MAT223 AYRIK MATEMATİK

Tamsayılar, Bölenler ve Asal Sayılar

6. Bölüm

Emrah Akyar

Anadolu Üniversitesi
Fen Fakültesi Matematik Bölümü, ESKİŞEHİR

2014–2015 Öğretim Yılı

Bölünebilme

Önce bazı temel gösterimleri verelim:
a ve b iki tamsayı olsun.

$$a \mid b$$

a böler b, a, b nin bölenidir, b, a nın bir katıdır, $\frac{b}{a} \in \mathbb{Z}$.

Bu durumda $b = m \cdot a$ olacak şekilde m tamsayısı vardır.

$$a \nmid b$$

a, b yi bölmez, $\frac{b}{a} \notin \mathbb{Z}$.

Eğer $a \nmid b$ ve $a > 0$ ise

$$b \div a = a \cdot q + r, \quad 0 < r < a$$

şeklinde kalanlı bölmeden söz edebiliriz.

Alıştırma (6.1.3-a)

$a \mid b$ ve $b \mid c$ ise $a \mid c$ olur. Gösteriniz.

$a \mid b$ ise $b = m_1 \cdot a$ olacak şekilde $m_1 \in \mathbb{Z}$ ve $b \mid c$ ise $c = m_2 \cdot b$ olacak şekilde $m_2 \in \mathbb{Z}$ tamsayıları vardır. Buradan,

$$c = m_2 b = \underbrace{m_2 m_1}_{m} a = ma \quad \Rightarrow \quad a \mid c.$$

Alıştırma (6.1.3-b)

$a \mid b$ ve $a \mid c$ ise $a \mid b + c$ ve $a \mid b - c$ olur. Gösteriniz.

$a \mid b$ ise $b = m_1 \cdot a$ olacak şekilde $m_1 \in \mathbb{Z}$ ve $a \mid c$ ise $c = m_2 \cdot a$ olacak şekilde $m_2 \in \mathbb{Z}$ tamsayıları vardır. Buradan,

$$b + c = m_1 a + m_2 a = \underbrace{(m_1 + m_2)}_{m} a = ma \quad \Rightarrow a \mid b + c,$$

$$b - c = m_1 a - m_2 a = \underbrace{(m_1 - m_2)}_{m'} a = m' a \quad \Rightarrow a \mid b - c.$$

Asal Sayılar

1, -1, p ve $-p$ sayıları dışında hiçbir sayıya bölünmeyen $p > 1$ tamsayısına *asal sayı* denir.

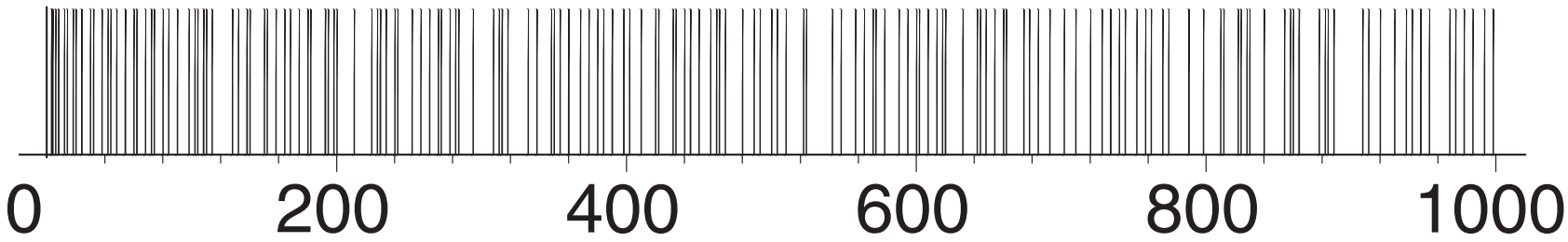
Ya da, $p > 1$ sayısı kendisinden küçük iki pozitif tamsayının çarpımı şeklinde yazılamıyorsa p ye asal sayı denir.

Asal olmayan $n > 1$ sayısına ise *bileşik sayı* (composite) denir (1 ne asal ne de bileşik sayıdır).

Asal sayılar çok eski çağlardan beri insanları büyülemiştir. Asal sayılar düzensiz bir şekilde sıralanmalarına karşın, birçok ilginç özelliği de taşırlar. Eski yunanlılar asal sayıların sonsuz çoklukta olduğunu biliyorlardı (hatta kanıtlamışlardı).

Ancak, asal sayılar ile ilgili birçok özelliğin kanıtlanması hiç de kolay değildir. Bugün asal sayılar ile ilgili hala kanıtlanamamış birçok özellik bulunmaktadır.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59
60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87
88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110
111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130
131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150
151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170
171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190
191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210
211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230
231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250
251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270
271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290
291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310
311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330
331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350
351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370
371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390
391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410
411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430
431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450
451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470
471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490



Şekil: 1 ile 1000 arasındaki asal sayılar için bir diagram.

Asal olmayan ve 1 den büyük herhangi bir tamsayıyı kendinden küçük iki sayının çarpımı şeklinde yazabiliriz. Eğer bu çarpanlar asal değilse, bu sayıları da kendilerinden küçük iki sayının çarpımı şeklinde yazabiliriz. Eğer böyle devam edecek olursak sonunda ilk sayıyı sadece asal sayıların çarpımı şeklinde yazabiliriz.
Eski yunanlılar bu özelliğin de farkındaydılar. Hatta bu çarpımın tek türlü şekilde olduğunu da kanıtlamışlardı.
Bugün hala verilen bir sayının asal çarpanlara ayrılması için kullanışlı bir yöntem yoktur. Elbette günümüzdeki bilgisayarlar sayesinde oldukça büyük sayıların asal çarpanlara nasıl ayrılacağını bulmak kolaylaşmıştır. Şu anda rekor 140 basamaklı sayılar civarındadır.

Asal Çarpanlara Ayırma

1 sayısından daha büyük ve asal olmayan her sayının asal sayıların çarpımı şeklinde yazılabileceğinden söz ettik.

Asal sayıları da sadece bir çarpanı olan sayılar (kendileri) ve 1 in de 0 tane asal sayının çarpımı şeklinde yazıldığını kabul edersek,

"Her pozitif tamsayı asal sayıların çarpımı şeklinde yazılabilir"

diyebiliriz.

Bunların ışığında, aşağıdaki önemli teoremden söz edebiliriz.

Teorem (Aritmetiğin Temel Teoremi)

Her pozitif tamsayı asal sayıların çarpımı şeklinde tek türlü yazılabilir.

Kanıtı *olmayana ergi* yöntemi ile yapacağız.

Tersine, kabul edelim ki iki farklı şekilde asal sayıların çarpımı olarak ifade edilebilen pozitif tamsayılar var olsun.

Bu sayıların **en küçüğünü** n ile gösterelim. Yani,

$$n = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_k \qquad (*)$$

n tamsayısının iki farklı asal çarpanlara ayrılmış şekli ve bu şekildeki sayıların en küçüğü n olsun.

Genelliği bozmaksızın $p_1, p_2, \ldots, p_m$ çarpanlarının en küçüğünün p_1 olduğunu kabul edelim (aksi halde çarpanların yerini değiştirebiliriz).

Bu durumda $p_1 \neq q_1$, $p_1 \neq q_2$, $\ldots$, $p_1 \neq q_k$ olur. Aksi halde $(*)$ eşitliğinin her iki tarafından p_1 sadeleşir ve n den daha küçük bir sayı elde ederdik.

O zaman her bir q_i sayısını p_1 ile bölersek,

$$\begin{aligned} q_1 &= a_1 p_1 + r_1, & 0 < r_1 < p_1 \\ q_2 &= a_2 p_1 + r_2, & 0 < r_2 < p_1 \\ &\vdots \\ q_k &= a_k p_1 + r_k, & 0 < r_k < p_1 \end{aligned}$$

olur.

Şimdi

$$n' = r_1 \cdot r_2 \cdots r_k$$

sayısını tanımlayalım. Bu durumda

$$n' = r_1 \cdot r_2 \cdots r_k < q_1 \cdot q_2 \cdots q_k = n$$

olur.

Eğer n' sayısının da iki farklı şekilde asal çarpanlara ayrıldığını gösterirsek kanıt biter.

1. $n' = r_1 \cdot r_2 \cdots r_k$.
   (Eğer r_i sayıları asal değilse onları da ayrı ayrı asal çarpanlara ayırıp yazabiliriz).
2. $n' = \underbrace{(q_1 - a_1 p_1)}_{r_1} \cdot \underbrace{(q_2 - a_2 p_1)}_{r_2} \cdots \underbrace{(q_k - a_k p_1)}_{r_k}$

   sağ taraftaki çarpma işlemi yapılırsa, $q_1 q_2 \cdots q_k$ hariç diğer tüm terimlerde p_1 çarpan olarak bulunur.

   $n = q_1 q_2 \cdots q_k$ eşitliğinden ve p_1, n nin bir çarpanı olduğundan $q_1 q_2 \cdots q_k$ sayısı p_1 ile bölünür.

   O halde n' sayısı da p_1 ile bölünür.

O zaman

$$\frac{n'}{p_1} = s_1 \cdot s_2 \cdots s_m$$

dersek,

$$n' = p_1 \cdot s_1 \cdot s_2 \cdots s_m$$

olur.

Böylece n' sayısının bir başka asal çarpanlara ayrılmış şeklini daha elde ettik.

Oysa varsayımımıza göre bu şekildeki sayıların en küçüğü n idi.

O halde varsayımımız hatalıdır.

Böyle bir sayı var olamaz.

Teorem

$\sqrt{2}$ irrasyonel bir sayıdır.

$\frac{a}{b}$, $(a, b \in \mathbb{Z},\ b \neq 0)$ şeklinde yazılamayan sayılar irrasyonel sayılardır.

Kabul edelim ki $\sqrt{2}$ rasyonel sayı olsun. O zaman

$$\sqrt{2} = \frac{a}{b}, \qquad (a, b \in \mathbb{Z},\ b \neq 0)$$

olur. Buradan

$$2b^2 = a^2$$

eşitliği elde edilir. Şimdi 2 asal çarpanının eşitliğin her iki tarafında kaçar kez yer aldığını hesaplayalım:

2, a nın asal çarpanı olarak m kez, b nin asal çarpanı olarak da n kez varsa, a^2 nin asal çarpanı olarak $2m$ ve b^2 nin asal çarpanı olarak da $2n$ kez vardır.

