

CORRECTION OF MIDTERM I

Problem 1. (20 points) Assume that a, m are two integers such that $G.C.D.(a, m) = 1$.

1. Why does there exist an integer x_1 such that $a.x \equiv 1 \pmod{m}$?
2. For $s = 1, 2, \dots$ let $x_s = \frac{1}{a} - \frac{1}{a}(1 - a.x_1)^s$. Prove that x_s is an integer and that it is a solution of $a.x \equiv 1 \pmod{m^s}$.

Proof.

1. Since $G.C.D.(a, m) = 1$ there exist integers x, y such that $a.x + m.y = 1$, therefore $a.x \equiv 1$.
2. Expand $(1 - a.x_1)^s = 1 + \sum_{k=1}^s \binom{s}{k} \cdot (-a.x_1)^k$, but all the $(a.x_1)^k, k \geq 1$ are multiples of a , therefore $\frac{1}{a} \cdot \sum_{k=1}^s \binom{s}{k} \cdot (-a.x_1)^k$ is an integer x_s .

Problem 2. (30 points) Let R be the ring $\left\{ a + b\sqrt{3} \mid a, b \in \mathbb{Z} \right\}$. We define a function N by:

$$N: \quad R \quad \longrightarrow \quad \mathbb{Z} \\ a + b\sqrt{3} \quad \longmapsto \quad a^2 - 3b^2$$

(Notice that N is not the square of the distance from 0 to α).

1. Show that $N(\alpha.\beta) = N(\alpha).N(\beta)$ for every α, β in R .
2. If α has an inverse in R for the multiplication, show that $N(\alpha) = 1$. (**Hint:** first show that $N(\alpha)$ must be ± 1 , and then show that it can't be -1).
3. Conversely, show that if $N(\alpha) = 1$ then α has an inverse in R .
4. Find 4 distinct examples of invertible elements in R .

Proof.

1. If $\alpha = a + b\sqrt{3}, \beta = c + d\sqrt{3}$ then $\alpha.\beta = (ac + 3bd) + (ad + bc)\sqrt{3}$, so $N(\alpha.\beta) = (ac + 3bd)^2 - 3(ad + bc)^2 = a^2c^2 + 6abcd + 9b^2d^2 - 3a^2d^2 - 6abcd - 3b^2c^2$, whereas $N(\alpha).N(\beta) = (a^2 - 3b^2).(c^2 - 3d^2) = a^2c^2 - 3a^2d^2 + 9b^2d^2 - 3b^2c^2$, the same.
2. $(\alpha.\beta = 1) \Rightarrow N(\alpha).N(\beta) = 1$, where $N(\alpha), N(\beta) \in \mathbb{Z}$, so necessarily $N(\alpha) = \pm 1$.
Now $a^2 - 3b^2 = -1$ is impossible because $a^2 + 1 \pmod{3}$ takes only the values 1 or 2.
3. $N(\alpha) = 1 \Rightarrow a - \sqrt{3}b \in R$ is the inverse of α , because $(a + b\sqrt{3}).(a - b\sqrt{3}) = a^2 - 3b^2 = 1$
4. $1, -1, 2 + \sqrt{3}, 2 - \sqrt{3}$ are examples, but then are lots of other examples.

Problem 3. (20 points) You probably remember that in class we proved that the (multiplicative) group of invertible elements of $\mathbb{Z}/p\mathbb{Z}$ is cyclic (for p prime).

1. Show that $(\mathbb{Z}/8\mathbb{Z})^\times$ (this means the multiplicative group of invertible elements in $\mathbb{Z}/8\mathbb{Z}$) is not cyclic. (Hint: what are the orders of the elements of $(\mathbb{Z}/8\mathbb{Z})^\times$?)
2. (**Extra credit: 15 points**) Can you deduce from above that the same result is true for higher powers (I mean in $\mathbb{Z}/2^n\mathbb{Z}$, for $n \geq 3$)? (try 2^4 or 2^5 , because a general proof is harder to obtain).

Proof.

Just realize that $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ and that all these elements are of order 2 (their squares are $\equiv 1 \pmod{8}$).

You can do the same for $\mathbb{Z}/16\mathbb{Z}$. In class I might indicate a general proof.

Problem 4. (30 points) We call $\sigma(n)$ the sum of all the divisors of the integer n . For example $\sigma(6) = 1 + 2 + 3 + 6 = 12$, and $\sigma(5) = 1 + 5 = 6$.

1. For any prime p , any integer $k \geq 1$, show that $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$.
2. If $G.C.D(m, n) = 1$ prove that $\sigma(m.n) = \sigma(m).\sigma(n)$. If you can't prove this then prove the simpler case $\sigma(p.q) = \sigma(p).\sigma(q)$, when p, q are two distinct primes.
3. Give a general formula for $\sigma(n)$ in terms of its decomposition in prime factors
 $n = p_1^{k_1} \dots p_n^{k_n}$

Proof.

1. The only divisors of p^k are $1, p, p^2, \dots, p^k$. Their sum is $\sum_{i=1}^k p^i = \frac{p^{k+1} - 1}{p - 1}$.
2. Let's write $m = p_1^{r_1} \dots p_k^{r_k}$, and $n = q_1^{s_1} \dots q_l^{s_l}$ where the p_i and the q_j are distinct. Then each divisor of $m.n$ can be written in a unique way as $\left(\prod p_i^{t_i} \right) \cdot \left(\prod q_j^{t_j} \right)$, therefore these divisors of $m.n$ are in bijection with the ordered pairs (a, b) where a is a divisor of m , and b a divisor of n . Since $\sigma(m).\sigma(n)$ is the sum of all products (divisor of m). (divisor of n), we get the result.
3. From above, one derives $\sigma(n) = \prod_{i=1}^n \frac{p_i^{k_i+1} - 1}{p_i - 1}$.

Remark.

One could solve the whole problem in one step, by expanding the product

$$S = (1 + p_1 + \dots + p_1^{k_1}) \dots (1 + p_n + \dots + p_n^{k_n})$$

and noticing that one gets exactly the sum of all divisors of n