Sayılar Kuramı Özeti

David Pierce

18 Mayıs 2024 taslağı

Bu notlar, derslerde söylendiğine sadece bir hatırlatmadır. Burada hata yapmamaya çalışıyorum, ama yazının matematiğinde veya Türkçesinde bir hata bulursanız lütfen bana haber verin.

İçindekiler

1 Öklid Algoritması

1.1 Sayma sayılarında

Sayma sayılarında $a_1 > a_2$ olduğunda, $a_2 > a_3 > \cdots > a_{n+1}$,

$$\begin{aligned} a_1 &= a_2 t_1 + a_3, \\ a_2 &= a_3 t_2 + a_4, \\ &\vdots \\ a_{n-2} &= a_{n-1} t_{n-2} + a_n, \\ a_{n-1} &= a_n t_{n-1} + a_{n+1}, \end{aligned}$$

ve $a_n = a_{n+1}t_n$ koşullarını sağlayan n ve $a_3, \ldots, a_{n+1}$ ve $t_1, \ldots, t_n$ sayıları vardır. O zaman tersine

$$\begin{aligned} a_{n+1} &= a_{n-1} - a_n t_{n-1} \\ &= a_{n-1} - (a_{n-2} - a_{n-1}t_{n-2}) \cdot t_{n-1} \\ &= a_{n-1} \cdot (1 + t_{n-2}t_{n-1}) - a_{n-2}t_{n-1} \\ &= \ldots \end{aligned}$$

Bu şekilde

$$a_1 x - a_2 y = (-1)^n a_{n+1}$$

Bézout Denklemini çözebiliriz, ve **çözümümüzü kontrol etmek kolaydır.**

Teorem (Öklid Algoritması)**.** *Yukarıdaki koşullarda* a_{n+1}*,*

- *a_1'i ve a_2'yi böler;*
- *onların her ortak böleni tarafından bölünür.*

*Kısaca a_1 ve a_2'nin **en büyük ortak böleni** vardır, ve bu bölen, a_{n+1}'dir:*

$$a_{n+1} = \text{ebob}(a_1, a_2).$$

Tersine n, ve $t_1, \ldots, t_n$, ve a_{n+1} sayılarını seçerek **kendi alıştırmalarımızı yaratabiliriz.**

Yukarıdaki durumda

$$\frac{a_1}{a_2} = t_1 + \frac{a_3}{a_2} = t_1 + \cfrac{1}{t_2 + \cfrac{a_4}{a_3}} = \ldots = t_1 + \cfrac{1}{t_2 + \cfrac{1}{\cdots + \cfrac{1}{t_n}}}.$$

Kısaltma olarak

$$\frac{a_1}{a_2} = [t_1, t_2, \ldots, t_n].$$

Aslında

$$\frac{a_1}{a_2} = \beta_1, \qquad \frac{a_2}{a_3} = \beta_2, \qquad \ldots, \qquad \frac{a_n}{a_{n+1}} = \beta_n$$

olduğunda $1 \leqslant k < n$ ise

$$\lfloor \beta_k \rfloor = t_k, \qquad \frac{1}{\beta_k - t_k} = \beta_{k+1},$$

ve son olarak

$$\beta_n = t_n,$$

ama β_{n+1} tanımlanmaz.

1.2 Gerçel Sayılarda

Yukarıda β_1, kesirli olmayan bir gerçel sayı olabilir, ve bu durumda her k için β_k tanımlanır. Şimdi özyineleme ile

$$[t_1] = t_1, \qquad [t_1, t_2, \ldots, t_{k+1}] = t_1 + \frac{1}{[t_2, \ldots, t_{k+1}]}$$

olsun, ve

$$\begin{aligned} p(t_1) &= t_1, \quad p(t_1, t_2, \ldots, t_{k+1}) = t_1 \cdot p(t_2, \ldots, t_{k+1}) + q(t_2, \ldots, t_{k+1}), \\ q(t_1) &= 1, \quad q(t_1, t_2, \ldots, t_{k+1}) = p(t_2, \ldots, t_{k+1}) \end{aligned}$$

olsun. O zaman

$$p_k = p(t_1, \ldots, t_k), \qquad q_k = q(t_1, \ldots, t_k)$$

tanımlandığında, tümevarım ile

$$[t_1, \ldots, t_k] = \frac{p_k}{q_k}.$$

Ayrıca

$$[t_1, \ldots, t_{k+1}] = \left[t_1, \ldots, t_{k-1}, t_k + \frac{1}{t_{k+1}}\right]$$

ve

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \cdots < \beta_1 < \cdots < \frac{p_4}{q_4} < \frac{p_2}{q_2}.$$

Örnek. $\beta_1 = \sqrt{41}$ olsun. O zaman

$$t_1 = 6, \quad \beta_2 = \frac{\sqrt{41}+6}{5},$$

$$t_2 = 2, \quad \beta_3 = \frac{\sqrt{41}+4}{5},$$

$$t_3 = 2, \quad \beta_4 = \sqrt{41}+6.$$

Bundan dolayı

$$t_4 = 2t_1, \qquad t_{k+4} = t_{k+1},$$

ve sonuç olarak

$$\sqrt{41} = [6, 2, 2, \sqrt{41} + 6], \qquad \frac{p_{k+3}}{q_{k+3}} = \left[6, 2, 2, 6 + \frac{p_k}{q_k}\right].$$

Şimdi

$$\begin{aligned}
[6, 2, 2, z + 6] &= \left[6, 2, 2 + \frac{1}{z + 6}\right] \\
&= \left[6, 2, \frac{2z + 13}{z + 6}\right] = \left[6, 2 + \frac{z + 6}{2z + 13}\right] \\
&= \left[6, \frac{5z + 32}{2z + 13}\right] = \left[6 + \frac{2z + 13}{5z + 32}\right] \\
&= \frac{32z + 205}{5z + 32},
\end{aligned}$$

dolayısıyla

$$(p_{k+3}, q_{k+3}) = (32p_k + 205q_k, 5p_k + 32q_k).$$

Ayrıca

$$[6] = 6, \qquad [6,2] = \frac{13}{2}, \qquad [6,2,2] = 6 + \frac{2}{5} = \frac{32}{5},$$

