# $\mathcal{C}_m^+$ : LLT numbers

Tony Reix (Tony.Reix@laposte.net)
2005, 6th of May - 2006, 21th of November (v0.7)

# 1 Definition of the LLT numbers

Let's say: $\mathcal{L}(x) = x^2 - 2$ , $\mathcal{L}^1 = \mathcal{L}$ , $\mathcal{L}^m = \mathcal{L} \circ \mathcal{L}^{m-1} = \mathcal{L} \circ \mathcal{L} \circ \mathcal{L} \ldots \circ \mathcal{L}$.

Where $\mathcal{L}(x)$ is the polynomial used in the Lucas-Lehmer Test (LLT) :
$S_0 = 4$ , $S_{i+1} = S_i^2 - 2 = \mathcal{L}(S_i)$ ; $M_q$ is prime $\iff S_{q-2} \equiv 0 \pmod{M_q}$.

Let's call $\mathcal{C}_m^+$ the sum of the positive coefficients of the polynomial $\mathcal{L}^m(x)$ and $\mathcal{C}_m^-$ the sum of the negative coefficients of the polynomial $\mathcal{L}^m(x)$ . We call $\mathcal{C}_m^+$ a *LLT number*: $\mathcal{C}_1^+ = 1,\ \mathcal{C}_2^+ = 3,\ \mathcal{C}_3^+ = 23,\ \mathcal{C}_4^+ = 1103,\ \mathcal{C}_5^+ = 2435423$ .

# 2 Properties of LLT numbers

Numerical experiments show the following properties (where $F_n = 2^{2^n} + 1$ is a prime Fermat number, and $M_q = 2^q - 1$ is a prime Mersenne number):

$$\mathcal{C}_m^+ \text{ is odd, and } \quad \mathcal{C}_m^+ + \mathcal{C}_m^- = -1 \text{ , for: } m \geq 1 \quad (\text{ LLT.1})$$

$$\mathcal{C}_m^+ = 2^m \prod_{i=1}^{m-1} \mathcal{C}_i^+ - 1 \quad \text{for: } m > 1 \quad (\text{ LLT.2})$$

$$p \text{ prime, } p \mid \mathcal{C}_m^+ \iff p = 2^m 3k - 1 (k \text{ odd}), \text{ or } p = 2^{m+1} 3k' + 1 \quad (\text{ LLT.3})$$

$$\text{The period of } \mathcal{C}_m^+ \pmod{F_n} \text{ is: } 2^n - 1 \quad n \geq 1 \quad (\text{ LLT.4})$$

$$\mathcal{C}_{m \equiv 1 \pmod{2^n - 1}}^+ \equiv -2 \pmod{F_n} \quad \text{for: } m > 1 \quad (\text{ LLT.5})$$

$$\mathcal{C}_m^+ \equiv 3 \pmod{10} \quad \text{for: } m \geq 1 \quad (\text{ LLT.6})$$

$$\prod_{i=1}^{2^n - 1} \mathcal{C}_i^+ \equiv 1 \pmod{F_n} \quad (\text{ LLT.7})$$

$$\text{The period of } \mathcal{C}_m^+ \pmod{M_q} \text{ is: } q - 1 \quad \text{for: } q \equiv 1 \pmod 4 \quad \text{LLT.8})$$

$$\mathcal{C}_{m \equiv 0 \pmod q}^+ \equiv 1 \pmod{M_q} \quad \text{for: } m > 1 \text{ and } q \equiv 1 \pmod 4 \quad (\text{ LLT.9})$$

$$\mathcal{C}_m^+ \equiv 2^{q-1} \pmod{M_q} \quad \text{for: } m > q \text{ and } q \equiv -1 \pmod 4 \quad (\text{ LLT.10})$$

$$\prod_{i=1}^{q-2} \mathcal{C}_i^+ \equiv 1 \pmod{M_q} \quad \text{for: } q \equiv -1 \pmod 4 \quad (\text{ LLT.11})$$

$$\mathcal{C}_m^+ \equiv -1 \pmod{2^q} \quad \text{for: } m \geq q \quad (\text{ LLT.12})$$

