Mersenne primes and Even Perfect numbers

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@math.ufl.edu
Webpage http://www.math.ufl.edu/~squash/
19 October, 2009 (at *02:47*)

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.* ♢

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

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

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

$$B \;=\; \sum_{\ell=0}^{L-1} 2^{\ell K} \;\overset{\text{note}}{\geqslant}\; 1 + 2^{1\cdot 2} \;=\; 5\,.$$

Hence M_n is composite. ♦

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

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

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 $p \not| x$, then $p^k \bullet\!\!\|\, y$.* ♢

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

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

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.) ♢

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

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

Hence $\boldsymbol{\sigma}(N) = 2N$. ♦

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

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

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

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

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

7i: $$B \;\bullet\!\!|\; [2^K - 1] \quad \text{and}$$

7ii: $$2^K \;\bullet\!\!\|\; \boldsymbol{\sigma}(B)\,.$$

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

Using divisibility. Courtesy (7i) we can factor

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

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

6′: $$\boldsymbol{\sigma}(B) \;=\; 2^K\cdot C\,.$$

[♡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 $k \not| n$ means "k does not divide n." Use $n \bullet\!\!|\; k$ and $n \not|\; k$ 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 $n \;\bullet\!\!\|\; p^E$ to emphasize that this is an assertion about n. Use ***PoT*** for Power of Two and ***PoP*** for Power of (a) Prime.

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

$$\begin{aligned} \boldsymbol{\sigma}(B) \;>\; B + C \;&=\; 2^K \cdot C\,, && \text{by (8),} \\ &=\; \boldsymbol{\sigma}(B)\,, && \text{thanks to } (6'). \end{aligned}$$

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

Last step: Showing M_K prime. Eqn $(6')$ now says

$$\boldsymbol{\sigma}(M_K) \;=\; 2^K \;=\; 1 + M_K\,. \qquad \blacklozenge$$

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

Filename: `Problems/NumberTheory/mersenne-perfect.latex`
As of: *Sunday 06Sep2009.* Typeset: *19Oct2009 at 02:47.*