

## KARAKTER TOPLAMLARI

Ahmet Çetintaş

Bilkent Üniversitesi, 06531-ANKARA

$f(x)$  tamsayı katsayılı bir polinom ve  $p$  tek asal sayı olmak üzere;  $\sum_{x=1}^p \left(\frac{f(x)}{p}\right)$  ifadesine karakter toplamı denir ( $\left(\frac{f(x)}{p}\right)$ : Legendre sembolüdür). Bu projede ise günümüz sayılar teorisinin popüler bir konusu olan sınırlı bir kümede tanımlanmış denklemlerin özel bir hali, " $f(x) \equiv y^2 \pmod{p}$ " denkleminin  $p$  modülündeki çözüm sayısı ele alınmıştır. Polinomların karakter toplamları hesaplanarak çözüm yoluna gidilmiştir. Polinom  $ax+b$  şeklinde iken çözüm kolay oluyor, ama derece artınca işler karışıyor. Amacımız polinomun derecesi 1 veya 2 iken genellemeler getirmek, 3 iken ise özel durumlarda çözüm yolları üretmektir. Nitekim sayılar teorisi, konu hakkındaki çalışmalarda polinomun derecesinin 3'ten büyük olduğu durumlara genellemeler getirememiş, sadece sınırlar koyabilmiştir. Sonuç olarak projede üretilen genellemelerin kullanışlı olduğu görülmüş ve uygulamaları yapılmıştır.

## GİRİŞ

" $f$  tamsayı katsayılı bir polinom ve  $p$  tek asal sayı olmak üzere  $f(x) \equiv y^2 \pmod{p}$  denkleminin,  $1 \leq x, y \leq p$  tamsayı çözümlerinin sayısı kaçtır?" sorusuna bir çok kaynakta rastlanılabilir. Polinomun derecesi 3'ten büyük iken günümüz matematiği kesin sonuçlara ulaşamamış, sadece sınırlar koyabilmiştir. Projede de polinomun derecesi 1, 2 ve 3 iken incelenmiş ve karakter toplamları hesaplanarak çözüme yoluna gidilmiştir.

7. Ulusal Matematik Olimpiyatları İkinci Aşama Sınavı'nda konu ile alakalı bir soru çıkmış olup, bu soru projenin esin kaynağını oluşturmuştur.

**AMAÇ:**  $f$ , 1., 2. veya 3. dereceden tamsayı katsayılı bir polinom ve  $p$  bir tek asal sayı olmak üzere  $f(x) \equiv y^2 \pmod{p}$  denkleminin  $0 \leq x, y \leq p-1$  çözüm sayılarını bulmada karakter toplamlarını hesaplayarak genellemeler getirmek ve bu genellemeleri kullanarak konu hakkındaki sorulara kolay çözümler üretmektir.

## KULLANILAN TEOREM VE SEMBOLLER

(1\*) **Euler Kriteri:**  $p$  bir asal sayı,  $d = (n, p-1)$  ve  $a \equiv 0 \pmod{p}$  olsun.  $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$  ancak ve ancak  $x^n \equiv a \pmod{p}$  denkleminin çözümü vardır. Eğer çözülebiliyorsa,  $d$  tane farklı çözümü vardır.

(2\*)  $a \equiv 0 \pmod{p}$  iken  $a \equiv x^2 \pmod{p}$  denkleminin çözümü varsa,  $a$ 'ya  $p$  modülünde kuadratik rezidü, çözüm yoksa kuadratik nonrezidü denir.

(3\*) **Legendre Sembolü:**  $p > 2$  asal sayıları için  $\left(\frac{a}{p}\right)$  ifadesine Legendre sembolü denir:

$$\left(\frac{a}{p}\right) = \begin{cases} 1; & a, p \text{ modülünde kuadratik rezidü ise,} \\ -1; & a, p \text{ modülünde kuadratik nonrezidü ise,} \\ 0; & a \equiv 0 \pmod{p} \text{ ise.} \end{cases}$$

(4\*)  $x^2 \equiv a \pmod{p}$  ifadesinin çözüm sayısına  $N_p$  dersek,  $N_p = 1 + \left(\frac{a}{p}\right)$  olduğu görülür.

(5\*) Euler kriterinden yola çıkarak  $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$  diyebiliriz.

**İspat:**

$$a \equiv 0 \pmod{p} \Rightarrow a^{\frac{p-1}{2}} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

$$a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Buna göre  $a^{\frac{p-1}{2}}$  ifadesi ya 1 ya da  $-1$ 'e denktir. Eğer  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  ise,  $x^2 \equiv a \pmod{p}$  denklemi çözülebilir (Euler kriteri). Böylece  $\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$ 'dir. Diğer yandan,  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$  ise,  $x^2 \equiv a \pmod{p}$  denklemi çözülemez (Euler kriteri), bu nedenle  $\left(\frac{a}{p}\right) = -1 \equiv a^{\frac{p-1}{2}}$  olmalıdır.