Properties (LLT.4), (LLT.5) and (LLT.7) could be used as a primality test for Fermat numbers, and properties (LLT.8), (LLT.9), (LLT.10) and (LLT.11) could be used as a primality test for Mersenne numbers, once proven ... But they would not lead to a faster test than Pépin's or LLT tests.
Examples:
$F_n = 2^{2^n} + 1$ is prime $\iff$ $\mathcal{C}_{2^n}^+ \equiv -2 \pmod{F_n}$ .
$M_q = 2^q - 1$ is prime $\iff$ $\mathcal{C}_q^+ \equiv 1 \pmod{M_q}$ ; (where: $q \equiv 1 (\text{mod } 4)$ ) .

**Proof** of (LLT.1):
Since $\mathcal{L}^1(-1) = -1$ then $\mathcal{L}^m(-1) = -1$, proving: $\mathcal{C}_m^+ + \mathcal{C}_m^- = -1$.

**Proof** of (LLT.2) (Hint by *Hurkyl* from www.physicsforums.com):
We have: $\mathcal{C}_2^+ = 3 = 2^2 \prod_{i=1}^{2-1} \mathcal{C}_i^+ - 1$ .
Let say (LLT.2) is true for $m$ and prove then it is true for $m+1$ .
From (LLT.1), we have: $\mathcal{C}_m^- = \mathcal{C}_m^+ + 1$ .
We have: $\mathcal{L}^m(x) = \sum_{j=0}^{2^{m-2}} c_j^+ x^{4j} - \sum_{j=1}^{2^{m-2}} c_j^- x^{4j-2}$ where $m > 1$.
Then, with $i$ such that $i^2 = -1$, we have: $\mathcal{L}^m(i) = \sum_{j=0}^{2^{m-2}} c_j^+ + \sum_{j=1}^{2^{m-2}} c_j^- = \mathcal{C}_m^+ + \mathcal{C}_m^- = 2\mathcal{C}_m^+ + 1$ . So: $\mathcal{C}_m^+ = \frac{\mathcal{L}^m(i)-1}{2}$ .
By the definition of the LLT: $\mathcal{L}^{m+1}(i) = (\mathcal{L}^m(i))^2 - 2 = 4\mathcal{C}_m^{+2} + 4\mathcal{C}_m^+ - 1$ .
Thus: $\mathcal{C}_{m+1}^+ = \frac{\mathcal{L}^{m+1}(i)-1}{2} = 2\mathcal{C}_m^+(\mathcal{C}_m^+ + 1) - 1 = (2^{m+1} \prod_{j=1}^{m-1} \mathcal{C}_j^+ - 2)(\mathcal{C}_m^+ + 1) - 1 = 2^{m+1} \prod_{j=1}^{m} \mathcal{C}_j^+ - 2\mathcal{C}_m^+ + 2(\mathcal{C}_m^+ + 1) - 2 - 1 = 2^{m+1} \prod_{j=1}^{m} \mathcal{C}_j^+ - 1$ . CQFD.

**Proof** of (LLT.6):
This is a direct consequence of (LLT.5) with $n = 1$ and that $\mathcal{C}_m^+$ numbers are odd.

**Proof** of (LLT.7):
With $m = 2^n$ in (LLT.2), then: $\mathcal{C}_{2^n}^+ = 2^{2^n} \prod_{i=1}^{2^n-1} \mathcal{C}_i^+ - 1 = (2^{2^n}+1) \prod_{i=1}^{2^n-1} \mathcal{C}_i^+ - (\prod_{i=1}^{2^n-1} \mathcal{C}_i^+ + 1) \equiv - \prod_{i=1}^{2^n-1} \mathcal{C}_i^+ - 1 \pmod{F_n}$. Now, by (LLT.5): $\mathcal{C}_{2^n}^+ \equiv -2 \pmod{F_n}$ , we prove: $\prod_{i=1}^{2^n-1} \mathcal{C}_i^+ \equiv -1 + 2 \equiv 1 \pmod{F_n}$ .

