On Digraphs under x^2 and x^2-2 modulo a Mersenne Prime

Tony Reix (tony.reix@laposte.net)
ZetaX (AOPS forum)
maxal (GIMPS forum)
2006, 13th of May (updated: 2007, 11th of April)

This paper presents how two theorems dealing with the Lucas-Lehmer Test for Mersenne numbers (LLT) were found and proven.
These theorems deal with computing the number of cycles of length L that appear in a Digraph under x^2 or x^2-2 modulo a Mersenne prime $M_q = 2^q-1$, where q is prime and $L \mid q-1$.

1 Introduction

The Lucas-Lehmer Test says that a Mersenne number $M_q = 2^q - 1$ (where q is prime) is prime iff $M_q \mid S_{q-2}$, where $S_0 = 4, S_{i+1} = S_i^2 - 2$.

Let call llt the function: $llt : x \mapsto x^2 - 2 \mod M_q$.
Let call $llt^{\perp}$ the function: $llt^{\perp} : x \mapsto x(x^2-3) \mod M_q$.

Let S be the finite set defined by: $S = \{x \text{ integer } ; 0 \leq x < M_q\}$ and let: $f : S \mapsto S$ be a function.

We define a directed graph G_f whose vertices are given by the elements of S and whose directed edges are $(x, f(x))$ for each $x \in S$.

2 Previous personal experimental research

Long time ago, I studied the topology of G_{llt}.
I (re)discovered that the structure of the digraph G_{llt} is made of:
One Tree: one reversed complete binary tree of height $q-1$ ending in 0, attached to the node -2 attached to the node 2 with a cycle of length 1, where the 2^{q-2} *roots* of the tree are all the numbers built by: $R_0 = 4$, $R_{i+1} = llt^{\perp}(R_i)$; and:
Cycles: a set of cycles of length L dividing $q-1$.

The existence and some properties of the **Tree** are well-known and proven. But at that time I found no study of the properties of the **Cycles**.

I computed the number of cycles of length L for $q = 3, 5, 7, 13, 17, 19, 31$, as shown in Table 9, by means of a `C` program that computes all pairs $(x, x^2 - 2 \pmod{M_q})$, finds the cycles and counts cycles of same length.

$L =$	1	2	3	4	5	6	8	9	10	12	15	16	18	30
$q =$														
3	2													
5	2	1		1										
7	2		2			4								
13	2	1	2	1		9				165				
17	2	1		3			30					2032		
19	2		2			4		56					7252	
31	2		2		6	4			48		2182			17894588

Table 1: Number of loops of length L under x^2-2 modulo the first Mersennes.

3 Example with $q = 5$

The Figure 1 shows the tree and cycles for $q = 5$.
As shown in table 9, there are two cycles of length 1: $(2 \leftrightarrow 2)$ and $(M_5 - 1 \leftrightarrow M_5 - 1)$, one cycle of length 2: $(12 \rightarrow -13 \rightarrow 12)$, and one cycle of length 4: $(3 \rightarrow 7 \rightarrow -15 \rightarrow 6 \rightarrow 3)$.

4 A problem by Daniel Shanks

Later, I discovered that Daniel Shanks, in his book "Solved and Unsolved Problems in Number Theory" (1962 Edition), has already studied the topology of the Digraph G_{llt}.
Page 215, in Chapter "Supplementary Comments, Theorems, and Exercises", Shanks provides the complete Digraph G_{llt} for $q = 5$, plus several useful properties. At the end of the page, he asked the reader to: "Develop a general theory for all prime M_p, proving the main theorems, if you can".
But he provided no hints !

5 Quadratic maps over $GF(p)$

In their paper: "On the iteration of certain quadratic maps over $GF(p)$", Troy Vasiga and Jeffrey Shallit consider the properties of certain graphs

