M E T U
Department of Mathematics

<table>
<tr><td colspan="2">Elementary Number Theory I
Midterm 1</td></tr>
<tr><td>Code : Math 365
Acad. Year : 2014
Semester : Fall
Instructor : Küçüksakallı</td><td rowspan="1">Last Name :
Name :
Student No. :
Signature :</td></tr>
<tr><td>Date : November 3, 2014
Time : 17:40
Duration : 100 minutes</td><td>8 QUESTIONS ON 4 PAGES
100 TOTAL POINTS</td></tr>
</table>

1	2	3	4	5	6	7	8		

1. (15pts) Let $a = 4321$ and $b = 3480$. Show that $\gcd(a, b) = 29$. Find $x, y \in \mathbb{Z}$ such that $ax + by = 29$.

Solution: Applying the Euclidean algorithm we find that

$$\begin{aligned} 4321 &= 1 \cdot 3480 + 841 \\ 3480 &= 4 \cdot 841 + 116 \\ 841 &= 7 \cdot 116 + 29 \\ 116 &= 4 \cdot 29 + 0. \end{aligned}$$

Thus we conclude that $\gcd(4321, 3480) = 29$. Applying the algorithm in reverse we find a pair of integers $x = 29$ and $y = -36$ such that $ax + by = 29$:

$$\begin{aligned} 29 &= 841 - 7 \cdot 116 \\ &= 841 - 7(3480 - 4 \cdot 841) \\ &= 29 \cdot 841 - 7 \cdot 3480 \\ &= 29(4321 - 3480) - 7 \cdot 3480 \\ &= 29 \cdot 4321 - 36 \cdot 3480. \end{aligned}$$

2. (10pts) Consider the Diophantine equation $20x + 35y = 1000$. Determine all solutions in integers. How many solutions are there in positive integers?

Solution: Note that $(x_0, y_0) = (50, 0)$ is a solution of the equation. Other solutions are given by $(x, y) = (50 - 7t, 0 + 4t)$ since $\gcd(20, 35) = 5$. In order to obtain solutions in positive integers, we must have $0 < t < 50/7$. There are only 7 solutions in positive integers corresponding $1 \leq t \leq 7$.

3. (15pts) When eggs in a basket are removed $5, 6, 7$ at a time, there remain $1, 2, 4$ eggs respectively. If there are less than 600 eggs in the basket, what are the possible numbers of eggs that could have been in the basket.

Solution: We are required to solve the following system:

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

Consider the corresponding equations $42x_1 \equiv 1 \pmod{5}$, $35x_2 \equiv 1 \pmod{6}$ and $30x_3 \equiv 1 \pmod{7}$. From these equations we find that $x_1 = 3, x_2 = 5$ and $x_3 = 4$ respectively. Thus

$$\tilde{x} = 1 \cdot 42 \cdot 3 + 2 \cdot 35 \cdot 5 + 4 \cdot 30 \cdot 4 \equiv 116 \pmod{210}$$

is a solution of the system. The possible numbers of eggs are $116, 326$ and 536 by Chinese remainder theorem.

4. (10pts) If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then show that $\gcd(ab, n) = 1$.

Solution: Since $\gcd(a, n) = 1$, there exist integers x, y such that $ax + ny = 1$. Since $\gcd(b, n) = 1$, there exist integers r, s such that $br + ns = 1$. Combining these two equations together, we obtain

$$1 = (ax + ny)(br + ns) = (ab)(xr) + (n)(ybr + sax + nys).$$

Since there exist integers $u = xr$ and $v = ybr + sax + nys$ such that $(ab)u + (n)v = 1$, we conclude that $\gcd(ab, n) = 1$.

5. (15pts) Show that there are infinitely many primes of the form $6k+5$ with elementary methods, i.e. do not use Dirichlet's theorem on primes in arithmetic progressions. Can your idea be generalized to show that there are infinitely primes of the form $8k+7$.