(6\*) **Teorem (Lagrange):**  $f(x)$  tamsayı katsayılı bir polinom iken  $f(x) \equiv 0 \pmod{p}$  denkleminin çözüm sayısı polinomun derecesini aşmaz.

## YÖNTEM

(A)  $ax + b \equiv y^2 \pmod{p}$  Şeklindeki Denklemlerin Çözüm Sayısı ( $a, b$  tamsayı,  $p$  tek asal sayı)

Konunun en kolay kısmı bu kısımdır. Çözüm sayısına  $M_p$  dersek,

$$M_p = \sum_{x=1}^p \left(1 + \left(\frac{ax+b}{p}\right)\right)$$

olacağı açıktır (bak. 4\*). Böylece

$$M_p = p + \sum_{x=1}^p \left(\frac{ax+b}{p}\right) \quad \left(\sum_{x=1}^p \left(\frac{ax+b}{p}\right) \text{ toplamını hesaplamamız sorunu çözer.}\right)$$

$a \equiv 0 \pmod{p}$  ise,

$$S = \{ax + b : x \text{ tamsayı ve } 1 \leq x \leq p\}$$

kümesini tanımlayalım ve bu kümenin  $p$  modunda tam kalanlar sistemi olduğunu ispatlayalım.  $ax + b \equiv ay + b \pmod{p} \Rightarrow x \equiv y \pmod{p}$  olacağı açıktır. Buna göre  $S$  kümesinin  $p$  tane elemanı  $p$  modülünde  $p$  farklı değer alacaktır. Böylece  $S$ ,  $p$  modülünde bir tam kalanlar sistemi olacaktır.

$$\sum_{x=1}^p \left(\frac{ax+b}{p}\right) = \sum_{z=1}^p \left(\frac{z}{p}\right).$$

**Lemma 1:**  $p$  modülünde  $n$ . dereceden rezidülerin sayısı  $\frac{p-1}{(p-1, n)}$ 'dir.

**İspat:** Euler kriterine göre (bak. 1\*),  $a \equiv 0 \pmod{p} \Rightarrow x^n \equiv a \pmod{p}$  denkleminin çözüm sayısı  $(p-1, n) = d$ 'dir. Buna göre çözüm tam olarak  $\frac{p-1}{d}$  tane  $a$  için olabilir. Böylece  $n$ . dereceden rezidülerin sayısı  $\frac{p-1}{d}$  olur. Böylece lemanın ispatı bitmiş olur.

$n = 2$  için  $(2, p-1) = 2$  olduğundan,  $p$  modülünde 2. dereceden, yani kuadratik rezidülerin sayısı  $\frac{p-1}{2}$  tanedir. Böylece kuadratik nonrezidülerin sayısı da  $\frac{p-1}{2}$  tane olacaktır.

$$\sum_{z=1}^p \left(\frac{z}{p}\right) = \left(\frac{p}{p}\right) + \sum_{z=1}^{p-1} \left(\frac{z}{p}\right) = 0 + 1 \cdot \frac{p-1}{2} + (-1) \cdot \frac{p-1}{2} = 0.$$

Karakter toplamının değeri 0 olarak bulundu.  $M_p = p + \sum_{x=1}^p \left(\frac{ax+b}{p}\right) = p$  olacaktır.

Çıkmış bir soru üzerinde yöntemin uygulamasını yapalım.

**SORU:** (16. Balkan Matematik Olimpiyadı, Makedonya, 1999)  $p > 2$  bir asal sayı ve  $p \equiv 2 \pmod{3}$  olmak üzere,

$$S = \{y^2 - x^3 - 1 : x, y \text{ tamsayı, } 0 \leq x, y \leq p-1\}$$

kümesi tanımlansın.  $S$  kümesinin  $p$  ile bölünebilen elemanları sayısının en fazla  $p-1$  olacağını gösteriniz.

**ÇÖZÜM:**  $T = \{x^3 : x \text{ tamsayı, } 0 \leq x \leq p-1\}$  olsun.  $T$  kümesinin  $p$  modülünde tam kalan sistemi olduğunu gösterelim. Lemma 1'den,  $p = 3m+2$  iken 3. dereceden rezidülerin sayısı  $\frac{p-1}{(3,3m+1)} = p-1$  olacaktır. Buna göre  $T$  kümesi  $p$  modülünde  $p$  farklı değer alacaktır. Böylece  $T$ ,  $p$  modülünde bir tam kalan sistemi olur.

$p \mid y^2 - x^3 - 1 \Rightarrow y^2 \equiv x^3 + 1 \pmod{p}$ ,  $x^3 \equiv z \pmod{p}$  yazalım.  $y^2 \equiv z + 1 \pmod{p}$  denkleminin tam olarak  $p$  tane ( $0 \leq y, z \leq p-1$ ) tane çözümü olacaktır (A bölümündeki sonuçtan). Buna göre  $S$  kümesinde  $p$  ile bölünebilen elemanların sayısına  $S(p)$  dersek,  $S(p) \leq p$  olacaktır. Ayrıca  $(x, y) = (0, 1)$  ve  $(x, y) = (2, 3)$  olduğu durumlarda  $y^2 - x^3 - 1 = 0$  oluyor. Bu iki durum birbirine denk ve  $p \mid y^2 - x^3 - 1$  olduğu durumlar olduğu için  $S(p) \leq p-1$  olmak zorundadır.

