

# MAT 3003 SOYUT CEBİR VE SAYILAR TEORİSİ I FİNAL SORULARI

Ad-Soyad:.....

21.01.2003

No :.....

**Soru 1)** 5 modunda 1 kalanını veren her asal sayının (11, 31, 41, vs. gibi) aslında  $k$  bir tamsayı olmak üzere  $10k+1$  şeklinde olması gerektiğini açıklayınız. (20 puan)

$p = 5n+1$  olsun.  $n$  tek ise  $p$  çift olacağından  $n$  çift olmalıdır.  $n = 2k$ ,  $k \in \mathbb{Z}$  denirse  $p = 5 \cdot 2k+1 = 10k+1$  olur.

**Soru 2)**  $n \in \mathbb{N}$  olmak üzere hiçbir tamsayının karesinin  $7n+5$  şeklinde olamayacağını gösteriniz. (20 puan)

Eğer  $7n + 5 = x^2$  olacak şekilde bir  $x$  tamsayısı bulunabilseydi, bu durumda

$$x^2 \equiv 5 \pmod{7}$$

kongrüansının bir çözümü de var olurdu. Halbuki  $5, Q_7 = \{1, 2, 4\}$  ün bir elemanı değildir. Yani  $5, 7$  modunda bir ikinci dereceden kalan değildir.

**Soru 3)**  $\varphi(mn) = \varphi(n)$  olacak şekildeki tüm  $m, n$  tamsayı çiftlerini belirleyiniz. (20 puan)

$(m,n) = 1$  ise  $\varphi(mn) = \varphi(m)\varphi(n) = \varphi(n)$  olması  $\varphi(m) = 1$  iken mümkündür. Bu da  $m = 1$  veya  $2$  iken söz konusudur. Yani verilen eşitlik  $n$  herhangi bir doğal sayı olmak üzere  $(1,n)$  ve  $(2,2n+1)$  ikilileri için sağlanır.

$(m,n) > 1$  ise  $\varphi(mn) = d \cdot \frac{\varphi(m)\varphi(n)}{\varphi(d)} = \varphi(n)$  olması

$\frac{\varphi(d)}{\varphi(m)} = d > 1$  olmasıyla mümkündür.  $d, m$  den büyük

olmadığından  $\varphi(d), \varphi(m)$  den büyük olamaz ve bu durum mümkün değildir. Yani aranan ikililer yukarıdaki iki çeşitten ibarettir.

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

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

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

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

**Soru 5)**  $x \equiv a \pmod{m}$  ve  $x \equiv a \pmod{n}$  kongrüans sisteminin çözümünü belirleyiniz. Çözüm hangi moddadır? (20 puan)

$x \equiv a \pmod{m}$  ise bir  $k$  tamsayısı için  $x = a + mk$  yazabiliriz. Bunu ikinci kongrüansta yerine koyarsak  $a + mk \equiv a \pmod{n}$  veya denk olarak  $mk \equiv 0 \pmod{n}$  elde ederiz. Buradan

$k \equiv 0 \pmod{\frac{n}{(m,n)}}$  elde edilir. Yani bir  $t$  tamsayısı için

$k = \frac{nt}{(m,n)}$  şeklindedir. Bu değeri  $x = a + mk$  eşitliğinde

yerine koyarsak  $x = a + \frac{mnt}{(m,n)}$  elde ederiz.

$\frac{mn}{(m,n)} = [m,n]$  olduğu hatırlanırsa son olarak

$x = a + [m,n]t$  ya da denk olarak  $x \equiv a \pmod{[m,n]}$  elde ederiz. Yani verilen sistemin çözümü  $[m,n]$  modunda  $a$  sayısının denklik sınıfındaki tüm tamsayılardır.

**Not:** Süre 60 dakikadır. Başarılar. İNC

--	--