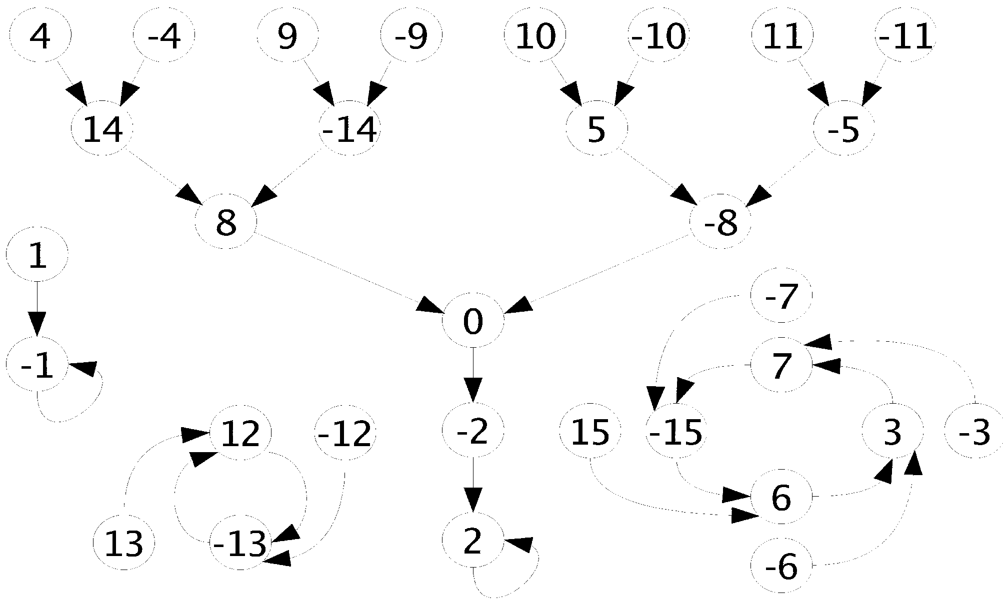


Figure 1: Tree and Cycles under $x^2 - 2$ modulo M_5.

based on iteration of the quadratic maps $x \to x^2$ and $x \to x^2 - 2$ over a finite field $GF(p)$.

They provide several interesting theorems about the tails and cycles of the iterations $x \to x^2$ and $x \to x^2 - 2$ modulo any prime.

They also focus on Fermat and Mersenne primes, proving the following theorems:

Theorem 1 (5) *When $p = 2^q - 1$, a Mersenne prime, the digraph $G_{x \to x^2}$ consists of cycles whose length divides $q - 1$. Off each element in these cycles there hangs a single element with tail length 1.*

Corollary 1 (3) *Let p be an odd prime with $p - 1 = 2^\tau \cdot \rho$, ρ odd. For each positive integer divisor d of ρ, $G_{x \to x^2}$ contains $\varphi(d)/(ord_d 2)$ cycles of length $ord_d 2$. There are ρ elements in all these cycles, and off each element in these cycles there hang reversed complete binary trees of height $\tau - 1$ containing $2^\tau - 1$ elements.*

Theorem 2 (17) *When $p = 2^q - 1$, a Mersenne prime, the digraph $G_{x \to x^2 - 2}$ consists of*

(i) A reversed complete binary tree of height $q - 1$ with root 0, attached to the node -2, which is attached to the node 2 with a cycle of length 1 on this

node. The nodes in this tree are given by $\theta^n + \theta^{-n}$, $0 \le n \le 2^{q-1}$, where θ is a zero of $X^2 - 4X + 1$.

(ii) A set of cycles of length dividing $q-1$. Off each element in these cycles there hangs a single element with tail length 1. The nodes in these cycles are given by $3^n + 3^{-n}$, $1 \le n \le 2^{q-1} - 2$.

Corollary 2 (15) *Let p be an odd prime with $p-1 = 2^\tau \cdot \rho$, $p+1 = 2^{\tau'} \cdot \rho'$, ρ, ρ' odd. For each divisor $d > 1$ of ρ, $G = G_{x \to x^2-2}$ contains $\varphi(d)/(2ord'_d 2)$ cycles of length $ord'_d 2$. There are ρ elements in all these cycles, and off each element in these cycles there hang reversed complete binary trees of height $\tau - 1$ containing $2^\tau - 1$ elements.*
Similarly, for each divisor $d' > 1$ of ρ', there exists $\varphi(d')/(2ord'_{d'} 2)$ cycles of length $ord'_{d'} 2$ and off each element in these cycles there hang reversed complete binary trees of height $\tau' - 1$ containing $2^{\tau'} - 1$ elements.
Finally, the element 0 is the root of a complete binary tree of height $\tau - 2$ (respectively $\tau' - 2$) when $p \equiv 1 \pmod 4$ (respectively $p \equiv 3 \pmod 4$), and G also contains the directed edges $(0, -2), (-2, 2), (2, 2)$.

6 L is independent of q under x^2 modulo M_q

Thanks to Shallit's formula, I wrote a PARI/gp program that enabled me to compute the number of cycles under x^2 modulo a Mersenne prime M_q for: $q = 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$, providing one or several values for each L from 1 to 12, and $14, 15, 18, 20, 21, 22, 30, 42, 44, 53, 60, 63, 88, 106, 126$.

Since all values found for each L were identical whatever the value of q, I guessed that the number of cycles of length L under x^2 modulo a Mersenne prime M_q does NOT depend on q.