**(B)  $ax^2 + bx + c \equiv y^2 \pmod{p}$  Şeklindeki Denklemlerin Çözüm Sayısı**

$a, b, c \in \mathbf{Z}$ ,  $p$  tek asal sayı,  $a \not\equiv 0 \pmod{p}$  iken  $ax^2 + bx + c \equiv y^2 \pmod{p}$  denkleminin çözüm sayısına  $Q_p$  diyelim:

$$Q_p = \sum_{x=1}^p \left[ \left( \frac{ax^2 + bx + c}{p} \right) + 1 \right] = p + \sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right)$$

olacaktır. Burada da  $\sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right)$  karakter toplamını hesaplamamız soruyu çözecektir. Öncelikle şuna dikkat edelim:

$$ax^2 + bx + c = a \left[ \left( x + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right].$$

Şimdi iki durumu ayrı ayrı inceleyelim: (i)  $p \mid b^2 - 4ac$ , (ii)  $p \nmid b^2 - 4ac$ :

(i)  $p \mid b^2 - 4ac$  olsun.

$$ax^2 + bx + c = a \left[ \left( x + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right] \equiv a \left( x + \frac{b}{2a} \right)^2 \pmod{p}.$$

**Lemma 2:**  $\left( \frac{a \cdot b}{p} \right) = \left( \frac{a}{p} \right) \cdot \left( \frac{b}{p} \right)$ .

**İspat:**  $\left( \frac{a \cdot b}{p} \right) \equiv (a \cdot b)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}} \cdot (b)^{\frac{p-1}{2}} \equiv \left( \frac{a}{p} \right) \cdot \left( \frac{b}{p} \right) \pmod{p}$ . Böylece lemmanın ispatı tamamlanmış olur.

$$\begin{aligned} \sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right) &= \sum_{x=1}^p \left( \frac{a \cdot \left( x + \frac{b}{2a} \right)^2}{p} \right) = \sum_{x=1}^p \left( \frac{a}{p} \right) \cdot \left( \frac{\left( x + \frac{b}{2a} \right)^2}{p} \right) \quad [\text{Lemma 2 'den}] \\ &= \left( \frac{a}{p} \right) \cdot \sum_{x=1}^p \left( \frac{\left( x + \frac{b}{2a} \right)^2}{p} \right). \end{aligned}$$

$$\sum_{x=1}^p \left( \frac{\left( x + \frac{b}{2a} \right)^2}{p} \right) = \sum_{z=1}^p \left( \frac{z^2}{p} \right) \text{ olacağı açıktır. } \sum_{z=1}^p \left( \frac{z^2}{p} \right) = (p-1) \cdot 1 + 0 = p-1 \text{ olup}$$

$$\sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right) = \left( \frac{a}{p} \right) \cdot (p-1)$$

olarak sonuca varılır.

(ii)  $p \nmid b^2 - 4ac$  olsun.  $d_1 = \frac{b}{2a}$ ,  $d = -\frac{b^2 - 4ac}{4a^2}$  olmak üzere,

$$ax^2 + bx + c = a \left[ \left( x + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right] = a((x + d_1)^2 + d)$$

bulunur ve

$$\sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right) = \sum_{x=1}^p \left( \frac{a((x + d_1)^2 + d)}{p} \right) = \sum_{z=1}^p \left( \frac{a(z^2 + d)}{p} \right) = \left( \frac{a}{p} \right) \cdot \sum_{z=1}^p \left( \frac{z^2 + d}{p} \right)$$

çıkar.

**Lemma 3:**  $1 \leq k \leq p-2 \Rightarrow \sum_{n=1}^{p-1} n^k \equiv 0 \pmod{p}$ .

**İspat:**  $u, p$  modülünde ilkel kök olmak üzere  $k \neq 0$  ve  $k \neq p-1$  ise,

$$\sum_{n=1}^{p-1} n^k = \sum_{s=1}^{p-1} (u^s)^k = \sum_{s=1}^{p-1} (u^k)^s = \frac{u^{k \cdot (p-1)} - 1}{u^k - 1} \cdot u \equiv 0 \pmod{p}$$

bulunur.

$$\sum_{z=1}^p \left( \frac{z^2 + d}{p} \right) \equiv \sum_{z=1}^p (z^2 + d)^{\frac{(p-1)}{2}} \pmod{p}.$$