ve

$$6^2 - 41 = -5, \qquad 13^2 - 41 \cdot 5^2 = 5,$$

ama

$$32^2 - 41 \cdot 5^2 = 1024 - 41 \cdot 25 = 1024 - 1025 = -1.$$

Ayrıca $205 = 41 \cdot 5$, dolayısıyla

$$(32z+205)^2 - 41 \cdot (5z+32) = (32^2 - 41 \cdot 5^2)z^2 - 41 \cdot (32^2 - 41 \cdot 5^2) = 41 - z^2,$$

ve sonuç olarak

$$p_{k+3}{}^2 - 41q_{k+3}^2 = -(p_k{}^2 - 41q_k{}^2).$$

Özellikle her (p_{6k}, q_{6k}),

$$x^2 - 41y^2 = 1$$

denklemini sağlar. Ayrıca

$$(p_6, q_6) = (32^2 + 205 \cdot 5, 5 \cdot 32 + 32 \cdot 5) = (2049, 320)$$

ve

$$\begin{aligned}(p_{6(k+1)}, q_{6(k+1)}) &= (32p_{6k+3} + 205q_{6k+3}, 5p_{6k+3}, 32q_{6k+3}) \\ &= (32(32p_{6k} + 205q_{6k}) + 205(5p_{6k} + 32q_{6k}), \\ &\quad 5(32p_{6k} + 205q_{6k}) + 32(5p_{6k} + 32q_{6k})) \\ &= (2049p_{6k} + 41 \cdot 320q_{6k}, 320p_{6k} + 2049q_{6k}).\end{aligned}$$

Teorem. *Kare olmayan bir d sayma sayısı için $\beta_1 = \sqrt{d}$ olsun.*

1. *Bir n için $\beta_{n+1} = \sqrt{d} + t_1$.*

2. *$\beta_{n+1} = \sqrt{d} + t_1$ olduğunda*

$$p_n{}^2 - dq_n{}^2 = (-1)^n, \qquad p_{2n}{}^2 - dq_{2n}{}^2 = 1.$$

3. *$a^2 - db^2 = 1$ olduğunda*

$$(a_1, b_1) = (A, B), \qquad (a_{k+1}, b_{k+1}) = (Aa_k + dBb_k, Ba_k + Ab_k)$$

ise her (a_k, b_k),

$$x^2 - dy^2 = 1$$

denklemini sağlar.

Bu genel teoremi göstermiyoruz ama her özel durumda gösterebiliriz.

Bu şekilde herhangi kare olmayan d sayma sayısı için

$$x^2 - dy^2 = 1$$

Pell Denkleminin, sonsuz sayıda çözümlerini bulabiliriz. Ayrıca

$$\sqrt{d} = \lim_{\ell \to \infty} \frac{p_{\ell n}}{q_{\ell n}}.$$

1.3 Lamé Teoremi

Sayma sayılarında, bildiğimiz gibi,

$$\begin{aligned} a_1 &= a_2 \cdot t_1 + a_3, \\ a_2 &= a_3 \cdot t_2 + a_4, \\ &\vdots \\ a_{n-1} &= a_n \cdot t_{n-1} + a_{n+1}, \\ a_n &= a_{n+1} \cdot t_n \end{aligned}$$

olduğunda,

$$a_{n+1} = \text{ebob}(a_1, a_2).$$

Ayrıca $t_n > 1$ varsayılabilir, ve bu durumda

$$a_2 < 10^\ell \implies n \leqslant 5\ell.$$

Bu sonuç, **Lamé Teoremidir,** ve bunu kanıtlayacağız. Yukarıdaki eşitliklerden

$$\begin{aligned} a_2 &\geqslant a_3 + a_4, \\ &\vdots \\ a_{n-1} &\geqslant a_n + a_{n+1}, \\ a_n &> a_{n+1}. \end{aligned}$$

Özyineleme ile

$$F_1 = 1, \qquad F_2 = 1, \qquad F_{k+2} = F_k + F_{k+1}$$

olsun. Bunlar, **Fibonacci Sayılarıdır.** O zaman

$$\begin{aligned} a_{n+1} &\geqslant F_2, \\ a_n &\geqslant F_3, \\ a_{n-1} &\geqslant F_4, \\ &\vdots \\ a_2 &\geqslant F_{n+1}. \end{aligned}$$

Şimdi

$$\varphi = \frac{1+\sqrt{5}}{2}, \qquad \psi = \frac{1-\sqrt{5}}{2}$$

olsun. Burada φ, **Altın Orandır.** Ayrıca φ ve ψ,

$$x^2 = x + 1$$

denkleminin çözümleridir. O zaman her (α, β) için

$$(\alpha\varphi^k + \beta\psi^k) + (\alpha\varphi^{k+1} + \beta\psi^{k+1}) = \alpha\varphi^{k+2} + \beta\psi^{k+2}.$$

Ayrıca

$$\begin{aligned} x + \quad y &= 1 \\ \varphi x + \psi y &= 1 \end{aligned}$$

lineer sisteminin çözümü

$$\left(\frac{\varphi}{\varphi - \psi}, \frac{-\psi}{\varphi - \psi} \right)$$

olduğundan

$$F_k = \frac{\varphi^k - \psi^k}{\varphi - \psi}$$

Binet Formülünü elde ediyoruz. Ayrıca tümevarım ile her durumda

$$F_k > \varphi^k / \varphi^2,$$

çünkü

$$F_1 = 1 > 1/\varphi^2, \qquad F_2 = 1 > 1/\varphi,$$

ve eğer

$$F_k > \varphi^k/\varphi^2, \qquad F_{k+1} > \varphi^{k+1}/\varphi^2$$

ise, o zaman

$$F_{k+2} = F_k + F_{k+1} > (\varphi^k + \varphi^{k+1})/\varphi^2 = \varphi^{k+2}/\varphi^2.$$

Bundan dolayı

$$a_2 > \varphi^{n-1}.$$

Ayrıca tümevarım ile

$$\varphi^{k+1} = F_{k+1}\varphi + F_k$$

olduğundan ve

k	1	2	3	4	5
F_k	1	1	2	3	5

olduğundan

$$\varphi^5 = 5\varphi + 3 = (11 + 5\sqrt{5})/2.$$

Son olarak

$$11 + 5\sqrt{5} > 20 \iff 5\sqrt{5} > 9 \iff 125 > 81$$

olduğundan $\varphi^5 > 10$, ve $a_2 > \varphi^{n-1}$ olduğundan

$$a_2 > 10^{(n-1)/5}.$$

Şimdi, eğer

$$a_2 < 10^{\ell}$$

ise, o zaman

$$\begin{aligned} 10^{(n-1)/5} &< 10^{\ell}, \\ n - 1 &< 5\ell, \\ n &\leqslant 5\ell. \end{aligned}$$

Örnek. $a_2 < 1000$ ise $n \leqslant 15$. Ayrıca

k	1	2	3	4	5	6	7	8	9	10
F_k	1	1	2	3	5	8	13	21	34	55
F_{k+10}	89	144	233	377	610	987	1597			

olduğundan $(a_1, a_2) = (1597, 987)$ ise $n = 15$.

