Algebra és számelmélet gyakorlat
2023/2024 I. félév

2023. Szeptember 15.

1. Fermat számok

Tekintsük a $2^k + 1$ alakú számokat:

$2^1 + 1 = 3$ prím
$2^2 + 1 = 5$ prím
$2^3 + 1 = 9$ nem prím
$2^4 + 1 = 17$ prím
$2^5 + 1 = 33$ nem prím
$2^6 + 1 = 65$ nem prím
$2^7 + 1 = 129$ nem prím
$2^8 + 1 = 257$ prím

1.1. Állítás. *Ha $k > 0$ és $2^k + 1$ prímszám, akkor k kettőhatvány.*

1.1. Bizonyítás. *Ha $k = 2^n \cdot m$ alakú, ahol m páratlan szám, akkor $2^k + 1 = \left(2^{2^n}\right)^m + 1$ osztható $2^{2^n} + 1$-gyel (nevezetes azonosság), s így következik, hogy ez maga a szám.*

Az $F_n = 2^{2^n} + 1$ alakú számokat Fermat-számoknak nevezzük.

1.1. Fermat prím

Fermat prímek-nek nevezzük a $p = 2^k + 1$ alakú, pontosabban a $2^{2^n} + 1$ alakú prímeket. A ma ismert Fermat-prímek:

$F_0 = 2^{2^0} + 1 = 3$
$F_1 = 2^{2^1} + 1 = 5$
$F_2 = 2^{2^2} + 1 = 17$
$F_3 = 2^{2^3} + 1 = 257$
$F_4 = 2^{2^4} + 1 = 65537$

Pierre Fermat (1601-1665) francia matematikus egy 1640-ben írott levelében azt a sejtést fogalmazta meg, hogy az F_n számok mind prímek. A sejtést 1732-ben Leonhard Euler cáfolta azzal, hogy megmutatta: $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ nem prím (Euler 1732)!

A sejtés olyannyira nem igaz, hogy mindmáig nem találtak további Fermat-prímeket, az újabb sejtés, hogy nincs is több.

1.2. Fermat prímek és szerkeszthetőség

A Fermat-prímek azért is érdekesek, mert Carl Friedrich Gauss (1777-1855) egy nevezetes eredménye szerint pontosan azok a szabályos n-szögek szerkeszthetők meg körzővel és vonalzóval, amelyekre n egyenlő 2 valamely hatványának és különböző Fermat-prímeknek a szorzatával.

2. Mersenne számok

Tekintsük a következő számokat:

$M_1 = 2^1 - 1 = 1$ nem prím
$M_2 = 2^2 - 1 = 3$ prím
$M_3 = 2^3 - 1 = 7$ prím
$M_4 = 2^4 - 1 = 15$ nem prím
$M_5 = 2^5 - 1 = 31$ prím
$M_6 = 2^6 - 1 = 63$ nem prím
$M_7 = 2^7 - 1 = 127$ prím

De $M_{11} = 2^{11} - 1 = 2047$ nem prím (osztható 89-cel és 23-mal).

Mersenne-számoknak nevezzük a $2^n - 1$ alakban felírható számokat. Egyes irodalmakban csak p prím kitevő esetén nevezik a számot Mersenne-számnak: $M_p = 2^p - 1$.

2.1. Mersenne-prímek

Mersenne-prímeknek nevezzük a $2^n - 1$ alakban felírható prímszámokat.

2.1. Állítás. *Ha $M_n = 2^n - 1$ prím, akkor n prímszám.*

2.1. Bizonyítás. *Indirekt bizonyítás: tegyük fel, hogy $n = ab$ összetett szám $(a, b > 1)$. Ekkor*

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a)^b - 1^b$$

ami osztható $2^a - 1$-gyel (nevezetes azonosság), ami nagyobb 1-nél, és nem egyenlő a számmal sem, tehát valódi osztó - ami ellentmondás.