$(z^2 + d)^{\frac{(p-1)}{2}}$  ifadesi binom açılımı ile yazıldığında terimlerin kuvvetlerine bakarsak,  $z^{p-1}$  teriminden başka, kuvveti  $p-1$ 'den büyük ya da eşit olan hiç bir terim yoktur. Ayrıca bu ifadelerin  $z = 1, 2, \dots, p$  için ayrı ayrı binom açılımlarını yazıp toplayalım, aynı binom katsayısına sahip olanları paranteze aldığımızda bu katsayıya  $\sum_{z=1}^p z^k$  ( $1 \leq k \leq p-2$ ) şeklinde bir çarpan gelecektir ki Lemma 3 'deki ispatımızdan, bu ifadelerin hepsi  $p$  ile bölünür. Dolayısıyla

$$\sum_{z=1}^p (z^2 + d)^{\frac{(p-1)}{2}} \equiv \sum_{z=1}^p z^{p-1} + 0 \equiv p-1 \pmod{p}.$$

Böylece  $\sum_{z=1}^p \left( \frac{z^2 + d}{p} \right) \equiv p-1 \pmod{p}$  olduğunu bulduk.  $-p \leq \sum_{z=1}^p \left( \frac{z^2 + d}{p} \right) \leq p$  olacağı açıktır (Legendre sembolü). Bu aralıkta alınabilecek değerler  $-1$  ve  $p-1$ 'dir.  $\sum_{z=1}^p \left( \frac{z^2 + d}{p} \right) = p-1$  olması için gerek ve yeter koşul  $\left( \frac{z^2 + d}{p} \right)$  ifadelerinden yalnız bir tanesinin  $0$ 'a eşit olması ve geri kalan  $p-1$  tanenin ise  $1$ 'e eşit olmasıdır.  $z^2 + d \equiv 0 \pmod{p} \Rightarrow (p-z)^2 + d \equiv 0 \pmod{p}$  olmak zorundadır. ( $d \not\equiv 0 \pmod{p}$  olduğu için  $z \not\equiv 0 \pmod{p}$  olur.) Buna göre  $\left( \frac{z^2 + d}{p} \right)$  ifadelerinden ya hiç biri  $0$ 'a eşit değildir ya da en az 2 tanesi  $0$ 'a eşit olacaktır. Böylece çelişki elde etmiş olduk.

Dolayısıyla

$$\sum_{z=1}^p \left( \frac{z^2 + d}{p} \right) = -1,$$

$$\sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right) = \left( \frac{a}{p} \right) \cdot \sum_{z=1}^p \left( \frac{z^2 + d}{p} \right) = -\left( \frac{a}{p} \right),$$

$$Q_p = p + \sum_{x=1}^p \left( \frac{ax^2 + bx + c}{p} \right) = p - \left( \frac{a}{p} \right).$$

Sonuç olarak,

$$Q_p = \begin{cases} p + \left(\frac{a}{p}\right)(p-1); & p \mid b^2 - 4ac \text{ ise} \\ p - \left(\frac{a}{p}\right); & p \nmid b^2 - 4ac \text{ ise} \end{cases}$$

çıkar. Böylece genel bir ifade bulmuş olduk. Şimdi bu yöntemi uygulamalarda kullanalım:

**SORU:** (1991 IMO 'ya Polonya tarafından önerilmiştir)  $a, b, c \in \mathbb{Z}$  ve  $p$  tek asal sayı olmak üzere, eğer  $f(x) = ax^2 + bx + c$ ,  $2p - 1$  tane ardışık  $x$  tamsayı değerinde tamkare oluyorsa,  $p \mid b^2 - 4ac$  olduğunu gösteriniz.

Soruyu  $p > 3$  için çözeceğiz. Çözümü görünce gerçekten çok kolay bir soruymuş diyebilirsiniz. Ama bu yöntemi kullanılmadan verilen çözüm uzun ve akla gelmesi zor bir çözümdür.

**ÇÖZÜM:**  $f(x)$  polinomunu  $p$  modülünde inceleyelim.  $f(x)$ ,  $x$ 'in  $2p - 1$  ardışık tamsayı değerinde tamkare oluyormuş. Bu  $x$ 'lerden öyle  $p$  tanesini alalım ki bunlar ardışık  $p$  tane tamsayı olsun. Bu durumda  $f(x) \equiv y^2 \pmod{p}$  denkleminin çözüm sayısı en az  $p$  olacaktır, çünkü  $p$  tane ardışık  $x$  değeri  $p$  modülünde bir tam kalan sistemi oluşturacaktır. Böylece  $x$ 'in her bir değeri için en az bir tane çözüm çıktığından en az  $p$  tane çözüme ulaşılacaktır.

Lagrange Teoremine göre (bak. 6\*),  $f(x) \equiv 0 \pmod{p}$ 'nin çözüm sayısı en fazla polinomun derecesi kadardır. Buna göre  $ax^2 + bx + c \equiv 0 \pmod{p}$  denkleminin en fazla 2 çözümü vardır.