Böylece,

$$\underbrace{2b^2}_{\substack{2n+1 \text{ tane } 2 \\ \text{çarpanı var}}} = \underbrace{a^2}_{\substack{2m \text{ tane } 2 \\ \text{çarpanı var}}}$$

Eşitliğin iki tarafındaki her iki sayı da tek türlü asal çarpanlara ayrıldığından,

$$\underbrace{2n+1}_{\text{Tek}} = \underbrace{2m}_{\text{Çift}}$$

olmalıdır.

Bu ise mümkün değildir.

O halde varsayımımız hatalıdır, $\sqrt{2}$ rasyonel sayı olamaz.

Alıştırma (6.3.3-a)

p bir asal sayı, a ve b tamsayılar ve $p \mid ab$ ise $p|a$ veya $p|b$ olur (ya da ikisini de böler).

p, ab nin asal çarpanlarından birisi ise ya a nın ya da b nin asal çarpanlarından biri olur.

Alıştırma (6.3.3-b)

a ve b tamsayılar ve $a \mid b$ olsun. Ayrıca, p asal sayı ve $p \mid b$ ancak $p \nmid a$ ise $p \mid \dfrac{b}{a}$ olduğunu gösteriniz.

$$p \mid b \quad \Rightarrow \quad p \mid a \cdot \frac{b}{a}$$

olur. $p \nmid a$ olduğundan yukarıdaki alıştırmadan $p \mid \dfrac{b}{a}$ olmalıdır.

Asal Sayılar Kümesi

Teorem

Sonsuz tane asal sayı vardır.

Kanıt.

Verilen her n pozitif tamsayısından daha büyük bir asal sayının var olduğunu göstermek yeterlidir.
Keyfi bir n pozitif tamsayısı verilsin. Bu sayıdan daha büyük bir p asal sayısının var olduğunu gösterelim: $\boxed{n! + 1} > n$ sayısını ele alalım.

- $n! + 1$ asal sayı ise $p = n! + 1$ alabiliriz.
- $n! + 1$ asal sayı değilse bu sayının herhangi bir asal çarpanını alalım ve p ile gösterelim.

  Bu durumda $p > n$ olur. Gerçekten de eğer $p \leq n$ olsaydı $p \mid n!$ olurdu. Kabulümüzden $p \mid n! + 1$.
  O halde $p \mid [n! - (n! + 1)]$ yani $p|1$. Bu ise p nin asal sayı olmasıyla çelişir. O halde $p > n$ olmalıdır.

Şimdiye kadar verdiğimiz asal sayıları gösterir tablo ve grafiklerde asal sayıların kimi zaman birbirlerine çok yakın olduğunu kimi zaman da birbirlerinden oldukça uzaklaştıklarını gözlemledik. Acaba hiç birisi asal olmayan 1 000 000 tane ardışık tamsayı var mıdır? Aşağıdaki teorem bu sorunun cevabının olumlu olduğunu göstermektedir.

Teorem

Her k pozitif tamsayısı için k tane hiç birisi asal olmayan ardışık tamsayı vardır.

Kanıt.

$n = k + 1$ alalım ve aşağıdaki sayıları inceleyelim:

$$\underbrace{\underbrace{n! + 2}_{2 \text{ ile bölünür.}}, \underbrace{n! + 3}_{3 \text{ ile bölünür.}}, \ldots, \underbrace{n! + n}_{n \text{ ile bölünür.}}}_{k \text{ tane}}$$

□

Az önce kanıtladığımız teoremin tersi de merak konusu olabilir. Birbirine çok yakın asal sayılar var mıdır? 2 hariç tüm asal sayılar tek sayı olduğuna göre iki asal sayının farkı en az 2 olabilir (2 ve 3 hariç). Bu şekildeki asal sayılara ikiz asal sayılar (twin primes) denir.

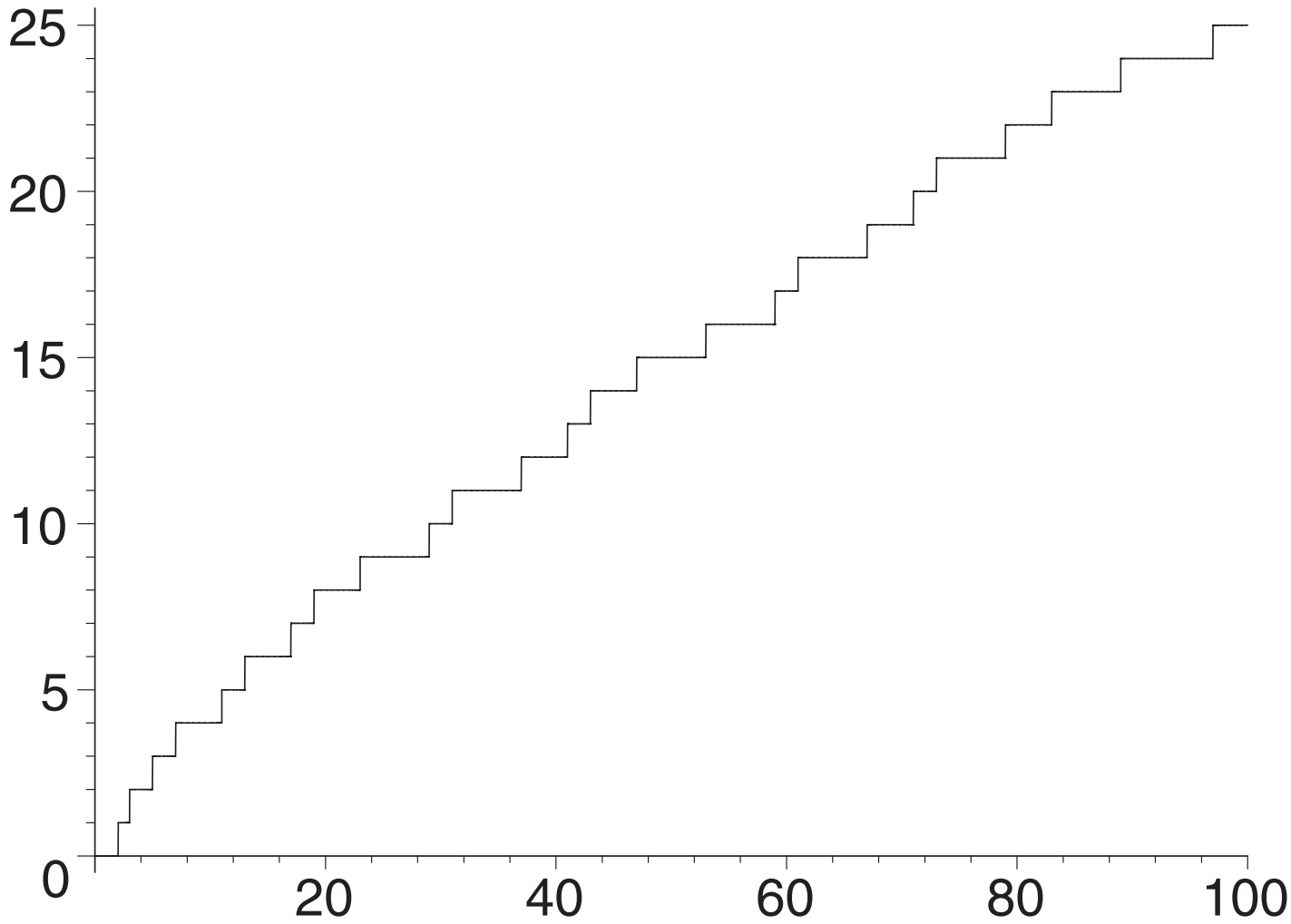
twin primes $(p, p+2)$	3, 5, 11, 17, 29, 41, 59, 71, ...
cousin primes $(p, p+4)$	3, 7, 13, 19, 37, 43, 67, 79, ...
sexy primes $(p, p+6)$	5, 7, 11, 13, 17, 23, 31, 37, ...
$(p, p+8)$	3, 5, 11, 23, 29, 53, 59, 71, ...
$(p, p+10)$	3, 7, 13, 19, 31, 37, 43, 61, ...
$(p, p+12)$	5, 7, 11, 17, 19, 29, 31, 41, ...

İkiz asal sayıların sayısının sonsuz olduğu sanısı halen kanıtlanamamıştır. Tüm ikiz asalların $6n \pm 1$ şeklinde olduğuna dikkat ediniz ((3,5) hariç).

