MSGSÜ – MAT316
Çalışma Soruları 2

6 Mart 2020

1. Bir $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ polinomu verilsin. Buna karşılık $\overline{f(X)} \in (\mathbb{Z}/m\mathbb{Z})[X]$ poinomunu $\overline{f(X)} = \overline{a_n}X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_1}X + \overline{a_0}$ ile tanımlayalım.
   (a) Gösteriniz ki $f(x) = 0$ denkleminin $\mathbb{Z}$'de bir çözümü varsa, $\overline{f(x)} = \overline{0}$ denkleminin de $\mathbb{Z}/m\mathbb{Z}$'de bir çözümü vardır. Karşıt örnek vererek bu iddianın tersinin doğru olmadığını gösteriniz.
   (b) Gösteriniz ki, bir a tamsayısı verildiğinde, $f(a) \equiv 0 \pmod{m}$ olması için gerek ve yeter koşul $\mathbb{Z}/m\mathbb{Z}$ 'de, $\overline{f(\overline{a})} = \overline{0}$ olmasıdır.

2. Doğrusal kalandaşlık denlemlerinden faydalanarak $\mathbb{Z}/m\mathbb{Z}$ halkasında,
   (a) Gösteriniz ki, $\overline{a}x = \overline{1}$ denkleminin çözümünün mevcut olabilmesi için gerek ve yeter koşul $ebob(a, m) = 1$ olmasıdır.
   (b) Gösteriniz ki, $\overline{a}x = \overline{1}$ denkleminin çözümü varsa, bu çözüm biriciktir.

3. **TANIM:** Eğer $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ için $\overline{a}x = \overline{1}$ denkleminin çözümü varsa, "$\overline{a}$, $\mathbb{Z}/m\mathbb{Z}$ halkasının tersinir (veya birimsel) elemanıdır" denir ve denklemin $(\overline{a})^{-1}$ ile gösterilen çözümüne "$\overline{a}$ 'nın $\mathbb{Z}/m\mathbb{Z}$ içindeki tersi" denir. $\mathbb{Z}/m\mathbb{Z}$ halkasının tersinir elemanlarının kümesi $U(\mathbb{Z}/m\mathbb{Z})$ ile gösterilir Aşağıdaki şıklarda, verilen $\mathbb{Z}/m\mathbb{Z}$ halkaları için $U(\mathbb{Z}/m\mathbb{Z})$ 'yi yazınız:
   (a) $\mathbb{Z}/25\mathbb{Z}$
   (b) $\mathbb{Z}/48\mathbb{Z}$
   (c) $\mathbb{Z}/71\mathbb{Z}$

4. $U(\mathbb{Z}/m\mathbb{Z})$'de
   (a) Gösteriniz ki, her $\overline{a}, \overline{b} \in U(\mathbb{Z}/m\mathbb{Z})$ için, $\overline{ab} \in U(\mathbb{Z}/m\mathbb{Z})$'dir.
   (b) Gösteriniz ki, $\overline{1} \in U(\mathbb{Z}/m\mathbb{Z})$'dir.
   (c) Gösteriniz ki, her $\overline{a} \in U(\mathbb{Z}/m\mathbb{Z})$ için $(\overline{a})^{-1} \in U(\mathbb{Z}/m\mathbb{Z})$'dir.

5. Gösteriniz ki, $ax + my = 1$ Diyofant denkleminin çözümünün mevcut olması için gerek ve yeter koşul, $\overline{a} \in U(\mathbb{Z}/m\mathbb{Z})$ olmasıdır.

6. **TANIM (GRUP):** Verilen bir G kümesi ve G üzerinde tanımlı bir $*$ işlemi,
   (a) Her $a, b \in G$ için $a * b \in G$
   (b) Her $a, b, c \in G$ için $(a * b) * c = a * (b * c)$
   (c) $\exists e \in G$, $a * e = e * a = a$
   (d) Her $a \in G$ için $\exists b \in G$; öyle ki, $a * b = b * a = e$

koşullarını sağlıyorsa, G'ye "$*$" işlemiyle birlikte bir grup adı verilir. Eğer "$*$" işlemi değişmeliyse; yani yukarıdaki özelliklere ek olarak her $a, b \in G$ için $a * b = b * a$ ise, G'ye değişmeli grup (veya abelyen grup) adı verilir. Eğer G, üzerindeki "$*$" işlemiyle bir grupsa, bunu belirtmek için $(G, *)$ notasyonu kullanıyoruz.
Gösteriniz ki, $U(\mathbb{Z}/m\mathbb{Z})$, $\mathbb{Z}/m\mathbb{Z}$ üzerindeki $\otimes$ işlemiyle birlikte değişmeli bir gruptur.

7. **TANIM1:** G sonlu bir küme olmak üzere, $(G, *)$ grubunun $\mid G \mid$ ile gösterilen mertebesi G'nin eleman sayısı olarak tanımlanır.
TANIM2: Verilen bir $(G, *)$ grubunda, bir $g \in G$ için g'nin $\mid g \mid$ ile gösterilen mertebesi, $g^k = e$ koşulunu sağlayan en küçük k tamsayısıdır.

   Eğer $\mid G \mid = n$ ise, her $g \in G$ için $g^n = e$ olduğu bilindiğine göre aşağıdakileri cevaplayınız.
   (a) Her $g \in G$ için, $\mid g \mid \leq n$;
   (b) Her $g \in G$ için, $|g| \big| n$ 'dir.
   (c) Herhangi bir k pozitif tamsayısı ve her $g \in G$ için

$$|g^k| = \frac{|g|}{ebob(k, |g|)}$$

8. **TANIM 1:** Bir H halkasında, verilen $a \neq 0$ elemanı için, $ab = 0$ olacak şekilde $0 \neq b \in H$ var ise, a'ya H halkasının sıfır bölenidir denir. Eğer H'nin hiç sıfır böleni yoksa, H'ye sıfır bölensizdir denir.
TANIM 2: Birimli, değişmeli, sıfır bölensiz bir halkaya tamlık bölgesi denir.
TANIM 3: 0 dışındaki tüm elemanları tersinir olan tamlık bölgelerine cisim adı verilir.
   (a) Gösteriniz ki, p asal sayıysa, $\mathbb{Z}/p\mathbb{Z}$ cisimdir.
   (b) Asal olmayan her m pozitif tamsayısı için $\mathbb{Z}/m\mathbb{Z}$ cisim değildir. Gösteriniz.

9. $ebob(a, m) = 1$ olmak üzere aşağıdakileri kanıtlayınız.
   (a) $ord_m(a) | \varphi(m)$;
   (b) $a^k \equiv 1 \pmod{m}$ ancak ve ancak $ord_m(a) | k$ ise;
   (c) $ord_m(a^k) = \dfrac{ord_m(a)}{ebob(k, ord_m(a))}$

10. Gösteriniz ki, $ebob(a, m) = 1$ olmak üzere $ord_m(a) = \varphi(m)$ olabilmesi için gerek ve yeter koşul $U(\mathbb{Z}/m\mathbb{Z})$ nin devirli grup olması ve $\langle \overline{a} \rangle = U(\mathbb{Z}/m\mathbb{Z})$ olmasıdır.