M E T U
Department of Mathematics

<table>
<tr><td colspan="2">Elementary Number Theory I
Midterm 2</td></tr>
<tr><td>Code : Math 365
Acad. Year : 2014
Semester : Fall
Instructor : Küçüksakallı

Date : December 8, 2014
Time : 17:40
Duration : 120 minutes</td><td>Last Name :
Name :
Student No. :
Signature :

8 QUESTIONS ON 4 PAGES
100 TOTAL POINTS</td></tr>
</table>

1	2	3	4	5	6	7	8		

1. (15pts) (a) Prove that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$.

Solution: Let p be an odd prime divisor of $n^2 + 1$. We have $n^2 + 1 \equiv 0 \pmod{p}$. Since n and p are relatively prime, we can talk about the order of n modulo p, say h. Note that $n^4 \equiv (n^2)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$. As a result $h = 1, 2$ or 4. Since $n^2 \equiv -1 \pmod{p}$, we can't have $h = 1$ or $h = 2$. Thus $h = 4$. Since $h = 4$ divides $\phi(p) = p - 1$. We conclude that p is of the form $4k + 1$.

(b) Prove that there are infinitely many primes of the form $4k + 1$.

Solution: Assume otherwise and let $\{p_1, p_2, \ldots, p_r\}$ be a complete list of primes of the form $4k + 1$. Consider $N = (2p_1 \cdots p_r)^2 + 1$. This is an odd integer and it is of the form $n^2 + 1$, thus its prime factors are of the form $4k + 1$ by the previous part. So we must have $p_i | N$ for some i. However this gives a contradiction since $p_i | N - (2p_1 \cdots p_r)^2 = 1$.

2. (10pts) Define $F(n) = \sum_{d|n} d^2$. Determine $F(7!)$.

Solution: Let $f(n) = n^2$ and let n_1, n_2 be relatively prime integers. Observe that

$$f(n_1 n_2) = (n_1 n_2)^2 = n_1^2 n_2^2 = f(n_1) f(n_2).$$

Thus $f(n)$ is a multiplicative function. It follows that $F(n)$ is a multiplicative function too. Therefore

$$\begin{aligned} F(7!) &= F(2^4 \cdot 3^2 \cdot 5 \cdot 7) \\ &= F(2^4) \cdot F(3^2) \cdot F(5) \cdot F(7) \\ &= (1 + 4 + 16 + 64 + 256) \cdot (1 + 9 + 81) \cdot (1 + 25) \cdot (1 + 49) \\ &= 40340300. \end{aligned}$$

3. (15pts) In a lengthy ciphertext message obtained by a linear cipher $\mathcal{C} \equiv a \cdot \mathcal{P} + b \pmod{26}$, the most frequently occuring letter is R and the second most frequent is W.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(a) Break the cipher by determining the values of a and b. (Hint: The most often used letter in English text is E, followed by T.)

Solution: We must have $a \cdot 4 + b \equiv 17 \pmod{26}$ and $a \cdot 19 + b \equiv 22 \pmod{26}$. Eliminating b, we obtain $a \cdot 15 = 5 \pmod{26}$. It follows that $a = 9$ and therefore $b = 7$.

(b) Write out the plaintext for the intercepted message "TBCC QBCC!".

Solution: Solving $\mathcal{P}$ from $\mathcal{C} \equiv a \cdot \mathcal{P} + b \pmod{26}$, we obtain that $\mathcal{P} \equiv a^{-1} \cdot (\mathcal{C} - b) \pmod{26}$. In order to recover the intercepted message, we simply compute

$$\mathcal{P} \equiv 3(\mathcal{C} - 7) \pmod{26}$$

The ciphertext T=19 corresponds to the plaintext K=10 since $3(19 - 7) = 10 \pmod{26}$. Similarly the ciphers B and C corresponds to the plaintexts I and L, respectively. Therefore the original message is "KILL BILL!".

4. (10pts) Let p be a prime and let $n = p^3$. Verify that $\sum_{d|n} \sigma(d)\phi(n/d) = n\tau(n)$.

Solution: Recall that $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$, $\phi(p^k) = p^k - p^{k-1}$ and $\tau(p^k) = k + 1$ for any $k \geq 1$. For $n = p^3$, we have

$$\begin{aligned}
\sum_{d|n} \sigma(d)\phi(n/d) &= \sigma(1)\phi(p^3) + \sigma(p)\phi(p^2) + \sigma(p^2)\phi(p) + \sigma(p^3)\phi(1) \\
&= (p^3 - p^2) + (p^3 - p) + (p^3 - 1) + (p^3 + p^2 + p + 1) \\
&= 4p^3 \\
&= \tau(n)n.
\end{aligned}$$

This verifies the formula above for $n = p^3$.