$f(x) \equiv y^2 \pmod{p}$  ifadesinde her  $x \in \{1, 2, \dots, p\}$  için en az bir tane  $y$  değeri bulabiliyorduk.  $y \not\equiv 0 \pmod{p}$  olursa en az iki çözüm bulabiliriz:  $(x, y)$  ve  $(x, -y)$ . Buna göre  $f(x) \equiv y^2 \pmod{p}$  ifadesinin en az  $2p - 2$  tane çözümü vardır. Şimdi bulduğumuz yöntemi burada kullanalım.  $f(x) \equiv y^2 \pmod{p}$  denkleminin çözüm sayısı  $Q_p$  ise,

$$Q_p = \begin{cases} p + \left(\frac{a}{p}\right)(p-1); & p \mid b^2 - 4ac \text{ ise} \\ p - \left(\frac{a}{p}\right); & p \nmid b^2 - 4ac \text{ ise} \end{cases} \quad (**)$$

bulunur. Bizim polinomumuzun en az  $2p - 2$  tane çözümü vardı.  $p > 3$  olduğu için  $2p - 2 > p + 1 \geq p - \left(\frac{a}{p}\right)$  dolayısıyla,  $p \nmid b^2 - 4ac$  olamaz. O halde  $p \mid b^2 - 4ac$  olmalıdır.

**SORU:** (7. Ulusal Matematik Olimpiyadı Birinci Soru)  $0 \leq x, y, z, w < 37$  olmak üzere  $x^2 + y^2 \equiv z^3 + w^3 \pmod{37}$  denklemini sağlayan  $(x, y, z, w)$  sıralı tamsayı dörtlülerinin sayısını bulunuz.

**ÇÖZÜM:** Görüldüğü gibi  $p = 37$  bir asal sayıdır.  $t = 0, 1, 2, \dots, p - 1$  olmak üzere  $x^2 + y^2 \equiv t \pmod{p}$  denkleminin çözüm sayısına  $a_t$ ,  $z^3 + w^3 \equiv t \pmod{p}$  denkleminin çözüm sayısına da  $b_t$  diyelim. Sonucun  $\sum_{k=0}^{p-1} (a_k \cdot b_k)$  olacağı açıktır.

$a_0$ 'ı hesaplayalım.  $x^2 + y^2 \equiv 0 \pmod{p} \Rightarrow y^2 \equiv -x^2 \pmod{p}$ . (\*\*) eşitliğini hatırlarsak,  $a_0 = \left(\frac{-1}{p}\right) \cdot (p-1) + p$  olduğu görülür.  $p = 37 \equiv 1 \pmod{4} \Rightarrow \left(\frac{-1}{37}\right) = 1$ , böylece  $a_0 = p - 1 + p = 2p - 1 = 2 \cdot 37 - 1 = 73$ .

Şimdi  $t = 1, 2, \dots, p - 1$  için  $a_t$ 'yi hesaplayalım:  $x^2 + y^2 \equiv t \pmod{p} \Rightarrow y^2 \equiv t - x^2 \pmod{p}$ . Yine (\*\*\*) eşitliğini hatırlarsak, her  $t \in \{1, 2, \dots, p - 2\}$  için  $a_t = p - \left(\frac{-1}{p}\right) = 37 - 1 = 36$ 'dır.

$b_0$ 'ı hesaplayalım:  $x^3 + y^3 \equiv 0 \pmod{p}$  olup  $x \equiv 0 \Leftrightarrow y \equiv 0$  olacaktır. Bu bir çözümdür.

$x \not\equiv 0$  ve  $y \not\equiv 0$  iken  $x = y \cdot s$  olacak şekilde  $s \in \{1, 2, \dots, p - 1\}$  alalım. Bu durumda  $x^3 + y^3 = x^3 + s^3 x^3 \equiv x^3 \cdot (s^3 + 1) \equiv 0 \pmod{p} \Rightarrow s^3 + 1 \equiv 0 \pmod{p}$ ,  $s^3 \equiv -1 \pmod{p}$  olmalıdır. Bu şartı sağlayan  $s$ 'lerin sayısının 3 olduğunu Lagrange Teoreminden söyleyebiliriz. Buna göre her  $x \in \{1, 2, \dots, p - 1\}$  için 3 tane  $y$  değeri bulabiliyoruz, öyle ki  $x^3 + y^3 \equiv 0 \pmod{p}$ 'dir. Buna göre  $p - 1$  tane  $x$  için  $3(p - 1)$  tane çözüm ikilisi buluyoruz. Bir de  $(x, y) = (0, 0)$  çözümü vardı. Böylece  $b_0 = 3p - 2 = 3 \cdot 37 - 2 = 109$  bulunur.

$\sum_{n=1}^{p-1} b_n = p^2$  'dir. Herhangi bir  $(x, y)$  ikilisi bu toplamda tam olarak bir defa sayılacak ve böylece toplam,  $(x, y)$  ikililerinin sayısına eşit olacaktır.  $(x, y)$  ikililerinin sayısının  $p^2$  tane olduğu açıktır.