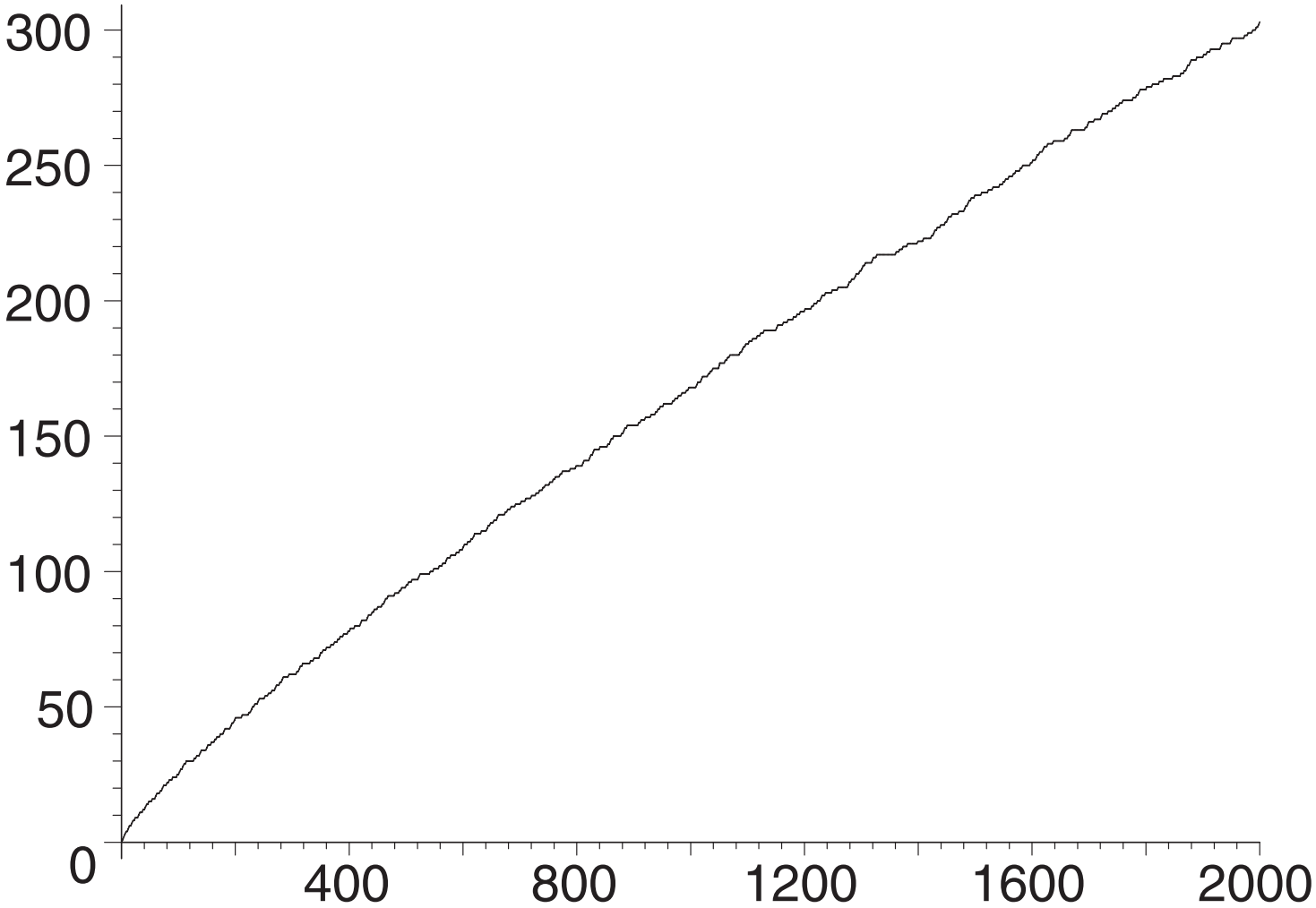
Sayılar teorisinin halen kanıtlanamamış problemlerinden birisi de Goldbach sanısı olarak bilinen ve 2 den büyük her çift sayı iki asal sayının toplamı şeklinde yazılabilir şeklinde ifade edilen problemdir.

$4 = 2+2,\ 6 = 3+3,\ 8 = 3+5,\ 10 = 7+3,\ 12 = 5+7,\ 14 = 3+11, \ldots$

Verilen bir n sayısına kadar olan asalların sayısını $\pi(n)$ ile gösterelim.



Şekil: $[1, 100]$ aralığında $\pi(n)$ fonksiyonunun grafiği



Şekil: $[1, 2000]$ aralığında $\pi(n)$ fonksiyonunun grafiği

Acaba verilen bir n sayısına kadar olan asal sayılar kaç tanedir?

Bu sorunun yanıtı Hadamard ve de la Vallee Poussin tarafından aşağıdaki teorem yardımıyla verilmiştir.

Teorem (Asal Sayı Teoremi)

$$\pi(n) \sim \frac{n}{\ln n}$$

Tekrar hatırlayacak olursak $\sim$ simgesinin anlamı n nin büyük değerleri için

$$\frac{\pi(n)}{\frac{n}{\ln n}}$$

değerinin 1 e yaklaştığıdır.

Alıştırma

200 basamaklı kaç tane asal sayı vardır?

10^{199} sayısına kadar olan asalların sayısını, 10^{200} sayısına kadar olan asalların sayısından çıkarırsak istenen sonucu elde ederiz.
Asal Sayı Teoreminden bu sayının yaklaşık olarak

$$\frac{10^{200}}{200 \ln 10} - \frac{10^{199}}{199 \ln 10} \approx 1.95 \cdot 10^{197}$$

olduğunu söyleyebiliriz.
Oldukça fazla sayıda asal sayı! 200 basamaklı tamsayılar

$$10^{200} - 10^{199} = 10^{199}(10 - 1) = 9 \cdot 10^{199}$$

tane olduğundan

$$\frac{9 \cdot 10^{199}}{1.95 \cdot 10^{197}} \approx 460$$

olur. Neredeyse her 460 sayıdan birisi asal sayı!

Pierre de Fermat
1601–1655
Fransız matematikçi(?)/Avukat

Fermat'ın Küçük Teoremi

Teorem (Fermat'ın Küçük Teoremi)

p bir asal sayı ve a herhangi bir tamsayı ise $p \mid a^p - a$.

Bu teorem şu şekilde de ifade edilebilir:

Eğer p asal sayı ve a, p ile bölünmeyen bir tamsayı ise $p \mid a^{p-1} - 1$.

Lemma

p bir asal sayı ve $0 < k < p$ ise $p \mid \binom{p}{k}$.

Kanıt.

$\binom{p}{k} = \dfrac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$ olduğundan p kesrin payını böler. Ancak, p kesrin paydasını bölmez (p asal $(0 < k < p)$ olduğundan ve çarpanlardan hiç birisini bölmüyorsa çarpımı da bölemeyeceğinden).
O halde Alıştırma 6.3.3 gereği p bu kesri böler. □

Kanıt.

Kanıtı a üzerinden tümevarım yöntemiyle yapalım:

- $a = 0$ için $p \mid 0^p - 0 \quad \Rightarrow \quad p \mid 0$ ✓.
- $a = 1$ için $p \mid 1^p - 1 \quad \Rightarrow \quad p \mid 0$ ✓.
- $b > 1$ için önermenin doğru olduğunu kabul edelim ve $a = b + 1$ alalım.

$$\begin{aligned} a^p - a &= (b+1)^p - (b+1) \\ &= b^p + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b + \cancel{1} - b - \cancel{1} \\ &= (b^p - b) + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b \end{aligned}$$

olur. İlk terim $(b^p - b)$, tümevarım hipotezine göre p ile bölünür. Diğer terimler de az önce kanıtladığımız lemma ya göre p ile bölünür.

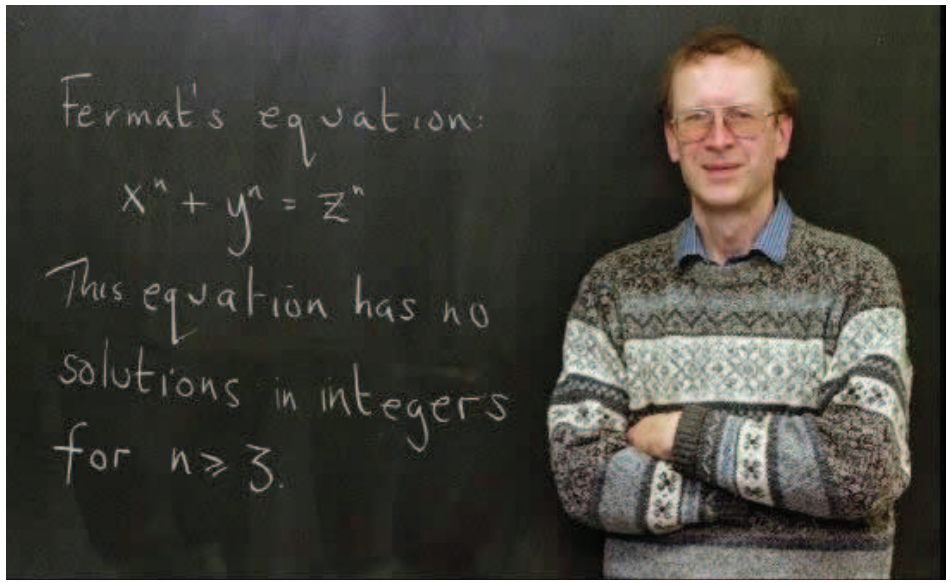
O halde $a^p - a$ da p ile bölünür.

□

Teorem (Fermat'ın Son Teoremi)

$n > 2$ ise iki tamsayının n. kuvvetleri toplamı hiçbir tamsayının n. kuvvetine eşit değildir.

Sir Andrew John Wiles (11 Nisan 1953) Princeton Üniversitesinde çalışan İngiliz matematikçi. 1995 yılında Fermat'ın son teoremini kanıtlamıştır.



Andrew Wiles, "Modular Elliptic Curves and Fermat's Last Theorem", *The Annals of Mathematics*, Second Series, Vol. 141, No. 3 (May, 1995), pp. 443-551.

Euclid Bölme Algoritması

a ve b tamsayılarının en büyük ortak böleni (greatest common divisor) hem a yı hem de b yi bölen en büyük pozitif tamsayıdır.

a ve b sayılarının en büyük ortak böleni

$$\gcd(a,b), \quad \text{ebob}(a,b), \quad \text{obeb}(a,b), \quad (a,b)$$

simgeleriyle gösterilir. Örneğin, $\gcd(1,6)=1$ ve $\gcd(4,6)=2$ olur.

Eğer $\gcd(a,b)=1$ ise a ve b sayılarına *aralarında asaldır* denir.

Benzer şekilde a ve b tamsayılarının en küçük ortak katı (least common multiple) hem a hem de b nin katı olan en küçük tamsayıdır.

a ve b sayılarının en küçük ortak katı ise

$$\text{lcm}(a,b), \quad \text{ekok}(a,b), \quad \text{okek}(a,b)$$

şeklinde gösterilir.

Alıştırma (6.6.2-a)

$\gcd(a, b) = \gcd(a, b - a)$ olduğunu gösteriniz.

