Kare Kalan Üzerine (*L. Gökçe*)

Sayılar teorisinde bazı zor problemlerin çözümünde *kare kalan* (*quadratic residue*) kavramını kullanmak çözümü oldukça kolaylaştırabilmektedir. Bu kavramı problemlerde uygulayabilmek için kare kalanın tanımını ve Legendre sembolünün kullanımı ile ilgili bazı özellikleri bilmemiz gerekecek.

Kare Kalan: $n>2$ bir tamsayı sayı olmak üzere $x^2 \equiv a \pmod{n}$ denkliğinin çözümü varsa a tamsayısına mod n de bir kare kalandır denir. Örneğin $x^2 \equiv 2 \pmod{7}$ denkliğinin çözümü olduğundan 2 sayısı mod 7 de kare kalandır. Fakat $x^2 \equiv 2 \pmod{4}$ denkliğinin çözümü olmadığından 2 sayısı mod 4 te kare kalan değildir.

Legendre Sembolü: $p>2$ bir asal sayı ve $(a,p)=1$ olsun. $\left(\frac{a}{p}\right)$ gösterimine Legendre sembolü denir ve $x^2 \equiv a \pmod{p}$ denkliğinin bir çözümü varsa $\left(\frac{a}{p}\right)=1$, ve $x^2 \equiv a \pmod{p}$ denkliğinin bir çözümü yoksa $\left(\frac{a}{p}\right)=-1$ olarak tanımlanır.

Örneğin $x^2 \equiv 2 \pmod{7}$ denkliğinin bir çözümü $x \equiv 3 \pmod{7}$ olduğundan $\left(\frac{2}{7}\right)=1$ dir. Bununla beraber, $x^2 \equiv 2 \pmod{4}$ denkliğinin çözümü olmadığından $\left(\frac{2}{4}\right)=-1$ dir.

Legendre Sembolünün Özellikleri: a, b tamsayılarının her biri p asal sayısı ile aralarında asal ise aşağıdaki eşitlikler geçerlidir.

1) $\left(\frac{-1}{p}\right)=\begin{cases} 1 & p=4k+1 \text{ ise} \\ -1 & p=4k+3 \text{ ise} \end{cases}$ olur.

2) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ dir.

3) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ dir

4) $a\equiv b(\text{mod } p)$ ise $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ dir.

5) p, q farklı asal sayılar ise $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ dir. (*Quadratic Reciprocity Teoremi*)

Problem 1: $y^2=x^3+23$ denkleminin tamsayılarda çözümünün olmadığını gösteriniz.

Çözüm: Önce x bir çift sayı iken mod 4 te denklemi inceleyelim. $y^2\equiv 23\equiv 3(\text{mod } 4)$ olduğundan çelişki elde edilir. Dolayısıyla x in tek sayı olması durumuna bakabiliriz. $x=4k-1$ veya $x=4k+1$ şeklinde olabilir Burada $k\in\mathbb{Z}$ dir.

Eğer $x=4k-1$ ise mod 4 te $y^2=x^3+23\equiv -1+23\equiv 2(\text{mod } 4)$ çelişkisi elde edilir. Son olarak $x=4k+1$ durumuna bakalım. Çözümün bu aşaması biraz teferruatlıdır.

$y^2+4=x^3+27=(x+3)(x^2-3x+9)$ yazalım. $x=4k+1$ iken $x^2-3x+9\equiv 3(\text{mod } 4)$ olur. Bu aşamada ispatı kolay bir iddiada bulunacağız:

İddia: $a\equiv 3(\text{mod } 4)$ ise a sayısının asal çarpanlarından en az biri $p=4t+3$ formatındadır. Burada $t\in\mathbb{Z}$ dir.

İspat: Aksini kabul edelim ve asal çarpanlara ayrılışı $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ şeklinde olan a sayısının tüm asal çarpanları $4t+1$ formatında olsun. Bu durumda $p_i\equiv 1(\text{mod } 4)$ olup $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_n^{\alpha_n}\equiv 1\cdot 1\cdots 1\equiv 1(\text{mod } 4)$ bulunur. Bu ise $a\equiv 3(\text{mod } 4)$ olması ile çelişir. O halde $a\equiv 3(\text{mod } 4)$ iken a sayısının asal çarpanlarından en az biri $p=4t+3$ formatındadır.

Şimdi bu iddiayı kullanarak $x^2-3x+9\equiv 3(\text{mod } 4)$ şeklindeki x^2-3x+9 sayısının bir asal çarpanının $p=4t+3$ olduğunu söyleyebiliriz. $y^2+4=(x+3)(x^2-3x+9)$ ifadesini mod p de incelersek $y^2+4\equiv 0(\text{mod } p)$ olup $y^2\equiv -4(\text{mod } p)$ elde edilir. Bu denkliğin çözümünün varlığını araştırmak için $\left(\frac{-4}{p}\right)$ Legendre sembolünün değerini hesaplamalıyız. Özellik 3 ten dolayı $\left(\frac{-4}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{4}{p}\right)$ dir. $m^2\equiv 4(\text{mod } p)$ şeklindeki bir denkliğin $m\equiv 2(\text{mod } p)$ gibi bir

çözümü olduğundan $\left(\frac{4}{p}\right)=1$ dir. Şimdi de $\left(\frac{-1}{p}\right)$ değerini hesaplayalım. $p=4t+3$ olduğunu hatırlarsak, Özellik 1 den dolayı $\left(\frac{-1}{p}\right)=-1$ dir. Böylece $\left(\frac{-4}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{4}{p}\right)=(-1)\cdot 1=-1$ olup $y^2\equiv -4(\text{mod}\, p)$ denkliğinin çözümünün olmadığı anlaşılır. Sonuç olarak $y^2=x^3+23$ denkleminin tamsayılarda çözümü yoktur.

Problem 2 (*L. Gökçe*)**:** $x^2=2011y+2013$ denkleminin tamsayılarda çözümünün olmadığını gösteriniz.

Çözüm: $p=2011$ asal sayıdır. mod 2011 de denklemi incelersek $x^2\equiv 2(\text{mod}\, 2011)$ olur. O halde bu denkliğin çözümünün varlığını araştırmak için $\left(\frac{2}{2011}\right)$ değerini hesaplamalıyız.

$p=2011=8k+3$ olduğundan Özellik 2 ye göre $\left(\frac{2}{2011}\right)=(-1)^{\frac{p^2-1}{8}}=(-1)^{8k^2+6k+1}=-1$ dir. Demek ki $x^2\equiv 2(\text{mod}\, 2011)$ denkliğinin de çözümü yoktur. Sonuç olarak $x^2=2011y+2013$ denkleminin de çözümü yoktur.