Şimdi başa dönelim ve  $\sum_{k=0}^{p-1} a_k \cdot b_k$  toplamını hesaplayalım:

$$\begin{aligned} \sum_{k=0}^{p-1} a_k \cdot b_k &= a_0 \cdot b_0 + \sum_{k=1}^{p-1} a_k \cdot b_k = a_0 \cdot b_0 + (p-1) \cdot \sum_{k=1}^{p-1} b_k \\ &= 73 \cdot 109 + 36 \cdot (\sum_{k=1}^p b_k - b_0) \\ &= 73 \cdot 109 + 36 \cdot (p^2 - 3p + 2) = 73 \cdot 109 + 36 \cdot 35 \cdot 36 = 53317 . \end{aligned}$$

Şimdi de sözkonusu yöntemi daha zor bir soruda kullanacağız:

**SORU:**  $p > 3$  asal sayı ve  $a \equiv 0 \pmod{p}$ . İspatlayınız ki,  $x^3 + ax \equiv y \pmod{p}$  denkliği  $y$  'nin  $p - \frac{1}{3}(p - (\frac{-3}{p}))$  değeri için çözülebilir ( $y = 0, 1, \dots, p-1$ ).

**ÇÖZÜM:**  $x^3 + ax \equiv t \pmod{p}$  ifadesinin çözüm sayısının en fazla 3 olacağını Lagrange Teoreminden (bak. 6\*) söyleyebiliriz.  $x^3 + ax \equiv y^3 + ay \pmod{p}$  denkleğinin çözüm sayısına bakalım:  $x^3 - y^3 + a(x - y) = (x - y)(x^2 + xy + y^2 + a) \equiv 0 \pmod{p}$ .  $x^2 + xy + y^2 + a \equiv 0 \pmod{p}$  denkleğinin çözüm sayısını hesaplayalım. Eğer bu denklekte de  $x = y$  çözümleri geliyorsa onları da sayacağız. Bu ikililerin sayısı  $T_p$  olsun. Sabit bir  $x$  değeri için  $x = c$  diyelim:

$$\begin{aligned} c^2 + cy + y^2 + a &= (c + \frac{y}{2})^2 + \frac{3y^2}{4} + a \equiv 0 \pmod{p} , \\ (c + \frac{y}{2})^2 &\equiv \frac{-3y^2}{4} - a \pmod{p} . \end{aligned}$$

Buna göre bu şekildeki  $(c, y)$  ikililerinin sayısı  $1 + (\frac{-(\frac{3y^2}{4} + a)}{p})$  'dir. Böylece bütün ikililerin sayısı da

$$\begin{aligned} \sum_{y=0}^{p-1} [1 + (\frac{-(\frac{3y^2}{4} + a)}{p})] &= p + \sum_{y=0}^{p-1} (\frac{-(\frac{3y^2}{4} + a)}{p}) \\ \sum_{y=0}^{p-1} (\frac{-(\frac{3y^2 + 4a}{4})}{p}) &= \sum_{y=0}^{p-1} (\frac{1}{p}) (\frac{-(3y^2 + 4a)}{p}) \\ &= \sum_{y=0}^{p-1} (\frac{-(3y^2 + 4a)}{p}) \end{aligned}$$

olarak bulunur. Yöntemimizi kullanarak bu toplamın değerini bulabiliriz:

$$\sum_{y=0}^{p-1} (\frac{-(3y^2 + 4a)}{p}) = -(\frac{-3}{p}) . \quad (\text{Çünkü } p \mid 48 \cdot a.)$$

Buna göre  $x^2 + xy + y^2 + a \equiv 0 \pmod{p}$  denkleğinin  $(x, y)$  sıralı ikili çözüm sayısı  $p - (\frac{-3}{p})$  imiş.

Diyelim ki,  $x^3 + ax \equiv c \pmod{p}$  ( $c = 0, 1, \dots, p-1$ ) denkleğinin yalnızca bir tane çözümü vardır; bu çözüm  $x_1$  olsun. Biraz evvel saydığımız ikililer içerisinde  $(x_1, x_1)$  ikilisi olabilir mi diye bakalım. Farzedelim ki,  $(x_1, x_1)$  ikilisi geçiyor:  $x_1^2 + x_1 \cdot x_1 + x_1^2 + a \equiv 3x_1^2 + a \equiv 0 \pmod{p} \Rightarrow x_1^2 \equiv \frac{-a}{3} \pmod{p}$ . Böylece  $x_1 \equiv 0 \pmod{p}$  çıkar.  $x_1^2 + x_1 \cdot y + y^2 + a \equiv 0 \pmod{p}$  denkleminin çözümlerine bakalım:

$$(y + \frac{x_1}{2})^2 \equiv \frac{-3x_1^2}{4} - a \equiv \frac{a}{4} - a \equiv \frac{-3}{4}a \equiv \frac{9x_1^2}{4} \pmod{p} .$$

$\frac{9x_1^2}{4}$  ifadesi kuadratik rezidüdür ve 2 farklı  $y$  değeri için denklik sağlanır. Buna göre de  $x_1$  'den farklı olan  $y$  değeri için  $y^3 + ay \equiv c \pmod{p}$  olacaktır ki bu baştaki kabulümüz ile çelişir.