$\gcd(a, b) = d_1$ ve $\gcd(a, b - a) = d_2$ olsun. Bu durumda

$$\begin{aligned} d_2 = \gcd(a, b - a) &\Rightarrow d_2 \mid a \text{ ve } d_2 \mid b - a, \\ &\Rightarrow d_2 \mid a + (b - a), \\ &\Rightarrow d_2 \mid b. \end{aligned}$$

O halde $d_2 \mid a$, $d_2 \mid b$ ve $\gcd(a, b) = d_1$ olduğundan $d_2 \mid d_1$ olur.

$$d_1 = \gcd(a, b) \Rightarrow d_1 \mid a \text{ ve } d_1 \mid b \Rightarrow d_1 \mid (b - a).$$

O zaman $d_1 \mid a$, $d_1 \mid b - a$ ve $\gcd(a, b - a) = d_2$ olduğundan $d_1 \mid d_2$ olur.

Böylece $d_1 \mid d_2$, $d_2 \mid d_1$ ve $d_1, d_2 > 0$ olduğundan

$$\gcd(a, b) = d_1 = d_2 = \gcd(a, b - a)$$

elde edilir.

Alıştırma

Her n pozitif tamsayısı için $8n+3$ ile $5n+2$ sayılarının aralarında asal olduğunu kanıtlayınız.

Az önceki alıştırmaya göre,

$$\begin{aligned}
\gcd(8n+3, 5n+2) &= \gcd(8n+3-(5n+2), 5n+2) \\
&= \gcd(5n+2, 3n+1) \\
&= \gcd(5n+2-(3n+1), 3n+1) \\
&= \gcd(3n+1, 2n+1) \\
&= \gcd(3n+1-(2n+1), 2n+1) \\
&= \gcd(2n+1, n) \\
&= \gcd(2n+1-n, n) \\
&= \gcd(n+1, n) \\
&= \gcd(n+1-n, n) = \gcd(1, n) = 1
\end{aligned}$$

olduğundan her n pozitif tamsayısı için $8n+3$ ile $5n+2$ aralarında asal olur.

Alıştırma (6.6.2-b)

b nin a ile bölümünden kalan r ise $\gcd(a,b) = \gcd(a,r)$ olduğunu gösteriniz.

b nin a ile bölümünden kalan r olduğuna göre, $b = qa + r$ olacak şekilde q tamsayısı vardır. O halde Alıştırma 6.6.2-a gereği

$$\left.\begin{aligned}
\gcd(a,b) &= \gcd(\underbrace{b-a}_{r_1}, a) \\
&= \gcd(\underbrace{r_1-a}_{r_2}, a) \\
&= \gcd(\underbrace{r_2-a}_{r_3}, a) \\
&\vdots \quad \vdots \\
&= \gcd(\underbrace{r_{q-1}-a}_{r}, a) \\
&= \gcd(r,a)
\end{aligned}\right\} \; q \text{ defa}$$

Not:
$\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)$ olduğundan q sayısını genelliği bozmaksızın pozitif kabul edebiliriz.

İki tamsayının en büyük ortak bölenini bu sayıları asal çarpanlarına ayırarak bulabiliriz.

Örneğin,

$$\begin{aligned} 900 &= 2^2 \cdot 3^2 \cdot 5^2 \\ 54 &= 2 \cdot 3^3 \end{aligned}$$

olduğundan $\gcd(900, 54) = 2 \cdot 3^2 = 18$ olur.

Ancak, çok büyük sayıları asal çarpanlarına ayırmak oldukça güç bir işlemdir.

Alıştırma 6.6.2 yi kullanarak iki sayının en büyük ortak bölenini sayıları asal çarpanlarına ayırmadan bulmaya yarayan aşağıdaki önemli yöntemi verebiliriz.

Euclid (Bölme) Algoritması: a ve b pozitif tamsayıları verilmiş olsun. Bu sayıların en büyük ortak böleni aşağıdaki şekilde bulunabilir:

1. Eğer $a > b$ ise a ile b yi değiştirelim.
2. Eğer $a > 0$ ise b yi a ya bölelim bu işlemin kalanını r ile gösterelim. b yi r ile değiştirip 1. adıma geri dönelim.
3. Eğer $a = 0$ ise b en büyük ortak bölen olur.

Örnek

$$\gcd(300, 18) = \gcd(18, 12) = \gcd(12, 6) = 6$$

$$\begin{array}{r|l} 300 & 18 \\ \cline{2-2} 288 & 16 \\ \cline{1-1} 12 & \end{array} \qquad \begin{array}{r|l} 18 & 12 \\ \cline{2-2} 12 & 1 \\ \cline{1-1} 6 & \end{array} \qquad \begin{array}{r|l} 12 & 6 \\ \cline{2-2} 12 & 2 \\ \cline{1-1} 0 & \end{array}$$

Önerme

Euclid algoritmasının her bir adımında a ve b sayılarının çarpımı en az yarıya iner.

Kanıt.

Euclid algoritmasında $a < b$ olmak üzere (a, b) sayılarının (r, a) sayıları ile değiştirildiğini kabul edelim.
r, b nin a ya bölümünden kalan olduğuna göre $r < a$ olur. Ayrıca, $r + a \leq b$ olur (eğer bölüm 1 olursa eşitlik sağlanır).
O halde

$$b \geq r + a > r + r = 2r$$

olur. Buradan da

$$b > 2r \quad \Rightarrow \quad ab > 2ra \quad \Rightarrow ar < \frac{1}{2}ab$$

sonucuna ulaşılır. □

Az önce kanıtladığımız önermeye göre eğer a ve b sayılarının en büyük ortak böleni k adımda hesaplanmış ise

$$1 < ar < \frac{1}{2^k}\, ab \quad \Rightarrow ab > 2^k$$

olur. Son eşitsizliğin her iki tarafının 2 tabanında logaritması alınırsa,

$$\log_2(ab) > k\cancel{\log_2 2}^{\,1} \Rightarrow \quad \log_2 a + \log_2 b > k$$

elde edilir. Böylece aşağıdaki sonucu elde ederiz.

Teorem

Euclid algoritması a ve b pozitif tamsayılarına uygulandığında adım sayısı en fazla

$$\log_2 a + \log_2 b$$

olur.

Alıştırma (6.6.9)

Euclid algoritması iki ardışık Fibonacci sayısına uygulanırsa kaç adımda sonuca ulaşılır.

Ardışık iki Fibonacci sayısını F_n ve F_{n+1} ile gösterelim. $n > 1$ için $F_n \nmid F_{n+1}$ olduğu açıktır. Ayrıca,

$$F_{n+1} \div F_n = 1F_n + \underbrace{(F_{n+1} - F_n)}_{F_{n-1}}$$

olduğundan

$$\left.\begin{array}{rcl} \gcd(F_n, F_{n+1}) & = & \gcd(F_{n-1}, F_n) \\ & = & \gcd(F_{n-2}, F_{n-1}) \\ & \vdots & \\ & = & \gcd(F_3, F_2) = 1 \end{array}\right\} \; n-1 \text{ adım}$$

elde edilir.

Daha önce

$$\gcd(300, 18) = \gcd(18, 12) = \gcd(12, 6) = 6$$

olduğunu gördük.

$300 = 16 \cdot 18 + 12$ olduğuna göre, $12 = 300 - 16 \cdot 18$ yazabiliriz. O halde

$$\gcd(300, 18) = \gcd(18, 300 - 16 \cdot 18)$$

olur.

Benzer şekilde

$$6 = 18 - 1 \cdot 12 = 18 - (300 - 16 \cdot 18) = 17 \cdot 18 - 300$$

olduğundan

$$\gcd(300, 18) = \gcd(300 - 16 \cdot 18, 18) = \gcd(300 - 16 \cdot 18, 17 \cdot 18 - 300)$$

elde edilir.

Bu durumu aşağıdaki şekilde genelleyebiliriz.

Teorem

$d = \gcd(a, b)$ ise m ve n tamsayılar olmak üzere,

$$d = am + bn$$

şeklinde yazılabilir.

Teoremden önce incelediğimiz örnek bize d sayısının sadece bu şekilde yazılabileceğini değil, bu yazımın nasıl bulunacağını da söyler.

Elbette d sayısının bu şekildeki yazılımı tek türlü değildir. Örneğin, $\gcd(111, 250) = 1$ sayısı

$$1 = -9 \cdot 111 + 4 \cdot 250 \quad \text{ve} \quad 1 = -259 \cdot 111 + 115 \cdot 250$$

şeklinde yazılabilir.

Alıştırma

Bir kabı, biri 17 diğeri 55 litre su alan ölçeklendirilmemiş iki kap yardımıyla tam olarak 1 litre suyla nasıl doldurursunuz açıklayınız.

Euclid bölme algoritmasını kullanarak 17 ve 55 sayılarının en büyük ortak bölenini bulalım.

$$\begin{aligned} \gcd(17,55) &= \gcd(4,17) && (55 = 3\times 17 + 4) \\ &= \gcd(1,4) && (17 = 4\times 4 + 1) \\ &= 1 \end{aligned}$$

olur. Tersten gidecek olursak,

$$\begin{aligned} 1 &= 17 - 4\times 4 \\ &= 17 - 4\times(55 - 3\times 17) \\ &= 13\times 17 - 4\times 55 \end{aligned}$$

elde ederiz. O halde 17 litrelik kap ile 13 kez su koyup, 55 litrelik kap ile 4 kez suyu boşaltırsak tam olarak 1 litre su elde ederiz.

Denklikler

a, b ve m tamsayılar ve $m > 0$ olsun. Eğer a ve b tamsayıları m ile bölündüğünde aynı kalanı veriyorsa

$$a \equiv b \pmod{m}$$

yazılır ve a denktir b mod m şeklinde okunur.

Buradan $q \equiv b \pmod{m}$ ise m, $b - a$ nın bir bölenidir diyebiliriz.

"$\equiv$" simgesi "$=$" simgesinin sağladığı birçok özelliği sağlar:

- $a \equiv a \pmod{m}$ (Yansıma)
- $a \equiv b \pmod{m}$ ise $b \equiv a \pmod{m}$ (Simetri)
- $a \equiv b \pmod{m}$ ve $b \equiv c \pmod{m}$ ise $a \equiv c \pmod{m}$ (Geçişme)

$a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ olsun. Aynı eşitliklerde olduğu gibi bu iki denkliğin toplamından, farkından ve çarpımından söz edebiliriz (bölümünü ileriye bırakıyoruz).