The number of cycles of length L for $L = 1..12^+$ is shown in table 2.

L	1	2	3	4	5	6	7	8	9	10	11	12	14	15
$\psi(L)$	1	1	2	3	6	9	18	30	56	99	186	335	1161	2182

Table 2: Number of cycles of length L under x^2 for $L = 1..12^+$.

Here is the PARI/gp program which enabled to compute table 2.

```
VS(q) = {
```

```
    cyc    = divisors(q-1);
    lencyc = vector(q-1);

    fac    = divisors(2^(q-1)-1);
    l      = length(fac);

    for(i=2, l,
        or = znorder(Mod(2, fac[i]));
        ep = eulerphi(fac[i]);
        lencyc[or] += ep/or;
    );

    for(i=1, q-1,
        if(lencyc[i] != 0,
            print(i, " ", lencyc[i]);
        );
    );
}
```

As an example, the number of cycles of length L under x^2 for $q = 127$ is given by table 3.

L	$\psi(L)$
1	1
2	1
3	2
6	9
7	18
9	56
14	1161
18	14532
21	99858
42	104715342801
63	146402730743693304
126	675163426430433459179525995420973028

Table 3: Number of cycles of length L under x^2 modulo $2^{127} - 1$.

7 OEIS A001037

The OEIS (The On-Line Encyclopedia of Integer Sequences!) is aimed at helping people to check if a sequence of integers is already known or not.

Typing the sequence: $1, 1, 2, 3, 6, 9, 18, 30, 56, 99, 186, 335$ on page: `http://www.research.att.com/~njas/sequences/index.html` , I was able to check that my sequence from 1 to 12 was identical to the beginning of sequence A001037, and that the other values of my sequence matched the A001037 sequence:
$[1, 2, 1, 2, 3, 6, 9, 18, 30, 56, 99, 186, 335, 630, 1161, 2182, 4080, 7710, 14532, 27594, 52377, 99858, 190557, 364722, 698870, 1342176, 2580795, 4971008, 9586395, 18512790, 35790267, 69273666, 134215680, 260300986, 505286415, 981706806]$.

This sequence is defined as:
"Number of degree-n irreducible polynomials over $GF(2)$", or:
"Number of n-bead necklaces with beads of 2 colors when turning over is not allowed and with primitive period n" or:
"Number of binary Lyndon words of length n."

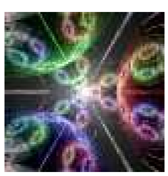
See: `http://www.research.att.com/~njas/sequences/A001037` .

And this sequence is built by the formula:

$$A001037(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) 2^d$$

8 Art Of Problem Solving forum - ZetaX

Then, on the "Art of Problem Solving" forum, I asked if someone were able to prove that $\psi(L) = A001037(L)$.

ZetaX  quickly provided the theorems and their proofs, as described in next section.

See: `http://www.artofproblemsolving.com/Forum/forum-6.html` .

9 Cycles under x^2 mod a Mersenne prime

Theorem 3 (ZetaX-1) *The number of cycles of length L (L divides $q-1$) in the digraph $G_{x\to x^2}$ modulo a Mersenne prime 2^q-1 is:*

$$\psi(L) = \frac{1}{L}\sum_{d|L}\mu(\frac{L}{d})2^d$$

Proof:
By the existence of a primitive root modulo 2^q-1, we can see it also as the following problem: Find the number of cycles of length l under the action $x \to 2x$ seen modulo 2^q-2.
Now canonically lets find the number of solutions of $2^n x \equiv x \pmod{2^q - 2} \iff (2^n-1)x \equiv 0 \pmod{2^q-2}$, since this is the number of x that are part of a cycle having an order dividing n.
Since $\gcd(2^q-2, 2^n-1) = 2^{\gcd(q-1,n)}-1$, we have only to consider n that divides $q-1$ and there are 2^n-1 solutions then.
Let $\psi(l)$ be the number of elements of cycles of exactly length l.
Now we have $2^n - 1 = \sum_{d|n}\psi(d)$. By the Moebius-inversion-formula, we get:

$$\psi(n) = \sum_{d|n}\mu(\frac{n}{d})(2^d-1) = \sum_{d|n}\mu(\frac{n}{d})2^d - \sum_{d|n}\mu(\frac{n}{d}) = \sum_{d|n}\mu(\frac{n}{d})2^d$$

But by dividing through n (since every cycle of length n contains n elements) we get the desired formula.

$\square$

Now looking back, we see that this argumentation doesn't work for the cycles of length 1, but for these we can verify it directly.

