STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1953 - 001

On Mersenne numbers and Poulet numbers

H.J.A. Duparc

1953

Rapport ZW 1953 - 001

On Mersenne numbers and Poulet numbers

by

H.J.A. Duparc.

Definition. A Mersenne number is a number $m = 2^p - 1$, where p is prime.
Definition. A Mersenne prime is a number $m = 2^p - 1$, which is prime.

Obviously every Mersenne prime is a Mersenne number.

Definition. A Poulet number (or pseudo prime) is a composite number m which satisfies $2^{m-1} \equiv 1 \pmod{m}$.

Definition. A super-Poulet number is a composite number all divisors of which are either prime or Poulet numbers.

Obviously every non prime divisor of a super-Poulet number is a super-Poulet number.

Theorem 1. Every Mersenne number is either a Poulet number or a prime.

Proof. Let $m = 2^p - 1$ be a composite Mersenne number. Since p is prime we have

$$p \mid 2^{p-1} - 1 \mid 2^p - 2 = m - 1,$$

hence

$$m = 2^p - 1 \mid 2^{m-1} - 1.$$

Theorem 2. Every composite Mersenne number is a super-Poulet number.

Proof. Let $m = 2^r - 1$ be a composite Mersenne number and let m_1 be an arbitrary divisor of m. We prove $2^{m_1-1} \equiv 1 \pmod{m_1}$.

We now prove this last relation by induction. We found in theorem 1 that $2^{m-1} \equiv 1 \pmod{m}$ and may assume this property proved for every divisor n of m with $n > m_1$, i.e. $2^{n-1} \equiv 1 \pmod{n}$. Now let m_2 be a divisor of m such that $\frac{m_2}{m_1} = q$ is prime. Since $q \mid m = 2^p - 1$, and since p is prime, we have $p \mid q-1$, hence

$$m_2 \mid m = 2^p - 1 \mid 2^{q-1} - 1 \mid 2^{(q-1)m_1} - 1 = 2^{m_2 - m_1} - 1.$$

By induction we have $2^{m_2-1} \equiv 1 \pmod{m_2}$, so we get $2^{m_1-1} \equiv 1 \pmod{m_2}$, hence $2^{m_1-1} \equiv 1 \pmod{m_1}$, which proves the theorem.

Theorem 3. If m is prime or pseudo prime, then $M = 2^m - 1$ is prime or pseudo prime.

Proof. From $2^{m-1} \equiv 1 \pmod{m}$ it follows

$$M = 2^m - 1 \mid 2^{2^{m-1}-1} - 1 \mid 2^{2^m - 2} - 1 = 2^{M-1} - 1,$$

which proves the assertion.

Corollary. From this theorem it follows for primes m that every Mersenne number $M = 2^m - 1$ is either prime or pseudo prime.

Further it is not true that if m is a super-Poulet number also $M = 2^m-1$ is a super-Poulet number. If we take $m = 2^{11}-1 = 2047 = 23.89$, then from theorem 2 it follows that m is a super-Poulet number. However $M = 2^{2047}-1$ is not a super-Poulet number for consider the number $d = 47(2^{89}-1)$, then $d \mid (2^{23}-1)(2^{89}-1)$, so d divides M, but $d \nmid 2^{d-1}-1$, since $2^{89}-1 \nmid 2^{47(2^{89}-1)-1}-1$, for

$$47(2^{89}-1)-1 \equiv 46 \not\equiv 0 (\mathrm{mod}\ 89).$$

We now prove the following

<u>Theorem 4</u>. Consider the sequence

$$m_h = 2^{m_{h-1}} - 1 \qquad (h = 1,2,\ldots),$$

where m_0 is prime. Then two cases are possible:

1°. There exists a positive integer k such that m_{k-1} is prime, m_k is not prime. Then all m_h with $0 \leqq h \leqq k-1$ are prime and all m_h with $h \geqq k$ are pseudo prime.

2°. No such integer k can be found. Then all elements of the sequence are prime.

<u>Proof</u>. 1°. Suppose that for a positive integer k we have m_{k-1} prime, m_k not prime. Then obviously m_h is prime if $0 \leqq h \leqq k-1$. Since m_k is not prime, by theorem 2 the number m_k is a pseudo prime and by theorem 3 all m_h with $h \geqq k$ are prime or pseudo prime. Since m_k is composite obviously all m_h with $h \geqq k$ are composite, hence all m_h with $h \geqq k$ are pseudo primes.

2°. If no integer k can be found for which m_k is composite, all elements of the sequence are prime.

<u>Remark</u>. I do not know whether a prime m_0 can be found for which case 2° holds.

The case 1° occurs for instance for $m_0 = 11$; then $k = 1$, for $2^{11}-1 = 23.89$ is composite. Hence by the theorem 4 we find

<u>Theorem 5</u>. There are infinitely many Poulet numbers.

Finally by the remark to theorem 3 we see that if m_h is a super-Poulet number, the number m_{h+1} is not necessarily so, for if $m_0 = 11$, then m_1 is a super-Poulet number, but m_2 is not.