Yanıtı Bilinmeyen Bir Soru

Önce yanıtını dünyada kimsenin bilmediği bir soru soracağım, sonra yanıtını dünyada kimsenin bilmediği bu soru üzerine birkaç kolay soru yanıtlayacağım.

Herhangi bir pozitif doğal sayı alalım, diyelim p. İlerde p'yi asal alacağız ama şimdilik p'nin asallığının önemi yok.

Önce bir tanım: $\mathbb{F}_p = \{0, 1, 2, \ldots, p - 1\}$ olsun.

Demek ki p'den küçük doğal sayılardan oluşan $\mathbb{F}_p$ kümesinin tam p öğesi var.

$\mathbb{F}_p$ kümesinden iki sayı şöyle toplanır (ve çarpılır): O iki sayıyı bildiğimiz gibi toplarız (çarparız), sonra o toplamı (çarpımı) p'ye bölüp kalanına bakarız. Bu kalan da $\mathbb{F}_p$ kümesindedir.

Örneğin $p = 7$ ise,

$$2 + 3 = 5$$
$$3 + 4 = 0$$
$$3 + 5 = 1$$
$$4 + 4 = 1$$
$$5 + 6 = 4$$
$$2 \times 3 = 6$$
$$3 \times 5 = 1$$
$$4 \times 6 = 3.$$

Örneğin, $3 \times 5 = 1$, çünkü 15'i 7'ye bölersek geriye 1 kalır.
Bir başka örnek: $p = 11$ ise,

$$6 + 6 = 1$$
$$8 + 9 = 6$$
$$4 + 6 = 10$$
$$5 + 6 = 0$$
$$4 \times 6 = 2$$
$$8 \times 9 = 6$$
$$10 \times 10 = 1$$

Son bir örnek daha: $p = 12$ ise,

$$3 \times 4 = 0$$
$$2 \times 6 = 0$$
$$4 \times 6 = 0$$

$\mathbb{F}_p$ kümesinde çıkarma da yapılabilir. Örneğin, $p = 13$ ise,

$$-1 = 12$$
$$-2 = 11$$
$$-3 = 10$$
$$-4 = 9$$
$$-5 = 8$$
$$-6 = 7$$

Dolayısıyla,

$$6 - 7 = -1 = 12$$
$$3 - 9 = -6 = 7$$
$$2 - 12 = -10 = 3$$

Soru şu:
Öyle bir asal p ve $\mathbb{F}_p$'nin öyle bir A altkümesini bulun ki,
1. $0 \notin A$.
2. A'dan her iki sayının çarpımı yine A'da olsun, yani A çarpma altında kapalı olsun; simgesel deyişle $AA \subseteq A$ olsun.
3. $\mathbb{F}_p$'nin 0 olmayan her x sayısı için, A kümesinde, $x = a - b$ eşitliğini sağlayan bir ve bir tek (a, b) çifti olsun. Simgesel de-

yişle, $\mathbb{F}_p = A - A$ ve A'nın a, b, c, d öğeleri $a - b = c - d$ eşitliğini sağlıyorsa, $a = c$ ve $b = d$ olsun.

Bu koşulları sağlayan üç asal sayı biliniyor: $p = 3$, 7 ve 73.

Birinci Örnek: $p = 3$, $\mathbb{F}_p = \{0, 1, 2\}$ ve $A = \{1, 2\}$. O zaman,

$$1 = 2 - 1$$
$$2 = 1 - 2.$$

Sağdaki sayıların A'da olduklarına dikkatinizi çekerim. Aynı zamanda, A çarpma işlemi altında kapalı.

İkinci Örnek: $p = 7$, $\mathbb{F}_p = \{0, 1, 2, ,3 , 4, 5, 6\}$, $A = \{1, 2, 4\}$. O zaman,

$$1 = 2 - 1$$
$$2 = 4 - 2$$
$$3 = 4 - 1$$
$$4 = 1 - 4$$
$$5 = 2 - 4$$
$$6 = 1 - 2$$

Sağdaki sayıların A'da olduklarına ve A'nın çarpma altında kapalı olduğuna yine dikkatinizi çekerim.

Üçüncü Örnek: $p = 73$, $\mathbb{F}_p = \{1, 2, 3, \ldots, 72\}$, $A = \{1, 2, 4, 8, 16, 32, 64, 55, 37\}$. O zaman,

$$5 = 37 - 32$$
$$7 = 8 - 1$$
$$9 = 64 - 55$$
$$10 = 1 - 64$$
$$11 = 2 - 64 \text{ vb.}$$

Bu üç asaldan başka, yukardaki koşulları sağlayan bir A'nın olduğu bir asal bilinmiyor. Belki de bu koşulları sağlayan bir başka asal sayı yoktur.

Bu soruyu yanıtlayabilirseniz dünyaca ünlü bir matematikçi olursunuz.

Sorunun (projektif) geometriyle ilgisi var.