10 Cycles under x^2-2 modulo M_q prime

Theorem 4 (ZetaX-2) *The number of cycles of length L (L divides $q-1 = 2^s u$) in the digraph $G_{x\to x^2-2}$ modulo a Mersenne prime 2^q-1 is:*

$$\varsigma(L) = \frac{1}{L}\left(\sum_{d|L}\mu\left(\frac{L}{d}\right)2^d - \sum_{2^s|d|L}\mu\left(\frac{L}{d}\right)2^{d-1}\right)$$

Definition: A primitive root is a ζ, such that $\zeta^k, k \in \{1,2,...,p-1\}$ gives all different prime residue classes $\pmod p$, so $\{1,2,3,...,p-1\}$. They exist modulo every power of an odd prime and some other cases and also in every finite field. Especially, they exist modulo ever prime p.

Now fix a primitive root $\zeta \pmod p$. Any prime residue class $x \pmod p$ can now be seen as some power $x \equiv \zeta^k \pmod p$ for suitable k. Since when also $y \equiv \zeta^l \pmod p$, it follows that $xy \equiv \zeta^k \zeta^l = \zeta^{k+l} \equiv \zeta^{(k+l) \pmod{p-1}} \pmod p$ (by Fermat's theorem), so you can see multiplication $\pmod p$ as addition $\pmod{p-1}$ (excluding 0). So considering these powers k, l is like taking logarithm in the real numbers.

But now back to the (less elementary !) problem concerning $x^2 - 2$:
Proof:
Let $p = 2^q - 1$ be a prime (so q is also prime). Lets work in the field $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ respectively (so the field with p elements and it's quadratic extension): Let $a_0, a_1, a_2, ..., a_n = a_0$ be a cycle (of length dividing n). When we can write $a_0 = x + x^{-1}$, we would get by induction that $a_k = x^{2^k} + x^{-2^k}$ for all k. Such x does not necessary exist in $\mathbb{F}_p$, but, since it is a quadratic equation, for sure in $\mathbb{F}_{p^2}$.
So $a = x + x^{-1}$ is part of a cycle of length dividing n iff:

$$x^{2^n} + x^{-2^n} = a_n = a_0 = x + x^{-1}$$

$$\iff x^{2^{n+1}} - x^{2^n+1} - x^{2^n-1} + 1 = 0$$

$$\iff (x^{2^n+1} - 1)(x^{2^n-1} - 1) = 0$$

yielding two equations to solve in $\mathbb{F}_{p^2}$ (under the additional condition of $x + x^{-1} \in \mathbb{F}_p$):

(a) $x^{2^n+1} = 1$

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

Since $p^2 - 1 = (p+1)(p-1) = 2^{q+1}(2^{q-1} - 1)$, all these solutions are already in $\mathbb{F}_p$ (because of order/primitive roots again).
Now that means we are looking for $x \in \mathbb{F}_p$ with $ord(x) \mid 2^n + 1$ or $ord(x) \mid 2^n - 1$.

Special case: $n \mid p - 1$ and n is odd.
Now also $2n \mid p-1$, and (because of $2^n+1; 2^n-1 \mid 2^{2n}-1 \mid 2^{q-1}-1$) there are already all $2^n + 1$ solutions for (a) and all $2^n - 1$ solutions for (b) contained in $\mathbb{F}_p$ (this statement is again based on the existence of a primitive root).
The only solution to both equations is $x = 1$. But when x is a solution, also x^{-1} is a solution, but x and it's inverse (and only those, since a quadratic

equation has just two roots) give the same $a = x + x^{-1}$, and the only self-inverse x are ± 1 (and -1 is for sure not a solution, 1 is).
So there are exactly $\frac{2^n+1+2^n-1}{2} = 2^n$ different such a. Now again using Moebius inversion gives the result for the odd n dividing $q-1$.

General case:
Let k_n be the number of solutions of (a).
Let l_n be the number of solutions of (b).
Then the number of cycles of length dividing n is $(k_n + l_n)/2$.
Now by the same reasons as before, we get that $k_n = \gcd(2^n+1, 2^{q-1}-1)$ and $l_n = \gcd(2^n-1, 2^{q-1}-1)$, thus, the problem is solved after using Moebius again.
Note that most of this arguing works for all primes, not just that of Mersenne type.

To simplify the formula, we just have to consider divisors of $q-1$ as length of cycles again, so let n be a divisor of $q-1$ from now on.
Let $\psi(n)$ denote the number of elements that are part of a cycle of a length dividing n.