2 Sayılar Kuramının Temelleri

İyisıralanmış bir küme, öyle doğrusal sıralanmış bir kümedir ki her boş olmayan altkümesinin en küçük elemanı vardır.

Eğer iyisıralanmış bir küme boş değilse, o zaman **en küçük** elemanı vardır. Ayrıca, bu kümenin bir a elemanı, kümenin en büyük elemanı değilse, o zaman a'dan büyük olan elemanların en küçüğü vardır, ve bu eleman, a'nın **ardılıdır.** Ne en küçük elemanı ne ardıl olan bir eleman, bir **limittir.**

Postulat. *Sayma sayıları,*

- *boş olmayan,*

- *en büyük elemanı olmayan,*
- *limiti olmayan*

iyisıralanmış bir küme oluşturur.

Tanım. Sayma sayıları kümesi

$$\mathbb{N},$$

ve $\mathbb{N}$'nin en küçük elemanı

$$1,$$

ve $\mathbb{N}$'nin her n elemanının ardılı,

$$n+1.$$

Teorem (Tümevarım)**.** *Eğer* $\mathbb{N}$*'nin bir altkümesi*

- 1*'i içerirse ve*

- *kümenin her elemanının ardılını da içerirse,*

o zaman bu altküme $\mathbb{N}$'nin kendisidir.

Teorem (Özyineleme)**.** *Eğer*

- *A, bir küme,*
- *$b \in A$,*
- *$f\colon A \to A$*

işe, o zaman

- *$g\colon \mathbb{N} \to A$,*
- *$g(1) = b$,*
- *her zaman $g(n+1) = f(g(n))$*

koşullarını sağlayan bir ve tek bir g vardır.

Tanım.

Toplama

$$n + (k + 1) = (n + k) + 1.$$

Çarpma

$$n \cdot 1 = n, \qquad n \cdot (k + 1) = n \cdot k + n.$$

Kuvvet alma

$$n^1 = n, \qquad n^{k+1} = n^k \cdot n.$$

Teorem. *Toplama ve çarpma, birleşmeli ve değişmelidir, ve çarpma, toplama üzerinde dağılır.*

Kanıt. Tümevarım. Değişmeli özelliğin her durumunda üç tümevarım kullanır, çünkü

$$1 + n = n + 1, \qquad 1 \cdot n = n,$$
$$(k+1) \cdot n = (k+n) + 1\text{ö} \quad (k+1) \cdot n = (k \cdot n) + n$$

eşitlikler de gösterilir. Ayrıntılar, bir **alıştırmadır.** □

Teorem.

$$a^{b+c} = a^b \cdot a^c, \qquad a^{b \cdot c} = (a^b)^c.$$

Kanıt. Bir **alıştırmadır.** □

Teorem. *Eğer $a < b$ ise, o zaman*

- *bir ve tek bir z için*
$$a + z = b;$$
- *bir ve tek bir y için*
$$a \cdot y \leqslant b \leqslant a \cdot y + a;$$

- *$a > 1$ olduğunda bir ve tek bir x için*

$$a^x \leqslant b < a^x \cdot a,$$

dolayısıyla bir ve tek bir y için

$$a^x \cdot y \leqslant b < a^x \cdot y + a^x \ \ \& \ \ y < a.$$

Örnek.

$$2024 = 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2+1} + 2^{2+1}.$$

3 Kalandaşlık

Tanım.

- $\omega = \mathbb{N} \cup \{0\}$,
- $\mathbb{Z} = \omega \cup \{-x \colon x \in \mathbb{N}\}$.

Okulda öğrendimiz gibi toplama ve çarpma, $\mathbb{Z}$'de tanımlanır, ve sonuç olarak $\mathbb{Z}$, değişmeli bir halka olur. Bu durumda $a \in \mathbb{N}$ olduğunda

$$a\mathbb{Z} = (a) = \{ax \colon x \in \mathbb{Z}\},$$

ve $n \in \mathbb{N}$ olduğunda tanıma göre

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n).$$

Ayrıca $\mathbb{Z}$'de

$$a \mid b \iff \exists x \; ax = b.$$

Şimdi $n \in \mathbb{N}$ olduğunda

$$a \equiv b \pmod{n} \iff n \mid a - b,$$

ve bu durumda a ve b, n **modülüsüne göre kalandaştır.** Sonuç olarak

$$a \equiv b \pmod{n} \iff a + (n) = b + (n).$$

Teorem (Öklid Lemması)**.** $\mathbb{Z}$*'de*

$$a \mid bc \;\; \& \;\; \text{ebob}(a, b) = 1 \implies a \mid c.$$

Kanıt. $a \mid bc \ \ \& \ \ ax + by = 1$ olduğunda

$$a \mid acx + bcy \ \ \& \ \ acx + bcy = c. \qquad \square$$

Teorem. *Bir* $ax \equiv b \pmod{n}$ *kalandaşlığının çözümleri varsa, o zaman aşağıdaki kuralları kullanarak çözümleri bulabiliriz. İlk olarak*

$$a \equiv b \pmod{n} \implies a \equiv b \pm n \pmod{n}.$$

Ayrıca

$$ax \equiv ab \pmod{n} \ \ \& \ \ \text{ebob}(a, n) = 1 \implies x \equiv b \pmod{n}.$$

Aslında $\text{ebob}(a, n) = 1$ *ise, o zaman*

$$\exists y \ ac + ny = 1$$

formülünü sağlayan c *vardır, ve bu durumda*

$$ax \equiv b \pmod{n} \iff x \equiv bc \pmod{n}.$$

Ayrıca

$$\begin{aligned} & ac \equiv bc && \pmod{nc} \\ \iff & a \equiv b && \pmod{n} \\ \iff & a \equiv b \vee a \equiv b+n \vee \cdots \vee a \equiv b+(c-1)\cdot n && \pmod{nc}. \end{aligned}$$

