \cdot 2 + 4 \cdot (154) \cdot (-7) =$$
$$(1001{-}1430{+}2184{-}4312) \pmod{2002} = (1001{-}1430{+}182{-}308) \pmod{2002} = 1447 \quad .$$

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.: Friday

There are 1000 years from now, and $250 - 10 + 2 = 242$ leap years. Today is day 3 so

$$3 + 1000 + 242 \pmod 7 = 3 + 6 + 4 \pmod 7 = 13 \pmod 7 = 6 \quad .$$

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

Ans.: -1 alias 102

Wilson's theorem claims that if p is a prime then $(p-1)! \pmod p = -1$. Since 103 is a prime, this follows.

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

Ans.: 1

Pascal's identity says

$$a^{p-1} \pmod p = 1 \quad ,$$

if $a \neq 0$. Since 1003 is a prime, it follows.

4. a (3 pts.) Define Euler's Toitent function $\phi(n)$.
$\phi(n)$ is the numebr of positive integers less than n that are relatively prime to n.
b (7 pts. altogether)
State (2 pts.) and prove (5 pts), Euler's Classical Formula for Euler's Toitent function $\phi(n)$.
(a)

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

(b) Write all the n fractions with denominator n and numerators from 1 to n

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$$

Now *reduce* them so that the top and bottom are relatively primes. The denominators that show up at the bottom are all divisors of n, and for each such divisor d, all the integers relatively prime to d show up. There are $\phi(d)$ of them. Adding them up gives 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.: $m = 8$

$n = 5 \cdot 11 = 55$, $\phi(n) = (5-1) \cdot (11-1) = 40$; $gcd(7, 40) = 1$, so $e = 7$ is an OK key. We need to find d

$$d = 7^{-1} \pmod 40 = 23$$

(either by trial-and-error or the Extended Euclidean algorithm applied to $gcd(40, 7)$

$$\mathbf{40} = 5 \cdot \mathbf{7} + 5 \quad ; \quad 5 = \mathbf{40} - 5 \cdot \mathbf{7}$$

$$\mathbf{7} = 1 \cdot 5 + 2 \quad ; \quad 2 = \mathbf{7} - 5 = 6 \cdot \mathbf{7} - \mathbf{40}$$

$$5 = 2 \cdot 2 + 1 \quad ; \quad 1 = 5 - 2 \cdot 2 == \mathbf{40} - 5 \cdot \mathbf{7} - 2(6 \cdot \mathbf{7} - \mathbf{40}) = 3 \cdot \mathbf{40} - 17 \cdot \mathbf{7}$$

Taking mod 40

$$7^{-1} \pmod{40} = -17 \pmod{40} = 23$$

So

$$m = c^{23} \pmod{55} = 2^{23} \pmod{55}$$

$$2^1 = 2 \quad ; \quad 2^2 = 4 \quad ; \quad 2^4 = 16 \quad ; \quad 2^8 = 16^2 \pmod{55} = 36 \quad ;$$

$$2^{16} = 36^2 \pmod{55} = 31 \quad ;$$

Hence

$$2^{23} \pmod{55} = 2^{16+4+2+1} \pmod{55} = 31 \cdot 16 \cdot 4 \cdot 2 \pmod{55} = 8 \quad .$$

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

Ans.: $\sigma(105) = 192$

$\sigma_2(105) = (1+3^2)(1+5^2)(1+7^2) = 13000,$

$\sigma_3(105) = (1+3^3)(1+5^3)(1+7^3)$

$\sigma_4(105) = (1+3^4)(1+5^4)(1+7^4)$

$\sigma_5(105) = (1+3^5)(1+5^5)(1+7^5)$

The prime factorization of 105 is

$$105 = 3 \cdot 5 \cdot 7 \quad .$$

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

Ans.: (a) 1

a:

b: 0

$2002 = 2 \cdot 7 \cdot 11 \cdot 13$ is a product **four** distinct primes, hence $\mu(2002) = (-1)^4 = 1$
$4004 = 2^2 \cdot 7 \cdot 11 \cdot 13$ is **not** a product of distinct primes, hence $\mu(4004) = 0$

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.: Yes; 17 is a quadratic residue of 281.

$\left(\frac{17}{281}\right)\left(\frac{281}{17}\right) = (-1)^{280)(16)/4} = 1$
But $281 \pmod 1)7 = 9$, hence
$\left(\frac{17}{281}\right)\left(\frac{9}{17}\right) = 1$
So

$$\left(\frac{17}{281}\right) = \left(\frac{9}{17}\right) = \left(\frac{3 \cdot 3}{17}\right) == \left(\frac{3}{17}\right)^2 = 1 \quad .$$

Since the Legendre symbol $\left(\frac{p}{q}\right)$ is either 1 or -1 its square is always 1. So we don't need to know $\left(\frac{3}{17}\right)$

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

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

(i)

$$\begin{array}{ccccccc} * & * & * & * & * & * & * \\ * & * & * & * & * & & \\ * & * & * & * & * & & \\ * & * & * & & & & \\ * & * & * & & & & \\ * & & & & & & \\ * & & & & & & \\ * & & & & & & \end{array} .$$

(ii) $(8, 5, 4, 3, 3, 1, 1)$

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

$$8 = 8 \cdot 1 \quad ; \quad 6 = 2 \cdot 3 \quad ; \quad 3 = 1 \cdot 3 \quad ; \quad 2 = 2 \cdot 1 \quad ; \quad 1 = 1 \cdot 1 \quad .$$

This becomes $1^8, 3^2, 3^1, 1^2, 1^1$
Combining, we get $1^{11}3^3$ and in the usual notation

$$\mu = (3, 3, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$$

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.

$$(3^3, 1^{11}) = (3^{2+1}, 1^{8+2+1}) = (6, 3.8, 2, 1)$$

Putting it in order, we get that indeed the reverse mapping gives $(8, 6, 3, 2, 1)$