**Proof** of (LLT.12):
Very easy from (LLT.2).

# 3 Relationship with Lucas numbers

$L^m(i) = V_{2^m}(1, -1)$, where $i$ is the square root of $-1$, $m$ is greater than 1, and $V_n(1, -1)$ is a Lucas number defined by: $V_0 = 2, V_1 = 1, V_{n+1} = V_n + V_{n-1}$. Look at "The Little Book of BIGGER primes" by Paulo Ribenboim, 2nd edition, page 59.
So, what I called LLT numbers are: $C_m^+ = \frac{V_{2^m} - 1}{2}$.

# 4 PARI/gp program

The LLT numbers can be efficiently computed by means of the PARI/gp program: `P=1; for(i=2,m, C=P*2^i-1; P=P*C; print(C))`

# 5 Examples

Examples:
$\mathcal{L}^2(x) = x^4 - 4x^2 + 2$
$\mathcal{L}^3(x) = x^8 - 8x^6 + 20x^4 - 16x^2 + 2$
$\mathcal{L}^4(x) = x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2$

$\mathcal{C}_2^+ = 4 \times 1 - 1 = 3 = 11_2$,
$\mathcal{C}_3^+ = 8 \times 1 \times 3 - 1 = 23 = 10111_2$,
$\mathcal{C}_4^+ = 16 \times 1 \times 3 \times 23 - 1 = 1103 = 10001001111_2$,
$\mathcal{C}_5^+ = 32 \times 1 \times 3 \times 23 \times 1103 - 1 = 2435423 = 1001010010100101011111_2$
$\mathcal{C}_6^+ = 11862575248703 = 10101100100111111000100101010100111111_2$
$\mathcal{C}_7^+ = 281441383062305809756861823 =$
$1110100011001101100001111001111001111111000100011101011110000110101010111111_2$

$\mathcal{C}_4^+ - \mathcal{C}_3^+ = 2^3.3^3.5^1$
$\mathcal{C}_5^+ - \mathcal{C}_4^+ = 2^4.3^3.5^1.7^2.23^1$
$\mathcal{C}_6^+ - \mathcal{C}_5^+ = 2^5.3^3.5^1.7^2.23^1.47^2.1103^1$
$\mathcal{C}_7^+ - \mathcal{C}_6^+ = 2^6.3^3.5^1.7^2.23^1.47^2.769^1.1103^1.2207^2.3167^1$
$\mathcal{C}_8^+ - \mathcal{C}_7^+ = 2^7.3^3.5^1.7^2.23^1.47^2.769^1.1087^2.1103^1.2207^2.3167^1.4481^2.11862575248703^1$

$n > 1$

$\bullet F_1 = 5$
$n > 2 : \mathcal{C}_n^+ \equiv 3 = (F_1 - 2 + F_0)/2 \equiv -2 \pmod{F_1}$

$\bullet F_2 = 17$
$n = 0 \,(\text{mod } 2^2 - 1) : \mathcal{C}_n^+ \equiv 6 = (F_2 - 2 + F_1)/2 - 4 \pmod{F_2}$
$n = 1 \,(\text{mod } 2^2 - 1) : \mathcal{C}_n^+ \equiv -2 \pmod{F_2}$

$n = 2\,(\mathrm{mod}\ 2^2 - 1) : \mathcal{C}_n^+ \equiv 3 \pmod{F_2}$

$\bullet F_3 = 257$
$n = 0\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv 136 = (F_3 - 2 + F2)/2\,(\mathrm{mod}\ F_3)$
$n = 1\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv -2 \pmod{F_3}$
$n = 2\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv 3 \pmod{F_3}$
$n = 3\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv 23 \pmod{F_3}$
$n = 4\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv 75 \pmod{F_3}$
$n = 5\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv 91 \pmod{F_3}$
$n = 6\,(\mathrm{mod}\ 2^3 - 1) : \mathcal{C}_n^+ \equiv 38 \pmod{F_3}$