Son olarak $\text{ebob}(m,n) = 1$ *ise, o zaman*

$$a \equiv b \pmod{mn} \iff a \equiv b \pmod{m} \ \& \ a \equiv b \pmod{n}.$$

Teorem (Çin Kalan Teoremi)**.** $\{n_1, \ldots, n_k\} \subseteq \mathbb{N}$ *olduğunda*

$$1 \leqslant i < j \leqslant k \implies \text{ebob}(n_i, n_j) = 1$$

olsun. O zaman

$$N = n_1 \ldots n_k$$

olduğunda her durumda

$$N_i = \frac{N}{n_i}$$

olduğunda öyle b_i vardır ki

$$b_i N_i \equiv 1 \pmod{n_i},$$

ve sonuç olarak

$$x \equiv a_1 \pmod{n_1} \ \& \ \cdots \ \& \ x \equiv a_k \pmod{n_k}$$

sisteminin çözümü,

$$x \equiv a_1 b_1 N_1 + \cdots + a_k b_k N_k \pmod{N}.$$

4 Asallık

Eğer

$$\text{ebob}(a, b) = 1$$

ise, o zaman a ve b, **birbirine asaldır.**

Eğer

$$p > 1 \ \ \& \ \ \forall x \ \ \text{ebob}(p, x) \in \{1, p\}$$

ise, o zaman p **asaldır.**

Teorem (Fermat)**.** *Eğer* $p \nmid a$ *ise, o zaman* $a^{p-1} \equiv 1 \pmod{p}$.

Kanıt. $p \nmid a$ olsun. $a^{p-1} \equiv 1 \pmod{p}$ için üç kanıt vardır.

1. $x + (p) \mapsto ax + (p)$ fonksiyonu

$$\{1 + (p), \ldots, p - 1 + (p)\}$$

kümesinin bir permütasyonudur; aslında ${\mathbb{Z}_p}^{\times}$ grubunun bir otomorfizmasıdır. Bundan dolayı

$$(p-1)! \equiv \prod_{1 \leqslant k < p} (ak) \equiv a^{p-1}(p-1)! \pmod{p}.$$

Şimdi Öklid Lemması sayesinde $(p-1)!$, p'ye asal olduğundan teorem çıkar.

2. ${\mathbb{Z}_p}^{\times}$ grubunun mertebesi $p-1$ olduğundan teorem çıkar.

3. Öklid Lemması sayesinde

$$(a+1)^p = a^p + \sum_{1 \leqslant k < p} b_k a^k + 1$$

olduğunda $p \mid b_k$, dolayısıyla

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

O zaman tümevarım ile $\mathbb{Z}_p$ halkasın her $x + (p)$ elemanı için

$$x^p + (p) = x + (p).$$

Bundan teorem çıkar. □

Sonuç olarak

$$a \equiv c \pmod{p} \ \& \ b \equiv d \pmod{p-1} \implies a^b \equiv c^d \pmod{p}.$$

Bunun ile $a^b \equiv x \pmod{p}$ kalandaşlıkları çözülebilir.

Fermat Teoreminin ikinci kanıtı ile daha genel bir teorem elde edilir (sonraki bölümlere bakın):

Teorem (Euler)**.** $|\mathbb{Z}_n{}^\times| = \varphi(n)$ *olduğunda,* $\operatorname{ebob}(a, n) = 1$ *ise*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Teorem (Aritmetiğin Temel Teoremi)**.** *Her sayma sayısı, bir ve tek bir şekilde, öyle*

$$p_1 \dots p_n$$

çarpımıdır ki her p_k *çarpanı asaldır ve*

$$p_1 \leqslant \dots \leqslant p_n.$$

Burada $n = 0$ olabilir, ve bu durumda $p_1 \dots p_n = 1$.

Kanıt. Sayma sayıları iyisıralandığından ve sayma sayılarında

$$a \mid b \implies a \leqslant b$$

olduğundan

- 1'den büyük olan her sayma sayısının asal bir çarpanı vardır;
- her sayma sayısı, asalların bir çarpımıdır.

Öklid Lemması sayesinde bu çarpım tektir. □

Teorem.

$$ab = \text{ebob}(a, b) \cdot \text{ekok}(a, b).$$

5 Aritmetik Fonksiyonlar

Tanım kümesi $\mathbb{N}$ olan bir fonksiyona **aritmetik** denir. Normalde değer kümesi $\mathbb{C}$'dir.

Örnek. Aşağıdaki eşitliklerinin tanımladığı σ, τ, φ, id, 1, ve ε aritmetik fonksiyonları vardır.

$$
\begin{aligned}
\sigma(n) &= \textstyle\sum_{d|n} d,\\
\tau(n) &= \textstyle\sum_{d|n} 1 = |\{x \in \mathbb{N} \colon x \mid n\}|,\\
\varphi(n) &= |{\mathbb{Z}_n}^{\times}| = |\{x \in \mathbb{Z} \colon 0 \leqslant x < n \wedge \operatorname{ebob}(x,n) = 1\}|,\\
\mathrm{id}(n) &= n,\\
1(n) &= 1,\\
\varepsilon(1) &= 1 \wedge \varepsilon(n+1) = 0,
\end{aligned}
$$

O zaman p asal olduğunda

$$
\begin{aligned}
\sigma(p^n) &= 1 + p + \cdots + p^n = (p^{n+1} - 1)/(p-1),\\
\tau(p^n) &= n + 1,\\
\varphi(p^n) &= p^n - p^{n-1} = p^n \cdot (1 - 1/p).
\end{aligned}
$$

Tanım. Bir f aritmetik fonksiyonu için, eğer $\operatorname{ebob}(a,b) = 1$ olduğunda

$$f(ab) = f(a) \cdot f(b)$$

ise, o zaman f **çarpımsaldır.**

Örneğin id, 1, ve ε carpımsaldır. Ayrıca f çarpımsal olduğunda,

- eğer $f(1) = 0$ ise, o zaman $f(n) = f(n \cdot 1) = f(n) \cdot f(1) = 0$;
- eğer $f(1) \neq 0$ ise, o zaman $f(1) = 1$, çünkü $f(1) \cdot f(1) = f(1)$.