Claim:

$$\psi(n) = \begin{cases} 2^n \text{ iff } 2n \mid q-1 \\ 2^{n-1} \text{ otherwise} \end{cases}$$

Proof:
Since $n \mid q-1$, we have $\gcd(2^n-1, 2^{q-1}-1) = 2^n-1$, so there are 2^n-1 solutions for (b).
Since 2^n+1 and 2^n-1 are co-primes, we get:

$$\gcd(2^n+1, 2^{q-1}-1) = \frac{\gcd(2^n-1, 2^{q-1}-1) \cdot \gcd(2^n+1, 2^{q-1}-1)}{\gcd(2^n-1, 2^{q-1}-1)}$$

$$= \frac{\gcd(2^{2n}-1, 2^{q-1}-1)}{\gcd(2^n-1, 2^{q-1}-1)} .$$

Now if $2n \mid q-1$, we get:

$$\frac{\gcd(2^{2n}-1, 2^{q-1}-1)}{\gcd(2^n-1, 2^{q-1}-1)} = \frac{2^{2n}-1}{2^n-1} = 2^n+1$$

and there are $(2^n-1+2^n+1)/2 = 2^n$ solutions then.

If otherwise $2n \nmid q-1$, we get:

$$\frac{\gcd(2^{2n}-1, 2^{q-1}-1)}{\gcd(2^n-1, 2^{q-1}-1)} = \frac{2^n-1}{2^n-1} = 1$$

and there are $(2^n - 1 + 1)/2 = 2^{n-1}$ solutions then.

Now when $\varsigma(n)$ describes the number of cycles of length exactly n, we get that $n \cdot \varsigma(n)$ is the number of elements that are part of such a cycle and by Moebius we reach:

$$n \cdot \varsigma(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \psi(d)$$

or equivalently:

$$\varsigma(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \psi(d).$$

To write it without that cases, let $q - 1 = 2^s u$, where u is odd. Then the formula reduces to:

$$\varsigma(n) = \frac{1}{n} \left(\sum_{2^s \nmid d|n} \mu\left(\frac{n}{d}\right) 2^d + \sum_{2^s|d|n} \mu\left(\frac{n}{d}\right) 2^{d-1} \right)$$

and to:

$$\varsigma(n) = \frac{1}{n} \left(\sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d - \sum_{2^s|d|n} \mu\left(\frac{n}{d}\right) 2^{d-1} \right)$$

□

Note that for the divisors of $\frac{q-1}{2}$ this is simply the formula from the x^2 case !

Here is the PARI/gp program that computes the number of cycles of length L under $llt(x) = x^2 - 2$ modulo a Mersenne number.

```
H(q)=
{
        s=0; while((q-1)%(2^s) == 0, s++); s--;
        print("q= ", q, " = 1 + 2^", s, ".", (q-1)/2^s, "\n");
        dq  = divisors(q-1);
        ldq = length(dq);

        print("L= ", 1, " -> 1");
        for(j=2, ldq,
                n  = dq[j];
                dn  = divisors(n);
                ldn = length(dn);
                S  = 0;
```

```
		for(i=1, ldn,
			ddn = dn[i];
				S += moebius(n/ddn)*2^(ddn);
			if(ddn%(2^s) == 0,
				S -= moebius(n/ddn)*2^(ddn-1);
			);
		);
		if(S != 0, print("L= ", n, " -> ", S/n););
	);
	print("\n");
}
```

11 Another proof by maxal (GIMPS forum)

One can show that the cycles in the LLT Digraph under the mapping $x \to x^2 - 2$ correspond to the cycles in the group $Z_{2^{q-1}-1}$ under the mapping $x \to 2x$ where elements x and $-x$ are considered the same.

For example, let $q = 5$. Then in Z_{15} we have the following cycles:
$0 \to 0$
$1 \to 2 \to 4 \to 8 \to 1$
$3 \to 6 \to 12 \to 9 \to 3$
$5 \to 10 \to 5$
$7 \to 14 \to 13 \to 11 \to 7$

If elements x and $-x$ are considered the same then we have the following cycles:
$0 \to 0$
$1 \to 2 \to 4 \to 8 \to 1$ and $7 \to 14 \to 13 \to 11 \to 7$ represent the same cycle.
$3 \to 6 \to 12 \to 9 \to 3$ becomes $3 \to 6 \to -3$
$5 \to 10 \to 5$ becomes $5 \to -5$
i.e., there are two 1-cycles, one 2-cycle, and one 4-cycle.

We call *conjugate* cycles containing x and $-x$ for some x. In the example above, $1 \to 2 \to 4 \to 8 \to 1$ and $7 \to 14 \to 13 \to 11 \to 7$ are conjugate cycles while $3 \to 6 \to 12 \to 9 \to 3$ is self-conjugate cycle.

