Sayılar Kuramı Özeti

David Pierce

10 Haziran 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

Bu bölümde sayma sayılarının ökulda öğrenilmiş özelliklerini varsayıyoruz. Bölüm 2'de bu özellikleri bir postulattan elde edeceğiz.

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 1 (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:*

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

Alıştırma 1. Tersine n, ve $t_1, \ldots, t_n$, ve a_{n+1} sayılarını seçerek a_1 ve a_2 için değerler bulup Bézout Denklemini çözün.

Yukarıdaki durumda

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

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.

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 1. $\beta_1 = \sqrt{41}$ 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 2. *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

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

Alıştırma 2. Farklı d'ler için Pell denklemini çözün.

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 2. $a_2 < 1000$ 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 1. Sayma sayıları kümesi

$$\mathbb{N},$$

ve $\mathbb{N}$'nin en küçük elemanı

$$1,$$

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

$$n + 1.$$

Teorem 3 (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 4 (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 2.

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

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

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

eşitlikler de gösterilir. □

Alıştırma 3. Kanıtın ayrıntıların verin.

Teorem 6.

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

Alıştırma 4. Teoremi kanıtlayın.

Teorem 7. *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 3.

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

3 Kalandaşlık

Tanım 3.

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

Okulda öğrendimiz gibi toplama ve çarpma, $\mathbb{Z}$'de tanımlanır. Sonuç olarak $\mathbb{Z}$, **değişmeli bir halka** olur.

Tanım 4. $n \in \mathbb{N}$ olduğunda

$$\{nx \colon x \in \mathbb{Z}\} = n\mathbb{Z} = (n)$$

olsun. Bu küme $\mathbb{Z}$'nin bir ideali olduğundan değişmeli bir halka olarak

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

tanımlanır. Şimdi $\mathbb{Z}$'de

$$(b) \subseteq (a) \iff a \mid b$$

olsun; bu durumda a, b'yi **böler.** Şimdi $n \in \mathbb{N}$ olduğunda

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

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

Sonuç olarak

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

ve ayrıca

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

Lemma 1. *$\mathbb{Z}$'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 8. *Bir*

$$ax \equiv b \pmod{n}$$

kalandaşlığının çözümleri varsa, o zaman aşağıdaki kuralları kullanarak çözümleri bulabiliriz. İlk olarak

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

Ayrıca Lemma 1'den

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

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

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

formülünü sağlayan c *vardır, ve bu durumda*

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

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 9 (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, Teorem 8'den

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

kalandaşlığını sağlayan b_i *vardır, ve sonuç olarak*

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

sisteminin çözümü,

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

Örnek 4. Yukarıdaki biçimde Çin Kalan Teoremi, lineer kalandaşlık sistemlerini çözmek için genel bir yöntem verir. İki küçük modülüs için çözümler bir tablodan elde edilebilir. Örnegin

$$x \equiv 5 \pmod 9 \ \& \ x \equiv 10 \pmod{16} \iff x \equiv 122 \pmod{144}.$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	81	18	99	36	117	54	135	72	9	90	27	108	45	126	63
1	64	1	82	19	100	37	118	55	136	73	10	91	28	109	46	127
2	128	65	2	83	20	101	38	119	56	137	74	11	92	29	110	47
3	48	129	66	3	84	21	102	39	120	57	138	75	12	93	30	111
4	112	49	130	67	4	85	22	103	40	121	58	139	76	13	94	31
5	32	113	50	131	68	5	86	23	104	41	122	59	140	77	14	95
6	96	33	114	51	132	69	6	87	24	105	42	123	60	141	78	15
7	16	97	34	115	52	133	70	7	88	25	106	43	124	61	142	79
8	80	17	98	35	116	53	134	71	8	89	26	107	44	125	62	143

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.** Bu notlarda p her zaman asal olacak.

Teorem 10 (Öklid Lemması)**.**

$$p \mid ab \ \ \& \ \ p \nmid a \implies p \mid b.$$

Kanıt. Sayfa 29'daki Lemma 1. □

Teorem 11 (Fermat)**.** *Eğer $p \nmid a$ ise, o zaman $a^{p-1} \equiv 1 \pmod{p}$.*

Fermat Teoremine üç kanıt vereceğiz.

