ÇANKAYA UNIVERSITY
Department of Mathematics and Computer Science

MATH 365
Elementary Number Theory I
SOLUTIONS
2^{nd} Midterm
December 17, 2007
16:40-18:00

Surname : ______________________
Name : ______________________
ID # : ______________________
Department : ______________________
Section : ______________________
Instructor : ______________________
Signature : ______________________

- The exam consists of 6 questions.
- Please read the questions carefully and write your answers under the corresponding questions. Be neat.
- Show all your work. Correct answers without sufficient explanation might not get full credit.
- Calculators are not allowed.

GOOD LUCK!

Please do not write below this line.

Q1	Q2	Q3	Q4	Q5	Q6	TOTAL
			CANCELLED			
20	20	20	20	20	10	110

1.
a) Does the congruence $28x \equiv 6 \pmod{70}$ have a solution?
b) Write a complete residue system modulo 11 consisting entirely of even integers.

Solution:

a) $28x \equiv 6 \pmod{70}$ has no solution since $(28, 70) \nmid 6$.

b) A complete residue system modulo 11 consisting entirely of even integers is

$$\{0, 12, 2, 14, 4, 16, 6, 18, 8, 20, 10\}.$$

---

2. Find all solutions $z, 0 < z < 500$, to

$$\begin{aligned} z &\equiv 1 \pmod{2} \\ z &\equiv 2 \pmod{3} \\ z &\equiv 3 \pmod{5} \\ z &\equiv 4 \pmod{7} \end{aligned}$$

Solution:

$b_1 = 2, b_2 = 3, b_3 = 5, b_4 = 7$
$c_1 = 1, c_2 = 2, c_3 = 3, c_4 = 4$

$B = b_1 b_2 b_3 b_4 = (2)(3)(5)(7) = 210$

$B_1 = \frac{B}{b_1} = \frac{210}{2} = 105, B_2 = \frac{B}{b_2} = \frac{210}{3} = 70, B_3 = \frac{B}{b_3} = \frac{210}{5} = 42, B_4 = \frac{B}{b_4} = 30$

$105x_1 \equiv 1 \pmod{2} \implies x_1 = 1$

$70x_2 \equiv 1 \pmod{3} \implies x_2 = 1$

$42x_3 \equiv 1 \pmod{5} \implies x_3 = 3$

$30x_4 \equiv 1 \pmod{7} \implies x_4 = 4$

$z = B_1 x_1 c_1 + B_2 x_2 c_2 + B_3 x_3 c_3 + B_4 x_4 c_4$

$z = (105)(1)(1) + (70)(1)(1) + (42)(3)(3) + (30)(4)(4)$

$z = 105 + 140 + 378 + 480$

$z = 1103$

$\implies z$ is of the form; $z = 1103 + 210t,\ 0 < 1103 + 210t < 500$

$\frac{-1103}{210} < t < -\frac{603}{210} \implies t = -5, -4, -3$

$t = -5 \implies z = 1103 - (210)(5) = 53$

$t = -4 \implies z = 1103 - (210)(4) = 263$

$t = -3 \implies z = 1103 - (210)(3) = 473$

$\implies z \in \{53, 263, 473\}$

3.
a) Give a careful statement of Fermat's (Little) Theorem.
b) Find the least residue of
$3^{32} + 8 \pmod{227}$

Solution:

a) **Theorem (Fermat):** If p is prime and a is an integer such that $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

for all integers a.

b) $3^5 \equiv 243 \equiv 16 \pmod{227} \Longrightarrow 3^{10} \equiv 16^2 \equiv 29 \pmod{227} \Longrightarrow 3^{20} \equiv 29^2 \equiv 160 \pmod{227}$.
$3^{30} = 3^{10} \times 3^{20} \equiv 29 \times 160 \equiv 100 \pmod{227} \Longrightarrow 3^{32} = 3^{30} \times 3^2 \equiv 100 \times 9 \equiv 219 \pmod{227}$
$\Longrightarrow 3^{32} + 8 \equiv 219 + 8 \equiv 0 \pmod{227}$.

4.
a) Find $1! + 2! + \cdots + 500! \pmod{189}$.
b) Give the least complete solution to the congruence $27x \equiv -18 \pmod{15}$

Solution:

a) Since $189 = 3^3 \times 7$ divides $9!$, we have $n! \equiv 0 \pmod{189}$ for every $n \geq 9$. Hence

$$\begin{aligned} 1! + 2! + \cdots + 500! &\equiv 1! + 2! + \cdots + 8! \pmod{189} \\ &\equiv 117 \pmod{189}. \end{aligned}$$

b) $\gcd(27, 15) = 3$

$x_0 = 1$ is one of the solutions

$x = x_0 + \frac{b}{d}t \Longrightarrow x = 1 + \frac{15}{3}t = 1 + 5t$ where $t = 0, 1, 2$

$t = 0 \Longrightarrow x = 1$

$t = 1 \Longrightarrow x = 1 + 5 = 6$

$t = 2 \Longrightarrow x = 1 + 10 = 11$

$\Longrightarrow x = 1, 6, 11$

---

5. Show that no integer has order 40 modulo 100.

THIS PROBLEM IS CANCELLED

THIS PROBLEM IS CANCELLED

THIS PROBLEM IS CANCELLED

---

6. (Bonus) Find all solutions to the following system of congruences.

$$\begin{aligned} 5x &\equiv 2 \pmod{9} \\ 2x &\equiv 5 \pmod{13} \\ 3x &\equiv 7 \pmod{17} \end{aligned}$$

Solution: Multiply by suitable numbers on both side of the equivalence to reduce the coefficients of x to 1.

$$\begin{array}{r} 2 \times 5x \equiv 2 \times 2 \pmod{9} \\ 7 \times 2x \equiv 7 \times 5 \pmod{13} \\ 6 \times 3x \equiv 6 \times 7 \pmod{17} \end{array} \quad \longrightarrow \quad \begin{array}{r} x \equiv 4 \pmod{9} \\ x \equiv -4 \pmod{13} \\ x \equiv 8 \pmod{17} \end{array}$$

Now we need to solve
$13 \times 17 b_1 \equiv 1 \pmod{9}$, $9 \times 17 b_2 \equiv 1 \pmod{13}$, $9 \times 13 b_3 \equiv 1 \pmod{17}$.

Reducing modulo the respective modulus, we get

$5b_1 \equiv 1 \pmod{9}$, $-3b_2 \equiv 1 \pmod{13}$, $-2b_3 \equiv 1 \pmod{17}$.

Multiply by suitable numbers on both sides of the equivalence to reduce the coefficients of b_i to 1.

$b_1 \equiv 2 \pmod{9}$, $b_2 \equiv 4 \pmod{13}$, $b_3 \equiv 8 \pmod{17}$.

So

$$\begin{aligned} x &\equiv 13 \times 17 \times 2 \times 4 + 9 \times 17 \times 4 \times (-4) + 9 \times 13 \times 8 \times 8 \pmod{9 \times 13 \times 17} \\ &\equiv 6808 \pmod{252} \\ &\equiv 841 \pmod{252}. \end{aligned}$$

Check that $5 \times 841 \equiv 2 \pmod{9}$, $2 \times 841 \equiv 5 \pmod{13}$, $3 \times 841 \equiv 7 \pmod{17}$