Denote by $c(k)$ the number of k-cycles in $Z_{2^{q-1}-1}$ and by $c'(k)$ the number of self-conjugate k-cycles. Then the number of k-cycles in the LLT Digraph is $C(k) = (c(k) - c'(k))/2 + c'(2k)$. (Gluing each pair of elements x and $-x$ into a single one contracts the cycles in $Z_{2^{q-1}-1}$. The contracted k-cycles are formed by: 1) pairs of conjugate k-cycles which glue into a single k-cycle under the contraction. The number of such pairs is $(c(k) - c'(k))/2$. 2) self-conjugate 2k-cycles which shrink their length by the factor of 2 under the contraction. The number of such cycles is $c'(2k)$).

For $q = 5$ we have $c(1) = 2$, $c(2) = 1$, $c(4) = 3$ and $c'(1) = 0$, $c'(2) = 1$, $c'(4) = 1$ implying $C(1) = 2$, $C(2) = 1$, $C(4) = 1$.

It is easy to see that $c(k) = \sum_{d|k} \mu(k/d)(2^d - 1)/k$ if k divides $(q-1)$, and $c(k) = 0$ otherwise.

Similarly, one can show that
1) for odd s, $c'(s) = 0$ except $c'(1) = 1$.
2) for odd s and for $t >= 1$ such that $2^t s$ divides $(q-1)$, $c'(2^t s) = \sum_{d|s} \mu(s/d) 2^{2^{t-1}d}/(2^t s)$ for $t >= 1$ and odd s.
3) for odd s and for $t >= 1$ such that $2^t s$ does not divide $(q-1)$, $c'(2^t s) = 0$.

In order to simplify things consider two functions that do not depend on q: $c1(k) = \sum_{d|k} \mu(k/d)(2^d - 1)/k c2(2^t s) = \sum_{d|s} \mu(s/d) 2^{2^{t-1}d}/(2^t s)$ for $t >= 1$ and odd s, and $c2(k) = 0$ for odd $k > 1$ and $c2(1) = 1$.

It can be shown that $c2(2m) = (c1(m) + c2(m))/2$ and, thus, $(c1(k) - c2(k))/2 + c2(2k) = c1(k)$.

Now let's compute the number of k-cycles in the LLT Digraph for k dividing $(q-1)$. For such k, we have $c(k) = c1(k)$ and $c'(k) = c2(k)$ but not necessary $c'(2k) = c2(2k)$ since $2k$ may not divide $(q-1)$. This happens when $(q-1)/k$ is odd number in which case the summand $c2(2k)$ happens to be excessive implying $C(k) = c1(k) - c2(2k)$.

Therefore, $C(k) = 0$ if k does not divide $(q-1)$, $C(k) = c1(k)$ if k divides $(q-1)$ and $(q-1)/k$ is even number, $C(k) = c1(k) - c2(2k) = (c1(k) - c2(k))/2$ if k divides $(q-1)$ and $(q-1)/k$ is odd number.

Properties:
$C(k) = 0$ if k does not divide $(q-1)$.
$C(k) = c1(k)$ if k divides $(q-1)$ and $(q-1)/k$ is even number.
$C(k) = c1(k) - c2(2k) = (c1(k) - c2(k))/2$ if k divides $(q-1)$ and $(q-1)/k$ is odd number.
$c1(k) = A059966(k)$
$c2(2k) = A000048(k)$
$c1(k) - c2(2k) = A051841(k)$

$L=$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$q=$																
3	2															
*5	2	1		1												
7	2		2			4										
*13	2	1	2	1		9						165				
*17	2	1		3				30								2032
19	2		2			4			56							
31	2		2		6	4				48					2182	
*61	2	1		1	6	9				99		165			2182	
*89	2	1		3				14			186					
127	2		2			4	18		56					576		
107	2															
*521	2	1		3	6			14		99			630			
607	2		2			4										
1279	2		2			4			56							
2203	2		2			4										
*2281	2	1	2	3	6	9		14		99		335			2182	
*3217	2	1	2	3		9		30				335				2032
*4253	2	1		1												
4423	2		2			4					186					
*9689	2	1		3			18	14						1161		
*9941	2	1		1	6		18			99				1161		
*11213	2	1		1												
*19937	2	1		3			18	30						1161		
*21701	2	1		1	6		18			99				1161		
*23209	2	1	2	3		9		14				335				
*44497	2	1	2	3		9		30	56			335				2032
86243	2												630			
110503	2		2			4	18		56					576		
*132049	2	1	2	3		9	18	30	56			335		1161		2032
216091	2		2		6	4	18		56	48				576	2182	
756839	2															
*859433	2	1		3			18	14								
1257787	2		2			4			56							
*1398269	2	1		1												
*2976221	2	1		1	6					99			630			
*3021377	2	1		3				30								4080
*6972593	2	1		3				30			186					2032
*13466917	2	1	2	1		9			56			165				
20996011	2		2		6	4	18		56	48				576	2182	
24036583	2		3			4										
25964951	2				6					48	186					
*30402457	2	1	2	3		9	18	14				335		1161		

Table 4: Number of loops of length L under x^2-2 modulo the first Mersennes.