Kanıt 1. Teorem 8 sayesinde $p \nmid a$ ise $\mathbb{Z}_p$ halkasında $a + (p)$ elemanının çarpımsal tersi vardır. Bu durumda $x + (p) \mapsto ax + (p)$ fonksiyonu

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

kümesinin bir permütasyonudur. Bundan dolayı

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

Şimdi Teorem 8'i kullanın. □

Kanıt 2. Bir R değişmeli halkasının çarpmaya göre terslenir elemanları bir $R^\times$ grubunu oluşturduğundan, Kanıt 1'deki gibi

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

Özellikle

$$|\mathbb{Z}_p{}^\times| = p - 1.$$

Gruplar Kuramından Lagrange Teoremini kullanın. □

Kanıt 3. Binom Açılımına göre

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

olduğunda

$$(a+1)^p = a^p + \sum_{i \leqslant k < p} \binom{p}{k} a^{p-k} + 1.$$

Özellikle

$$k!(p-k)! \mid p!.$$

Ayrıca $1 \leqslant k < p$ ise

$$\text{ebob}(k!(p-k)!, p) = 1$$

olduğundan, Lemma 1 sayesinde

$$k!(p-k)! \mid (p-1)!,$$

dolayısıyla

$$p \mid \binom{p}{k},$$

ve sonuç olarak

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

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

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

□

Sonuç olarak

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

Alıştırma 5. Birkaç tek p için

$$0 \leqslant x \leqslant p-1 \ \& \ 1234^{5678} \equiv x \pmod{p}$$

veya

$$-\frac{p-1}{2} \leqslant x \leqslant \frac{p-1}{2} \ \& \ 1234^{5678} \equiv x \pmod{p}$$

gibi sistemler çözün.

Fermat Teoreminin Kanıt 2'si ile daha genel bir teorem elde edilir (Bölüm 5'e bakın):

Teorem 12 (Euler)**.** $|\mathbb{Z}_n{}^{\times}| = \varphi(n)$ *olduğunda,* $\text{ebob}(a,n) = 1$ *ise*

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

Teorem 13 (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 14.

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

5 Aritmetik Fonksiyonlar

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

Örnek 5. 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 5. 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 15. 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 6. (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 16. *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

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

$$= \left(\sum_{c|a} f(c) \cdot g\left(\frac{a}{c}\right) \right) \sum_{e|b} f(e) \cdot g\left(\frac{b}{e}\right)$$
$$= (f * g)(a) \cdot (f * g)(b). \qquad \square$$

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 17. *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 18. $*$ *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 $f * g = \varepsilon$. □

Alıştırma 6. $*$ işleminin birleşmeli ve $f * \varepsilon = f$ eşitliğinin doğru olduğunu gösterin.

Teorem 19. *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

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

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

Şimdi tanıma göre μ,

$$1*\mu=\varepsilon$$

eşitliğini sağlayan aritmetik fonksiyonu olsun.

Teorem 20. μ *çarpımsaldır,* $\mu(p^2)=0$*, ve*

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

Teorem 21 (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 22. $\varphi * 1 = \mathrm{id}$, *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 23. $*$ *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* $\mathrm{id} \cdot \mu$.

Alıştırma 7. Aşağıdaki eşitlikleri kanıtlayın.

$$\prod_{d|n} d = n^{\tau(n)}/2, \qquad \sum_{d|n} d \cdot \mu(d) = \prod_{p|n}(1-p),$$

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

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

6 Karesel Kalıntılar

Tek ve asal bir sayı p olarak yazılsın. Fermat Teoremi (yani sayfa 34'teki Teorem 11) için ilk iki kanıtımızdaki gibi $\mathbb{Z}_p$ değişmeli 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,
- $\mathbb{Z}$'nin çarpımsal etkisiz elemanını (yani 1'i) içerir;

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

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

Özellikle

$$xy + (p) = (x + (p))(y + (p)).$$

Teorem 24.

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

Kanıt. Eğer $a^2 \equiv 1 \pmod{p}$ ise, o zaman

$$p \mid a^2 - 1,$$

dolayısıyla

$$p \mid (a+1)(a-1).$$

Öklid Lemması (yani sayfa 33'teki Teorem 10) sayesinde

$$p \mid a + 1 \vee p \mid a - 1.$$ □

Örnek 7. Asal olmayan bir modülüse göre Teorem 24 yanlış olabilir:

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

Teorem 25 (Wilson)**.** $(p-1)! \equiv -1 \pmod{p}$.

