ÇANKAYA UNIVERSITY
Department of Mathematics and Computer Science

MATH 365
Elementary Number Theory I
FALL 2007
Final
SOLUTIONS
January 18, 2008
15:00-16:50

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
20	20	20	20	20	10	110

1. Find all integer solutions to the congruence $42x \equiv 90 \pmod{156}$.

Solutions:

By applying the Euclidean algorithm, we have

$$\begin{aligned} 156 &= 3 \cdot 42 + 30 \\ 42 &= 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

So $\gcd(42, 156) = 6$, and we are expecting 6 incongruent solutions this congruence.
Now

$$\begin{aligned} 6 &= 30 - 2 \cdot 12 \\ &= 30 - 2(42 - 30) \\ &= 3 \cdot 30 - 2 \cdot 42 \\ &= 3(156 - 3 \cdot 42) - 2 \cdot 42 \\ &= (3)(156) - (11)(42). \end{aligned}$$

Multiplying both sides by 15, we get $90 = (45)(156) - (165)(42)$. So $90 \equiv -165 \cdot 42 \pmod{156}$, which means $-165 \equiv -9 \pmod{156}$ is a solution. Therefore, the six solutions are given by $x = -9 + \frac{156}{6}t$, where $t = 0, 1, \cdots, 5$, i.e., $x \equiv -9, 17, 43, 69, 95, 121 \pmod{156}$.

---

2. Find the 2 smallest positive integers x such that

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{11} \\ x &\equiv 4 \pmod{13}. \end{aligned}$$

Solution:

Obviously $7, 11, 13$ are pairwise relatively prime, so by the Chinese Remainder Theorem (CRT) this system has a unique solution mod $7 \times 11 \times 13 = 1001$.

$$\begin{aligned} (11 \times 13)\, b_1 &\equiv 1 \,(\mathrm{mod}\, 7) \Longleftrightarrow 3b_1 \equiv 1 \,(\mathrm{mod}\, 7) \Longleftrightarrow b_1 \equiv 5 \,(\mathrm{mod}\, 7) \\ (7 \times 13)\, b_2 &\equiv 1 \,(\mathrm{mod}\, 11) \Longleftrightarrow 3b_2 \equiv 1 \,(\mathrm{mod}\, 11) \Longleftrightarrow b_2 \equiv 4 \,(\mathrm{mod}\, 11) \\ (7 \times 11)\, b_3 &\equiv 1 \,(\mathrm{mod}\, 13) \Longleftrightarrow -b_3 \equiv 1 \,(\mathrm{mod}\, 13) \Longleftrightarrow b_3 \equiv -1 \,(\mathrm{mod}\, 13) \end{aligned}$$

and $x \equiv (143)\,(5)\,(2) + (91)\,(4)\,(3) + (77)\,(-1)\,(4) \equiv 212 \,(\mathrm{mod}\, 1001)$.

Thus the two solutions are 212 and 1213.

3.
a) Give a careful statement of Wilson's Theorem.
b) Is $4\,(29!) + 5!$ divisible by 31?

Solution:

(a) **Wilson's theorem:** If p is prime, then

$$(p-1)! \equiv -1 \pmod{p}\,.$$

(b) Since 31 is prime, it follows from Wilson's theorem that

$$-1 \equiv 30! \equiv (29!)\,30 \equiv (29!)\,(-1) \pmod{31}\,.$$

Upon multiplying both sides by -1, we see that $29! \equiv 1 \pmod{31}$ and so

$$4\,(29!) + 5! \equiv 4\,(1) + 120 \equiv 124 \equiv 4 \cdot 31 \equiv 0 \pmod{31}\,.$$

4.
(a) Add two negative integeres to the set $\{6, 11, 14, 28\}$ so that the six integers you have will form a complete residue system modulo 6. Justify your answer.
b) Does 41 divide $7 \cdot 3^{20} + 6$?

Solution:

(a) A complete residue system modulo 6 is a set of six integers in which no two are congruent to each other. Note that

$$\begin{aligned} 6 &\equiv 0 \pmod 6 \\ 11 &\equiv 5 \pmod 6 \\ 14 &\equiv 2 \pmod 6 \\ 28 &\equiv 4 \pmod 6 . \end{aligned}$$

So we need to find two negative integers which are congruent to 1 and 3 modulo 6. Since $-5 \equiv 1 \pmod 6$ and $-3 \equiv 3 \pmod 6$, the numbers $6, 11, 14, 28, -5, -3$ form a complete residue system modulo 6.

(b) We want to find out whether $7 \cdot 3^{20} + 6 \equiv 0 \pmod{41}$.
Note that $3^4 = 81 \equiv -1 \pmod{41}$. So $3^{20} \equiv (-1)^5 \equiv -1 \pmod{41}$. Thus $7 \cdot 3^{20} + 6 \equiv 7\,(-1) + 6 \equiv -1 \pmod{41}$. Since $-1 \not\equiv 0 \pmod{41}$, 41 does not divide $7 \cdot 3^{20} + 6$.