Teorem. φ *çarpımsaldır.*

Kanıt. Çin Kalan Teoremi sayesinde $\text{ebob}(a, b) = 1$ ise

$$\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b,$$

dolayısıyla

$$\mathbb{Z}_{ab}{}^{\times} \cong \mathbb{Z}_a{}^{\times} \times \mathbb{Z}_b{}^{\times},$$

ve sonuç olarak

$$\varphi(ab) = |\mathbb{Z}_{ab}{}^{\times}| = |\mathbb{Z}_a{}^{\times}| \cdot |\mathbb{Z}_b{}^{\times}| = \varphi(a) \cdot \varphi(b). \qquad \square$$

Aritmetiğin Temel Teoremi sayesinde her n için, n'nin tüm p asal bölenleri için,

$$n = \sum_{p|n} p^{n(p)}$$

sağlayan $n(p)$ üsleri vardır. O zaman

$$\varphi(n) = \prod_{p|n} \varphi(p^{n(p)}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Eğer f ve g aritmetik fonksiyon ise, o zaman bunların $f * g$ **Dirichlet konvolüsyonü**

$$(f * g)(n) = \sum_{ab=n} f(a) \cdot g(b) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right)$$

kuralı tarafından tanımlanır. Örneğin

$$\sigma = \mathrm{id} * 1$$

ve

$$\tau = 1 * 1.$$

Örnek. (Bunu kullanmayacağız.) *Riemann zeta fonksiyonu,*

$$\zeta(s) = \sum_{n\in\mathbb{N}} 1/n^s$$

tarafından tanımlanır, ve bu durumda

$$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_p 1/(1-p^{-s}).$$

Daha genelde her f aritmetik fonksiyonu için $\sum_{n\in\mathbb{N}} f(n)/n^s$ *Dirichlet serisi* vardır, ve

$$\left(\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}\right) \sum_{n\in\mathbb{N}} \frac{g(n)}{n^s} = \sum_{n\in\mathbb{N}} \frac{(f*g)(n)}{n^s}.$$

Teorem. *Eğer f ve g çarpımsal ise, o zaman $f * g$ de çarpımsaldır.*

Kanıt. Aritmetiğin Temel Teoremi sayesinde $\operatorname{ebob}(a, b) = 1$ ise, o zaman birebir ve örten olarak

$$(c, e) \mapsto ce \colon \{c \colon c \mid a\} \times \{e \colon e \mid b\} \to \{d \colon d \mid ab\}.$$

Bundan dolayı

$$
\begin{aligned}
(f*g)(ab) &= \sum_{d|ab} f(d)\cdot g\left(\frac{ab}{d}\right) \\
&= \sum_{c|a}\sum_{e|b} f(ce)\cdot g\left(\frac{ab}{ce}\right) \\
&= \sum_{c|a}\sum_{e|b} f(c)\cdot f(e)\cdot g\left(\frac{a}{c}\right)\cdot g\left(\frac{b}{e}\right) \\
&= \sum_{c|a} f(c)\cdot g\left(\frac{a}{c}\right)\sum_{e|b} f(e)\cdot g\left(\frac{b}{e}\right) \\
&= \left(\sum_{c|a} f(c)\cdot g\left(\frac{a}{c}\right)\right)\sum_{e|b} f(e)\cdot g\left(\frac{b}{e}\right) \\
&= (f*g)(a)\cdot(f*g)(b).
\end{aligned}
$$

□

Örneğin σ ve τ çarpımsaldır, dolayısıyla

$$\sigma(n) = \prod_{p|n}(p^{n(p)+1} - 1)/(p-1),$$
$$\tau(n) = \prod_{p|n}(n(p)+1).$$

Eğer $\sigma(n) = 2n$ ise, o zaman n **mükemmeldir.**

Teorem. *Çift mükemmel bir sayı olmak için,* $2^n - 1$ *farkının asal olduğu bir*

$$2^{n-1} \cdot (2^n - 1)$$

çarpımı olmak, gerek ve yeter bir koşuldur.

Kanıt. Eğer $2^n - 1$ asal ise, o zaman

$$\sigma(2^{n-1} \cdot (2^n - 1)) = \sigma(2^{n-1}) \cdot \sigma(2^n - 1) = (2^n - 1) \cdot 2^n,$$

dolayısıyla $2^{n-1} \cdot (2^n - 1)$ mükemmeldir. (Öklid bunu gösterdi.) Tersine a tek olduğunda $2^{n-1} \cdot a$ mükemmel ise, o zaman

$$2^n \cdot a = \sigma(2^{n-1} \cdot a) = (2^n - 1) \cdot \sigma(a),$$

dolayısıyla $2^n \mid \sigma(a)$, ve bu durumda bir b için

$$2^n \cdot b = \sigma(a).$$

Öyleyse

$$a = (2^n - 1) \cdot b = \sigma(a) - b,$$

ve sonuç olarak

$$\sigma(a) = a + b.$$

Ayrıca b, a'nın bir bölenidir. Eğer $n > 1$ ise, o zaman $b < a$, ve bu durumda $b = 1$ ve a asaldır. □

Teorem. $*$ *işlemi değişmelidir ve birleşmelidir, ve her aritmetik* f *için*

$$f * \varepsilon = f,$$

ve $f(1) \neq 0$ *ise*

$$f * g = \varepsilon$$

koşulunu sağlayan bir g *vardır. Bunlardan dolayı* 1*'de* 0 *olmayan aritmetik fonksiyonlar,* $*$ *altında abelyan bir grup oluşturur.*

Kanıt. $*$ işlemi değişmelidir çünkü

$$\begin{aligned}
(g * f)(n) &= \textstyle\sum_{ab=n} g(a) \cdot f(b) && \text{[tanım]} \\
&= \textstyle\sum_{ab=n} f(b) \cdot g(a) && [\,\cdot \text{ değişmeli}] \\
&= \textstyle\sum_{ba=n} f(b) \cdot g(a) && [\,\cdot \text{ değişmeli}] \\
&= (f * g)(n). && \text{[tanım]}
\end{aligned}$$