Kanıt. $\{1, \ldots, p-1\}$ kümesinin

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

koşulunu sağlayan bir $x \mapsto x'$ permütasyonu vardır. O halde $x'' = x$. Ayrıca Teorem 24 sayesinde

$$1 < x < p-1 \implies x' \neq x.$$

Bundan dolayı

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

olduğunda (buradaki ϖ harfi, yazılmış bir π harfidir),

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

yazılabilir. Bu durumda

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

Alıştırma 8. Özel durumlarda Wilson Teoremini kanıtlayın, örneğin $p = 11$ ise

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

Tanım 6. Eğer G çarpımsal bir grup ise

$$\{g^2 \colon g \in G\} = G^2$$

olsun. Şimdi $a \in \mathbb{Z} \setminus (p)$ 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 26. *$a \in \mathbb{Z} \setminus (p)$ olduğunda*

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

kalandaşlığının çözülebilmesi için gerek ve yeter bir koşul,

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

Kanıt.

$$\begin{aligned} ax^2 + bx + c \equiv 0 &\iff 4a^2x^2 + 4abx \equiv -4ac \\ &\iff (2ax + b)^2 \equiv b^2 - 4ac. \end{aligned}$$

□

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

Örnek 8.

x	±1	±2	±3	±4	±5	±6	±7	±8	(mod 17)
x^2	1	4	-8	-1	8	2	-2	-4	(mod 17)

1.

$$\begin{aligned} 5x^2 + 6x + 7 \equiv 0 &\iff (5x)^2 + 2 \cdot 3 \cdot 5x + 9 + 35 \equiv 9 \\ &\iff (5x + 3)^2 \equiv -26 \equiv 8 \end{aligned}$$

$$\iff 5x + 3 \equiv \pm 5$$
$$\iff 5x \equiv 2, -8$$
$$\iff x \equiv 14, -56 \equiv -3, -5 \pmod{17}.$$

Kontrol:

$$5(-3)^2 + 6(-3) + 7 = 45 - 18 + 7 = 34 = 17 \cdot 2,$$
$$5(-5)^2 + 6(-5) + 7 = 125 - 30 + 7 = 102 = 17 \cdot 6.$$

2.
$$5x^2 + 6x + 8 \equiv 0 \pmod{17}$$
kalandaşlığının çözümü yoktur çünkü
$$6^2 - 4 \cdot 5 \cdot 8 = 36 - 160 = -124 \equiv -5 \pmod{17}.$$

Örnek 9.

x	± 1	± 2	± 3	± 4	± 5	± 6	± 7	± 8	(mod 19)
x^2	1	4	9	-3	6	-2	-8	7	(mod 19)

Alıştırma 9. Bazı ikinci dereceden kalandaşlıklar yazıp çözün.

Teorem 27. *Örten bir homomorfizma olarak*

$$x \mapsto \left(\frac{x}{p}\right) : \mathbb{Z} \smallsetminus (p) \to \mathbb{Z}^{\times}.$$

Özellikle

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

Kanıt. İlk olarak

$$\mathbb{Z}_p{}^{\times} = G, \qquad\qquad G^2 = H$$

olduğunda, örten bir homomorfizma olarak

$$x + (p) \mapsto x^2 + (p) \colon G \to H.$$

Teorem 24'ten bu homorfizmanın çekirdeği,

$$\langle -1 + (p) \rangle.$$

Bu grubun mertebesi 2 olduğundan

$$[G : H] = 2.$$

Sonuç olarak $a \in G \setminus H$ olduğunda

$$G/H = \{H, aH\}.$$

Şimdi

$$h(H) = 1, \qquad h(aH) = -1$$

olduğunda, izomorfizma olarak

$$h \colon G/H \to \mathbb{Z}^{\times}.$$

O zaman $x + (p) = g$ olduğunda

$$\left(\frac{x}{p}\right) = h(gH).$$

Böylece fonksiyon olarak $x \mapsto (x/p)$,

$$h \circ (g \mapsto gH) \circ (x \mapsto x + (p))$$

bileşkesidir, ve bu bileşkede her fonksiyon bir homomorfizmadır. □

Teorem 28.