12 Nber of cycles of length < 17 under $x^2 - 2$

13 Nber of cycles for Mersenne composites

$L =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	22	28
$q =$																	
11 r	2	2	2	2	9					1		2			1		
11 t	2				6					40							
23 r	2	2									15				10	1	
23 t	2										186					95232	
29 r	6	4	14		4	16			80		4	56		328	2		256
29 t	2	2		1			18				186			1161			4792905

Table 5: Number of cycles of length L under x^2-2 modulo the first Mersennes composites. (r:real t:theoretical)

14 Ratio $(M_q - 1)/order(3, M_q)$

Let call: $\eta(q,b)$ the number of distinct numbers $b^n + 1/b^n \pmod{M_q}$ for q, and $\theta(q,b) = \frac{M_{q-1}}{\eta(q,b)}$.
Let call: $\rho(q,b) = \frac{M_q-1}{order(b,M_q)}$.

The table 6 shows that there is a relationship between $\eta(q,b)$ and $\rho(q,b)$:

For $q = 3, 5, 7, 17, 19$ we have: $order(3, Mq)/\eta(q, 3) = 2$.
For $q = 13, 31$ we have: $(order(3, Mq) + 2)/\eta(q, 3) = 2$.

15 $2\eta(3, M_q) = order(3, M_q) + 2$ Proof by ZetaX

Let p be any odd prime. Let $f(x) := x + \frac{1}{x} \mod p$, then we want the size (lets call it $\eta(k,p)$) of the set $\{f(k^n) | n \in \mathbb{N}\}$.
First lets find out how often $f(x) \equiv f(y) \mod p$ with $x, y \not\equiv 0 \mod p$ happens: This means $x + \frac{1}{x} \equiv y + \frac{1}{y} \mod p \iff x^2y + y \equiv xy^2 + x \mod p$ $\iff (xy-1)(x-y) \equiv 0 \mod p$. This means that either $x \equiv y \mod p$, the trivial case, or $xy \equiv 1 \mod p$. But: when $x \equiv \pm 1 \mod p$, then only the case $x \equiv y \mod p$ can occur.

q	$\theta(q,3)$	$\theta(q,q)$	$\theta(q,3q)$	$\theta(q,6q)$	$\rho(q,3)$	$\rho(q,q)$	$\rho(q,3q)$	$\rho(q,6q)$
3	1	1			1	1	2	2
5	1	$\frac{2^4+4}{\eta(q,q)} = 10$		$\frac{2^4}{\eta(q,6q)} = 8$	1	10	3	15
7	1	1		$\frac{2^6}{\eta(q,6q)} = 2$	1	1	2	2
13	$\frac{2^{12}+8}{\eta(q,3)} = 9$	$\frac{2^{12}+4}{\eta(q,q)} = 10$		1	9	10	13	1
17	1	$\frac{2^{16}}{\eta(q,q)} = 2$		$\frac{2^{16}+2}{\eta(q,6q)} = 3$	1	2	3	3
19	1	1		$\frac{2^{18}+2}{\eta(q,6q)} = 6$	1	1	6	6
31	$\frac{2^{30}+2}{\eta(q,3)} = 3$				3	1	2	2
61					9	90	99	99
89					1	10	3	3
107					1	3	2	2
127					3	1	2	2
521					1	2	31	31
607					3	3	126	126
1279					3	1	2	2

Table 6: .

