MAT 3013 SOYUT CEBİR VE SAYILAR TEORİSİ I 2.ARASINAV SORULARI

Ad-Soyad:....CEVAP ANAHTARI......... 13.12.2004

No :..

Soru 1) $p>3$ asal olmak üzere

$$(p-3)! \equiv (p-1)/2 \ (p)$$

olduğunu gösteriniz.

Wilson Teoremine göre p asal iken $(p-1)! \equiv -1 \ (p)$ olur. Bunu $(p-1)(p-2)(p-3)! \equiv -1 \ (p)$ olarak düşünebiliriz. Denk olarak $(-1)(-2)(p-3)! \equiv p-1 \ (p)$ yazılırsa $(p-3)! \equiv (p-1)/2 \ (p)$ elde edilir.

Soru 2) Z_{21}'de $x^2+2x-3 \equiv 0 \ (21)$ kongrüansının çözümlerini belirleyiniz.

Verilen kongrüansın diskriminantı $\Delta = 4+4\cdot3 = 16$ olup $\mathbf{Z_{21}}$'de 16'nın karekökleri ±4 ve ±10 olduğundan çözümler

$$x_1 = \frac{-2+4}{2} = 1, \quad x_2 = \frac{-2-4}{2} = -3,$$

$$x_3 = \frac{-2+10}{2} = 4, \quad x_4 = \frac{-2-10}{2} = -6$$

şeklindedir. Yani sorulan tüm çözümler, 21 modunda 1, 4, 15 ve 18 in denklik sınıflarındaki tüm tamsayılardır.

Soru 3) n bir tamsayı olmak üzere $n^{33}-n$ farkının 17 ile bölündüğünü gösteriniz.

n, 17 ile bölünüyorsa sonuç aşikârdır. $(n,17) = 1$ ise Fermat Teoremine göre $n^{16} \equiv 1 \ (17)$ yazabiliriz. İki tarafın karesi alınarak $n^{32} \equiv 1 \ (17)$ elde ederiz. Son olarak iki tarafı n ile çarparak $n^{33} \equiv n \ (17)$ buluruz ki bunun anlamı da $n^{33}-n$ farkının 17 ile bölündüğüdür.

Soru 4)

$$x \equiv a \ (m)$$
$$x \equiv a \ (n)$$

sisteminin çözümünün $x \equiv a \ ([m,n])$ olduğunu gösteriniz.

k bir tamsayı olmak üzere, $x = a+mk$ değeri ikincide yerine konulduğunda $a+mk \equiv a \ (n)$ veya denk olarak, $mk \equiv 0 \ (n)$ elde edilir. Bu son kongrüansın çözümü ise $k \equiv 0 \ \frac{n}{(m,n)}$ şeklindedir. Bu çözüm t bir tamsayı olmak üzere $k = \frac{n}{(m,n)}t$ şeklinde düşünülebilir. Bu değer yukarıda x için bulunan ifadede yerine konulursa $x = a + m\frac{nt}{(m,n)} = a + t[m,n]$ veya istendiği şekilde $x \equiv a \ ([m,n])$ elde edilir.

Soru 5) $f(x) = x^{17}+6x^{14}+2x^5+1 \equiv 0 \ (5)$ kongrüansının tüm köklerini belirleyiniz.

Euler Teoremi gereği $x^5 \equiv x \ (5)$ tir. O halde

$$x^{17} = (x^5)^3x^2 \equiv x^3x^2 = x^5 \equiv x \quad (5)$$
$$x^{14} = (x^5)^2x^4 \equiv x^2x^4 = x^6 = x^5x \equiv xx = x^2 \quad (5)$$

ve son olarak

$$x^5 \equiv x \quad (5)$$

olduğu kullanılarak verilen polinomun

$$x + 6x^2 + 2x + 1 \equiv 0 \quad (5)$$

şekline geleceği açıktır. Katsayıları da 5 modunda indirgersek

$$x^2 + 3x + 1 \equiv 0 \quad (5)$$

veya denk olarak

$$x^2 - 2x + 1 \equiv 0 \quad (5)$$

elde ederiz. Yani, $f(x) \equiv 0 \ (5)$ kongrüansını çok daha basit olan

$$g(x) \equiv (x-1)^2 \quad (5)$$

kongrüansına çevirmiş oluruz. Bu kongrüansın tek kökü ise $x \equiv 1 \ (5)$ tir. Yani $f(x) \equiv 0 \ (5)$ kongrüansının da tek kökü, $x \equiv 1 \ (5)$ tir.

<u>**Not:**</u> *Süre 70 dakikadır. Başarılar.* **İNC**