Sayılar Kuramı (MAT 316)

Final sınavı

David Pierce

28 Haziran 2024
Matematik Böl., MSGSÜ

Sınıfta ön sıra 1 ve sol sütun 1 olsun. Oturduğunuz yer için $(\text{sıra}, \text{sütun}) = (k, \ell)$ ise

$$1 \leqslant M \leqslant 4 \ \ \& \ \ M \equiv k + 2 \cdot (\ell - 1) \pmod 4$$

olacak şekilde, okuyacağım her kağıdın üstüne adınızı, soyadınızı, ve M'nin değerini yazın. Problemlerde

M	p	a	b	d	M	p	a	b	d
1	19	5	-30	130	3	19	3	10	458
2	23	3	87	269	4	23	5	90	269

Problem 2'de tablonun j numaralı sütununda ve $i \cdot 9$ numaralı satırında olan girdisi, 271 modülüsüne göre 6^{9i+j} kuvveti ile kalandaştır. Ayrıca

- b'nin değerleri, 0 numaralı sütundadır;
- 134'ten büyük olan üsler için

$$6^{x+135} \equiv -6^x \pmod{271}$$

kuralı kullanılabilir.

Problem 3 için aşağıdaki değerler kullanılabilir.

x	11	12	16	17	19	20	21	22
x^2	121	144	256	289	361	400	441	484

Tabii ki yazınızı okuyup anlayabilmem gerekiyor! İyi çalışmalar dilerim.

Problem 1. Yukarıda verilen p ve a için:

(a) Wilson Teoremini kullanmadan

$$(p-2)! \equiv 1 \pmod p$$

kalandaşlığını gösterin.

(b) Wilson Teoremini kullanarak, ama Euler Kriterini kullanmadan, $\varpi = (p-1)/2$ olduğunda, aşağıdaki iki kalandaşlığı gösterin.

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

Problem 2.

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

(a) Verilen b için $x^6 \equiv b \pmod{271}$ kalandaşlığını çözün.

(b) Çözümlerden hangileri $(x/271) = 1$ denklemini de çözer?

Problem 3. Sayma sayılarında, $x^2 - dy^2 = \pm 1$ denklemi için sonsuz bir çözüm kümesi bulun.

Çözüm. Problem 1.

(a) Yöntem: $\{2, \ldots, p-2\}$ kümesinin,

$$x \neq x', \qquad x'' = x, \qquad xx' \equiv 1 \pmod{p}$$

özdeşliklerini sağlayan $x \mapsto x'$ permütasyonu vardır. O halde

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

eşitliğini sağlayan bir $\{a_1, \ldots, a_{\varpi-1}\}$ kümesi vardır, ve sonuç olarak

$$(p-2)! \equiv (a_1 a_1') \cdots (a_{\varpi-1} a_{\varpi-1}') \equiv 1^{\varpi-1} \equiv 1 \pmod{p}.$$

Ayrıca

$$(p-x)' = p - x'.$$

Özel olarak

- 19 modülüsüne göre

x	± 2	± 3	± 4	± 7
x'	∓ 9	∓ 6	± 5	∓ 8

  dolayısıyla

$$1 \equiv (2 \cdot 10)(3 \cdot 13)(4 \cdot 5)(6 \cdot 16)(7 \cdot 11)(8 \cdot 12)(9 \cdot 17)(14 \cdot 15) \equiv 17!$$

- 23 modülüsüne göre

x	± 2	± 3	± 4	± 5	± 7
x'	∓ 11	± 8	± 6	∓ 9	± 10

  dolayısıyla

$$1 \equiv (2 \cdot 12)(3 \cdot 8)(4 \cdot 6)(5 \cdot 14)(7 \cdot 10)(9 \cdot 18)(11 \cdot 21)(13 \cdot 16)(15 \cdot 20)(17 \cdot 19) \equiv 21!$$

(b) Yöntem: $\{1, \ldots, p-1\}$ kümesi,

$$ab_k' \equiv c_k \pmod{p}$$

kalandaşlığını sağlayan, ayrık bir

$$\{1, a\} \cup \{p-1, p-a\} \cup \{b_1, c_1\} \cdots \cup \{b_n, c_n\}$$

bileşimi olarak yazılabilir.

