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

Ad-Soyad:....CEVAP ANAHTARI.......... **29.12.2005**

No :...

Soru 1) p asal ise $(a+b)^p = a^p+b^p$ (p) olduğunu gösteriniz.

p asal iken p'nin k=0 ve k=p hariç tüm $\binom{p}{k}$ Binom katsayılarının p ile bölündüğünü biliyoruz. Bu yüzden $(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^p$ açılımında ilk ve son terim hariç diğer tüm terimlerin katsayıları p ile bölüneceğinden sonuç görülür.

Soru 2) p>2 olsun. p'nin asal olması için gerek ve yeter şartın $(p-2)!\equiv 1$ (p) olduğunu gösteriniz.

Wilson teoremi gereği p'nin asal olması için gerek ve yeter şart $(p-1)! \equiv -1$ (p) olmasıdır. Bu ifade

$$(p-1)! = (p-1)(p-2)!$$

şeklinde düşünülürse ve $p-1 \equiv -1$ (p) olduğu hatırlanırsa

$$(p-1)! = (-1)(p-2)! \equiv -1 \ (p)$$

bulunur. İki taraf –1 ile çarpılırsa sonuç elde edilir.

Soru 3) n bir doğal sayı olmak üzere hiçbir tamsayının karesinin 11n+2 şeklinde olamayacağını gösteriniz.

Eğer $11n+2 = x^2$ olacak şekilde bir x tamsayısı bulunabilseydi, $x^2 \equiv 2$ (11) kongrüansının bir çözümü de var olurdu. Halbuki 11, 8 modunda ± 1 olmadığından 2, Q_{11}'in bir elemanı değildir. Yani 2, 11 modunda bir ikinci dereceden kalan değildir.

Soru 4) $\left(\frac{5}{p}\right) = 1$ özelliğindeki tüm p asallarını belirleyiniz.

Gauss'un indirgeme kuralı yardımıyla

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} = 1$$

olduğundan $\left(\frac{5}{p}\right) = 1$ olması için $\left(\frac{p}{5}\right) = 1$ olmalıdır. O halde p'nin 5 modunda bir tam kare olması gerekir. 5 modundaki tam kareler 1 ve 4 olduğundan $\left(\frac{5}{p}\right) = 1$ olması için p 'nin 5 modunda 1 veya 4'e denk olması gerekli ve yeterlidir. Daha belirleyici olarak, $p \equiv 1$ (10) veya $p \equiv 9$ (10) olması da gerek ve yeter şart olarak verilebilir. Ayrıca p = 2 nin de bu şartı sağladığı açıktır.

Soru 5) p ve q, 4 modunda bire denk olan iki farklı asal sayı olsun. $x^2 \equiv p$ (q) kongrüansının çözümü varsa, $x^2 \equiv q$ (p) kongrüansının da çözümünün olduğunu gösteriniz.

m ve n tamsayılar olmak üzere, p = 4m+1 ve q = 4n+1 olsun.

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{2m2n}$$
$$= \left(\frac{q}{p}\right)$$

olacağından, $x^2 \equiv p$ (q) ve $x^2 \equiv q$ (p) denklemlerinin ya ikisinin de çözümü vardır, ya da ikisinin de çözümü yoktur.

<u>Not:</u> *Süre 60 dakikadır. Başarılar.* **İNC**