REMARKS ON LUCAS–LEHMER TEST

V. Barbera

Abstract

This paper presents some remarks on Lucas–Lehmer test for primality test of Mersenne numbers.

Lucas–Lehmer test[1]

The result, tested only for small p values, is obtained from elementary steps.

In Lucas–Lehmer test with p an odd prime:

$s_0=4$ *and* $s_i=s_{i-1}^2-2$ *if* $i>0$

$M_p=2^p-1$ *is prime if* $s_{p-2}=0\,mod\,(2^p-1)$

Let's consider instead $L_i=s_{i-1}-2$ *we have*

$L_1=2$ *and* $L_i=L_{i-1}^2+4\cdot L_{i-1}$ *if* $i>1$

2^p-1 *is prime if* $L_{p-1}=-2\,mod\,(2^p-1)$ *indeed* $L_{p-1}=s_{p-2}-2$

Now some observations:

$$L_2=12=4\cdot L_1^1+L_1^2=4\cdot 2^1+2^2$$

$$L_3=192=16\cdot L_1^1+20\cdot L_1^2+8\cdot L_1^3+1\cdot L_1^4=16\cdot 2^1+20\cdot 2^2+8\cdot 2^3+2^4$$

$$L_4=37632=64\cdot L_1^1+336\cdot L_1^2+672\cdot L_1^3+660\cdot L_1^4+352\cdot L_1^5+104\cdot L_1^6+16\cdot L_1^7+L_1^8$$

$$L_5=256\cdot L_1^1+5440\cdot L_1^2+45696\cdot L_1^3+201552\cdot L_1^4+537472\cdot L_1^5+940576\cdot L_1^6+1136960\cdot L_1^7+980628\cdot L_1^8$$
$$+615296\cdot L_1^9+283360\cdot L_1^{10}+95680\cdot L_1^{11}+23400\cdot L_1^{12}+4032\cdot L_1^{13}+464\cdot L_1^{14}+32\cdot L_1^{15}+L_1^{16}$$

$$L_6=1024\cdot L_1^1+87296\cdot L_1^2+2968064\cdot L_1^3+53796160\cdot L_1^4+\ldots$$
$$\ldots$$

if $a_{m,i}$ *is the coefficient of* $L_1^m=2^m$ *for element* L_i *we note that*

$$a_{1,i}=4^{i-1}$$

$$a_{2,i}=\binom{2^{i-1}+1}{3}\cdot\frac{2^{i-1}}{2}$$

$$a_{3,i}=\binom{2^{i-1}+2}{5}\cdot\frac{2^{i-1}}{3}$$

$$a_{4,i}=\binom{2^{i-1}+3}{7}\cdot\frac{2^{i-1}}{4}$$

therefore if $s_{p-2}=L_{p-1}+2$:

$$s_{p-2}=\left(2^{2\cdot(p-2)}+1\right)\cdot 2^1+\binom{2^{p-2}+1}{3}\cdot\frac{2^{p-2}}{2}\cdot 2^2+\ldots+\binom{2^{p-2}+j-1}{2\cdot j-1}\cdot\frac{2^{p-2}}{j}\cdot 2^j+\ldots+2^{p-1}\cdot 2^{(2^{p-2}-1)}+2^{2^{p-2}}$$

References

[1] https://en.wikipedia.org/wiki/Lucas%E2%80%93Lehmer_primality_test