---

5. Break the modulus into prime powers to find the least complete solution.

$$4x^2 - 12x + 5 \equiv 0 \pmod{77}.$$

Solution: The prime power factors of 77 are 7 and 11. By testing values in complete residue systems we find that a complete solution to

$$4x^2 + 2x + 5 \equiv 0 \pmod{7}$$

is $x = -3, -1$; and a complete solution to

$$4x^2 - x + 5 \equiv 0 \pmod{11}$$

is $x = -3, 6$.

Now we use the Chinese Remainder Theorem (CRT) to solve the simultaneous congruences

$$\begin{aligned} x &\equiv -3 \text{ or } -1 \pmod{7} \\ x &\equiv -3 \text{ or } 6 \pmod{11}, \end{aligned}$$

which involves solving

$$\begin{aligned} 11x_1 &\equiv 1 \pmod{7} \\ 7x_2 &\equiv 1 \pmod{11} \end{aligned}$$

Solutions are $x_1 = 2$ and $x_2 = -3 \pmod{11}$. Then by the CRT, the simultaneous solutions are

$$\begin{aligned} x &= (11)(2)(-3 \ \text{ or } \ -1) + (7)(-3)(-3 \ \text{ or } \ 6) \\ &= -192, -148, -3, 41 \end{aligned}$$

This is a complete solution to the original congruce. The least complete solution is $x = 6, 38, 41, 74$.

---

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

$$\begin{aligned} x &\equiv 34 \pmod{105} \\ x &\equiv 79 \pmod{330} \end{aligned}$$

Solution: Since $105 = 3 \times 5 \times 7$ and $330 = 2 \times 3 \times 5 \times 11$, this system is equivalent to

$$\begin{aligned} x &\equiv 34 \pmod{3} \\ x &\equiv 34 \pmod{5} \\ x &\equiv 34 \pmod{7} \\ x &\equiv 79 \pmod{2} \\ x &\equiv 79 \pmod{3} \\ x &\equiv 79 \pmod{5} \\ x &\equiv 79 \pmod{11}. \end{aligned}$$

Reducing modulo the respective modulus, we get

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 6 \pmod{7} \\ x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{11}. \end{aligned}$$

So we are left with

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{3} \\ x &\equiv -1 \pmod{5} \\ x &\equiv -1 \pmod{7} \\ x &\equiv 2 \pmod{11}. \end{aligned}$$

Now we need to solve

$$\begin{aligned} 3 \times 5 \times 7 \times 11 b_1 &\equiv 1 \,(\mathrm{mod}\, 2)\,, 2 \times 5 \times 7 \times 11 b_2 \equiv 1 \,(\mathrm{mod}\, 3)\,, 2 \times 3 \times 7 \times 11 b_3 \equiv 1 \,(\mathrm{mod}\, 5) \\ 2 \times 3 \times 5 \times 11 b_4 &\equiv 1 \,(\mathrm{mod}\, 7)\,, 2 \times 3 \times 5 \times 7 b_5 \equiv 1 \,(\mathrm{mod}\, 11)\,. \end{aligned}$$

Reducing modulo the respective modulus, we get

$$\begin{aligned} b_1 &\equiv 1 \,(\mathrm{mod}\, 2)\,, -b_2 \equiv 1 \,(\mathrm{mod}\, 3)\,, 2b_3 \equiv 1 \,(\mathrm{mod}\, 5) \\ b_4 &\equiv 1 \,(\mathrm{mod}\, 7)\,, b_5 \equiv 1 \,(\mathrm{mod}\, 11)\,. \end{aligned}$$

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

$$\begin{aligned} b_1 &\equiv 1 \,(\mathrm{mod}\, 2)\,, b_2 \equiv -1 \,(\mathrm{mod}\, 3)\,, b_3 \equiv 3 \,(\mathrm{mod}\, 5) \\ b_4 &\equiv 1 \,(\mathrm{mod}\, 7)\,, b_5 \equiv 1 \,(\mathrm{mod}\, 11)\,, \end{aligned}$$

So

$$\begin{aligned} x &\equiv 3 \times 5 \times 7 \times 11 \times 1 \times 1 \times + 2 \times 5 \times 7 \times (-1) \times 1 + 2 \times 3 \times 7 \times 11 \times 3 \times (-1) \\ &\quad + 2 \times 3 \times 5 \times 11 \times 1 \times (-1) + 2 \times 3 \times 5 \times 7 \times 1 \times 2 \,(\mathrm{mod}\, 2 \times 3 \times 5 \times 7 \times 11) \\ &\equiv -911 \,(\mathrm{mod}\, 2310)\,. \end{aligned}$$

Check that $-911 \equiv 349 \,(\mathrm{mod}\, 105)$ and $-911 \equiv 79 \,(\mathrm{mod}\, 330)$.