5. (15pts) (a) Find all values of n such that $\phi(n) = 24$.

Solution: The prime factors of n must be from the set $\{2, 3, 5, 7, 13\}$. To see this note that any prime factor p of n must be less than $n + 1 = 25$. Moreover we can't have $p = 11, 17, 19, 23$ either. Otherwise $\phi(n)$ would be divisible by $10, 16, 18, 22$ respectively which is impossible. If $13|n$, then n must be $39, 52, 78$. If $7|n$, then $n = 35, 56, 70, 84$. The remaining values are $45, 72, 90$. In total there are ten different values.

(b) Find the smallest 6 values of n such that $15|\phi(n)$.

Solution: Suppose that $n = p_1^{r_1} \cdots p_k^{r_k}$. There are two possibilities. We may have $15|\phi(p_i^{r_i})$ for some $1 \leq i \leq k$. It is also possible that $3|\phi(p_i^{r_i})$ for some i and $5|\phi(p_j^{r_j})$ for some $j \neq i$. The first few integers fitting into the first pattern are $31, 61, 62, 93, 122, 124, 151, \ldots$. The first few integers in the second pattern are $77, 99, 143, 154, \ldots$. Thus the smallest six values of such integers are $31, 61, 62, 77, 93$ and 99.

6. (10pts) If m and n are relatively prime positive integers, then show that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

Solution: Since m and n are relatively prime we have $m^{\phi(n)} \equiv 1 \pmod{n}$ and $n^{\phi(m)} \equiv 1 \pmod{m}$ by Euler's theorem. Moreover $n^{\phi(m)} \equiv 0 \pmod{n}$ and $m^{\phi(n)} \equiv 0 \pmod{m}$. It follows that $m^{\phi(n)} + n^{\phi(m)}$ is congruent to $1 + 0 = 1$ modulo both m and n. Since m and n are relatively prime $m^{\phi(n)} + n^{\phi(m)}$ is congruent to a unique integer x modulo mn by Chinese remainder theorem. Obviously $x = 1$ and this finishes the proof.

7. (15pts) Assume that the order of a modulo n is h and the order of b modulo n is k.
(a) Show that the order of ab modulo n divides hk.

Solution: It is enough to show that $(ab)^{hk} \equiv 1 \pmod{n}$. We have

$$(ab)^{hk} = (a^h)^k \cdot (b^k)^h \equiv 1^k \cdot 1^h \equiv 1 \pmod{n}.$$

Thus hk is divisible by the order of ab modulo n.

(b) If $\gcd(h, k) = 1$ then show that order of ab modulo n is precisely hk.

Solution: Let ℓ be the order of ab modulo n. By the previous part we know that $\ell | hk$. We need to show that $hk|\ell$. Since h and k are relatively prime, it is enough to show that $h|\ell$ and $k|\ell$. Using the hypothesis we obtain $(ab)^\ell = a^\ell b^\ell \equiv 1 \pmod{n}$. Raising the last congruence to the power k we get $(a^\ell b^\ell)^k \equiv a^{\ell k} 1^\ell \equiv 1 \pmod{n}$. It follows that $h|\ell k$. Since $\gcd(h, k) = 1$, we must have $h|\ell$. Similarly one can show that $k|\ell$. This finishes the proof.

8. (10pts) Let $n > 1$ be an integer with prime factorization $n = p_1^{r_1} \cdots p_k^{r_k}$. Show that

$$\sum_{d|n} d\mu(d) = (1 - p_1) \cdots (1 - p_k).$$

Solution: Let $d = d_1 d_2$ with $\gcd(d_1, d_2) = 1$. Then we have $d\mu(d) = [d_1\mu(d_1)][d_2\mu(d_2)]$ since d and $\mu(d)$ are both multiplicative functions. It follows that $d\mu(d)$ and therefore $\sum_{d|n} d\mu(d)$ is multiplicative. It suffices to show that

$$\sum_{d|p^k} d\mu(d) = 1 - p$$

for some prime number p. Note that this sum is trivial after the first two terms since $\mu(p^i) = 0$ for $i \geq 2$. Thus $\sum_{d|p^k} d\mu(d) = 1 \cdot \mu(1) + p \cdot \mu(p) = 1 - p$ and this finishes the proof.