MAT 3013 SOYUT CEBİR VE SAYILAR TEORİSİ I FİNAL SORULARI

Ad-Soyad:.....CEVAP ANAHTARI..... **11.01.2005**

No :.....

Soru 1) $n \in Z$ için 2^n-1 sayısı asal ise n'nin asal olması gerektiğini ispatlayınız.

Tersine n sayısının asal olmadığını kabul edelim. O halde $1< a,b < n$ olmak üzere $n = ab$ şeklinde yazılabilir. Bu takdirde

$$2^n - 1 = 2^{ab} - 1$$
$$= (2^a)^b - 1$$
$$= (2^a-1)((2^a)^{b-1}+(2^a)^{b-2} + \dots + 2^a+1)$$

yazılabileceğinden 2^n-1 farkının asal olmayacağı sonucu elde edilir. Bu ise bir çelişkidir. O halde n asal olmalıdır.

Soru 2) $n \in \mathbf{N}$ olmak üzere hiçbir tamsayının karesinin $7n+6$ şeklinde olamayacağını gösteriniz. (20 puan)

Eğer $7n+6=x^2$ olacak şekilde bir x tamsayısı bulunabilseydi, bu durumda $x^2 \equiv 6$ (7) kongrüansının bir çözümü de var olurdu. Halbuki 6, $Q_7 = \{1,2,4\}$ ün bir elemanı değildir. Yani 6, 7 modunda bir ikinci dereceden kalan değildir.

Soru 3) $ax \equiv 20$ (24) kongrüansının çözümü olmayacak şekildeki tüm a tamsayılarını belirleyiniz.

Bu kongrüansın çözümünün olması için gerek ve yeter şart $(a,24)|20$ olması gerektiği olduğundan çözüm olmaması için a sayısını (a,24), 20 yi bölmeyecek şekilde seçmemiz gerekir. Yani (a,24) = 3, 6, 8, 12 veya 24 olursa bu kongrüansın çözümü olmayacaktır.

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) $p \geq 5$ olsun. p'nin asal olması için gerek ve yeter şartın $6(p-4)! \equiv 1$ (p) olduğunu gösteriniz.

Wilson teoreminin $(p-1)! \equiv -1$ (p) şeklindeki ifadesinde bu değerler yerine konulduğunda

$$(p-1)! = (p-1)\cdot(p-2)\cdot(p-3)\cdot(p-4)!$$
$$\equiv (-1)\cdot(-2)\cdot(-3)\cdot(p-4)! \equiv -1 \ (p)$$

ve buradan $6(p-4)! \equiv 1$ (p) elde edilir.

Not: *Süre 70 dakikadır. Başarılar.* ***İNC***