- $a + c \equiv b + d \pmod{m}$ (Alıştırma)
- $a - c \equiv b - d \pmod{m}$ (Alıştırma)
- $ac \equiv bd \pmod{m}$

  $a \equiv b \pmod{m}$ ise $m \mid b - a$ olur. Buradan, $b - a = k_1 m$ olacak şekilde k_1 tamsayısı vardır.

  Benzer şekilde $c \equiv d \pmod{m}$ ise $m \mid d - c$ olur. Yani, $d - c = k_2 m$ olacak şekilde k_2 tamsayısı vardır.

  Birinci eşitliği d ile ikinci eşitliği de a ile çarpıp toplarsak,

$$\begin{array}{rrl} & bd - \cancel{ad} & = k_1 dm \\ + & \cancel{ad} - ac & = k_2 am \\ \hline & bd - ac & = \underbrace{(k_1 d + k_2 a)}_{k} m \end{array}$$

  olur. O halde $m \mid bd - ac$. Yani, $ac \equiv bd \pmod{m}$ olur.

Bir denkliğin her iki tarafı aynı k tamsayısı ile çarpılırsa denklik bozulmaz. Yani,

$$a \equiv b \pmod{m} \text{ ise } ak \equiv bk \pmod{m}$$

olur.

Bu durumda Fermat'ın Küçük Teoremini şu şekilde de ifade edebiliriz:

$$p \text{ asal ise } a^p \equiv a \pmod{p}.$$

Alıştırma (6.7.1)

$12345 \equiv 54321 \pmod{m}$ olacak şekildeki en büyük m tamsayısı nedir?

$m = 54321 - 12345 = 41976$ alınırsa, istenen sonuç elde edilir.

Alıştırma (6.7.2-a,b)

Aşağıdakilerden hangileri doğrudur?

- $a \equiv b \pmod{c}$ ise $a + x \equiv b + x \pmod{c + x}$ olur.

  Doğru Değil!

  $$5 \equiv 8 \pmod{3}. \text{ Ancak, } \underbrace{5+2}_{2} \not\equiv \underbrace{8+2}_{0} \pmod{3+2}$$

- $a \equiv b \pmod{c}$ ise $ax \equiv bx \pmod{cx}$

  Doğrudur.
  Gerçekten de $a \equiv b \pmod{c}$ ise $c \mid b - a$ olur. Buradan $b - a = kc$ olacak şekilde k tamsayısı vardır. O halde

  $$x(b-a) = xkc \quad \Rightarrow \quad cx \mid x(b-a) \quad \Rightarrow \quad ax \equiv bx \pmod{cx}$$

  olur.

Alıştırma (6.7.2-c,d)

- $$\left.\begin{array}{ll} a \equiv b & (\text{mod } c) \\ x \equiv y & (\text{mod } z) \end{array}\right\} \Rightarrow a + x \equiv b + y \quad (\text{mod } c + z)$$

Doğru değil!

$$\left.\begin{array}{rcll} 3 & \equiv & 6 & (\text{mod } 3) \\ 10 & \equiv & 3 & (\text{mod } 7) \end{array}\right\} \text{ Ancak, } \underbrace{3 + 10}_{3} \not\equiv \underbrace{6 + 3}_{9} \quad (\text{mod } 3 + 7)$$

- $$\left.\begin{array}{ll} a \equiv b & (\text{mod } c) \\ x \equiv y & (\text{mod } z) \end{array}\right\} \Rightarrow ax \equiv by \quad (\text{mod } cz)$$

Doğru değil!

$$\left.\begin{array}{ll} 7 \equiv 10 & (\text{mod } 3) \\ 2 \equiv 10 & (\text{mod } 2) \end{array}\right\} \text{ Ancak, } \underbrace{7 \cdot 2}_{2} \not\equiv \underbrace{10 \cdot 10}_{4} \quad (\text{mod } 3 \cdot 2)$$

Alıştırma (6.7.3)

$a \equiv b \pmod 0$ nasıl tanımlanabilir?

$$\begin{aligned} a \equiv b \pmod 0 &\Rightarrow b - a = k \cdot 0 \qquad (k \in \mathbb{Z}) \\ &\Rightarrow b - a = 0 \\ &\Rightarrow b = a \end{aligned}$$

O halde eşitlik, denkliğin özel bir halidir.

Acayip Sayılar

Soru

Perşembe + Cuma = ?

Günlerin pazar ile başladığını kabul edersek,

0	1	2	3	4	5	6
Pazar	Pazartesi	Salı	Çarşamba	Perşembe	Cuma	Cumartesi

$$\text{Perşembe} + \text{Cuma} = ?$$
$$4 + 5 = ?$$
$$9 = ?$$

$$9 \equiv 2 \mod 7 \quad \Rightarrow \quad \text{Perşembe} + \text{Cuma} = \text{Salı}$$

Buradan,

$$\begin{aligned} \text{Çarşamba} \cdot \text{Perşembe} &= \text{Cuma}, \\ (\text{Perşembe})^2 &= \text{Salı}, \\ \text{Pazartesi} - \text{Cumartesi} &= \text{Salı} \end{aligned}$$

yazılabilir.

Bu işlemler ayrıca değişme, birleşme, vb özellikleri de sağlar:

- $\text{Salı} + \text{Cuma} = \text{Cuma} + \text{Salı}$
- $(\text{Pzt} + \text{Salı}) + \text{Çarş} = \text{Pzt} + (\text{Salı} + \text{Çarş})$
- $(\text{Pzt} \cdot \text{Salı}) \cdot \text{Çarş} = \text{Pzt} \cdot (\text{Salı} \cdot \text{Çarş})$
- $(\text{Pzt} + \text{Cuma})\text{Cuma} = \text{Pzt}$
- $\text{Çarş} + \underbrace{\text{Pazar}}_{0} = \text{Çarş}$
- $\text{Cuma} \cdot \underbrace{\text{Pazar}}_{0} = \text{Pazar}$
- $\text{Cuma} \cdot \underbrace{\text{Pzt}}_{1} = \text{Cuma}$

Soru

Peki bölme işleminden söz edebilir miyiz?

$$\text{Cumartesi} \;\big|\; \underline{\text{Çarşamba}} \qquad 6 \;\big|\; \underline{3} \qquad \text{Salı ?}$$
$$? \qquad\qquad\qquad 2$$

Sağlamasını yapalım: Salı $\cdot$ Çarşamba $=$ Cumartesi✓

$$\text{Peki} \qquad \text{Salı} \;\big|\; \underline{\text{Çarşamba}} \qquad \frac{2}{3}? \qquad \text{Tamsayı Değil?}$$
$$? \qquad\qquad\qquad$$

$\dfrac{\text{Salı}}{\text{Çarşamba}} = X$ dersek, Çarşamba $\cdot\, X =$ Salı olacak şekildeki X leri arıyoruz.

Çarşamba $\cdot$ Çarşamba $=$ Salı olduğundan, $\dfrac{\text{Salı}}{\text{Çarşamba}} =$ Çarşamba olur.

Böylece yeni sayılar (kesirli sayılar) tanımlamaya gerek kalmadan bölme işlemini *7 sayıdan oluşan* bu acayip sayılarımıza taşıyabiliriz.

Acaba bu işlemi her zaman yapabilir miyiz?

$$\frac{\text{Çarşamba}}{\text{Cuma}} = X \quad \Rightarrow \quad X \cdot \text{Cuma} = \text{Çarşamba}$$

X i bulabilmek için X in farklı değerleri için $X \cdot \text{Cuma}$ işleminin sonucunun da farklı olması gerekir!

Gerçekten de, eğer farklı X ler için $X \cdot \text{Cuma}$ farklı olmazsa yani,

$$X \cdot \text{Cuma} = Y \cdot \text{Cuma} \qquad (*)$$

olursa,

$$\underbrace{(X - Y)}_{\neq 0} \cdot \underbrace{\text{Cuma}}_{\neq 0} = \underbrace{\text{Pazar}}_{0}$$

olur.

Bu ise sıfırdan farklı iki sayının çarpımının sıfır olması demektir (Pazar olmayan iki günün çarpımı da pazar değildir).

$(*)$ eşitliğini denklikler yardımıyla

$$(x - y) \cdot 5 \equiv 0 \mod 7$$

şeklinde yazabiliriz. Burada x ve y sayıları X ve Y günlerine karşılık gelmektedir.

Buradan $7 \mid (x - y) \cdot 5$ olur.

7, 5 ve $(x - y)$ sayılarının çarpımını böldüğünden ve *7 asal olduğundan* bu sayılardan en az birini de bölmelidir.

Ancak, $7 \nmid 5$ ve x ve y negatif olmayan 7 den küçük sayılar olduğundan $7 \nmid x - y$ olur.

O halde $(*)$ eşitliğinin doğru olamayacağını söyleyebiliriz.

Böylece $X \cdot$ Cuma sonuçlarının tümü farklı olur ve bunların sayısı 7 olur. Yani, haftanın her günü $X \cdot$ Cuma şeklinde yazılabilir.

O halde Çarşamba da $X \cdot$ Cuma şeklinde yazılabilir. Yani, Cuma ile bölme işlemi iyi tanımlıdır.

Böylece Pazar hariç herhangi bir gün ile bölme işlemi yapılabilir.

Eğer Pazar ile bölme yaparsak,

$$X \cdot \text{Pazar}$$

işleminin sonucu tüm X değerleri için aynı (Pazar) olur.

O halde yukarıda işaret edilen nedenden ötürü Pazar ile bölme mümkün değildir.

Acaba burada haftanın günlerinin sayısının 7 olmasının bir önemi var mı?

Bir haftadaki gün sayısının 10, 13 ya da 365 olduğu bir toplulukta da benzer olarak aynı işlemleri tanımlayamaz mıyız?

Bir haftadaki gün sayısı m olsun. Yeni gün isimleri üretmektense haftanın günlerini $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ ile gösterelim.

Önce sayıların üzerindeki çizginin anlamını açıklayalım: Örneğin, $\overline{2}$ sadece haftanın 2. gününe değil, $m+2.$, $2m+2.$, vb. günlerine de karşılık gelmektedir (yani m ile bölündüğünde 2 kalanını veren günler).

