05. メルセンヌ素数と完全数

代数Ⅱ

メルセンヌ数

アイデアは，2のべき乗は2の倍数だけど，そこから1を引く

$$M_n = 2^n - 1$$

n	1	2	3	4	5	6	7	･･･
値	1	3	7	15	31	63	127	･･･

- メルセンヌ数が素数となるとき，nは素数

メルセンヌ数の性質

- M_nが素数ならばnは素数であるが，
  nが素数であってもM_nは素数とは限らない
  – $2^{ab}-1=(2^a-1)(1+2^a+2^a+\cdots+2^{(b-1)a})$
  (対偶「 nが合成数ならば，M_nは合成数」）
- $M_p=2^p-1$が素数であるならば
  $2^{p-1}(2^p-1)$は完全数となる

メルセンヌ素数

$$M_p=2^p-1$$

p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917(2001年）, 20996011, 25964951, 30402457, 32582657, 37156667, 42643801(2009年), 43112609(2008年), 57885161(2013年)

素数判定法

- リュカ・テスト

  pが$(4j+3)$型の素数のとき，$S_0=3, S_n={S_{n-1}}^2-2$と定義すると
  $S_k(0 \le k \le p-2)$ はM_pで整除されないならば，M_pは合成数である.
  S_{p-2}がM_pで整除されるならば，M_pは素数である

- リュカ・レーマー・テスト
  - さらに改良したもの

未解決問題

- メルセンヌ素数は無限に存在するか？
- 素数pに対してMpが合成数であるとき，これをメルセンヌ合成数と呼ぶ，これは無限に存在するか？
- 完全平方数となるメルセンヌ数Mpが存在するか（pが素数の時）