$c \in \{0, 1, \dots, p-1\}$  iken  $x^3 + ax \equiv c \pmod{p}$  denkleğinin 3 farklı çözümü olduđu  $c$  'lere 3 'lü  $c$ , iki farklı çözümü olduđu  $c$  'lere de 2 'li  $c$  diyelim. 3 'lü  $c$  'lerin sayısı  $c_3$ , 2 'li  $c$  'lerin sayısı  $c_2$  olmak üzere,  $x^3 + ax \equiv y \pmod{p}$  denkleğinin çözümünün olmadığı  $y$  'lerin sayısı  $2c_3 + c_2$  olacaktır. Her bir 3 'lü  $c$  için 2 tane, 2 'li  $c$  için ise 1 tane  $y$  çözüme ulaşamıyor.

Şimdi göstermemiz gereken şey  $p - (2c_3 + c_2) = p - \frac{1}{3}(p - (\frac{-3}{p}))$ ,  $2c_3 + c_2 = \frac{1}{3}(p - (\frac{-3}{p}))$  olduğudur.

$T_p$  sayısında verdiğimiz şartı sağlayan ikilileri saydık. 3 'lü bir  $c$  için  $x_1, x_2$  ve  $x_3$  çözümler olsun. Biz  $T_p$  sayısında  $(x_1, x_2), (x_3, x_2), (x_1, x_3), (x_2, x_1), (x_2, x_3), (x_3, x_1)$  ikilerini saydık. Böylece bu 3 'lü  $c$  'nin çözümlerinin oluşturduğu ikilileri 6 sefer saydık. 2 'li bir  $c$  için ise,  $x_1$  ve  $x_2$  çözüm olmak üzere,  $T_p$  sayısında  $(x_1, x_2), (x_2, x_1)$  ikilileri ile  $(x_1, x_1)$  ve  $(x_2, x_2)$  çözüm ikililerinden yalnızca birini saydık. Yalnızca birini saydığımızı ispatlayalım. Farzedelim ki ikisini birden saydık. Buna göre  $3x_1^2 + a \equiv 3x_2^2 + a \equiv 0 \pmod{p} \Rightarrow x_1^2 \equiv x_2^2 \pmod{p}$  olduğundan ancak  $x_1 \equiv -x_2$  olabilir.  $x_1^3 + ax_1 \equiv x_2^3 + ax_2 \equiv c \pmod{p}$  idi.  $x_1^3 + ax_1 \equiv -x_2^3 - ax_2 \equiv c \pmod{p}$  olacaktır ki bu da  $c \equiv 0 \pmod{p}$  demektir. Fakat  $x^3 + ax \equiv 0 \pmod{p}$  ifadesinin ya 1 ya da 3 farklı çözümü olabilir. Çünkü,  $x.(x^2 + a) \equiv 0 \pmod{p}$ .  $x \equiv 0$  bir çözümdür.  $-a$  kuadratik rezidü ise, 2 tane daha farklı çözüm gelecektir.  $-a$  kuadratik rezidü değilse, başka çözüm gelmeyecektir. Böylece 2 'li bir  $c$  'nin  $x_1$  ve  $x_2$  çözümlerinin oluşturduğu 3 tane 2 'liyi sayıyoruz. Buna göre  $T_p = 6.c_3 + 3.c_2$  'dir. Buradan da,  $2c_3 + c_2 = \frac{1}{3}(p - (\frac{-3}{p}))$  bulunur ve ispat tamamlanır.

### (C) $x^3 + \ell \equiv y^2 \pmod{p}$ Şeklindeki Denkliklerin Çözüm Sayısı

(i)  $p \equiv 2 \pmod{3}$  bir asal sayı olmak üzere  $x^3 + \ell \equiv y^2 \pmod{p}$  denkleminin  $(x, y)$  çözümü sayısına  $L_p$  diyelim ( $\ell = 1, 2, \dots, p$ ).  $L_p = p + \sum_{x=1}^p (\frac{x^3 + \ell}{p})$  olacaktır.

$$T(\ell) = \sum_{x=1}^p (\frac{x^3 + \ell}{p})$$

diyelim.  $T(1) = 0$  olduğü Balkan Olimpiyadı sorusunda gösterilmişti. Aynı mantıkla  $T(\ell) = 0$  ( $\ell = 1, 2, \dots, p$ ) diyebiliriz. Buna göre  $x^3 + \ell \equiv y^2 \pmod{p}$  denkleği  $p \equiv 2 \pmod{3}$  iken  $p$  tane çözüme sahiptir.