- Eğer $(a/p) = -1$ ise, o zaman $n = \varpi - 2$ ve her durumda $b_k \neq c_k$, dolayısıyla Wilson Teoreminden

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv a \cdot (p-a)(p-1)(b_1 c_1) \cdots (b_{\varpi-2} c_{\varpi-2}) \\ &\equiv a^{\varpi} \pmod{p}. \end{aligned}$$

- Eğer $(a/p) = 1$ ise, o zaman $n = \varpi - 1$ ve $(b_{\varpi-2}, b_{\varpi-1}) = (c_{\varpi-2}, c_{\varpi-1})$ varsayılabilir, dolayısıyla

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv a \cdot (p-a)(p-1)(b_1 c_1) \cdots (b_{\varpi-3} c_{\varpi-3}) b_{\varpi-2} b_{\varpi-1} \\ &\equiv a^{\varpi-1} \cdot -a \pmod{p}. \end{aligned}$$

Özel olarak

- 19 modülüsüne göre
  - $a = 3$ olduğunda

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

  dolayısıyla $(\pm 3/19) = \mp 1$ ve

$$\begin{aligned} -1 &\equiv 18! \\ &\equiv 3(2 \cdot 11)(4 \cdot 15)(5 \cdot 12)(6 \cdot 10)(7 \cdot 14)(8 \cdot 17)(9 \cdot 13)(16 \cdot 18) \\ &\equiv 3^9, \\ 1 &\equiv -3^9 \equiv (-3)^9; \end{aligned}$$

– $a = 5$ olduğunda

$$\begin{array}{c|ccccc} x & \pm1 & \pm2 & \pm3 & \pm4 & \pm9 \\ \hline 5x' & \pm5 & \mp7 & \pm8 & \pm6 & \pm9 \end{array},$$

dolayısıyla $(\pm5/19) = \pm1$ ve

$$\begin{aligned} -1 &\equiv 18! \\ &\equiv 5(2\cdot 12)(3\cdot 8)(4\cdot 6)(7\cdot 17)9\cdot 10(11\cdot 16)(13\cdot 15)(14\cdot 18) \\ &\equiv -5^9 =\equiv (-5)^9, \\ 1 &\equiv 5^9; \end{aligned}$$

- 23 modülüsüne göre
  – $a = 3$ olduğunda

$$\begin{array}{c|cccccc} x & \pm1 & \pm2 & \pm4 & \pm6 & \pm7 & \pm8 \\ \hline 3x' & \pm3 & \mp10 & \mp5 & \mp11 & \pm7 & \pm9 \end{array},$$

dolayısıyla $(\pm3/23) = \pm1$ ve

$$\begin{aligned} -1 &\equiv 22! \\ &\equiv 3(2\cdot 13)(4\cdot 18)(5\cdot 19)(6\cdot 12)7(8\cdot 9) \\ &\quad (10\cdot 21)(11\cdot 17)(14\cdot 15)16(20\cdot 22) \\ &\equiv -3^{11} \equiv (-3)^{11}, \\ 1 &\equiv 3^{11}; \end{aligned}$$

- $a = 5$ olduğunda

$$\begin{array}{c|cccccc} x & \pm1 & \pm2 & \pm3 & \pm4 & \pm8 & \pm10 \\ \hline 5x' & \pm5 & \mp9 & \mp6 & \pm7 & \mp8 & \mp11 \end{array},$$

dolayısıyla $(\pm5/23) = \mp1$ ve

$$\begin{aligned} -1 &\equiv 22! \\ &\equiv 5(2\cdot 14)(3\cdot 17)(4\cdot 7)(6\cdot 20)(8\cdot 15) \\ &\quad (9\cdot 21)(10\cdot 12)(11\cdot 13)(16\cdot 19)(18\cdot 22) \\ &\equiv 5^{11}, \\ 1 &\equiv -5^{11} \equiv (-5)^{11}. \end{aligned}$$