$a+b$ nin m ile bölümünden kalan c olmak üzere, $\overline{a}+\overline{b}=\overline{c}$ şeklinde toplama işlemini tanımlayabiliriz. Benzer şekilde çıkarma ve çarpma işlemleri de tanımlanabilir. Böylece üzerinde temel aritmetik işlemlerin olduğu m tane sayıdan oluşan yeni bir sayı sistemi elde ederiz. Bu aritmetik işlemlerin özel olarak $m=7$ için sağladığı bazı özellikleri az önce inceledik.

Bu çeşit aritmetiğe *modüler aritmetik* denir.

Yine bölme işleminin üzerinde ayrıca durmak gerekir. $m = 7$ durumu için hatırlarsanız bölme işlemi tanımlarken 7 nin asallığı kullanıldı.

Modülün asal olup olmaması modüler aritmetik üzerinde çok büyük bir fark yaratır. Biz bundan sonraki bölümlerde genelde hep modülün asal olduğu durumları inceleyeceğiz. Bu durumu belirtmek için de genelde modülü p ile göstereceğiz.

Bu durumda $\overline{0}, \overline{1}, \ldots, \overline{p-1}$ sayılarından oluşan ve dört işlemin yukarıdaki şekilde tanımlandığı sisteme *asal cisim* (prime field) denir.

En küçük asal sayı 2 olduğundan en basit asal cisim $\overline{0}$ ve $\overline{1}$ sayılarından oluşan iki elemanlı cisimdir. Toplama ve çarpma aşağıdaki tablolarla verilebilir:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Çoğu zaman sayıların üzerindeki çizgi işareti koyulmaz. Ancak, bu durumda $1+1$ işleminin sonucunun 2 mi yoksa 0 mı olduğunu bilmemiz gerekir. Bunun için 2-elemanlı cebirde $+$ işareti $\oplus$ işaretiyle, $\cdot$ işareti de $\odot$ işareti ile değiştirilir.

Bu notasyonlarla toplam ve çarpım tablolarını

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

şeklinde yazabiliriz.

Bu cisim oldukça basit olmasına karşın bilgisayar bilimleri, bilişim sistemleri, matematiksel mantık vb. alanlar bu cismi sıklıkla kullanır. Bu cismin elemanları "EVET–HAYIR", "DOĞRU–YANLIŞ", "SİNYAL VAR–SİNYAL YOK", vb. şekillerde yorumlanabilir.

Alıştırma (6.8.3)

Bir örnek ile modül 6 ya göre sıfırdan farklı bir sayı ile bölme işleminin her zaman geçerli olmayabileceğine bir örnek veriniz.
Örneğinizi asal olmayan herhangi bir modül için genelleştiriniz.

$2 \cdot 0 \equiv 2 \cdot 3 \mod 6$ olur. Fakat, $0 \not\equiv 3 \mod 6$.

Genelleyecek olursak, $a, b > 1$ olmak üzere modül $m = ab$ şeklinde ise

$$a \cdot 0 \equiv a \cdot b \mod m \text{ olmasına karşın, } 0 \not\equiv b \mod m$$

olur.

Modüler Aritmetikte Bölme

Modüler aritmetikte bölme işlemini yapabilmek için modülün asal sayı olması gerektiğinden epeyce söz ettik. Ancak, bölme işleminin nasıl yapılacağından hiç bahsetmedik.

$p = 7$ iken bir bölme işlemi yapmıştık. Tek yaptığımız 0 ile $p - 1$ arasındaki tüm sayıların eşitliği sağlayıp sağlamadığını kontrol etmekti.

Ancak, p asal sayısı çok büyük ise bu yöntem hiç de akılcı değildir. Örneğin,

Soru

$\overline{53}$ *sayısını mod* 234 527 *ye göre* $\overline{2}$ *sayısına bölersek sonuç nedir?*

Daha basit bir soru ile başlayalım: mod 234 527 ye göre $\overline{1}$ in $\overline{2}$ ye bölümü nedir?

Eğer $\frac{\overline{1}}{\overline{2}} = \overline{a}$ ise her iki tarafı $\overline{53}$ ile çarparak $\frac{\overline{53}}{\overline{2}} = \overline{a} \cdot \overline{53}$ elde ederiz.

Bu eşitliğin sağ tarafı ise kolayca hesaplanabilir.

Genelleyecek olursak, bir p asal modülü verildiğinde $1 \leq a \leq p-1$ olacak şekildeki a sayısı için

$$\overline{ax} = \overline{1}$$

eşitliğini sağlayan $0 \leq x \leq p-1$ olacak şekildeki x sayısını arıyoruz (Az önceki örnekteki $\overline{2}$ yerine $\overline{a}$ alındı, $\overline{a}$ yerine ise $\overline{x}$ alındı).

Ya da denklikler ile ifade edecek olursak,

$$ax \equiv 1 \mod p$$

olur.

Euclid bölme algoritması yardımıyla bu problemin çözümü oldukça kolaydır:

a ve p sayılarının en büyük ortak bölenini hesaplayalım.

p asal sayı ve $a < p$ olduğu için bu iki sayının en büyük ortak böleninin 1 olduğunu hemen söyleyebilirsiniz. Ancak, Euclid bölme algoritması bize

$$\gcd(a, p) = 1 = au + pv$$

olacak şekildeki u ve v tamsayılarının nasıl bulunacağını da söyler.
Bu eşitlik yardımıyla

$$au \equiv 1 \mod p$$

yazabiliriz. Geriye sadece bu u sayısının 1 ile $p-1$ arasında olup olmadığını kontrol etmek kalır.

Bunun için u nun p ye bölümünden kalanı x ile gösterelim.
Yani, $x \equiv u \mod p$ olsun. Her iki tarafı aynı sayı ile çarpabiliriz. O halde a ile çarparsak $ax \equiv au \equiv 1 \mod p$ olur. $0 \leq x \leq p-1$ olduğundan istenen x sayısı elde edilmiş olur.

Örnek

$a = 2$ ve $p = 234\,527$ için bu yöntemi uygulayalım.

$234\,527 = 117\,263 \cdot 2 + 1$ olduğundan

$$1 = \underbrace{2}_{a} \cdot \underbrace{(-117\,263)}_{u} + \underbrace{234\,527}_{p} \cdot \underbrace{1}_{v}$$

olur. Dikkat ederseniz u sayısı 1 ile $p-1$ arasında değil. Bu durumda x sayısını bulmak için -117263 sayısının 234527 ile bölümünden kalanı bulmalıyız.

$$\begin{array}{r|l} -117\,263 & 234\,527 \\ \cline{2-2} -234\,527 & -1 \\ \cline{1-1} 117\,264 & \end{array}$$

olduğuna göre $x = 117\,264$ olur.

Böylece, $\overline{\frac{1}{2}} = 117\,264$ elde edilir.

Alıştırma (6.8.4)

Mod 234 527 ye göre $\overline{1}/\overline{53}$ işleminin sonucu nedir?

$$\begin{aligned} \gcd(53, 234\,527) &= \gcd(2, 53) && (234\,527 = 4\,425 \cdot 53 + 2) \\ &= \gcd(1, 2) = 1 && (53 = 26 \cdot 2 + 1) \end{aligned}$$

olur. Tersten gidersek,

$$1 = 53 - 26 \cdot 2 = 53 - 26 \cdot (234\,527 - 4\,425 \cdot 53) = 53 \cdot \underbrace{115\,051}_{u} + 234\,527 \cdot \underbrace{(-26)}_{v}$$

elde ederiz. $1 \leq 115\,051 \leq p - 1$ koşulu sağlandığından,

$$\frac{\overline{1}}{\overline{53}} = \overline{115\,051}$$

olur.

Sayılar Teorisi ve Kombinatorik

Önceki derslerde bahsettiğimiz tümevarım yöntemi, güvercin yuvası ilkesi, içerme–dışlama prensibi gibi kombinatoryal yöntemler sayılar teorisinde de oldukça kullanışlıdır.
Tümevarım yöntemini sayılar teorisinde defalarca kez kullandık. Şimdi güvercin yuvası ilkesinin kullanımına bir örnek verelim.

Örnek

$a_1, a_2, \ldots, a_n$ doğal sayıları verildiğinde, elemanları toplamı n ile bölünecek şekilde bu sayıların boş kümeden farklı bir alt kümesi vardır.

Aşağıdaki n tane sayıyı ele alalım:

$$\begin{aligned} b_1 &= a_1 \\ b_2 &= a_1 + a_2 \\ b_3 &= a_1 + a_2 + a_3 \\ &\vdots \\ b_n &= a_1 + a_2 + a_3 + \cdots + a_n \end{aligned}$$

Eğer bu şekilde tanımladığımız $b_1, b_2, \ldots, b_n$ sayılarından en az birisi n ile bölünüyorsa istenen alt küme elde edilmiş olur.

Eğer hiç birisi n ile bölünmüyorsa, $b_1, b_2, \ldots, b_n$ sayılarının n ile bölümünden kalanları sırasıyla $r_1, r_2, \ldots, r_n$ ile gösterelim.

$i = 1, 2, \ldots, n$ için (güvercinler) $0 < r_i < n$ olduğundan $n - 1$ farklı kalan vardır (güvercin yuvaları). Güvercin yuvası ilkesine göre n ile bölündüğünde aynı kalanı verecek b_i ve b_j sayıları vardır.

Genelliği bozmaksızın $1 \leq i < j \leq n$ olduğunu kabul edelim.

O zaman bu b_i ve b_j sayılarının farkı n ile bölünür.

$$b_j - b_i = a_{i+1} + a_{i+2} + \cdots + a_j$$

olduğundan

$$\{a_{i+1}, a_{i+2}, \ldots, a_j\}$$

alt kümesi istenen alt küme olur.

Şimdi de içerme–dışlama prensibinin kullanıldığı bir örneği inceleyelim.

Örnek

$1, 2, \ldots, 1200$ sayılarının kaç tanesi 1200 ile aralarında asaldır?