Az M_2, M_3, M_5 és M_7 Mersenne-prímeket már az ókorban ismerték. Az M_{13}, M_{17} és M_{19} prímeket P. A. Cataldi fedezte fel 1588-ban. Leonhard Euler nevéhez fűződik az M_{31} Mersenne-prím felfedezése 1750-ben. Több mint 100 éven át ez volt a legnagyobb ismert prím. 1876-ban E. Lucas (1842-1891) megállapította, hogy M_{127} is prím - ez 39 számjegyű: 170141183460469231731687303715884105727.

További Mersenne-prímek: $M_{61}, M_{89}, M_{107}, M_{521}, M_{607}, M_{1279}, M_{2203}, M_{2281}$

Mindmáig nem ismert, hogy mely p prímek esetén lesz M_p prím, illetve, hogy végtelen sok Mersenne-prím van-e.

A Mersenne-prímek szoros kapcsolatban állnak az úgynevezett tökéletes számokkal.

2.2. Marin Mersenne

Marin Mersenne (1588-1648) francia matematikus, minorita szerzetes volt, aki 1644-ben megadta az M_p prímek listáját, ahol $p \leq 257$. Szerinte $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ esetén kapunk M_p prímeket. De ez $p = 67, 257$ estén nem igaz, másrészt kimaradtak a $p = 61, 89, 107$ prímek, melyekre M_p prímszám.

2.3. Nagy prímek keresése

1996-ban indult egy program, a Nagy internetes Mersenne-prím keresés (Great Internet Mersenne Prime Search, GIMPS), melyben ma 240 ezer személyi komputeren fut a kliensprogram, a kutatásban bárki részt vehet. A kutatás akkor fejeződik be, ha valaki megtalálja az első, legalább 100.000.000 számjegyből álló Mersenne-prímet.

1. Melyik igaz a következök közül?
   (a) $c \mid a+b \Rightarrow c \mid a$ és $c \mid b$
   (b) $c \mid a+b$ és $c \mid a-b \Rightarrow c \mid a$ és $c \mid b$
   (c) $c \mid a$ és $d \mid b \Rightarrow cd \mid ab$.
2. Igazoljuk, hogy
   (a) $a-b \mid a^n - b^n$
   (b) $a+b \mid a^n + b^n$, ha n páratlan
   (c) $a+b \mid a^n - b^n$, ha n páros
3. Igazoljuk, hogy
   (a) $13 \mid 14 \cdot 15^{100} - 53 \cdot 67^{100}$
   (b) $61 \mid 5^{2018} + 6^{2018}$
4. Igazoljuk, hogy $30 \mid 11^{11} + 12^{12} + 13^{13}$
5. Bizonyítsuk be, hogy ha $11 \mid 7a+5b$, akkor $11 \mid 9a+8b$
6. Bizonyítsuk be, hogy ha $23 \mid 5a+9b$, akkor $23 \mid 3a+10b$
7. Bizonyítsuk be, hogy $n(n^2+5)$ osztható 6-tal!
8. Bizonyítsuk be, hogy $2^{70}+3^{70}$ osztható 13-mal!
9. Lássuk be, hogy ha $\overline{abc}$ háromjegyü szám osztható 37-tel, akkor $\overline{bca}$ is.
10. Igazoljuk, hogy $120 \mid 11^{12} - 1$

11. Határozzuk meg az Euklideszi algoritmussal 112 és 301 legnagyobb közös osztóját! Írjuk föl a legnagyobb közös osztót $112x + 301y$ alakban, ahol x és y egész!

12. Határozzuk meg az Euklideszi algoritmussal 504 és 372 legnagyobb közös osztóját! Írjuk föl a legnagyobb közös osztót $504x + 372y$ alakban, ahol x és y egész!

13. Igazoljuk, hogy $19 \mid 3^{6n} - 2^{6n}$

14. Döntsük el, melyek prímszámok az alábbiak közül. Amelyik nem az, annak adjunk meg egy osztóját.

    a.) $7^{21} - 4^{21}$

    b.) $7^{21} + 4^{21}$

    c.) $2^{111111} + 1$

15. Mely pozitív n-ekre igaz, hogy $n - 1 \mid n^2 + 1$

Károly Müllner
Email: mullni@hotmail.com