Olimpiyat Soruları Köşesi

Korkmaz Sönmez

Problem [25'inci Uluslararası Matematik Olimpiyatları, 1984/2]: *Öyle a ve b doğal sayıları bulun ki hem*

$$ab(a+b) \not\equiv 0 \bmod 7$$

hem de

$$(a+b)^7 - a^7 - b^7 \equiv 0 \bmod 7^7$$

olsun.

İlk Adım: *b*'nin 1 Olduğunu Varsayabiliriz.

Kanıt: Nitekim, $ab(a+b) \not\equiv 0 \bmod 7$ varsayımından dolayı, b sayısı 7'ye bölünmez, dolayısıyla b ile 7^7 aralarında asaldır, yani b sayısı modülo 7^7 tersinirdir. Böylece, denkliği b'nin modülo 7^7 tersiyle çarparak b'nin 1'e eşit olduğunu varsayabiliriz.

Bunu daha ayrıntılı gösterelim: x sayısı,

$$bx \equiv 1 \bmod 7^7$$

denkliğini sağlasın. O zaman $bx \equiv 1 \bmod 7$ denkliği de sağlanır. $(a+b)^7 - a^7 - b^7 \equiv 0 \bmod 7^7$ denkliğinin her iki tarafını da x^7 ile çarparak,

$$(ax+1)^7 - (ax)^7 - 1 \equiv 0 \bmod 7^7$$

denkliğini ve $c = ax$ tanımını yaparak

$$(c+1)^7 - c^7 - 1 \equiv 0 \bmod 7^7$$

denkliğini elde ederiz. $ab(a+b) \not\equiv 0 \bmod 7$ denksizliğini de x^3 ile çarparsak,

$$0 \not\equiv ab(a+b)x^3 = (ax)(bx)(ax+bx) \equiv c(c+1) \bmod 7$$

elde ederiz. Demek ki,

$$c(c+1) \not\equiv 0 \bmod 7,$$
$$(c+1)^7 - c^7 - 1 \equiv 0 \bmod 7^7 \qquad (*)$$

sistemini çözmeliyiz. □

İkinci Adım: (*) Denkliğini Sadeleştirme.

$(c+1)^7$ terimini açarak (*) denkliğini sadeleştirelim:

$$7c^6 + 21c^5 + 35c^4 + 35c^3 + 21c^2 + 7c \equiv 0 \bmod 7^7.$$

Her tarafı 7'ye bölerek,

$$c^6 + 3c^5 + 5c^4 + 5c^3 + 3c^2 + c \equiv 0 \bmod 7^6$$

elde ederiz. Ama c sayısı modülo 7^6 tersinirdir. Dolayısıyla bir adet c de sadeleşir:

$$c^5 + 3c^4 + 5c^3 + 5c^2 + 3c + 1 \equiv 0 \bmod 7^6.$$

Dikkat ederseniz, $c = -1$, bu denkliğin bir çözümü, hatta $c = -1$, sadece denkliğin değil,

$$c^5 + 3c^4 + 5c^3 + 5c^2 + 3c + 1 = 0$$

eşitliğinin de bir çözümü, ama bu çözüm

$$c(c+1) \not\equiv 0 \bmod 7$$

koşulu tarafından yasaklanmış. Gene de bu bilgiden yararlanabiliriz: -1 sayısı

$$X^5 + 3X^4 + 5X^3 + 5X^2 + 3X + 1$$

polinomununun bir kökü olduğundan $X+1$ polinomu, $X^5 + 3X^4 + 5X^3 + 5X^2 + 3X + 1$ polinomununun bir çarpanıdır:

$$\begin{array}{r|l}
X^5 + 3X^4 + 5X^3 + 5X^2 + 3X + 1 & X+1 \\
\hline
-(X^5 + X^4) & X^4 + 2X^3 + 3X^2 + 2X + 1 \\
\cline{1-1}
2X^4 + 5X^3 & \\
-(2X^4 + 2X^3) & \\
\cline{1-1}
3X^3 + 5X^2 & \\
-(3X^3 + 3X^2) & \\
\cline{1-1}
2X^2 + 3X & \\
-(2X^2 + 2X) & \\
\cline{1-1}
X + 1 & \\
-(X + 1) & \\
\cline{1-1}
0 &
\end{array}$$

