

Mersenne primes and Even Perfect numbers

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 23 September, 2017 (at 15:50)

Prolegomenon. Here is some notation^{♥1} used in the sequel. Employ \mathbb{P} for the set of primes, and \mathbb{D} for the set of odd posints. For n a positive integer, use $M_n := [2^n - 1]$ to name the n^{th} **Mersenne number**.

1: Lemma. *If M_n is prime then n is prime.* \diamond

Proof. Proving the contrapositive, suppose n factors non-trivially as

$$n = K \cdot L, \quad \text{where } K, L \in [2.. \infty).$$

Recall the polynomial identity

$$x^L - 1 = [x - 1] \cdot [1 + x + x^2 + \dots + x^{L-1}].$$

Setting $x := 2^K$ gives factorization that $M_n = A \cdot B$, where $A := 2^K - 1 \stackrel{\text{note}}{\geq} 3$, and

$$B = \sum_{\ell=0}^{L-1} 2^{\ell K} \stackrel{\text{note}}{\geq} 1 + 2^{1 \cdot 2} = 5.$$

Hence M_n is composite. \diamond

2a: Lemma. *For each posint k : $\sigma(k)=k+1$ IFF $k \in \mathbb{P}$.* \diamond

2b: Lemma. $\forall n, k \in \mathbb{Z}$, nec. $\text{Gcd}(n, k) \bullet [n - k]$. In particular, $[k+1] \perp k$. \diamond

2c: Coprimeness Lemma. *Suppose d, x, y are integers, $k \in \mathbb{N}$ and $p \in \mathbb{P}$. Then:*

i: If $d \bullet [xy]$ and $d \perp x$, then $d \bullet y$.

ii: If $p^k \bullet [xy]$ and $p \nmid x$, then $p^k \bullet y$. \diamond

^{♥1}Use \equiv_N to mean “congruent mod N ”. Let $n \perp k$ mean that n and k are co-prime. Use $k \bullet n$ for “ k divides n ”. Its negation $k \nmid n$ means “ k does not divide n .” Use $n \bullet k$ and $n \nmid k$ for “ n is/is-not a multiple of k .” Finally, for p a prime and E a natnum: Use double-verticals, $p^E \bullet n$, to mean that E is the **highest** power of p which divides n . Or write $n \parallel p^E$ to emphasize that this is an assertion about n . Use **PoT** for Power of Two and **PoP** for Power of (a) Prime.

3: Even-perfect Thm. *If M_K is prime, where $K \in \mathbb{Z}_+$, then*

$$N := 2^{K-1} \cdot M_K \stackrel{\text{note}}{=} 2^{K-1} \cdot [2^K - 1]$$

is perfect and even. (Attributed to EUCLID.)

Conversely, suppose N is an even perfect number. There there exists a posint K such that

$$N = 2^{K-1} \cdot M_K,$$

and M_K is prime. (Proved by Leonhard EULER.) \diamond

Pf of (\Rightarrow). Primeness of M_K forces $K \geq 2$, so 2^{K-1} is even, ditto N . Necessarily $2^{K-1} \perp [2^K - 1]$, so

$$\begin{aligned} \sigma(N) &= \sigma(2^{K-1}) \cdot \sigma(M_K) \\ &= [2^K - 1] \cdot \sigma(M_K) \end{aligned}$$

4:
$$\begin{aligned} &= [2^K - 1] \cdot [M_K + 1], \text{ by (2a),} \\ &= [2^K - 1] \cdot 2^K. \end{aligned}$$

Hence $\sigma(N) = 2N$. \diamond

Pf of (\Leftarrow). Factor the highest power-of-2 out of N as

$$\mathbf{5:} \quad N = 2^{K-1} \cdot B$$

with $K \in [2.. \infty)$ and $B \in \mathbb{D}$. Since $K \geq 2$, our 2^{K-1} is even, so $2^{K-1} \perp B$. Hence

$$\begin{aligned} \mathbf{6:} \quad 2^K \cdot B &= 2N = \sigma(N), \quad \text{since } N \text{ is perfect} \\ &= \sigma(2^{K-1}) \cdot \sigma(B) \\ &= [2^K - 1] \cdot \sigma(B). \end{aligned}$$

Note $2^K \perp [2^K - 1]$, courtesy (2b). So we may apply the Coprimeness Lemma twice to conclude that

$$\begin{aligned} \mathbf{7i:} \quad &B \bullet [2^K - 1] \quad \text{and} \\ \mathbf{7ii:} \quad &2^K \bullet \sigma(B). \end{aligned}$$

(One can finish the proof using either (7i) or (7ii); we will use the former.)

Using divisibility. Courtesy (7i) we can factor

$$\mathbf{8:} \quad B = [2^K - 1] \cdot C, \quad \text{where } C \in \mathbb{Z}_+.$$

(Indeed $C \in \mathbb{D}$, since B is odd.) Plugging this in to (6) gives $2^K \cdot [2^K - 1] \cdot C = [2^K - 1] \cdot \sigma(B)$. Hence

$$\mathbf{6':} \quad \sigma(B) = 2^K \cdot C.$$

Lower-binding $\sigma(B)$. Note $B > C$ (since $2^K - 1 > 1$, recalling that $K \geq 2$). Were $C \neq 1$, then $B > C > 1$ would be *distinct* factors of B . Hence

$$\begin{aligned}\sigma(B) &> B + C = 2^K \cdot C, && \text{by (8),} \\ &= \sigma(B), && \text{thanks to (??').}\end{aligned}$$

The contradiction “ $\sigma(B) > \sigma(B)$ ” forces C to be 1. So (8) and (5) yield that $N = 2^{K-1} \cdot M_K$.

Last step: Showing M_K prime. Eqn (??') now says

$$\sigma(M_K) = 2^K = 1 + M_K. \quad \blacklozenge$$

So, happily, Lemma 2a implies that M_K is prime.

Filename: Problems/NumberTheory/mersenne-perfect.tex
As of: Sunday 06Sep2009. Typeset: 23Sep2017 at 15:50.