A new property of Mersenne numbers: $M_q = (8x)^2 - (3qy)^2 = (1 + Sq)^2 - (Dq)^2$

Tony Reix (Tony.Reix@laposte.net)
2004, 11th of September

Theorem 1 (Reix) *Let $M_q = 2^q - 1$ (q prime > 3) be a Mersenne number. For each pair (a, b) of positive integers such that: $M_q = ab$, there exists a unic pair (x, y) or (S, D) of positive integers such that:*

$$\textbf{\textit{I:}}\ \ M_q = (8x)^2 - (3qy)^2 \qquad \textbf{\textit{II:}}\ \ M_q = (1 + Sq)^2 - (Dq)^2$$

(I discovered property **I** some years ago and I produced a complete, correct, but long and awful proof. I then received the following nicer proof from an anonymous reviewer. I discovered property **II** recently and proof is mine.)

Proof of I: Lets have: $M_q = 2^q - 1 = ab$ (with q odd prime) and:

$$\begin{cases} A = (a + b)/2 \\ B = (a - b)/2 \end{cases}$$

Then, for each pair (a, b) is associated a unic pair (A, B) such that:

$$M_q = A^2 - B^2 \qquad [= ((a + b)^2 - (a - b)^2)/4 = 4ab/4 = ab]$$

$$\text{So we must prove: } \begin{cases} 8 \mid A \\ 3 \mid B \\ q \mid B \end{cases}$$

- Since $2 \equiv -1 \pmod 3$, we have $2^{2p+1} \equiv (-1)^{2p+1} \equiv -1 \pmod 3$. Then with $q = 2p + 1$ we have $a \times b = M_q = 2^{2p+1} - 1 \equiv -2 \equiv 1 \pmod 3$. Since $1 \times 1 \equiv 2 \times 2 \equiv 1 \pmod 3$ we have $a \equiv b \pmod 3$, and thus $3 \mid (a - b)$ and $3 \mid B$.

- Since every prime divisor of M_q is congruent to $1 \pmod q$, we have $a \equiv b \equiv 1 \pmod q$ and $q \mid (a - b)$ and then $q \mid B$.

- Since every prime divisor of M_q is congruent to: $\pm 1 \pmod 8$ we have: $b \equiv \pm 1 \pmod 8$, and $b^2 \equiv 1 \pmod{16}$.

Since (with q prime > 3) $M_q \equiv -1 \pmod{16}$, then: $ab \equiv -1 \pmod{16}$, and thus: $2bA = ab + b^2 = b(a + b) \equiv -1 + 1 \equiv 0 \pmod{16}$.

Finally, since b is odd, that entails: $a + b \equiv 0 \pmod{16}$, and $16 \mid (a + b)$, and thus: $8 \mid A$.

Proof of II: Since a and b divide M_q, we have: $a = 1+2q\alpha$ and $b = 1+2q\beta$. Thus: $M_q = ab = (1 + 2q\alpha)(1 + 2q\beta) = 1 + 2q(\alpha + \beta) + 4q^2\alpha\beta$.

With $\alpha > \beta$, lets have: $S = \alpha + \beta$, $P = \alpha\beta$, and $D = \alpha - \beta$. We have the property: $S^2 - D^2 = 4P$. Thus: $M_q = 1+2Sq+4Pq^2 = 1+2Sq+(S^2-D^2)q^2$ and finally: $M_q = (1 + Sq)^2 - (Dq)^2$.

□