Kummer Toplamı

Metin Can Aydemir

August 21, 2022

Kummer Toplamı

q asalı $3k+1$ formatında olsun. 1'in q. dereceden kökü $\zeta = e^{\frac{2\pi i}{q}}$ olsun. Buna göre

$$\sum_{m=0}^{q-1} \zeta^{m^3}$$

toplamını hesaplayınız.

Çözüm

q asal olduğundan en az bir ilkel kökü vardır, bu köke r diyelim. $v(n)$ ile r'ye göre n'nin q modunda indeksini gösterelim. Yani $(n,q)=1$ ise

$$r^k \equiv n \pmod{q}$$

olan en küçük pozitif tam sayı k'ya $v(n)$ diyelim. $n \in \{1,2,\ldots,q-1\}$ için $v(n)$'lerden 3 ile bölünenlerin kümesi A, $3k+1$ formatındaki sayıların kümesi B, $3k+2$ formatındakilerin kümesi C olsun.

$$\eta_0 = \sum_{i\in A} \zeta^i, \quad \eta_1 = \sum_{j\in B} \zeta^j, \quad \eta_2 = \sum_{k\in C} \zeta^k$$

diyelim. Bu durumda

$$1 + 3\eta_0 = \sum_{m=0}^{q-1} \zeta^{m^3}$$

olduğunu görmek kolaydır. Kısaca $1+3\eta_j = z_j$ diyelim. 1'in küp kökü $\omega = e^{\frac{2\pi i}{3}}$ olsun. $(n,q)=1$ ise $\chi(n) = \omega^{v(n)}$ olarak, $(n,q)\neq 1$ ise $\chi(n)=0$ olarak tanımlarsak

$$z_0 = \sum_{i=0}^{q-1} (1 + \chi(i) + \overline{\chi}(i))\zeta^i$$

olacaktır çünkü $i=0$ ise $1+\chi(i)+\overline{\chi}(i) = 1$, $i\neq 0$ ise

$$1 + \chi(i) + \overline{\chi}(i) = 1 + \omega^{v(i)} + \overline{\omega}^{v(i)} = 1 + \omega^{v(i)} + \omega^{2v(i)}$$

ve eğer $v(i) \equiv 0 \pmod 3$ ise bu sayı 3, değilse 0 olacaktır. Benzer şekilde

$$z_1 = \sum_{j=0}^{q-1} (1 + \omega^2\chi(j) + \omega\overline{\chi}(j))\zeta^j$$

$$z_2 = \sum_{k=0}^{q-1} (1 + \omega\chi(k) + \omega^2\overline{\chi}(k))\zeta^k$$

olacaktır.

$$\sum_{i=0}^{q-1} \zeta^i = 0$$

olduğundan bizim sadece

$$\tau = \sum_{n=0}^{q-1} \chi(n)\zeta^n$$

toplamını hesaplamamız yeterlidir çünkü bu toplamı bilirsek

$$\overline{\tau} = \sum_{n=0}^{q-1} \overline{\chi}(n)\zeta^{-n} = \sum_{n=0}^{q-1} \overline{\chi}(n)\zeta^{q-n} = \sum_{n=1}^{q} \overline{\chi}(q-n)\zeta^n = \sum_{n=0}^{q-1} \overline{\chi}(q-n)\zeta^n = \sum_{n=0}^{q-1} \overline{\chi}(n)\zeta^n$$

olur ve istenilen tüm toplamlar bulunur.

Not: Yukarıdaki toplamda son kısımda $n \neq 0$ için $\overline{\chi}(q-n) = \overline{\chi}(n)$ olduğunu görmek için χ'in tanımından dolayı $v(q-n) \equiv v(n) \pmod 3$ olduğunu göstermek yeterlidir. Bunun için de

$$r^{v(q-n)} + r^{v(n)} = r^{v(n)}(r^{v(q-n)-v(n)} + 1) \equiv q - n + n \equiv 0 \pmod q$$

$$\implies r^{v(q-n)-v(n)} \equiv -1 \equiv r^{\frac{q-1}{2}} \pmod q \implies v(q-n) - v(n) \equiv \frac{q-1}{2} \pmod{q-1}$$