Demek ki,

$$X^5 + 3X^4 + 5X^3 + 5X^2 + 3X + 1 = (X^4 + 2X^3 + 3X^2 + 2X + 1)(X+1)$$

Dolayısıyla

$$c^5 + 3c^4 + 5c^3 + 5c^2 + 3c + 1 = (c^4 + 2c^3 + 3c^2 + 2c + 1)(c+1),$$

yani,

$$c^4 + 2c^3 + 3c^2 + 2c + 1 \equiv 0 \bmod 7^6.$$

Ama,

$$c^4 + 2c^3 + 3c^2 + 2c + 1 = (c^2 + c + 1)^2.$$

Demek ki,

$$c^2 + c + 1 \equiv 0 \bmod 7^3 \qquad (**)$$

denkliğini çözmek gerekli ve aynı zamanda yeterli.

Üçüncü Adım. (**) Denkliğini Çözmek.

Birinci Çözüm. Önce $c-1$'in modülo 7 ve 7^3 tersinir olduğunu gözlemleyelim. Nitekim öyle olmasaydı, 7, $c-1$'i bölerdi ve (**) denkliğinden dolayı

$$3 \equiv c^2 + c + 1 \equiv 0 \bmod 7$$

olurdu. Demek ki, $c \not\equiv 1 \bmod 7$ koşulunu sürekli aklımızda tutarak, (**) denkliğini $c-1$ ile çarpabiliriz:

$$c^3 - 1 = (c-1)(c^2 + c + 1) \equiv 0 \bmod 7^3,$$

yani

$$c \not\equiv 1 \bmod 7,$$
$$c^3 \equiv 1 \bmod 7^3$$

sistemini çözmemiz gerektiğini anlarız. Ama Euler

$$x^{\varphi(7^3)} \equiv 1 \bmod 7^3,$$

teoremine göre, her 7'ye asal her x için,
ve

$$\varphi(7^3) = 7^3 - 7^2 = 343 - 49 = 294 = 98\times 3.$$

Yani 7'ye asal her x için,

$$(x^{98})^3 \equiv 1 \bmod 7^3.$$

Şimdi, 7'ye asal herhangi bir x için,c'yi x^{98} alabiliriz, yeter ki $x^{98} \not\equiv 1 \bmod 7$ olsun. Fermat Teoremi'nden dolayı,

$$x^6 \equiv 1 \bmod 7.$$

Demek ki,

$$x^4 \equiv x^{6\times 14 + 4} \equiv x^{98} \not\equiv 1 \bmod 7$$

olmalı. Eğer $x = 2$ alırsak,

$$x^4 = 2^4 = 16 \equiv 2 \not\equiv 1 \bmod 7$$

olur ve sorun kalmaz. Demek ki, $c = 2^{98}$ sayısı (**) ve (*) sistemlerinin bir çözümüdür.

Sonuç olarak $a = 2^{98}$, $b = 1$ sorunun yanıtıdır.

Modülo $7^3 = 343$ çalıştığımız için 2^{98} çözümünü daha da küçültebiliriz:

$2^{10} = 1024 = 3\cdot 7^3 - 5 \equiv -5 \bmod 7^3$,
$2^{20} \equiv 25 \bmod 7^3$,
$2^{40} \equiv 625 \equiv -61 \bmod 7^3$,
$2^{80} \equiv 61^2 = 3721 \equiv -52 \bmod 7^3$,
$2^{90} \equiv 2^{80}2^{10} \equiv (-52)(-5) = 260 \equiv -83 \bmod 7^3$,
$2^8 = 256 \equiv -87 \bmod 7^3$,
$2^{98} \equiv 2^{90}2^8 \equiv (-83)(-87) = 7221 \equiv 18 \bmod 7^3$;

Demek ki $a = 18$, $b = 1$ alabiliriz.