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

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 çift olmalı ve $p \equiv 1 \pmod 4$. □

Teorem aşikâr değildir:

Teorem 29. $\{p\colon p \equiv 3 \pmod 4\}$ *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

$$x \equiv 1 \pmod 4$$

kalandaşlığını sağlar. □

Teorem 28, sonraki teoremin özel bir durumudur.

Teorem 30 (Euler Kriteri)**.**

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

Kanıt. Eğer $n \equiv a^2 \pmod{p}$ ise, o zaman Fermat Teoreminden

$$1 \equiv a^{p-1} \equiv n^{\varpi} \pmod{p}.$$

Diğer durumda $x \mapsto x'$, Wilson Teoreminin kanıtında kullandığımız fonksiyon olsun. O zaman

$$xnx' \equiv n \pmod{p}$$

olduğundan

$$nx' \not\equiv x \pmod{p}.$$

Şimdi

$$1 \leqslant b_k \leqslant p-1 \ \ \& \ \ b_k \equiv n{a_k}' \pmod{p}$$

olduğunda

$$\{1, \ldots, p-1\} = \{a_1, b_1, \ldots, a_{\varpi}, b_{\varpi}\}$$

yazılabilir. Wilson Teoremi sayesinde

$$\begin{aligned} -1 \equiv (p-1)! &\equiv (a_1 \cdot b_1) \cdots (a_{\varpi} \cdot b_{\varpi}) \\ &\equiv (a_1 \cdot n{a_1}') \cdots (a_{\varpi} \cdot n{a_{\varpi}}') \equiv n^{\varpi} \pmod{p}. \end{aligned}$$

□

Yukarıdaki kanıtta $n \equiv a^2 \pmod{p}$ ise

$$\{1, \ldots, p-1\} = \{a, p-a\} \cup \{a_1, b_1, \ldots, a_{\varpi-1}, b_{\varpi-1}\}$$

yazılabilir, ve bu durumda

$$-1 \equiv -a^2 \cdot n^{\varpi-1} \equiv -n^{\varpi} \pmod{p}.$$

Alıştırma 10. Özel durumlarda Euler Kriterini kanıtlayın, örneğin $p = 11$ ve $n = 2$ ise

x	1	3	4	5	9
x'	1	4	3	9	5
$2x'$	2	8	6	7	10

tablosundan

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

dolayısıyla

$$2^5 \equiv -1 \pmod{11},$$

ve ayrıca hiç sayının karesi 2 ile kalandaş olamaz (çünkü her durumda $x \not\equiv 2x'$); ama $n = 3$ ise

x	1	2	4	5	6	8
x'	1	6	3	9	2	7
$3x'$	3	7	9	5	6	10

tablosundan

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

dolayısıyla

$$3^5 \equiv 1 \pmod{11},$$

ve ayrıca $5^2 \equiv 3 \pmod{11}$.

7 İlkel Kökler

Teorem 31. 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 bölme ile 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

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

Tanım 7. Eğer ${\mathbb{Z}_n}^{\times} = \langle a+(n) \rangle$ ise, o zaman a, n'nin **ilkel bir köküdür** (*primitive root*).

Teorem 32. *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

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

Örnek 10. 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	$\pmod{40}$
2^k	2	4	8	16	-9	-18	5	10	20	-1	$\pmod{41}$
3^k	3	9	-14	-1							$\pmod{41}$

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

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

Alıştırma 11. Bazı asal sayıların ilkel köklerini bulun ve bunların kuvvetlerini kullanarak bazı $x^a \equiv b$ ve $a^x \equiv b$ kalandaşlıklarını çözün.

