MAT 3013 SOYUT CEBİR VE SAYILAR TEORİSİ I ARASINAV SORULARI

Ad-Soyad:..CEVAP ANAHTARI..... **29.07.2011**

No :.....

Soru 1) p ve q farklı tek asalları iki tamkare toplamı olarak yazılabilirse p·q çarpımının 4 modunda 1 olduğunu gösteriniz.

p ve q asalları iki tam karenin toplamı olarak yazılabildiğine göre 4 modunda bire denktirler. Yani k ve t birer tamsayı olmak üzere p = 4k+1 ve q = 4t+1 şeklinde yazılabilirler. O halde

$$p.q = (4k+1)(4t+1) = 4(4kt+k+t) + 1$$

olup parantez içindeki ifade bir tamsayı olduğundan p.q çarpımı 4 modunda bire denktir.

Soru 2) $3x-6y \equiv 5\ (13)$ kongrüansının çözüm kümesini bulunuz.

(3,6,13)=1 olup 5'i böldüğünden çözüm vardır. Verilen kongrüans $3x \equiv 6y+5\ (13)$ ve denk olarak $3x \equiv 6y+18\ (13)$ şeklinde yazılabilir. (3,13)=1 olduğundan her iki tarafı 3 ile bölebiliriz ve $x \equiv 2y+6\ (13)$ elde ederiz. y'ye 13 modundaki değerleri vererek çözüm kümesini

Ç = {(6,0), (8,1), (10,2), (12,3), (1,4), (3,5), (5,6), (7,7), (9,8), (11,9), (0,10), (2,11), (4,12)}

olarak buluruz.

Soru 3) $(p-2)!(p^2-1) \equiv -1\ (p)$ olduğunu gösteriniz.

Wilson teoremine göre p asal iken $(p-1)! \equiv -1\ (p)$ olur. $(p-1)! = (p-1)(p-2)!$ olduğundan

$$\begin{aligned}(p-2)!(p^2-1) &= [(p-1)!/(p-1)](p^2-1)\\ &= (p-1)!(p+1)\\ &\equiv -1.1\\ &= -1\ (p)\end{aligned}$$

olur.

Soru 4) $x^{32}+5x^{31}+4x^{27}+6x^{24}+8x^{19}+3x^{15}+4x^7+5x^6+5 = 0$ denkleminin 7 modundaki tüm çözümlerini bulunuz.

Her x tamsayısı için $x^6 \equiv 1\ (7)$ olduğundan bu değer yerine konulduğunda verilen polinom sadeleşerek şu hale dönüşür:

$$x^2+5x+4x^3+6+8x+3x^3+4x+10 \equiv 0\ (7).$$

Dolayısıyla 7 modunda çalıştığımızı akılda tutarak

$$x^2+3x+2 \equiv 0\ (7)$$

kongrüansını elde ederiz. Bunun çözümlerinin 5 ve 6 olduğu kolayca görülebilir.

Soru 5) Her a, b, c $\in$ Z için (a+cb,b) = (a,b) olduğunu gösteriniz.

(a,b) = d olsun. Yani d|a ve d|b olsun ve ayrıca k pozitif tamsayısı k|a ve k|b özelliğinde herhangi bir tamsayı iken k|d olduğunu kabul edelim. (a+cb,b) = d olduğunu göstermeliyiz. Yani d|(a+cb) ve d|b olduğunu, ikinci olarak da k pozitif tamsayısı k|(a+cb) ve k|b özelliğinde herhangi bir tamsayı iken k|d olduğunu göstermeliyiz. Bu üç ifadeden d|b olduğu zaten veriliyor. d, a ve b'yi böldüğünden bunların herhangi bir lineer toplamını da böler, örneğin d|(a+cb) olur. Son olarak k|(a+cb) ve k|b olsun. Aynı şekilde k, a+cb ve b sayılarının tüm lineer toplamlarını da böler. Bunlar arasında işimize yarayan (a+cb) + (-c)b lineer toplamıdır ki bu da a'ya eşittir. O halde k|a elde edilir. Verilenler arasında k|b de olduğundan varsayım gereği bu iki şartı sağlayan her k pozitif tamsayısı d'yi de böleceğinden sonuç görülür.

Not: Süre 70 dakikadır. Başarılar... İNC