Bilkent Üniversitesi
Matematik Bölümü

Ayın Sorusu

Mart 2016

Soru: Her kare-bölensiz $n > 1$ sayısı için

$$p \mid n \quad \text{ve} \quad n \mid p^2 + p \cdot m^p$$

olmasını sağlayan bir p asal sayısı ve bir m tam sayısı bulunduğunu gösteriniz.

Çözüm: n sayısının en büyük asal böleni p olsun. $m^p \equiv -p \pmod{\frac{n}{p}}$ koşulunu sağlayan bir m bulursak çözüm tamamlanır. $[0, \frac{n}{p}]$ aralığındaki $\frac{n}{p}$ ile aralarında asal olan tüm sayılar $m_1, m_2, \ldots, m_t$ olsun. $m_1^p, m_2^p, \ldots, m_t^p$ sayıları $\pmod{\frac{n}{p}}$ de farklıysa, $\{m_1^p, m_2^p, \ldots, m_t^p\} \equiv \{m_1, m_2, \ldots, m_t\} \pmod{\frac{n}{p}}$ elde ederiz. Fakat $-p$ sağdaki kümenin elemanı olduğundan soldaki kümenin de elemanıdır ve dolayısıyla istenilen m sayısı bulunmuştur.

Şimdi $m_1^p, m_2^p, \ldots, m_t^p$ sayılarının birbirinden farklı olduğunu gösterelim. Aksini varsayarsak $x \not\equiv y \pmod{\frac{n}{p}}$ ve $x^p \equiv y^p \pmod{\frac{n}{p}}$ koşullarını sağlayan x, y alalım. O zaman $s \equiv \frac{x}{y}$ sayısı $s^p \equiv 1 \pmod{\frac{n}{p}}$ ve $s \not\equiv 1 \pmod{\frac{n}{p}}$ koşullarını sağlayacaktır.
d, $s^d \equiv 1 \pmod{\frac{n}{p}}$ koşullarını sağlayan en küçük tam sayı olsun. O zaman $d > 1$, $d \mid p$ ve $d \mid \phi(\frac{n}{p}) \Rightarrow p \mid \phi(\frac{n}{p})$. Fakat $q_1, \ldots, q_k$ n nin diğer asal bölenleri olmak üzere $\phi(\frac{n}{p}) = (q_1 - 1) \cdots (q_k - 1)$. p nin tanımına göre $p > q_1, \ldots, q_k$ ve bu da $p \mid (q_1 - 1) \cdots (q_k - 1)$ ile çelişiyor. İspat tamamlandı.

Not. Çözümdeki $m^p \equiv -p \pmod{\frac{n}{p}}$ koşulu Çinli kalan teoremi kullanılarak

$$m^p \equiv -p \pmod{q_1}, \ \ldots, m^p \equiv -p \pmod{q_k}$$

gibi yazılabilir. Bu koşullar simetrik olduğundan birini çözmek yeterlidir. Diğer bir deyişle $p > q$ asal olmak üzere, $m^p \equiv -p \pmod{q}$ koşulunu sağlayan bir m tam sayısı bulmamız gerekiyor. g sayısı $\pmod{q}$ de ilkel kök olmak üzere, r sayısı $g^r \equiv -p \pmod{q}$ koşulunu sağlasın. s sayısını p nin $\pmod{q-1}$ de çarpmaya göre tersi olarak alırsak ($p > q$ olduğundan $\gcd(p, q-1) = 1$ ve p nin $\pmod{q-1}$ de tersi bulunuyor) $m = g^{rs}$ istenilen koşulları sağlar.