8 Karesel Karşılıklılık

Bu bölümde tekrar p tek ve asal bir sayı ve $(p-1)/2 = \varpi$ olsun. Ayrıca $n \in \mathbb{Z} \setminus (p)$ ve $1 \leqslant k \leqslant \varpi$ olduğunda

$$kn - p \cdot \left\lfloor k \cdot \frac{n}{p} \right\rfloor = r_k$$

olsun. Bu durumda

$$1 \leqslant r_k \leqslant p-1 \ \ \& \ \ kn \equiv r_k \pmod{p}.$$

Şimdi

$$\{1,\dots,\varpi\}\cap\{r_1,\dots,r_\varpi\}=\{a_1,\dots,a_\ell\},$$
$$\{\varpi+1,\dots,p-1\}\cap\{r_1,\dots,r_\varpi\}=\{b_1,\dots,b_m\},$$

ve

$$\ell+m=\varpi$$

koşullarını sağlayan ℓ, m, ve $a_1\dots,a_\ell$, ve $b_1,\dots,b_m$ vardır. O zaman

$$\{a_1,\dots,a_\ell\}\cup\{b_1,\dots,b_m\}=\{r_1,\dots,r_\varpi\}.$$

Ayrıca

$$\{a_1,\dots,a_\ell\}\cup\{p-b_1,\dots,p-b_m\}=\{1,\dots,\varpi\}$$

çünkü

$$\{a_1,\dots,a_\ell\}\cup\{p-b_1,\dots,p-b_m\}\subseteq\{1,\dots,\varpi\}$$

ve soldaki sayılar birbirinden farklıdır çünkü $x+(p)\mapsto nx+(p)$ göndermesi, ${\mathbb{Z}_p}^\times$ kümesinin bir permütasyonudur, dolayısıyla

$${\mathbb{Z}_p}^\times=\{kn+(p)\colon 1\leqslant k\leqslant\varpi\}\cup\{-kn+(p)\colon 1\leqslant k\leqslant\varpi\},$$

ve ayrıca

$$-kn \equiv p - r_k \pmod{p}.$$

Teorem 33 (Gauss Lemması)**.**

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

Kanıt. Yukarıdaki küme eşitliklerinden

$$a_1 \cdots a_\ell \cdot b_1 \cdots b_m = r_1 \cdots r_\varpi$$

ve

$$a_1 \cdots a_\ell \cdot (p - b_1) \cdots (p - b_m) = (\varpi!).$$

Aynı zamanda ilk tanımlardan

$$r_1 \cdots r_\varpi \equiv \varpi! \cdot n^\varpi \pmod{p}$$

ve

$$a_1 \cdots a_\ell \cdot (p - b_1) \cdots (p - b_m) \equiv (-1)^m a_1 \cdots a_\ell \cdot b_1 \cdots b_m \pmod{p}.$$

O zaman

$$\varpi! \equiv (-1)^m \varpi! \cdot n^\varpi \pmod{p},$$

dolayısıyla

$$1 \equiv (-1)^m \cdot n^\varpi \pmod{p}.$$

Şimdi, Euler Kriteri (yani Teorem 30) sayesinde,

$$1 \equiv (-1)^m \cdot \left(\frac{n}{p}\right) \pmod{p}. \qquad \square$$

Şimdi

$$1 + \cdots + \varpi = \frac{\varpi \cdot (\varpi + 1)}{2} = \frac{p^2 - 1}{8}$$

eşitliğini fark edelim.

Lemma 2.

$$(n-1)\cdot\frac{p^2-1}{8}\equiv\left\lfloor\frac{n}{p}\right\rfloor+\cdots+\left\lfloor\varpi\cdot\frac{n}{p}\right\rfloor+m\pmod 2.$$

Kanıt. Yukarıdaki küme eşitliklerinden

$$a_1+\cdots+a_\ell+b_1+\cdots+b_m=r_1+\cdots+r_\varpi$$

ve

$$a_1+\cdots+a_\ell+(p-b_1)+\cdots+(p-b_m)=1+\cdots+\varpi.$$

Aynı zamanda ilk tanımlardan

$$r_1+\cdots+r_\varpi=(1+\cdots+\varpi)\cdot n-p\cdot\left(\left\lfloor\frac{n}{p}\right\rfloor+\cdots+\left\lfloor\varpi\cdot\frac{n}{p}\right\rfloor\right).$$

O zaman modülüs olarak 2'ye göre

$$(1+\cdots+\varpi)\cdot n\equiv\left\lfloor\frac{n}{p}\right\rfloor+\cdots+\left\lfloor\varpi\cdot\frac{n}{p}\right\rfloor+a_1+\cdots+a_\ell+b_1+\cdots+b_m$$

ve

$$1 + \cdots + \varpi \equiv a_1 + \cdots + a_\ell + b_1 + \cdots + b_m + m. \qquad \square$$

Teorem 34.

