(One Wrong and One not-so-interesting)

Conjectures about the order of 3 modulo a Mersenne prime

Tony Reix

tony.reix@laposte.net

2009, 11th of March

– Version 0.2 –

Consider the table 2 on page 3, with $M_q = 2^q - 1$ prime.

The first part of the table has been built by computing $order(3, M_q)$ by means of the PARI/gp code:
`Mq=3^q-1 ; znorder(Mod(3,Mq))`
and with the help of factors from the Cunningham project managed by Samuel Wagstaff. So, these are exact values.

The second part of the table has been built by the following process:
1) Find I the greatest i such that $M_q \equiv 1 \pmod{3^i}$;
2) With $n = (M_q - 1)/3^o, o = 0..I$ compute $3^n \pmod{M_q}$ and find O the greatest o such that $3^n \equiv 1 \pmod{M_q}$.
So, these values are a upper limit of the order of 3 modulo a Mersenne prime.

We see: $O \leq I$.

Based on the data in table 2, it seems that we have the conjecture:

Conjecture 1 (Reix)

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

However, it's wrong...
David Broadhurst has found counter-examples by simply finding some small dividers of $M_q - 1$ and by computing:
`q= 3217 ; M=2^q-1 ; Mod(3,M)^((M-1)/13/3)`
which gives: $1 \pmod{M_{3217}}$. Easy...

So, the last (not so much) interesting question is: does the highest power of 3 that divides the order of 3 modulo a Mersenne prime is 2 ? or not...
So, my guess is: yes. But maybe the STRONG "law of SMALL numbers" will apply there again ?! (even if the numbers are quite big !).

So here is the new (but no as nice as the previous one was...) conjecture:

q	p such that $p \mid (M_q - 1)/order(3, M_q)$
3217	13
9689	29
9941	5
11213	5
23209	5
44497	7
110503	7
132049	5
132049	7
216091	71

Table 1: Counter-examples .

Conjecture 2 (Reix)

$$\textit{The highiest } O \textit{ such that } order(3, M_q) = \frac{M_q - 1}{3^O \times k} \quad \textit{is} \quad 2 \ .$$

q	$3^O = \frac{M_q - 1}{order(3, M_q) \times k}$	O	$I = \max i /$ $M_q \equiv 1 \pmod{3^i}$
3	1	0	1
5	1	0	1
7	1	0	2
13	9	2	2
17	1	0	1
19	1	0	3
31	3	1	2
61	9	2	2
89	1	0	1
107	1	0	1
127	3	1	3
521	1	0	1
607	3	1	2
1279	3	1	3
2203	1	0	2
2281	1	0	2
3217	3	1	2
4253	1	0	1
4423	3	1	2
9689	1	0	1
9941	3	1	1
11213	3	1	1
19937	3	1	1
21701	1	0	1
23209	9	2	2
44497	1	0	4
86243	1	0	1
110503	3	1	3

Table 2: $\approx (M_q - 1)/order(3, M_q)$.