Çözüm. Problem 2. $x \equiv 6^t \pmod{271}$ olsun. O zaman bir c için

$$6^{6t} \equiv 6^c \pmod{271},$$

dolayısıyla

$$6t \equiv c \pmod{270}.$$

- $6^c \equiv -30 \pmod{271}$ ise $c \equiv 36 \pmod{270}$, dolayısıyla

$$\begin{aligned} 6t &\equiv 36 \pmod{270}, \\ t &\equiv 6 \pmod{45}, \\ t &\equiv 6, 51, 96, 141, 186, 231 \pmod{270}, \\ x &\equiv 44, 123, 79, -44, -123, -79 \pmod{271}. \end{aligned}$$

Sadece $44, 79, -123$, $(x/271) = 1$ çözer.

- $6^c \equiv 87 \pmod{271}$ ise $c \equiv 72 \pmod{270}$, dolayısıyla

$$\begin{aligned} 6t &\equiv 72 \pmod{270}, \\ t &\equiv 12 \pmod{45}, \\ t &\equiv 12, 57, 102, 147, 192, 237 \pmod{270}, \\ x &\equiv 39, -8, -47, -39, 8, 47 \pmod{271}. \end{aligned}$$

Sadece $39, -47, 8$, $(x/271) = 1$ çözer.

- $6^c \equiv 10 \pmod{271}$ ise $c \equiv 54 \pmod{270}$, dolayısıyla

$$\begin{aligned} 6t &\equiv 54 \pmod{270}, \\ t &\equiv 9 \pmod{45}, \\ t &\equiv 9, 54, 99, 144, 189, 234 \pmod{270}, \\ x &\equiv 19, 10, -9, -19, -10, 9 \pmod{271}. \end{aligned}$$

Sadece $10, -19, 9$, $(x/271) = 1$ çözer.

- $6^c \equiv 90 \pmod{271}$ ise $c \equiv 18 \pmod{270}$, dolayısıyla

$$\begin{aligned} 6t &\equiv 18 \pmod{270}, \\ t &\equiv 3 \pmod{45}, \\ t &\equiv 3, 48, 93, 138, 183, 228 \pmod{270}, \\ x &\equiv -55, -86, -31, 55, 86, 31 \pmod{271}. \end{aligned}$$

Sadece $-86, 55, 31$, $(x/271) = 1$ çözer.

Çözüm. Problem 3. $d = 130$ olsun.

$$\begin{aligned}
\sqrt{130} &= 11 + \sqrt{130} - 11, \\
\frac{1}{\sqrt{130} - 11} &= \frac{\sqrt{130} + 11}{9} = 2 + \frac{\sqrt{130} - 7}{9}, \\
\frac{9}{\sqrt{130} - 7} &= \frac{\sqrt{130} + 7}{9} = 2 + \frac{\sqrt{130} - 11}{9}, \\
\frac{9}{\sqrt{130} - 11} &= \sqrt{130} + 11.
\end{aligned}$$

Ayrıca

$$[11, 2, 2] = \left[11, 2 + \frac{1}{2}\right]\left[11, \frac{5}{2}\right] = 11 + \frac{2}{5} = \frac{57}{5}.$$

O zaman

$$\begin{aligned}
(a_1, b_1) &= (57, 5), \\
(a_{m+1}, b_{m+1}) &= (a_1 a_m + d b_1 b_m, b_1 a_m + a_1 b_m) \\
&= (57 a_m + 650 b_m, 5 a_m + 57 b_m)
\end{aligned}$$

olduğunda her m için

$$a_m{}^2 - 130 b_m{}^2 = (-1)^m$$

çünkü

$$\begin{aligned}
57^2 &= 2500 + 700 + 41 = 3249, \\
130 \cdot 5^2 &= 130 \cdot 25 = 650 \cdot 5 = 3250,
\end{aligned}$$

ve ayrıca

$$\begin{aligned}
&(a_1 x + d b_1 y)^2 - d(b_1 x + a_1 y)^2 \\
&\qquad = (a_1{}^2 - d b_1{}^2) x^2 + 0xy - d(a_1{}^2 - d b_1{}^2) y^2 = -(x^2 - d y^2),
\end{aligned}$$

dolayısıyla tümevarım sayesinde genel iddia doğrudur.