Look at the set $\text{Pow}(k) := \{k^n \mod p | n \in \mathbb{Z}\}$ (we can use $\mathbb{Z}$ instead of $\mathbb{N}$ because of Fermat's Little Theorem). It has size $|\text{Pow}(k)| = ord(k,p)$. Additionally, we can pair up the elements $k^n \mod p$ and $k^{-n} \mod p$ for each n, since they give the same value $f(k^n) \equiv f(k^{-n}) \mod p$, and only those are equal (note that $1, -1 \mod p$ will be left alone, but each noted as "pair" with one element). Since different pairs give different values, we have that $\eta(k,p) =$ "number of such pairs". Thus when $-1 \in \text{Pow}(k)$ (1 is always in the set), there will be $\frac{ord(k,p)-2}{2} + 2 = \frac{ord(k,p)+2}{2}$ pairs, thus by the above $\eta(k,p) = \frac{ord(k,p)+2}{2} \iff 2\eta(k,p) = ord(k,p) + 2$. Similar when -1 is not in the set: $2\eta(k,p) = ord(k,p) + 1$
This for example gives $\eta(3,7) = 4$.
To find out if -1 is in the set, we need to know if the order of $k \mod p$ is even or odd (this suffices to know: when $ord(k,p)$ would be odd, we couldn't have $2\eta(k,p) = ord(k,p) + 2 \mod 2$, and analogous for the other case). When s is the biggest integer with $2^s | p-1$, we could calculate $k^{\frac{p-1}{2^s}} \mod p$ (since $\frac{p-1}{2^s}$ is the biggest odd divisor of $p-1$) and look if it is $1 \mod p$ or not (the order is odd iff it is $1 \mod p$). When $4 \nmid p-1$, we just ask whether k is a quadratic residue $\mod p$ or not, which can be checked by Jacobi symbols. Special case $k = 3, p = 2^q - 1$: Then $4 \nmid p-1$, thus we use Legendre symbols (Jacobi is not needed since both numbers are prime) and the law of quadratic

reciprocity: $\left(\frac{3}{2^q-1}\right) = -\left(\frac{2^q-1}{3}\right) = -1$. This shows that the order of 3 $\mod p$ is even. Thus for Mersenne primes $p = M_q$, it is: $2\eta(3,p) = ord(3,p) + 2$.

16 Conjecture: $\frac{M_q-1}{order(3,M_q)} = 3^n$ with $n = 0, 1, 2$

Based on the data in table 7, we have the conjecture:

$$\frac{M_q - 1}{order(3, M_q)} = 3^n \quad \text{with} \quad n = 0, 1, 2$$

It seems that the conjecture is wrong for: $q = 3217$. But I do not understand the explanation ...

q	$(M_q - 1)/order(3, M_q)$
3	1
5	1
7	1
13	9
17	1
19	1
31	3
61	9
89	1
107	1
127	3
521	1
607	3
1279	3

Table 7: .

17 Loops under $x^3 - 3x$ Modulo a Mersenne

I computed the number of cycles of length L for $q = 3, 5, 7, 13, 17, 19, 31$, as shown in Table 9, by means of a `C` program that computes all pairs $(x, x^3 - 3x \pmod{M_q})$, finds the cycles and counts cycles of same length.
There are at least 1 cycle of length 2^i, for $i = 0 \ldots q-2$. They are related to the tree under $x^2 - 2$ and do not appear here below, for the q such that M_q is prime.

$L =$	1	2	3	**4**	5	6	**8**	9	10	12	15	**16**	18	36	128	256
$q =$																
3	2															
5	2	2														
7	2		2													
11	9	18			32				53							
13	2	2	6			12				30						
17	2	2					2					4			2	84
19	2		2			12		14		36				252		
31	2															

Table 8: Number of cycles of length L under $x^3 - 3x$ modulo the first Mersennes, without the cycles related to the tree under $x^2 - 2$.

We name $C_{q,n,l}$ a cycle of length l under the llt function of degree n, modulo the Mersenne prime $M_q = 2^q - 1$.
We recall that $llt_0 : x \mapsto 2$, $llt_1 : x \mapsto x$, $llt_2 : x \mapsto x^2 - 2$, $llt_3 : x \mapsto x^3 - 3x$.
For $q = 7$, there are 2 cycles $C_{7,2,3}$ and 4 cycles $C_{7,2,6}$. Under $x^3 - 3x$, 3 of the $C_{7,2,6}$ are connected to the 4th cycle $C_{7,2,6}$; and this cycle is connected to one of the $C_{7,2,3}$, which is connected to it-self. The second cycle $C_{7,2,3}$ is connected to node 126, which is connected to node 2, connected to it-self.

18 Loops under $x^2 - 2$ Modulo a Fermat

$L =$	1	3	5	7	15
$n =$					
1	2				
2	2	1			
3	2			9	
4	2	1	3		1091

Table 9: Number of cycles of length L under $x^2 - 2$ modulo the first Fermat primes.

Obviously, the length of cycles divide $2^n - 1$.
Looking at OEIS, this looks like the following suites: A000048 (and A056303, A114702), A060172, A066313, A060481.
2 formulae:

$$\psi(L) = \frac{1}{2L} \sum_{\text{odd } d|L} \mu(d) 2^{\frac{L}{d}}$$

$$\psi(L) = \frac{1}{L} \sum_{d|L} \mu(d) a(\frac{L}{d})$$