İşlemin birleşmeli olduğu ve $f * \varepsilon = f$, **alıştırmadırlar.** Sonda f verildiğinde $f(1) \neq 0$ ise, özyineleme ile

$$g(1) = \frac{1}{f(1)}$$

ve $n > 1$ olmak üzere

$$g(n) = -\sum_{ab=n \wedge a \neq 1} f(a) \cdot g(b)/f(1)$$

olsun. O zaman $f * g = \varepsilon$. $\square$

Teorem. *Eğer $f * g = \varepsilon$ ve f çarpımsal ise, o zaman g de çarpımsaldır.*

Kanıt. Tümevarım kullanacağız. Birden kesin büyük olan her m için, $m = ab$ ve $\text{ebob}(a, b) = 1$ olduğunda,

$$g(m) = g(a) \cdot g(b)$$

göstereceğiz. Eğer bir n için n'nin m özbölenleri için iddia doğru ise, şimdi $n = ab$ ve $\text{ebob}(a, b) = 1$ olsun. o zaman

$$\begin{aligned} 0 &= \varepsilon(n) \\ &= (f * g)(n) \\ &= \textstyle\sum_{d|n} f(d) \cdot g(n/d) \\ &= \textstyle\sum_{c|a} \sum_{e|b} f(ce) \cdot g(ab/ce). \end{aligned}$$

Buna $f(1) \cdot (g(a)g(b) - g(ab))$ ekleyerek

$$\begin{aligned} f(1) \cdot (g(a) \cdot g(b) - g(ab)) &= \sum_{c|a} \sum_{e|b} f(c) \cdot f(e) \cdot g(a/c) \cdot (b/e) \\ &= (f * g)(a) \cdot (f * g)(b) \\ &= 0 \end{aligned}$$

ederiz, dolayısıyla $g(a) \cdot g(b) = g(ab)$. □

Şimdi tanıma göre μ,

$$1 * \mu = \varepsilon$$

eşitliğini sağlayan aritmetik fonksiyonu olsun.

Teorem. μ *çarpımsaldır,* $\mu(p^2) = 0$, *ve*

$$p_1 < \cdots < p_s \implies \mu(p_1 \cdots p_s) = (-1)^s.$$

Teorem (Möbius Tersleme Teoremi)**.**

$$F = \sum_{d|n} f(d) \implies f(n) = \sum_{d|n} F(d) \cdot \mu(n/d).$$

Kanıt. $F = f * 1$ ise

$$F * \mu = (f * 1) * \mu = f * (1 * \mu) = f * \varepsilon = f. \qquad \square$$

Teorem. $\varphi * 1 = \mathrm{id}$, *yani*

$$\sum_{d|n} \varphi(d) = n.$$

Kanıt. Her taraf çarpımsaldır ve

$$(\varphi * 1)(p^s) = \sum_{0 \leqslant k \leqslant s} \varphi(p^k) = 1 + \sum_{0 < k \leqslant s} (p^k - p^{k-1}) = p^s. \qquad \square$$

Teorem. $*$ *altında üreteçleri* 1 *ve* id *olan grup*

- $\mathbb{Z} \times \mathbb{Z}$ *çarpımına izomorftur,*
- τ, σ, φ, *ve* μ *fonsiyonlarını içerir.*

Ayrıca id*'in tersi* $\mathrm{id} \cdot \mu$.

Alıştırmalar. Aşağıdaki eşitlikleri kanıtlayın.

$$\prod_{d|n} d = n^{\tau(n)}/2.$$

$$\sum_{d|n} 1/d = \sigma(n)/n.$$

$$\sum_{d|n} d \cdot \mu(d) = \prod_{p|n} (1-p).$$

$$\sum_{d|n} \tau(d) \cdot \mu(d) = \prod_{p|n} -1.$$

Ayrıca $*$'a göre φ'nin tersini bulun.

6 Karesel Kalıntılar

Tek ve asal bir sayı p olarak yazılsın. O zaman

$$\mathbb{Z}_p{}^{\times} = \mathbb{Z}_p \setminus \{0 + (p)\},$$

yani $\mathbb{Z}_p$ halkasında çarpmaya göre $0 + (p)$ elemanı hariç her elemanın tersi vardır. Kısaca $\mathbb{Z}_p$ bir cisimdir. Ayrıca $\mathbb{Z} \setminus (p)$, $\mathbb{Z}$'nin

- çarpma işlemi altında kapalıdır,
- çarpımsal etkisiz elemanını (yani 1'i) içerir;

kısaca $\mathbb{Z} \setminus (p)$, bir "birliktir" (*monoid*) ve $\mathbb{Z}$'nin bir altbirliğidir. Homomorfizma olarak

$$x \mapsto x + (p) \colon \mathbb{Z} \setminus (p) \to {\mathbb{Z}_p}^{\times}.$$

Teorem. 0 *olmayan, katsayıları* $\mathbb{Z}$*'den gelen, başkatsayısı* p*'nin bir katı olmayan bir* f *polinomunun derecesi* n *ise, o zaman*

$$|\{x + (p) \colon f(x) \equiv 0 \pmod{p}\}| \leqslant n.$$

Kanıt. Tümevarım.

1. Eğer $n = 0$ ise, o zaman f sabittir ve $f \not\equiv 0 \pmod{p}$.
2. Bir m için
   - iddia n'nin m olduğu durumda doğru,
   - f'nin derecesinin $m + 1$ olduğu $f(a) \equiv 0 \pmod{p}$

olsun. O zaman bir g polinomu için

$$f(x) \equiv g(x) \cdot (x - a) \pmod{p}.$$

Bu durumda eğer $f(b) \equiv 0 \pmod{p}$ ise, o zaman

$$p \mid g(b) \cdot (b - a).$$

Öklid Lemması sayesinde

$$a \not\equiv b \pmod{p} \implies g(b) \equiv 0 \pmod{p}. \qquad \square$$

Örnek. Teoremin özel bir durumu olarak

$$x^2 \equiv 1 \iff x \equiv \pm 1 \pmod{p}.$$

Asal olmayan bir modülüse göre teorem yanlış olabilir:

$$x^2 \equiv 1 \iff x \equiv \pm 1, \pm 3 \pmod{8}.$$

Şimdi

$$\frac{p-1}{2} = \varpi$$

olsun (bu harf, yazılmış bir π harfidir).

Teorem (Wilson)**.** $(p-1)! \equiv -1 \pmod{p}$.