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \text{ } \textit{olduğunda,} \\ -1, & p \equiv \pm 3 \pmod 8 \text{ } \textit{olduğunda.} \end{cases}$$

Kanıt. Lemma 2 ve Gauss Lemması. $\square$

Teorem 35. *Eğer q, p'den farklı olan tek ve asal bir sayı ise, o zaman*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4},$$

dolayısıyla

$$\left(\frac{q}{p}\right) = \begin{cases} -(p/q), & p \equiv q \equiv 3 \pmod 4 \text{ } \textit{olduğunda,} \\ (p/q), & \textit{diğer durumda.} \end{cases}$$

Kanıt. Lemma 2'de $n = q$ olduğunda

$$m \equiv \left\lfloor \frac{q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor \pmod 2.$$

Ayrıca

$$\left\{ (i,j) \colon 1 \leqslant i \leqslant \frac{p-1}{2} \ \ \& \ \ 1 \leqslant j \leqslant \frac{q-1}{2} \right\} = A$$

olduğunda

$$\left\lfloor \frac{q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor = \left| \left\{ (i,j) \in A \colon j < \frac{iq}{p} \right\} \right|.$$

Simetriden

$$\left\lfloor \frac{p}{q} \right\rfloor + \cdots + \left\lfloor \frac{q-1}{2} \cdot \frac{p}{q} \right\rfloor = \left| \left\{ (i,j) \in A \colon i < \frac{jp}{q} \right\} \right|.$$

Son olarak

$$A = \left\{ (i,j) \in A \colon j < \frac{iq}{p} \right\} \cup \left\{ (i,j) \in A \colon i < \frac{jp}{q} \right\},$$

bu birleşim ayrıktır, dolayısıyla

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{|A|},$$

ama aynı zamanda

$$|A| = \frac{(p-1)(q-1)}{4}.$$ □

Örnek 11.

$$\begin{aligned}\left(\frac{1000}{727}\right) = \left(\frac{273}{727}\right) = \left(\frac{3\cdot 7\cdot 13}{727}\right) &= \left(\frac{3}{727}\right)\left(\frac{7}{727}\right)\left(\frac{13}{727}\right)\\ = -\left(\frac{727}{3}\right)\cdot -\left(\frac{727}{7}\right)\left(\frac{727}{13}\right) &= \left(\frac{1}{3}\right)\left(\frac{-1}{7}\right)\left(\frac{12}{13}\right)\\ = -\left(\frac{3}{13}\right) = -\left(\frac{13}{3}\right) &= -1.\end{aligned}$$

Bundan dolayı

$$125x^2 + 50x + 3 \equiv 0 \pmod{727}$$

kalandaşlığının çözümü yoktur. Aynı zamanda

$$\left(\frac{-1000}{727}\right) = \left(\frac{-1}{727}\right) \cdot -1 = 1,$$

dolayısıyla

$$251x^2 + 2x + 1 \equiv 0 \pmod{727}$$

kalandaşlığının çözümü vardır. Aslında

$$251x^2 + 2x + 1 \equiv 0 \iff (502x + 2)^2 \equiv -1000 \equiv 454 \pmod{727}.$$