Çözüm. $d = 269$ olsun.

$$\begin{aligned}
\sqrt{269} &= 16 + \sqrt{269} - 16, \\
\frac{1}{\sqrt{269} - 16} &= \frac{\sqrt{269} + 16}{13} = 2 + \frac{\sqrt{269} - 10}{13}, \\
\frac{13}{\sqrt{269} - 10} &= \frac{\sqrt{269} + 10}{13} = 2 + \frac{\sqrt{269} - 16}{13}, \\
\frac{13}{\sqrt{269} - 16} &= \sqrt{269} + 16.
\end{aligned}$$

Ayrıca

$$[16, 2, 2] = \left[16, 2 + \frac{1}{2}\right]\left[16, \frac{5}{2}\right] = 16 + \frac{2}{5} = \frac{82}{5}.$$

O zaman

$$\begin{aligned}
(a_1, b_1) &= (82, 5), \\
(a_{m+1}, b_{m+1}) &= (a_1 a_m + d b_1 b_m, b_1 a_m + a_1 b_m) \\
&= (82 a_m + 1345 b_m, 5 a_m + 82 b_m)
\end{aligned}$$

olduğunda her m için

$$a_m{}^2 - 269 b_m{}^2 = (-1)^m$$

çünkü

$$\begin{aligned}
82^2 &= 6400 + 320 + 4 = 6724, \\
269 \cdot 5^2 &= 1345 \cdot 5 = 6725,
\end{aligned}$$

ve ayrıca

$$\begin{aligned}
&(a_1 x + d b_1 y)^2 - d(b_1 x + a_1 y)^2 \\
&\qquad = (a_1{}^2 - d b_1{}^2) x^2 + 0xy - d(a_1{}^2 - d b_1{}^2) y^2 = -(x^2 - d y^2),
\end{aligned}$$

dolayısıyla tümevarım sayesinde genel iddia doğrudur.

Çözüm. $d = 458$ olsun.

$$\begin{aligned}
\sqrt{458} &= 21 + \sqrt{458} - 21, \\
\frac{1}{\sqrt{458}-21} &= \frac{\sqrt{458}+21}{17} = 2 + \frac{\sqrt{458}-13}{17}, \\
\frac{17}{\sqrt{458}-13} &= \frac{\sqrt{458}+13}{17} = 2 + \frac{\sqrt{458}-21}{17}, \\
\frac{17}{\sqrt{458}-21} &= \sqrt{458}+21.
\end{aligned}$$

Ayrıca

$$[21,2,2] = \left[21, 2+\frac{1}{2}\right]\left[21,\frac{5}{2}\right] = 21 + \frac{2}{5} = \frac{107}{5}.$$

O zaman

$$\begin{aligned}
(a_1, b_1) &= (107, 5), \\
(a_{m+1}, b_{m+1}) &= (a_1 a_m + d b_1 b_m, b_1 a_m + a_1 b_m) \\
&= (107 a_m + 2290 b_m, 5 a_m + 107 b_m)
\end{aligned}$$

olduğunda her m için

$$a_m{}^2 - 458 b_m{}^2 = (-1)^m$$

çünkü

$$\begin{aligned}
107^2 &= 10000 + 1400 + 49 = 11449, \\
458 \cdot 5^2 &= 2290 \cdot 5 = 11450,
\end{aligned}$$

ve ayrıca

$$\begin{aligned}
&(a_1 x + d b_1 y)^2 - d(b_1 x + a_1 y)^2 \\
&\qquad = (a_1{}^2 - d b_1{}^2) x^2 + 0xy - d(a_1{}^2 - d b_1{}^2) y^2 = -(x^2 - d y^2),
\end{aligned}$$

dolayısıyla tümevarım sayesinde genel iddia doğrudur.