Her üç örnekte de, A kümesi 2 ve 2'nin üslerinden oluşuyor. Örneğin, $p = 73$ olduğunda, kolayca hesaplanabileceği üzere,

$$A = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8\}$$
$$= \{1, 2, 4, 8, 16, 32, 64, 55, 37\}.$$

Eğer p, yukardaki koşulları sağlayan bir A kümesinin olduğu bir asalsa, aşağıdaki savları kanıtlayalım:

Birinci Sav: $p = |A|^2 - |A| + 1$. (Burada $|A|$, A'nın eleman sayısı anlamına gelir.)

Kanıt: A^2, A'nın (a, b) çiftleri kümesi olsun. Yani

$$A^2 = \{(a, b) : a, b \in A\}$$

olsun. A^2 kümesinin $|A|^2$ tane elemanı vardır.

$\delta(A^2)$ de, A^2 kümesinin "çarprazı" olsun. Yani

$$\delta(A^2) = \{(a, a) : a \in A\}$$

olsun. $\delta(A^2)$ kümesinin $|A|$ tane elemanı vardır.

Dolayısıyla, $A^2 \setminus \delta(A^2)$ kümesinin, yani

$$\{(a, b) : a, b \in A \text{ ve } a \neq b\}$$

kümesinin $|A|^2 - |A|$ tane elemanı vardır.

$\mathbb{F}_p \setminus \{0\}$ kümesi, $\mathbb{F}_p$'nin 0 olmayan elemanları olsun. Bu kümenin $p - 1$ tane elemanı vardır.

$\mathbb{F}_p$'nin 0 olmayan her x sayısı için, A kümesinde, $x = a - b$ eşitliğini sağlayan bir ve bir tek (a, b) çifti olduğuna göre,

$$f(a, b) = a - b$$

olarak tanımlanan $f : A^2 \setminus \delta(A^2) \to \mathbb{F}_p \setminus \{0\}$ göndermesi (fonksiyonu) birebir ve örtendir, yani bir eşlemedir. Dolayısıyla $A^2 \setminus \delta(A^2)$ ve $\mathbb{F}_p \setminus \{0\}$kümelerinin eleman sayısı birbirine eşittir. Demek ki $|A|^2 - |A| = p - 1$ eşitliği geçerlidir. Bu da aşağı yukarı kanıtlamak istediğimiz eşitlik.

İkinci Sav: $1 \in A$.

Kanıt: A kümesinden herhangi bir eleman alalım, bu elema-

na a diyelim. $\mathbb{F}_p$ kümesi sonlu olduğundan, $\mathbb{F}_p$ kümesinin

$$a, a^2, a^3, a^4, \ldots$$

elemanları hepsi birbirinden değişik olamaz. Demek ki $a^n = a^m$ eşitliğini sağlayan birbirinden değişik n ve m doğal sayıları var. Eğer $n > m$ ise, bu eşitlikten $a^{n-m} = 1$ eşitliği çıkar. A kümesi çarpma altında kapalı olduğundan, a^{n-m} sayısı, yani 1, A kümesindedir.

Üçüncü Sav: Eğer $x \in \mathbb{F}_p \setminus \{0\}$ ise, $\mathbb{F}_p \setminus \{0\}$ kümesinde $xy = 1$ eşitliğini sağlayan bir y elemanı vardır.

Kanıt: $\mathbb{F}_p$ kümesi sonlu olduğundan, $\mathbb{F}_p$ kümesinin

$$x, x^2, x^3, x^4, \ldots$$

elemanları hepsi birbirinden değişik olamaz. Demek ki $x^n = x^m$ eşitliğini sağlayan birbirinden değişik n ve m doğal sayıları var. Eğer $n > m$ ise, bu eşitlikten $x^{n-m} = 1$ eşitliği çıkar. Şimdi, $y = x^{n-m-1}$ istediğimiz eşitliği sağlar.

Dördüncü Sav: $2 \in A$.

Kanıt: a, b elemanları, $1 = a - b$ eşitliğini sağlayan A'nın elemanları olsun. Her iki tarafı da b^{-1} elemanıyla çarpalım: $b^{-1} = ab^{-1} - 1$. Bu son eşitlikten, $1 = ab^{-1} - b^{-1}$ çıkar. Demek ki,

$$1 = a - b$$
$$1 = ab^{-1} - b^{-1}$$

Dolayısıyla $a = ab^{-1}$, yani $b = 1$. Bundan da $a = 2$ çıkar. Demek ki $2 \in A$.

A kümesi çarpma altında kapalı olduğundan, yukardaki savdan, 2, 4, 8, 16, ... sayılarının da A'da oldukları anlaşılır.

Beşinci Sav: $3 \notin A$.

Kanıt: Eğer $3 \in A$ ise, o zaman, $2 = 4 - 2$ ve $2 = 3 - 1$ eşitliklerinden, $4 = 3$ çıkar, yani $1 = 0$, bu imkânsızdır. Demek ki $3 \in A$.

Altıncı Sav: Eğer $p \neq 3$ ise $5 \notin A$.

Kanıt: Diyelim $5 \in A$. O zaman, $4 = 5 - 1$ ve $4 = 8 - 4$ eşitliklerinden, $5 = 8$ çıkar, yani $3 = 0$, yani $p = 3$. Oysa, varsayıma göre $p \neq 3$. Demek ki $5 \notin A$.

Savları (ve kanıtları) çoğaltmayı size bırakıyorum.