Ayrıca $347^2 \equiv 454 \pmod{727}$, ama bunu öğrenmek için bir yöntem vermedik. İstenen bilgi, aşağıdaki tablodan alınabilir.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0	1	5	25	125	625	217	358	336	226	403	561	624	212	333	211	328	186	203	288	713	657	377
22	431	701	597	77	385	471	174	143	715	667	427	681	497	304	66	330	196	253	538	509	364	366
44	376	426	676	472	179	168	113	565	644	312	106	530	469	164	93	465	144	720	692	552	579	714
66	662	402	556	599	87	435	721	697	577	704	612	152	33	165	98	490	269	618	182	183	188	213
88	338	236	453	84	420	646	322	156	53	265	598	82	410	596	72	360	346	276	653	357	331	201
110	278	663	407	581	724	712	652	352	306	76	380	446	49	245	498	309	91	455	94	470	169	118
132	590	42	210	323	161	78	390	496	299	41	205	298	36	180	173	138	690	542	529	464	139	695
154	567	654	362	356	326	176	153	38	190	223	388	486	249	518	409	591	47	235	448	59	295	21
176	105	525	444	39	195	248	513	384	466	149	18	90	450	69	345	271	628	232	433	711	647	327
198	181	178	163	88	440	19	95	475	194	243	488	259	568	659	387	481	224	393	511	374	416	626
220	222	383	461	124	620	192	233	438	9	45	225	398	536	499	314	116	580	719	687	527	454	89
242	445	44	220	373	411	601	97	485	244	493	284	693	557	604	112	560	619	187	208	313	111	555
264	594	62	310	96	480	219	368	386	476	199	268	613	157	58	290	723	707	627	227	408	586	22
286	110	550	569	664	412	606	122	610	142	710	642	302	56	280	673	457	104	520	419	641	297	31
308	155	48	240	473	184	193	238	463	134	670	442	29	145	725	717	677	477	204	293	11	55	275
330	648	332	206	303	61	305	71	355	321	151	28	140	700	592	52	260	573	684	512	379	441	24
352	120	600	92	460	119	595	67	335	221	378	436	726	722	702	602	102	510	369	391	501	324	166
374	103	515	394	516	399	541	524	439	14	70	350	296	26	130	650	342	256	553	584	12	60	300
396	46	230	423	661	397	531	474	189	218	363	361	351	301	51	255	548	559	614	162	83	415	621
418	197	258	563	634	262	583	7	35	175	148	13	65	325	171	128	640	292	6	30	150	23	115
440	575	694	562	629	237	458	109	545	544	539	514	389	491	274	643	307	81	405	571	674	462	129
462	645	317	131	655	367	381	451	74	370	396	526	449	64	320	146	3	15	75	375	421	651	347
484	281	678	482	229	418	636	272	633	257	558	609	137	685	517	404	566	649	337	231	428	686	522
506	429	691	547	554	589	37	185	198	263	588	32	160	73	365	371	401	551	574	689	537	504	339
528	241	478	209	318	136	680	492	279	668	432	706	622	202	283	688	532	479	214	343	261	578	709
550	637	277	658	382	456	99	495	294	16	80	400	546	549	564	639	287	708	632	252	533	484	239
572	468	159	68	340	246	503	334	216	353	311	101	505	344	266	603	107	535	494	289	718	682	502
594	329	191	228	413	611	147	8	40	200	273	638	282	683	507	354	316	126	630	242	483	234	443
616	34	170	123	615	167	108	540	519	414	616	172	133	665	417	631	247	508	359	341	251	528	459
638	114	570	669	437	4	20	100	500	319	141	705	617	177	158	63	315	121	605	117	585	17	85
660	425	671	447	54	270	623	207	308	86	430	696	572	679	487	254	543	534	489	264	593	57	285
682	698	582	2	10	50	250	523	434	716	672	452	79	395	521	424	666	422	656	372	406	576	699
704	587	27	135	675	467	154	43	215	348	286	703	607	127	635	267	608	132	660	392	506	349	291

Aslında 5, 727'nin ilkel bir köküdür, ve tabloda 727'ye göre 5'in kuvvetleri verilir. Özellikle

$$\begin{aligned} 454 &\equiv 5^{220+20} \equiv 5^{240} \equiv 5^{2\cdot 120}, \\ 5^{120} &\equiv 5^{110+10} \equiv 380 \equiv -347 \pmod{727}. \end{aligned}$$

Şimdi

$$\begin{aligned} 251x^2 + 2x + 1 \equiv 0 &\iff 502x + 2 \equiv \pm 347 \\ &\iff 502x \equiv 345, -349 \pmod{727}. \end{aligned}$$

Öklid Algoritması veya tablodan

$$502 \cdot 42 \equiv 1 \pmod{727},$$

ve bundan dolayı

$$\begin{aligned} 251x^2 + 2x + 1 \equiv 0 &\iff x \equiv 42 \cdot 345, -42 \cdot 349 \\ &\iff x \equiv 677, 609 \pmod{727}. \end{aligned}$$