Kanıt. $\{2, \ldots, p-2\}$ kümesinin

$$x \neq x' \ \ \& \ \ x \cdot x' \equiv 1 \pmod{p}$$

koşulunu sağlayan bir $x \mapsto x'$ permütasyonu vardır, ve $x'' = x$, dolayısıyla

$$\{2, \ldots, p-2\} = \{a_1, a_1{}', \ldots, a_{\varpi-1}, a_{\varpi-1}{}'\}$$

yazılabilir. Bu durumda

$$(p-1)! \equiv 1 \cdot a_1 \cdot a_1{}' \cdots a_{\varpi-1} \cdot a_{\varpi-1}{}' \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}. \ \square$$

Örnek. $10! \equiv 1 \cdot (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10 \equiv 10 \equiv -1 \pmod{11}$.

Tanım. G bir grup ise $G^2 = \{g^2 \colon g \in G\}$ olsun; özellikle

$$\{x^2 \colon x \in {\mathbb{Z}_p}^\times\} = ({\mathbb{Z}_p}^\times)^2$$

olsun. O zaman $a \in \mathbb{Z} \setminus (p)$ olduğunda,

- $a + (p) \in ({\mathbb{Z}_p}^\times)^2$ ise a, p modülüsüne göre bir **karesel kalıntıdır** (*quadratic residue*), ve

  $$\left(\frac{a}{p}\right) = 1$$

  yazılır;

- diğer durumda a, p'e göre bir **karesel olmayan kalıntıdır** (*quadratic nonresidue*), ve

  $$\left(\frac{a}{p}\right) = -1$$

  yazılır.

Burada (a/p) bir **Legendre sembolüdür.**

Teorem. *$a \in \mathbb{Z} \setminus (p)$ olduğunda*

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

kalandaşlığının çözülebilmesi için gerek ve yeter bir koşul,

$$\left(\frac{b^2 - 4ac}{p}\right) = 1.$$

Böylece **ikinci dereceden (*quadratic*) kalandaşlıklar çözmek için, karesel kalıntıların farkında olmak zorundayız.**

Teorem. *Homomorfizma olarak $x \mapsto (x/p) \colon \mathbb{Z} \setminus (p) \to \mathbb{Z}^\times$, yani*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Kanıt. İlk olarak ${\mathbb{Z}_p}^\times$ değişmeli olduğundan

$$({\mathbb{Z}_p}^\times)^2 < {\mathbb{Z}_p}^\times,$$

yani $({\mathbb{Z}_p}^\times)^2$ bir gruptur ve ${\mathbb{Z}_p}^\times$ grubunun bir altgrubudur. Ayrıca homomorfizma olarak

$$x \mapsto x^2 \colon \mathbb{Z}_p \to ({\mathbb{Z}_p}^\times)^2.$$

Bu homomorfizmanın çekirdeği $\langle -1 + (p) \rangle$, dolayısıyla

$${\mathbb{Z}_p}^\times / ({\mathbb{Z}_p}^\times)^2 \cong \mathbb{Z}_2.$$

Ayrıca

$$\mathbb{Z}^\times \cong \mathbb{Z}_2.$$

Sonunun *izomorfizma* olduğu üç homomorfizma vardır:

$$\begin{aligned}
x \mapsto x + (p) \quad &: \mathbb{Z} \setminus (p) \to {\mathbb{Z}_p}^\times, \\
x \mapsto x \cdot ({\mathbb{Z}_p}^\times)^2 &: {\mathbb{Z}_p}^\times \to {\mathbb{Z}_p}^\times / ({\mathbb{Z}_p}^\times)^2, \\
x \mapsto h(x) \quad &: {\mathbb{Z}_p}^\times / ({\mathbb{Z}_p}^\times)^2 \to \mathbb{Z}^\times.
\end{aligned}$$

O zaman

$$\left(\frac{a}{p}\right) = h\Big(\big(a+(p)\big)\cdot(\mathbb{Z}_p{}^{\times})^2\Big),$$

yani $x \mapsto (x/p)$, üç homomorfizmanın bileşkesidir. □

Teorem.

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4.$$

Kanıt. Wilson Teoremi sayesinde

$$-1 \equiv 1\cdot(p-1)\cdot 2\cdot(p-2)\cdots\varpi\cdot(p-\varpi) \equiv (-1)^{\varpi}(\varpi!)^2 \pmod p.$$

Eğer $p \equiv 1 \pmod 4$ ise, o zaman ϖ çifttir, ve sonuç olarak

$$(\varpi!)^2 \equiv -1 \pmod p.$$

Özellikle $(-1/p) = 1$. Tersine $a^2 \equiv -1 \pmod p$ ise Fermat Teoremi sayesinde

$$1 \equiv a^{p-1} \equiv (a^2)^{\varpi} \equiv (-1)^{\varpi} \pmod p,$$

dolayısıyla ϖ çiftir ve $p \equiv 1 \pmod 4$. $\square$

Teorem aşikâr değildir:

Teorem. $\{p\colon p \equiv 3 \pmod 4\}$ *ve* $\{p\colon p \equiv 1 \pmod 4\}$ *kümelerinin her biri sonsuzdur.*

Kanıt. Verilen kümelerden hiçbiri, elemanları asal olan, sonlu olan bir $\{q_1, \ldots, q_n\}$ kümesi tarafından kapsanmaz. Zira:

- $4q_1 \cdots q_n - 1$ farkının asal bölenlerinden
  - hiçbiri $\{q_1, \ldots, q_n\}$ kümesindedır,
  - en az biri
    $$x \equiv 3 \pmod 4$$
    kalandaşlığını sağlar, çünkü $4q_1 \cdots q_n - 1$ farkının kendisi sağlar.

- Eğer $p \mid (2q_1 \cdots q_n)^2 - 1$ ise, o zaman $p \notin \{q_1, \ldots, q_n\}$, ama p'ye göre -1 bir karesel kalıntıdır, dolayısıyla $p \equiv 1 \pmod 4$. □

Teorem (Euler Kriteri)**.**

$$\left(\frac{n}{p}\right) \equiv n^{\varpi} \pmod p.$$

Kanıt. Liseli cebirden

$$x^{p-1} - 1 = (x^{\varpi} - 1)(x^{\varpi} + 1).$$

Fermat Teoremi sayesinde, $\{1, \ldots, p-1\}$ kümesinin

- tümü,
$$x^{p-1} \equiv 1 \pmod p$$
kalandaşlığını sağlar, ve

- yarısı, karesel kalıntı olduğundan,

$$x^{\varpi} - 1 \equiv 0 \pmod{p}$$

  kalandaşlığını sağlar, dolayısıyla
- diğer yarısı, p modülüsü asal olduğundan,

$$x^{\varpi} + 1 \equiv 0 \pmod{p}$$

  kalandaşlığını sağlar. □

7 İlkel Kökler

Örnek. Eğer $\mathbb{Z}_n{}^{\times} = \langle a + (n) \rangle$ ise, o zaman a, n'nin **ilkel bir köküdür** (*primitive root*).