Eğer x için 2 yerine başka bir sayı alsaydık bir başka çözüm bulabilirdik. Aşağıda bir başka yöntemle bir başka çözüm bulacağız.

Ama bunu daha şimdiden bulabiliriz: Eğer c,

$$c \not\equiv 1 \bmod 7,$$
$$c^3 \equiv 1 \bmod 7^3$$

sisteminin bir çözümüyse, c^2 de aynı sistemin bir çözümüdür. Dolayısıyla $a = 18^2 = 324$ ve $b = 1$ de problemin bir çözümüdür.

İkinci Çözüm. $u, v, w \in \{0, 1, 2, 3, 4, 5, 6\}$ olmak üzere

$$c = u + 7v + 7^2w$$

yazalım ve c'nin

$$c^2 + c + 1 \equiv 0 \bmod 7^3 \qquad (**)$$

denkleminin çözümü olması için u, v ve w'yi bulalım.

Önce u'yu bulalım. Bunun için modülo 7 çalışmak yeterli:

$$u^2 + u + 1 \equiv c^2 + c + 1 \equiv 0 \bmod 7.$$

Bu denkliği sağlayan iki tane u var:

$$u = 2 \text{ ve } u = 4.$$

Bunlardan birini seçelim. Diyelim u = 2'yi seçtik. Demek ki,

$$c = 2 + 7v + 7^2w.$$

Şimdi v'yi bulalım. v'yi bulmak için modülo 7^2 çalışmak yeterli:

$$0 \equiv c^2 + c + 1 \equiv (2 + 7v)^2 + (2 + 7v) + 1$$
$$= 4 + 28v + 2 + 7v + 1 = 7 + 35v \bmod 7^2.$$

Sadeleştirerek,

$$1 + 5v \equiv 0 \bmod 7$$

buluruz. Buradan da kolayca $v = 4$ çıkar. Demek ki,

$$c = 2 + 7v + 7^2w = 2 + 7\cdot 4 + 7^2w = 30 + 7^2w.$$

Son olarak w sayısını bulalım:

$$0 \equiv c^2 + c + 1$$
$$\equiv (30 + 7^2w)^2 + (30 + 7^2w) + 1$$
$$\equiv 30^2 + 60w7^2 + 30 + 7^2w + 1$$
$$= 931 + 61w7^2 \bmod 7^3,$$

yani

$$931 + 61w7^2 \equiv 0 \bmod 7^3,$$

yani

$$7^2\cdot 19 + 33w7^2 \equiv 0 \bmod 7^3.$$

Sadeleştirerek,

$$19 + 33w \equiv 0 \bmod 7,$$

yani

$$5 + 5w \equiv 0 \bmod 7,$$

yani $w = 6$ bulunur. Demek ki,

$$c = 30 + 7^2w = 30 + 7^26 = 324.$$

Eğer u için 2 yerine 4 alsaydık, $v = 2$ ve $w = 0$ bulurduk, yani daha önce bulduğumuz,

$$c = u + 7v + 7^2w = c = 4 + 7\cdot 2 + 7^20 = 18$$

çözümünü bulurduk.

Yukardaki yöntem aslında MD-2004-III'te gördüğümüz ***Hensel Önsavı***'nın bir uygulamasıdır.

Tartışma. $0 \le c < 7^3$ eşitsizliklerini sağlayan en fazla 2 çözüm vardır (yukarda bulduğumuz 18 ve 324). Bunu şöyle görebiliriz:

$$c^2 + c + 1 \equiv 0 \bmod 7^3$$

ise, 4 modulo 7^3 tersinir olduğundan,

$$(c + 1/2)^2 + 3/4 = c^2 + c + 1 \equiv 0 \bmod 7^3$$

ve

$$(c + 1/2)^2 \equiv -3/4 \bmod 7^3$$

olur. Eğer d, $-3/4$ sayısının kareköküyse,

$$c = 1/2 + d$$

olmalı. Ama modülo 7^3, bir sayının en fazla iki karekökü vardır. (Neden?) ♠