olur ve $q - 1 \equiv 0 \pmod 3$ olduğundan $v(q-n) \equiv v(n) \pmod 3$ olur. Soruya dönersek

$$\tau\overline{\tau} = |\tau|^2 = \sum_{n_1=1}^{q-1} \sum_{n_2=1}^{q-1} \chi(n_1)\overline{\chi}(n_2)\zeta^{n_1-n_2}$$

olacaktır. $n_2 \equiv nn_1 \pmod q$ dersek

$$|\tau|^2 = \sum_{n_1=1}^{q-1} \sum_{n=1}^{q-1} \chi(n_1)\overline{\chi}(n_1 n)\zeta^{n_1-nn_1} = \sum_{n_1=1}^{q-1} \sum_{n=1}^{q-1} \overline{\chi}(n)\zeta^{n_1-nn_1}$$

olur eğer $n \equiv 1 \pmod q$ ise $\sum_{n_1=1}^{q-1} \zeta^{n_1-nn_1} = q - 1$ olur, değilse -1 olacaktır. Buradan da

$$|\tau|^2 = q\overline{\chi}(1) + \sum_{n=1}^{q-1} \overline{\chi}(n)(-1) = q$$

bulunur. τ'nun uzunluğu $\sqrt{q}$ bulunur ve $\tau = \sqrt{q}e^{i\theta_q}$ olarak yazabiliriz. Buradan z_j'leri hesaplayalım,

$$z_0 = \tau + \overline{\tau} = 2\sqrt{q}\cos\theta_q$$

$$z_1 = \omega^2\tau + \omega\overline{\tau} = 2\sqrt{q}\cos\left(\theta_q - \frac{2\pi}{3}\right)$$

$$z_2 = \omega\tau + \omega^2\overline{\tau} = 2\sqrt{q}\cos\left(\theta_q + \frac{2\pi}{3}\right)$$

θ_q'un gerçekte kaç olduğunu buradan bulamayız ama başka yolla hesaplayıp buraya dönebiliriz. $q \equiv 1 \pmod 3$ olan bir asal için

$$4q = a^2 + 27b^2$$

olacak şekilde tek bir (a, b) negatif olmayan tamsayı çifti olduğunu biliyoruz. Bunun internette farklı birçok ispatı olduğundan bunun ispatını geçiyorum. Şimdi $\cos 3\theta_q$'yı hesaplayalım.

$$\tau^2 = \sum_{x=1}^{q-1} \sum_{y=1}^{q-1} \chi(x)\chi(y)\zeta^{x+y}$$

olur, eğer yukarıda yaptığımız işlemlerin benzerlerini yaparsak $y \equiv xt \pmod q$ yazarsak

$$\tau^2 = \sum_{x=1}^{q-1}\sum_{t=1}^{q-1} \chi^2(x)\chi(t)\zeta^{x(1+t)} = \sum_{t\not\equiv -1} \chi(t) \sum_{x=1}^{q-1} \overline{\chi}(x)\zeta^{x(1+t)} = \sum_{t\not\equiv -1} \chi(t)\chi(1+t)\overline{\tau}$$

olur. Bunu da τ ile çarparsak

$$\tau^3 = q\sum_{t=1}^{q-1} \chi(t(1+t)) = q(K+L\omega)$$

olarak yazabiliriz (K ve L tamsayıdır). $\overline{\tau}^3 = q(K+L\overline{\omega})$ olur.

$$\tau^3\overline{\tau}^3 = |\tau|^6 = q^3 = q^2(K+L\omega)(K+L\overline{\omega}) \implies q = K^2 - KL + L^2 \implies 4q = (2K-L)^2 + 3L^2$$

$\tau^3 - \overline{\tau}^3 = qL(\omega - \overline{\omega}) = iqL\sqrt{3}$ olur.