1200 sayısını asal çarpanlarına ayırırsak $1200 = 2^4 \cdot 3 \cdot 5^2$ olur.

O halde verilen sayılardan 2,3 ve 5 ile bölünenler 1200 ile aralarında asal değildir. c_1 ile bu sayılardan 2 ile bölünenlerin kümesini, c_2 ile bu sayılardan 3 ile bölünenlerin kümesini ve c_3 ile 5 ile bölünenlerin kümesini gösterecek olursak,

$$|c_1| = \frac{1200}{2}, \quad |c_2| = \frac{1200}{3}, \quad |c_3| = \frac{1200}{5},$$

$$|c_1 c_2| = \frac{1200}{6}, \quad |c_1 c_3| = \frac{1200}{10}, \quad |c_2 c_3| = \frac{1200}{15},$$

$$|c_1 c_2 c_3| = \frac{1200}{30}$$

olur.

Şimdi içerme–dışlama prensibini kullanacak olursak,

$$\begin{aligned} |\bar{c}_1 \bar{c}_2 \bar{c}_3| &= 1200 - \left(\frac{1200}{2} + \frac{1200}{3} + \frac{1200}{5} \right) \\ &\quad + \left(\frac{1200}{2 \cdot 3} + \frac{1200}{2 \cdot 5} + \frac{1200}{3 \cdot 5} \right) - \frac{1200}{2 \cdot 3 \cdot 5} \\ &= 320 \end{aligned}$$

elde edilir.

Eğer yukarıdaki eşitliğin sağ tarafını 1200 parantezine alırsak,

$$\begin{aligned} &1200 \cdot \left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{2 \cdot 5} + \frac{1}{3 \cdot 5} - \frac{1}{2 \cdot 3 \cdot 5} \right) \\ &\qquad = 1200 \cdot \left(1 - \frac{1}{2} \right) \cdot \left(1 - \frac{1}{3} \right) \cdot \left(1 - \frac{1}{5} \right) \end{aligned}$$

elde ederiz.

Genelleyecek olursak, n bir doğal sayı olsun ve $1, 2, \ldots, n$ sayılarından n ile aralarında asal olanların sayısını $\phi(n)$ ile gösterelim.

Açıktır ki, $\phi(1) = 1$ ve p bir asal sayı ise bu sayıdan küçük olan her sayı p ile aralarında asal olur. Yani $\phi(p) = p - 1$ olur.

Eğer n sayısı asal sayı değil ve $p_1, p_2, \ldots, p_r$ sayıları n nin farklı asal çarpanları ise yine içerme–dışlama prensibi yardımıyla

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

yazılabilir. (Alıştırma 6.9.2)

Asallık Testleri

Acaba 123 456 sayısı asal mıdır? Elbette çift sayı olduğu için asal olmadığını hemen söyleyebiliriz.

Peki 1 234 567 sayısı asal mıdır? Bu sorunun cevabını hemen vermek mümkün olmasa da eğer böyle bir zorunluluk varsa $2, 3, 4, 5, \ldots$ sayıları ile bölünebilir olup olmadığına bakabilirsiniz. Yeterince sabırlıysanız 127 ye ulaştığınızda $1\,234\,567 = 127 \cdot 9\,721$ sonucuna yani bu sayının asal olmadığı sonucuna ulaşırsınız.

Peki ya 1 234 577? Yine bu sayının $2, 3, 4, 5, \ldots$ sayıları ile bölünüp bölünmediğini kontrol edebilirsiniz. Ancak, bu kez uygun bir bölen bulmanız mümkün değildir. Elbette bu sayıya kadar olan tüm sayılarla değil, 1 234 577 sayısının karekökü olan $1\,111.1\ldots$ sayısına kadar olan tüm sayılarla bölünebilirliğe bakmak yeterlidir.

Son olarak

$$1\,111\,222\,233\,334\,444\,555\,566\,667\,777\,888\,899\,967$$

sayısı için ne söyleyebilirsiniz?

Eğer bu sayı asalsa (ki öyle) 10^{36} dan daha büyük olan bu sayının 10^{18} den daha büyük olan karakökünе kadar olan tüm sayılar ile tek tek bölünebilirliğinin incelenmesi gerekir.

Bu ise günümüzün en güçlü bilgisayarları için dahi çok zor bir işlemdir.

Fermat Testi

Maple, Matlab, vb. bilgisayar programları yukarıdaki sayının asal olup olmadığını inanılmayacak kadar kısa sürelerde söyleyebilir. Peki bu nasıl mümkün oluyor? Bir yaklaşım Fermat'ın Küçük Teoreminden yararlanmaktır.

Fermat'ın Küçük Teoremi'ni kullanırsak p asal ise $a = 2$ için $p \mid 2^p - 2$ olması gerektiğini söyleyebiliriz. Eğer p yi tek sayı olarak kabul edersek (bu durumda sadece 2 yi gözardı etmiş oluruz), p asal ise $p \mid 2^{p-1} - 1$ olacağını Fermat'ın Küçük Teoreminden biliyoruz.

$n \mid 2^{n-1} - 1$ koşulunu asal olmayan sayılar için test edecek olursak, öncelikle her n tam sayısı için $2^{n-1} - 1$ tek sayı olduğundan çift sayılar için koşulun sağlanmayacağını hemen söyleyebiliriz.

Bazı tek sayılar için elde edilen sonuçlar ise aşağıda görülmektedir.

$$9 \nmid 2^8 - 1 = 255, \qquad 15 \nmid 2^{14} - 1 = 16383,$$
$$21 \nmid 2^{20} - 1 = 1048575, \quad 25 \nmid 2^{24} - 1 = 16777215$$

Bir n sayısının asal olup olmadığı $n \mid 2^{n-1} - 1$ koşuluyla test edilebilir gibi gözükse de bu yöntemin bazı kusurları vardır:

Büyük Üsleri Nasıl Hesaplayabiliriz?

$2^{n-1} - 1$ ifadesi çok basit bir ifade gibi gözükse de bu ifadenin hesaplanması hiç de kolay değildir.

Gerçekten de, 2^{n-1} sayısını hesaplamak için $n - 2$ kez 2 ile çarpma işleminin yapılması gereklidir. 100 basamaklı bir n sayısı için bu yaklaşık 10^{100} adım demektir.

Ancak, biraz hile ile adım sayısını azaltmak mümkündür. Örneğin, 2^{24} sayısını hesaplamak için $2^3 = 8$ ile başlayıp, karesini alıp $2^6 = 64$, tekrar kare alarak $2^{12} = 4096$, son bir kez daha kare alarak, $2^{24} = 16777216$ sonucuna 23 kez çarpma yapmak yerine sadece 5 kez çarpma yaparak ulaşabiliriz.

Bu yöntem 24 çift sayı olduğu için sadece çift sayılar için kullanılabilir gibi gözükse de tek sayılar için de benzer sonucu elde edebiliriz.

Örneğin, 2^{29} sayısını

$$2^2 = 4, \quad 2^3 = 8, \quad 2^6 = 64, \quad 2^7 = 128, \quad 2^{14} = 16384,$$
$$2^{28} = 268435456, \quad 2^{29} = 536870912$$

şeklinde hesaplayabiliriz.

Bu durumda 2 nin tek kuvveti hesaplanacak ise bir önceki çift kuvvet yukarıdaki işlemler sondan başa doğru düşünülerek hesaplanıp, daha sonra 2 ile çarpılarak elde edilebilir.

Büyük Sayılardan Nasıl Kaçınabiliriz?

Her ne kadar yukarıdaki şekilde işlem sayısı azaltılabilse de elde edilen sayılar çok büyük sayılardır.

Eğer n, 100 basamaklı bir sayı ise sadece 2^{n-1} sayısı değil, bu sayının basamak sayısı da astronomik bir sayıdır. Değil bu sayının n ile bölünebilirliğinin kontrol edilmesi, bu sayının yazılması bile çok mümkün değildir.

Bu durumda n ile bölünebilirliği kontrol etmenin bir yolu, sayı n den büyük olduğunda n ile bölümünden kalanı kullanmaktır (başka bir ifade ile mod n ile çalışmaktır).

Örneğin, $25 \mid 2^{24} - 1$ koşulunun sağlanıp sağlanmadığını kontrol etmek istiyorsak, önce 2^{24} sayısını hesaplamalıyız.

- Yukarıdaki yöntemle $2^3 = 8$ ile başlarsak, $2^6 = 64$ olur.
- Elde edilen sayı 64, 25 den daha büyük olduğu için $64 \div 25$ işleminin kalanı 14 ile 64 ü değiştirelim.
- Bir sonraki adımda 2^{12} sayısına ulaşmak için tekrar kare alırsak, $14^2 = 196$ elde ederiz.
- Yine elde edilen sayı 196, 25 den büyük olduğu için $196 \div 25$ işleminin kalanı 21 ile bu sayıyı değiştirelim.
- Son kez kare alırsak, 2^{24} ü elde ederiz. $21^2 = 441$ sayısının 25 ile bölümünden kalan ise 16 olur.

Böylece $16 - 1 = 15$ sayısı 25 ile bölünmediğinden 25 asal sayı değildir.

Bu yöntem elle hesaplamada çok da kullanışlı olmasa da bilgisayar üzerinde kolayca uygulanabilir.

Eğer n sayısı 2 lik sistemde k basamaklı ise 2^n sayısı en fazla $2k$ çarpma yapılarak hesaplanabilir.

Bu hesaplama esnasında sayıları küçük tutmak için her bir adımda n ile sadece bir kez bölme yapılarak kalanlar hesaplanacaktır.

Bu durumda her bir adımda çalışılan sayılar n^2 sayısından daha büyük olmayacaktır.

Sahte Asallar

Fermat Teoremini kullanarak elde ettiğimiz bu yöntemin önemli bir kusuru daha vardır.

Biliyoruz ki, n sayısı $2^{n-1}-1$ sayısını bölmüyorsa (test başarısız ise) bu sayı asal sayı değildir.
Peki ya tersi durumda, yani $n \mid 2^{n-1}-1$ ise bu durumda n asal sayıdır diyebilir miyiz?

