MAT 3013 SOYUT CEBİR VE SAYILAR TEORİSİ I FİNAL SORULARI

Ad-Soyad:……....*CEVAP ANAHTARI*....... **01.09.2003**

No :..

Soru 1) (a,b) = 1 ise (a-b, a+b) = 1 veya 2 olduğunu gösteriniz. (20 puan)

d = (a-b, a+b) diyelim. Bu durumda d bir ortak bölen olup d| (a-b) ve d| (a+b) dir. O halde d| ((a+b)+(a-b)), yani d| 2a ve benzer şekilde d| ((a+b)-(a-b)), yani d| 2b elde edilir. Yani d, 2a ve 2b sayılarının bir ortak bölenidir. (a,b) = 1 verildiğinden dolayı (2a,2b) = 2 dir. O halde d bir ortak bölen olduğu için 2a ve 2b nin obebi olan 2 yi de bölmek zorundadır. O halde d=1 veya d=2 olabilir.

Soru 2) $n \in \mathbf{N}$ olmak üzere hiçbir tamsayının karesinin 7n+3 şeklinde olamayacağını gösteriniz. (20 puan)

Eğer $7n + 3 = x^2$ olacak şekilde bir x tamsayısı bulunabilseydi, bu durumda

$$x^2 \equiv 3 \quad (7)$$

kongrüansının bir çözümü de var olurdu. Halbuki 3, $Q_7 = \{1, 2, 4\}$ ün bir elemanı değildir. Yani 3, 7 modunda bir ikinci dereceden kalan değildir.

Soru 3) Her m>1 sayısı için m!+2 ile m!+m sayıları arasında kaç tane asal sayı bulunduğunu belirleyiniz. (20 puan)

m!+2 sayısı 2 ile, m!+3 sayısı 3 ile ve bu düşünce ile m!+m sayısı da m ile bölünebileceğinden bu aralıkta hiçbir asal sayı yoktur.

Soru 4) p ve q, 4 modunda bire denk olan iki farklı asal sayı olsun. $x^2 \equiv p$ (q) kongrüansının çözümünün olması için gerek ve yeter şartın $x^2 \equiv q$ (p) kongrüansının çözümünün olması olduğunu gösteriniz. (20 puan)

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.

Soru 5) a ile b sıfırdan farklı iki tamsayı ise

$$ax \equiv a \ (ab)$$
$$bx \equiv b \ (ab)$$

kongrüans sistemini çözünüz. (20 puan)

Birinci kongrüansı a, ikinciyi b ile bölersek

$$x \equiv 1 \ (b) \ \text{ ve } \ x \equiv 1 \ (a)$$

kongrüanslarını elde ederiz. Birinciden t bir tamsayı olmak üzere $x = 1 + bt$ yazılıp ikincide yerine konulursa $1 + bt \equiv 1$ (a) kongrüansı elde edilir. Denk olarak $bt \equiv 0$ (a) yazabiliriz. Bu da b ile bölündüğünde $t \equiv 0 \left(\frac{a}{(a,b)}\right)$ veya denk olarak $t = \left(\frac{a}{(a,b)}\right)k$, $k \in Z$ halini alır ki bu değer yukarıda yerine yazılınca $x = 1 + \frac{ab}{(a,b)}k$ veya $x = 1 + [a,b]k$ elde edilir. Yani aranan ortak çözüm, $x \equiv 1$ ([a,b]) şeklindedir.

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