Teorem. *Her asal sayının ilkel kökü vardır.*

Kanıt. $\mathbb{Z}_n{}^{\times}$ grubu, sonlu ve değişmeli gruplardan biri olduğundan, bu grupların sınıflandırması sayesinde

$$\mathbb{Z}_n{}^{\times} \cong \mathbb{Z}_{a(1)} \oplus \mathbb{Z}_{a(2)} \oplus \cdots \oplus \mathbb{Z}_{a(m)} \ \ \& \ \ a(m) \mid \cdots \mid a(2) \mid a(1) \mid \varphi(n)$$

koşullarını sağlayan $a(1), a(2), \ldots, a(m)$ vardır. O zaman ${\mathbb{Z}_n}^\times$ grubunun her elemanı

$$x^{a(1)} = 1$$

polinomunu sağlar. Eğer n bir p asalı ise, o zaman $a(1) = \varphi(n)$ olmalı ve sonuç olarak

$${\mathbb{Z}_p}^\times \cong \mathbb{Z}_{p-1}. \qquad \square$$

Bunun ile asal modülüslere göre $x^a \equiv b$ ve $a^x \equiv b$ kalandaşlıkları çözülebilir.

Örnek. Aşağıdaki tablodan 2, 3, 4, ve 5 sayılarından hiçbiri 41'in ilkel bir kökü değildir.

k	1	2	3	4	5	6	7	8	9	10	(mod 40)
2^k	2	4	8	16	-9	-18	5	10	20	-1	(mod 41)
3^k	3	9	-14	-1							(mod 41)

Nitekim 6, 41'in ilkel bir köküdür:

k	1	2	3	4	5	6	7	8	9	10	$\pmod{40}$
6^k	6	-5	11	-16	-14	-2	-12	10	19	-9	$\pmod{41}$
6^{10+k}	-13	4	-17	-20	3	18	-15	-8	-7	-1	$\pmod{41}$
6^{20+k}	-6	5	-11	16	14	2	12	-10	-19	9	$\pmod{41}$
6^{30+k}	13	-4	17	20	-3	-18	15	8	7	1	$\pmod{41}$

O zaman bir $x^a \equiv b \pmod{41}$ kalandaşlığını çözmek için $x \equiv 6^y \pmod{41}$ olsun. Bu durumda

$$
\begin{aligned}
& x^{456} \equiv 160 && \pmod{41} \\
\iff\ & x^{16} \equiv -4 && \pmod{41} \\
\iff\ & 6^{16y} \equiv 6^{32} && \pmod{41} \\
\iff\ & 16y \equiv 32 && \pmod{40} \\
\iff\ & 2y \equiv 4 && \pmod{5} \\
\iff\ & y \equiv 2 && \pmod{5} \\
\iff\ & y \equiv 2, 7, 12, 17, 22, 27, 32, 27 && \pmod{40}.
\end{aligned}
$$

Sonuç olarak tablodan

$$x^{456} \equiv 160 \iff x = \pm 4, \pm 5, \pm 12, \pm 15 \pmod{41}.$$

Bunu **kontrol edelim.** İlk olarak

- $456 \equiv 16 \pmod{40}$,
- $160 \equiv -4 \pmod{41}$ çünkü $41 \cdot 4 = 164$,

- $4^{16} \equiv 16^8 \equiv 256^4 \equiv 10^4 \equiv 100^2 \equiv 18^2 \equiv 324 \equiv -4 \pmod{41}$ çünkü

$$41 \cdot 6 = 246 = 256 - 10,$$
$$41 \cdot 2 = 82 = 100 - 18,$$
$$41 \cdot 8 = 328 = 324 + 4.$$

- Bu şekilde

$$4^{456} \equiv 4^{16} \equiv -4 \equiv 160 \pmod{41}.$$

Diğer çözümler, 4'ten aşağıdaki gibi çıkar. Önce

$$6^{16y} \equiv 1 \pmod{41} \iff 16y \equiv 0 \pmod{40} \iff 5 \mid y,$$

ve $40/5 = 8$, dolayısıyla $x^{16} \equiv 1 \pmod{41}$ kalandaşlığının çözümleri, 41'e göre 6^5 kuvvetinin 8 kalandaş olmayan kuvvetidir. Bu şekilde

$$\{x \in {\mathbb{Z}_{41}}^{\times} : x^{16} = 1\} = \langle 6^5 + (41) \rangle$$

ve bu grubun mertebesi 8'dir. Şimdi ebob$(8,3)=1$ olduğundan $6^{15}+(41)$ de grubun bir üretecidir. Ayrıca $6^{15}\equiv 3 \pmod{41}$, ve zaten bildiğimiz gibi 41'e göre 3'ün kuvvetleri, sırasıyla $3, 9, -14, -1, -3, -9, 14$, ve 1; kısaca $\pm 1, \pm 3, \pm 9, \pm 14$. Son olarak

$$\pm 3 \cdot 4 \equiv \pm 12 \;\; \& \;\; \pm 9 \cdot 4 \equiv \mp 5 \;\; \& \;\; \pm 14 \cdot 4 \equiv \pm 15 \pmod{41},$$

Böylece yeni bir şekilde $x^{16} \equiv 1 \pmod{41}$ kalandaşlığının çözümlerini bulduk.

Başka bir alıştırma için

$$\begin{aligned}
46^x \equiv 5 &\iff (-5)^x \equiv 5 && \pmod{41}\\
&\iff 6^{2x} \equiv 6^{22} && \pmod{41}\\
&\iff 2x \equiv 22 && \pmod{40}\\
&\iff x \equiv 11 && \pmod{20}\\
&\iff x \equiv 11, 31 && \pmod{40}.
\end{aligned}$$