MAT 3013 SOYUT CEBİR VE SAYILAR TEORİSİ I 1.ARASINAV SORULARI

Ad-Soyad:.....CEVAP ANAHTARI……..... 08.11.2004

No :..

Soru 1) p asal ise 2^p-2 farkının p ile bölünebilmesi gerektiğini gösteriniz. n asal değilken 2^n-2 farkı n ile bölünmeli midir?

Euler ya da Fermat teoremi gereği $2^{p-1} = 1$ (p) ya da denk olarak $2^p = 2$ (p) yazılabilir. Yani 2^p-2 farkı p ile bölünebilirdir. n asal değilken $2^{\varphi(n)} = 1$ (n) olup $\varphi(n)$ her zaman n-1 olmadığından 2^n-2 farkı n ile bölünmeyebilir. Örneğin n = 6 iken $2^6-2 = 62$ olup 6 ile bölünmez.

Soru 2) Bir p asal sayısı iki karenin toplamı olarak ifade edilebiliyorsa φ(p) sayısı 4 ile bölünebilirdir. Gösteriniz.

Bir çift sayının karesi 4 modunda sıfıra; bir tek sayının karesi de 4 modunda bire denk olduğundan $p = x^2+y^2$ şeklinde yazılabiliyorsa $p \equiv 0$, 1 veya 2 (4) olduğunu biliyoruz. $p \equiv 0$ ve 2 (4) iken $p > 2$ olduğundan p asal olmaz. O halde $p \equiv 1$ (4)'tür. Yani p = 4k+1, $k \in \mathbb{Z}$ şeklindedir. Ancak φ(p) = p–1 olduğundan

$$\varphi(p) = \varphi(4k+1) = 4k$$

elde edilir ve bu 4 ile bölünebilirdir.

Soru 3) $f(x) = x^{18} + 2x^{17} + x^{16} + x + 1$ (17) kongrüansının tüm çözümlerini belirleyiniz.

Euler ya da Fermat teoremi gereği $x^{16} = 1$ (17) dir. Bu kullanılarak

$$\begin{aligned} f(x) &= x^{18} + 2x^{17} + x^{16} + x + 1 \\ &= x^2 + 2x + 1 + x + 1 \ (17) \\ &= x^2 + 3x + 2 \ (17) \end{aligned}$$

elde edilir. O halde çözümler x = -1 = 16 (17) ve x = -2 = 15 (17) dir.

Soru 4) (a,m), (b,m) veya (c,m)'den en az biri *1* ise $ax+by+cz \equiv d\ (m)$ kongrüansının m^2 tane çözümü oluşunu açıklayınız.

(a,m) = 1 olsun. $ax+by+cz \equiv d\ (m)$ kongrüansını $ax \equiv d-by-cz\ (m)$ şeklinde düşünürsek ve bir an için sağ tarafın sabit olduğunu varsayarsak (a,m) = 1 olduğundan bu son kongrüansın bir tek çözümü olacağını söyleyebiliriz. Ancak bu çözüm, her bir (y,z) ikilisi için bir tektir. Dolayısıyla toplam çözüm sayısı (y,z) ikililerinin sayısı kadardır. Bu sayı ise $m \cdot m = m^2$'dir.

Soru 5) 3 ile bölünebilme kuralını elde ediniz.

$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10^1 + a_0$ olsun.

$$f(x) = a_k \cdot x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_1 \cdot x + a_0$$

tanımlayalım. $10 \equiv 1$ (3) olduğundan $f(10) \equiv f(1)$ (3) olur. Yani f(10) ve f(1)'in ya ikisi de 3 ile bölünebilir ya da ikisi de bölünemez. f(10) = n olup

$$f(1) = a_k + a_{k-1} + \ldots + a_1 + a_0$$

yani n'nin rakamlar toplamıdır. O halde n'nin 3 ile bölünebilmesi demek rakamlar toplamının 3 ile bölünebilmesi demektir.

Not: Süre 70 dakikadır. Başarılar... İNC