$\bullet F_4 = 65537$
$n = 0\,(\mathrm{mod}\ 2^4 - 1) : \mathcal{C}_n^+ \equiv 32896 = (F_4 - 2 + F_3)/2\,(\mathrm{mod}\ F_4)$
$n = 1\,(\mathrm{mod}\ 2^4 - 1) : \mathcal{C}_n^+ \equiv -2 \pmod{F_4}$
$n = 2\,(\mathrm{mod}\ 2^4 - 1) : \mathcal{C}_n^+ \equiv 3 \pmod{F_4}$
$n = 3\,(\mathrm{mod}\ 2^4 - 1) : \mathcal{C}_n^+ \equiv 23 \pmod{F_4}$
$n = 4\,(\mathrm{mod}\ 2^4 - 1) : \mathcal{C}_n^+ \equiv 1103 \pmod{F_4}$
$\ldots$
$n = 14\,(\mathrm{mod}\ 2^4 - 1) : \mathcal{C}_n^+ \equiv 23133 \pmod{F_4}$

$\bullet F_5$
$\mathcal{C}_{32}^+ \equiv 45817857 \pmod{F_5}$

$\bullet F_2 : \quad 3 \times 6 \equiv 1 \pmod{F_2}$
$\bullet F_3 : \quad 3 \times 23 \times 75 \times 91 \times 38 \times 136 \equiv 1 \pmod{F_3}$
$\bullet F_4 : \quad 3 \times 23 \times 1103 \times \ldots \times 23133 \times 32896 \equiv 1 \pmod{F_4}$
$\bullet F_5 : \prod_{i=1}^{2^5-1} \mathcal{C}_i^+ \equiv 4249149439 \pmod{F_5}$

# 6 Other functions

The following polynomials also have interesting properties:

$$\mathcal{A}(x) = x^2 - 3 \ \ ; \ \ \mathcal{B}(x) = x^{2k} - 2 \ \ ; \ \ \mathcal{C}(x) = x^{2k} - 2^{2k} \pm 2$$

About $\mathcal{A}(x) = x^2 - 3$, we have (where $\mathcal{C}_m^+$ is the sum of the positive coefficients of the polynomial $\mathcal{A}(x)$), since $\mathcal{A}^{2k+1}(1) = -2$ and $\mathcal{A}^{2k}(1) = 1$:

$$\mathcal{C}_m^+ = 2^{m-1} 3 \prod_{i=1}^{m-1} \mathcal{C}_i^+ + 1 \quad m \text{ odd}$$

$$\mathcal{C}_m^+ = 2^{m-1} 3 \prod_{i=1}^{m-1} \mathcal{C}_i^+ - 2 \quad m \text{ even}$$

# 7 Related numbers

$$\text{Let say: } \mathcal{A}_1 = 1 \text{ and } \mathcal{A}_m = 2^m \prod_{i=1}^{m-1} \mathcal{A}_i + 1 \quad \text{for: } m > 1$$

Then, we have: $\mathcal{A}_m(m = 1, ...) = 1, 5, 41, 3281, 21523361, 926510094425921, ...$

If $F_n$ is prime, then: $\mathcal{A}_{2^n} \equiv 0 \pmod{F_n}$.
And $\mathcal{A}_{2^5} \equiv 5162152 \pmod{F_5}$.

If $M_n = 2^n - 1$ is prime, then: $\mathcal{A}_n \equiv \mathcal{A}_{m \equiv 1 \pmod{n-1}} \equiv -1 \pmod{M_n}, m > 1$.
And $\mathcal{A}_{11} \equiv 301 \pmod{M_{11}}$.

$18 \mid (\mathcal{A}_m - \mathcal{C}_m^+)$.
$\mathcal{A}_{2^m} - \mathcal{C}_{2^m}^+ \equiv 2 \pmod{F_m}$ if $F_m$ is prime.