Solution: Assume to the contrary $\{q_1, \dots, q_s\}$ is a complete set of primes of the form $6k+5$. Consider $N = 6q_1 \cdots q_s - 1$ and let $N = r_1 \dots r_t$ be its prime factorization. Note that $r_k \neq 2, 3$ for all k. Moreover not all r_k can be of the form $6k+1$. Otherwise their product should be of the form $6k+1$. Thus there is a prime r_k of the form $6k+5$. So we must have $r_k = q_i$ for some $1 \leq i \leq s$. From this we obtain $q_i|1$ which is a contradiction.

This proof cannot be generalized to show that there are infinitely primes of the form $8k+7$. The main problem is that there four different family of primes modulo 8, namely $8k+1, 8k+3, 8k+5$, and $8k+7$. This is in contrast with the situtation modulo 4 and 6 for which there are only two families. To be precise, observe that $8 \cdot 7 \cdot 23 - 1 = 3 \cdot 3 \cdot 11 \cdot 13$ and none of the divisors is of the form $8k+7$.

6. (10pts) Consider the 120 digit number $N = 321321 \dots 321$ consisting of 40 consecutive 321's. Determine the remainder of N upon division by 37. (Hint:$10^3 \equiv 1 \pmod{37}$)

Solution: Note that $N = 321 \cdot 1000^0 + 321 \cdot 1000^1 + \dots + 321 \cdot 1000^{39}$. Since $111 = 37 \cdot 3$, we have $10^3 = 9 \cdot 111 + 1 \equiv 1 \pmod{37}$. It follows that $N \equiv \sum_{i=0}^{39} 321 \cdot 1^i \pmod{37}$. Therefore $N \equiv 40 \cdot 321 \equiv 3 \cdot 25 \equiv 1 \pmod{37}$.

7. (15pts) Factor $n = 60997$ with the help of the congruences

$$247^2 \equiv 2^2 \cdot 3 \pmod{n} \qquad \text{and} \qquad 248^2 \equiv 3 \cdot 13^2 \pmod{n}.$$

Solution: Given congruences imply that $(247{\cdot}248)^2 \equiv (2{\cdot}3{\cdot}13)^2 \pmod{n}$. Set $x = 247{\cdot}248$ and $y = 2 \cdot 3 \cdot 13$. Note that $x = 61256$ and $y = 78$. In order to apply the quadratic sieve method, we want to compute $\gcd(x - y, n)$. We have $x - y = 61178$ and applying the Euclidean algorithm we obtain

$$\begin{aligned} 61178 &= 1 \cdot 60997 + 181 \\ 60997 &= 337 \cdot 181 + 0. \end{aligned}$$

Dividing n by 181, we find that $n/181 = 337$. This gives a factorization of n, that is $n = 337 \cdot 181$.

8. (10pts) Let $n = 2821$. Note that $n = 7 \cdot 13 \cdot 31$. Show that $a^{60} \equiv 1 \pmod{n}$ for any integer a with $\gcd(a, n) = 1$. Is n a Carmichael number?

Solution: Suppose that a is an integer relatively prime to n. Note that a is not divisible by the prime factors of n, namely $7, 13$ and 31. By Fermat's little theorem we have $a^{p-1} \equiv 1 \pmod{p}$ for each $p \in \{7, 13, 31\}$. The least common multiple of $6, 12, 30$ is equal to 60 and we have $a^{60} \equiv 1 \pmod{p}$ for each $p \in \{7, 13, 31\}$. Since $7, 13$ and 31 and relatively prime to each other, Chinese remainder theorem implies that there exists a unique solution x (modulo n) such that $a^{60} \equiv x \pmod{n}$. It is obvious that we can take $x = 1$. Therefore $a^{60} \equiv 1 \pmod{n}$ for any integer a with $\gcd(a, n) = 1$.

The integer n is a Carmichael number because n is a composite number satisfying

$$a^{n-1} = (a^{60})^{47} \equiv 1 \pmod{n}$$

for integers a with $\gcd(a, n) = 1$.