$$\tau^3 = \left[\sum_{x=1}^{q-1} \chi(x)\zeta^x\right]^3 = \sum_{x=1}^{q-1} \chi^3(x)\zeta^{3x} + 3\xi = \sum_{x=1}^{q-1} \zeta^{3x} + 3\xi$$

olarak yazarsak ξ de cebirsel tamsayı olacaktır (algebraic integer). $\overline{\tau}^3$ de hesaplanır, farkı alınırsa $\tau^3 - \overline{\tau}^3$ sayısı bir cebirsel tamsayının 3 katı olacaktır, yani $iqL\sqrt{3}$ sayısı bir cebirsel sayının 3 katı olacaktır. Buradan da $3 \mid L$ bulunur. Yani $a = 2K - L$ ve $b = \frac{L}{3}$ dersek

$$4q = a^2 + 27b^2$$

olur.

$$\tau^3 = q^{\frac{3}{2}}e^{3i\theta_q} = q(K+L\omega) = \frac{1}{2}q(a+3ib\sqrt{3}) \implies \cos 3\theta_q = \frac{a}{2\sqrt{q}}, \quad \sin 3\theta_q = \frac{3b\sqrt{3}}{2\sqrt{q}}$$

elde edilir. Buradan olası θ_q'uların sayısını sonlu sayıya azaltırız çünkü sadece $[0,\pi)$ aralığındaki θ_q'ları arıyoruz.

$$z_0 + z_1 + z_2 = 3 + 3(\eta_0 + \eta_1 + \eta_2) = 0$$

$$2(z_1z_2+z_1z_3+z_2z_3) = (z_1+z_2+z_3)^2 - (z_1^2+z_2^2+z_3^2) = -(\tau+\overline{\tau})^2 - (\omega^2\tau+\omega\overline{\tau})^2 - (\omega\tau+\omega^2\overline{\tau})^2 = -6\tau\overline{\tau} = -6q$$

$$z_1z_2z_3 = (\tau+\overline{\tau})(\omega^2\tau+\omega\overline{\tau})(\omega\tau+\omega^2\overline{\tau}) = \tau^3 + \overline{\tau}^3 = q(2K-L) = qa$$

olur. Yani z_1, z_2, z_3 sayıları

$$z^3 - 3qz - qa = 0$$

denkleminin kökleridir. Burada a'nın işaretini de bulmalıyız.

$$N = \sum_{u=0}^{q-1} \left[1 + \chi(u(u+1)) + \chi^2(u(u+1))\right] = \sum_{u=0}^{q-1} \left[1 + \chi(u(u+1)) + \overline{\chi}(u(u+1))\right] = q + (A+B\omega) + (A+B\overline{\omega}) = q+a$$

elde edilir. Ayrıca bu sayı

$$v^3 \equiv u(u+1) \pmod q$$

denkliğinin çözüm sayısıdır. Bu denklikte v'nin $u \equiv 0, -1$ için birer, diğer değerler için üçer çözümü vardır. Yani

$$N \equiv q + a \equiv 1 + a \equiv 2 \pmod 3 \implies a \equiv 1 \pmod 3$$

olacaktır. Bu bize aynı zamanda a'nın işaretini de verir çünkü $4q = a^2 + 27b^2$ eşitliğinde a ve $-a$'dan sadece bir tanesi $3k+1$ formatındadır. Yani Kummer toplamının hangi polinomun kökü olduğunu biliyoruz ama hangi kökü olduğu θ_q'ya bağlı çıkıyor. $\cos 3\theta_q$'u biliyoruz ama buradan tek bir θ_q değeri gelmiyor.

Bu denklemin köklerinin $(-2\sqrt{q}, -\sqrt{q})$, $(-\sqrt{q}, \sqrt{q})$ ve $(\sqrt{q}, 2\sqrt{q})$ aralıklarında oldukları görülebilir ama farklı q değerleri için Kummer toplamı bu üç aralığın herhangi birinde bulunabilir. Hatta Heath-Brown

ve Patterson adlı matematikçiler Kummer toplamının bu aralıklar arasındaki dağılımın incelenen veriler arttıkta $1:1:1$ oranına yakınsadığını göstermiştir.

Örnek: $q = 13$ için $4q = 52 = 5^2 + 27 \cdot 1^2$ olduğundan ve $a \equiv 1 \pmod 3$ olması gerektiğinden $a = -5$ olacaktır. Buradan da Kummer toplamı

$$z^3 - 39z + 65 = 0$$

denkleminin bir çözümü olarak bulunur.