(ii)  $s \equiv 0 \pmod{p}$  olsun.  $p = 3m + 1 \Rightarrow T(\ell.s^3) = (\frac{s}{p})T(\ell)$  olduğunu ispatlayalım.

$$\begin{aligned} T(\ell.s^3) &= \sum_{x=0}^{p-1} (\frac{x^3 + \ell.s^3}{p}) \quad (x = t.s \text{ dersek}) \\ &= \sum_{t=0}^{p-1} (\frac{t^3.s^3 + \ell.s^3}{p}) = \sum_{t=0}^{p-1} (\frac{s^3}{p}) \cdot (\frac{t^3 + \ell}{p}) \\ &= \sum_{t=0}^{p-1} (\frac{s}{p}) \cdot (\frac{t^3 + \ell}{p}) = (\frac{s}{p}) \cdot \sum_{t=0}^{p-1} (\frac{t^3 + \ell}{p}) = (\frac{s}{p}) \cdot T(\ell). \end{aligned}$$

(iii)  $p = 3m + 1$  ve  $n, p$  modülünde ilkel bir kök olmak üzere  $T(1) + T(n^2) + T(n^4) = 0$  olduğunu ispatlayalım.

$$\begin{aligned} T(1) &= \sum_{x=0}^{p-1} (\frac{x^3 + 1}{p}) = (\frac{1}{p}) + \sum_{s=1}^{p-1} (\frac{n^{3s} + 1}{p}) = 1 + \sum_{s=1}^{p-1} (\frac{n^{3s} + 1}{p}), \\ T(n^2) &= \sum_{x=0}^{p-1} (\frac{x^3 + n^2}{p}) = (\frac{n^2}{p}) + \sum_{s=1}^{p-1} (\frac{n^{3s} + n^2}{p}) = 1 + \sum_{s=1}^{p-1} (\frac{n^{3s-2} + 1}{p}), \\ T(n^4) &= \sum_{x=0}^{p-1} (\frac{x^3 + n^4}{p}) = (\frac{n^4}{p}) + \sum_{s=1}^{p-1} (\frac{n^{3s} + n^4}{p}) = 1 + \sum_{s=1}^{p-1} (\frac{n^{3s-4} + 1}{p}) \end{aligned}$$

ve böylece

$$\begin{aligned} T(1) + T(n^2) + T(n^4) &= 3 + \sum_{s=1}^{p-1} [(\frac{n^{3s} + 1}{p}) + (\frac{n^{3s-2} + 1}{p}) + (\frac{n^{3s-4} + 1}{p})] \\ &= 3 + 3 \cdot \sum_{s=1}^{p-1} (\frac{n^s + 1}{p}) = 3 + 3 \cdot [\sum_{x=1}^{p-1} (\frac{x}{p}) - (\frac{1}{p})] \\ &= 3 + 3 \cdot (-1) = 0. \end{aligned}$$

**(D)  $x^3 + kx \equiv y^2 \pmod{p}$  Şeklindeki Denkliklerin Çözüm Sayısı**

$p = 4m + 3$  şeklinde bir asal sayı ve  $k \not\equiv 0 \pmod{p}$  iken  $x^3 + kx \equiv y^2 \pmod{p}$  denkleğinin çözüm sayısı

$$p + \sum_{x=0}^{p-1} \left( \frac{x^3 + kx}{p} \right)$$

olacaktır.

$$s(k) = \sum_{x=0}^{p-1} \left( \frac{x^3 + kx}{p} \right)$$

olsun.  $s(k) = 0$  olduğunu gösterelim.  $p = 4m + 3$  olduğu için  $\left(\frac{-1}{p}\right) = -1$  'dir. Böylece  $x \not\equiv 0 \pmod{p}$  iken  $\left(\frac{x^3+kx}{p}\right)$  ve  $\left(\frac{-x^3-kx}{p}\right)$  ifadelerinden tam olarak bir tanesi 1, bir tanesi  $-1$  değerini alır. Buna göre

$$\left(\frac{x^3 + kx}{p}\right) + \left(\frac{-x^3 - kx}{p}\right) = 0$$

olacaktır.  $x = 0 \Rightarrow \left(\frac{x^3+kx}{p}\right) = 0$  'dir. O zaman  $s(k) = 0$  olur. Denkleğın çözüm sayısı da  $p$  olarak bulunur.

**TARTIŞMA VE SONUÇ**

$f$ , 1. ve 2. dereceden bir polinom iken genellemeler getirilmez. 3. derecede iken özel durumlara çözümler üretilmiştir. Genellemelerin kullanışlı olduğu görülmüş, konu ile alakalı sorulara kolay çözümler getirmede kullanılabilirliği anlaşılmıştır.

**KAYNAKLAR**

- [1] Serguei A. Stepanev, Arithmetics of Algebraic Curves.
- [2] Alan Baker, A Concise Introduction to the Theory of Numbers.
- [3] I. M. Vinogradow, An Introduction to the Theory of Numbers.
- [4] Charles Vanden Eynden, Number Theory.
- [5] Ulusal ve Uluslararası Matematik Olimpiyatları Soruları.

**TEŞEKKÜRLER**

Bu çalışmanın her aşamasında bana büyük destek veren Matematik Öğretmenim *Oğün Bilge* 'ye, projenin esin kaynağı olan sorunun sahibi Sayın *Okan Tekman* 'a teşekkürü bir borç bilirim. Ayrıca çalışmalarım boyunca benden yardımlarını esirgemeyen başta okul yöneticilerim Sayın *Mahmut Açıl* ve Sayın *Coşkun Özsolak* 'a, tüm öğretmenlerime, sınıf arkadaşlarıma ve okul çalışanlarına minnetlerimi sunarım.