Fermat Teoreminden bu sonucu çıkartmak mümkün değildir. Acaba $n \mid 2^{n-1}-1$ koşulunu sağlayan n bileşik (composite) sayısı var mıdır?

Ne yazık ki, bu sorunun cevabı "evet" dir.

Bu koşulu sağlayan en küçük bileşik sayı $341 = 11 \cdot 31$ sayısıdır. Gerçekten de

$$341 \mid 2^{340}-1$$

koşulu sağlanır.

$341 = 11 \cdot 31$ olduğundan

$$341 \mid 2^{340} - 1$$

olduğunu görmek için hem $11 \mid 2^{340} - 1$ hem de $31 \mid 2^{340} - 1$ olduğunu görmek yeterlidir.
11 asal olduğundan Fermat'ın Küçük Teoreminden $11 \mid 2^{10} - 1$ yazabiliriz.
Ayrıca, a bir tamsayı ve n de pozitif bir tamsayı ise her zaman

$$a - 1 \mid a^n - 1$$

olduğundan (Alıştırma 6.1.6-b), $a = 2^{10}$ ve $n = 34$ alınırsa

$$2^{10} - 1 \mid 2^{340} - 1$$

elde edilir. Buradan

$$11 \mid 2^{10} - 1 \text{ ve } 2^{10} - 1 \mid 2^{340} - 1 \quad \Rightarrow \quad 11 \mid 2^{340} - 1$$

olur. Yine Alıştırma 6.1.6-b yi $a = 2^5$ ve $n = 68$ için kullanırsak,

$$31 = 2^5 - 1 \mid (2^5)^{68} - 1 = 2^{340} - 1$$

olur.

Bu şekilde asal olmadığı halde Fermat Testinden geçen sayılara *sahte asallar* (pseudoprimes, fake primes) denir.

Tabanı 2 olarak aldığımızda 1 ile 10000 arasında bu sayılardan 22 tane mevcuttur.

O halde elde ettiğimiz asallık testi bu sayılarda doğru sonuç vermeyecektir. Bir başka ifadeyle test bu haliyle bir asallık testi olamaz.

Bazı tabanlardaki sahte asallar aşağıda listelenmiştir.

a	a–tabanındaki sahte asallar
2	341, 561, 645, 1105, 1387, 1729, 1905, ...
3	91, 121, 286, 671, 703, 949, 1105, 1541, 1729, ...
4	15, 85, 91, 341, 435, 451, 561, 645, 703, ...
5	4, 124, 217, 561, 781, 1541, 1729, 1891, ...

Bu durumda aklımıza gelen bir başka yol Fermat'ın Küçük Teoreminin gücünü tam olarak kullanmak olabilir.

Yani, n sayısının asallığını kontrol etmek için $2, 3, \ldots, n-1$ için tek tek $n \mid 3^n - 3$, $n \mid 4^n - 4, \ldots$ ifadelerinin doğruluğu kontrol edilebilir.

Örneğin, yukarıda incelediğimiz sahte asal 341 için $341 \mid 3^{341} - 3$ koşulu sağlanmaz.

Eğer yeterince sabırlıysanız aşağıdaki test sizi doğru sonuca ulaştıracaktır:

$n > 1$ tamsayısının asal sayı olması için gerek ve yeter koşul her $a = 1, 2, 3, \ldots, n-1$ için $n \mid a^{n-1} - 1$ Fermat Testinin sağlanmasıdır.

Bu test bize asal sayıların her taban için Fermat Testini sağladığını, öte yandan n bileşik sayı ise n ile aralarında asal olmayan ve her bir $1 \leq a \leq n-1$ için koşulu sağlamayan a tamsayılarının var olduğunu söyler.

Ancak, gerçekte Fermat Testi çok da kullanışlı değildir.

Size yüzlerce basamaklı bir n sayısının verildiğini ve bu sayının asallığının incelenmesinin istendiğini düşünün.

Fermat Testini önce tabanı 2 alıp, eğer koşul sağlanıyorsa sonra tabanı 3 alıp, eğer şanslıysanız ve sayı asal değilse koşul sağlanmayana kadar; sayı asal ise $n-1$ e kadar bu şekilde devam etmelisiniz.

Bunun yerine süreci biraz kısaltıp, n ile ortak böleni olan ilk a sayısına kadar devam etmek yeterlidir. Çünkü, bu sayı n nin en küçük asal çarpanı olacaktır.

Ancak, Bu bile süreci çok fazla kısaltmaz. Gerçekten de, $n = p \cdot q$ şeklinde yazılabiliyorsa (p ve q birbirinden farklı 100 basamaklı asal sayılar olsun bu durumda n, 200 ya da 199 basamaklıdır), p ve q nun en küçüğüne kadar olan tüm sayıları tek tek denemeliyiz.

Bu ise 10^{99} dan da fazla deneme demektir!

Diğer taraftan 2 ile başlayıp sıra ile gitmek yerine $1 \leq a \leq n-1$ olacak şekilde n ile aralarında asal olmayan rastgele bir a tamsayısı seçip, a yı taban alarak testi uygulayabiliriz.
Eğer bu a için test başarısız ise n nin asal olmadığını hemen söyleyebiliriz.

Acaba bu durumda daha kısa sürede cevap verme şansımız daha mı yüksektir? Elbette bu n ye bağlıdır ve n nin bazı değerleri için durum oldukça kötüdür.

Örneğin, p ve q farklı asal sayılar olmak üzere $n = p \cdot q$ ise n ile aralarında asal olmayan sayıları kolayca yazabiliriz.

$$\underbrace{p, 2p, \ldots, (q-1)p, qp, q, 2q, \ldots, (p-1)q, pq}_{p+q-1 \text{ tane (2 tane } pq \text{ olduğundan)}}$$

$2 \cdot 10^{99} < p + q - 1 < 2 \cdot 10^{100}$ olduğundan testi başarısız kılacak a sayısına rastlama olasılığı

$$\frac{2 \cdot 10^{100}}{10^{199}} = 2 \cdot 10^{-99}$$

olur. Bu ise uygulamada çok da anlamlı olmayan bir olasılıktır.

Carmichael Sayıları

Ne yazık ki sahte asallardan daha da kötü, n ile aralarında asal olan ve her a tabanı için Fermat testini sağlayan fakat asal olmayan sayılar da mevcuttur. Bu sayılara Carmichael sayıları[1] denir. Bu sayılardan bazıları aşağıda verilmiştir.

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, \ldots$$

Bu sayılar oldukça ender olmasına karşılık Fermat Testinin yeterince tatmin edici olmadığının bir göstergesidir.

[1] İlk olarak 1910 yılında R. D. Carmichael bu sayıların varlığını keşfetmiş ve 15 tanesini hesaplamıştır. Ayrıca bu sayıların sonlu sayıda olmadığı sanısını da ortaya atmıştır. 1956 da Erdos büyük Carmichael sayılarının hesaplanması için bir yöntem vermiş. 1994 de ise Alford tarafından Carmichael sayılarının sonlu olmadığı kanıtlanmıştır.

Miller–Rabin Testi 1970 lerin sonunda M. Rabin ve G. Miller Fermat Teoremini biraz daha güçlendirerek Carmichael sayıları gibi sorunların da üstesinden gelebilecek basit bir yöntem buldular.

Bu yöntemi en küçük Carmichael sayısı 561 üzerinde inceleyelim:

$(x^2-1)=(x-1)(x+1)$ özdeşliğini kullanarak $a^{560}-1$ ifadesini çarpanlara ayıralım:

$$\begin{aligned} a^{560}-1 &= (a^{280}-1)(a^{280}+1) \\ &= (a^{140}-1)(a^{140}+1)(a^{280}+1) \\ &= (a^{70}-1)(a^{70}+1)(a^{140}+1)(a^{280}+1) \\ &= (a^{35}-1)(a^{35}+1)(a^{70}+1)(a^{140}+1)(a^{280}+1) \end{aligned}$$

Eğer 561 asal ise Fermat Teoremine göre her $1 \leq a \leq 560$ için $561 \mid a^{560}-1$ olmalıdır. Ayrıca, bir asal sayı bir çarpımı bölüyorsa çarpanlardan en az birini de böler. Bu durumda

$$561 \mid a^{35}-1, \quad 561 \mid a^{35}+1, \quad 561 \mid a^{70}+1, \quad 561 \mid a^{140}+1, \quad 561 \mid a^{280}+1$$

ifadelerinden en az birisi doğru sağlanmalıdır.

Oysa, $a=2$ için bu ifadelerin hiç birisi sağlanmaz.

Miller-Rabin testi yukarıda bahsedilen yöntemi kullanır.

Asal olup olmadığını öğrenmek istediğimiz $n > 1$ tek sayısı verilmiş olsun. Bu durumda $1 \leq a \leq n-1$ olacak şekilde rastgele bir a sayısı seçelim ve $a^n - a$ ifadesini ele alalım.

Bu ifadeyi $a(a^{n-1} - a)$ şeklinde çarpanlara ayırıp, $x^2 - 1 = (x-1)(x+1)$ özdeşliğini kullanarak az önceki gibi ayırabildiğimiz kadar çarpanlara ayıralım.

Son olarak da her bir çarpanın n ile bölünüp bölünmediğine bakalım.

Eğer test başarısız ise hemen n asal değildir diyebiliriz.

Peki ya test başarılı ise?

Maalesef bu durumda n sayısı bileşik sayı olabilir.

Bu durumun ortaya çıkma olasılığı $1/2$ den daha küçüktür (a yı rastgele bir sayı olarak seçmiştik). Eğer bu işlemi rastgele seçilen farklı a sayıları için 10 kez tekrarlayacak olursak, testin hatalı sonuç verme olasılığı 2^{-10} dan $(2^{-10} < \frac{1}{1000})$ daha da az olur.

Eğer 100 kez tekrarlayacak olursak bu olasılık $2^{-100} < 10^{-30}$ unda altındadır ki, bu oldukça küçük bir olasılıktır.

Algoritma yeterli sayıda tekrar edildiğinde hatalı sonuç verme olasılığı çok küçük olduğundan Maple, Matlab gibi programlarda bu algoritma kullanılır.