Some Extensions to Touchard’s Theorem on Odd Perfect Numbers

Paolo Starni

Abstract

The multiplicative structure of an odd perfect number $n$, if any, is $n = \pi^\alpha M^2$, where $\pi$ is prime, $\gcd(\pi, M) = 1$ and $\pi \equiv \alpha \equiv 1 \pmod{4}$. An additive structure of $n$, established by Touchard, is that “$(n \equiv 9 \pmod{36}) \text{ OR } (n \equiv 1 \pmod{12})$”. A first extension of Touchard’s result is that the proposition “$(n \equiv x^2 \pmod{4x^2}) \text{ OR } (n \equiv \pi \equiv 1 \pmod{4x})$” holds for $x = 3$ (the extension is due to the fact that the second congruence contains also $\pi$). We further extend the proof to $x = \alpha + 2$, $\alpha + 2$ prime, with the restriction that the congruence modulo $4x$ does not include $n$. Besides, we note that the first extension of Touchard’s result holds also with an exclusive disjunction, so that $\pi \equiv 1 \pmod{12}$ is a sufficient condition because $3 \nmid n$.

1 Introduction

Without explicit definitions all the numbers considered here must be taken as strictly positive integers.

Definition 1. $n$ is said to be perfect if and only if $\sigma(n) = 2n$, where $\sigma(n)$ is the sum of the divisors of $n$.

Euler [1, p. 19] established a multiplicative structure of odd perfect numbers:

Statement 1 (Euler). If $n$ is an odd perfect number, then $n = \pi^\alpha M^2$, where $\pi$ is prime, $\gcd(\pi, M) = 1$ and $\pi \equiv \alpha \equiv 1 \pmod{4}$. 

1
In what follows you have to consider that \( n \), with the notation used in Statement 1, is an odd perfect number and that the proofs of all the theorems are given in Section 2.

**Note 1** (factors of \( n \) related to \( \sigma(\pi^\alpha) \)). *We can find factors of \( n \) considering that:*

\[
n = \pi^\alpha M^2 = \frac{\sigma(\pi^\alpha)}{2} \sigma(M^2)
\]

*and*

\[
\sigma(\pi^\alpha) = (\pi + 1)(1 + \pi^2 + \pi^4 + \ldots + \pi^{\alpha-1}).
\]  

(1)

Since \( \gcd(\pi^\alpha, \sigma(\pi^\alpha)) = 1 \), we have that \( \frac{\pi^\alpha + 1}{2} \mid M^2 \). In particular, if \( \frac{\pi^\alpha + 1}{2} \) is squarefree, then \( \left(\frac{\pi^\alpha + 1}{2}\right)^2 \mid M^2 \).

With regard to the additive structure of \( n \), related to the division by 4, it holds \( n \equiv 1 \pmod{4} \); in fact, in Statement 1, \( M^2 \equiv 1 \pmod{4} \) because square of an odd integer.

Touchard [6] found the additive structure of \( n \) in relation to the division by 3:

**Statement 2** (Touchard).

\[(n \equiv 9 \pmod{36}) \text{ OR } (n \equiv 1 \pmod{12}).\]

Statement 2 may be rewritten in a little more extended form:

**Theorem 1.** \((n \equiv 9 \pmod{36}) \text{ OR } (n \equiv \pi \equiv 1 \pmod{12})\).

Given \( \alpha \) as in Statement 1 we obtain:

**Theorem 2.** If \( \alpha + 2 \) is prime, then

\[(n \equiv (\alpha + 2)^2 \pmod{4(\alpha + 2)^2}) \text{ OR } (\pi \equiv 1 \pmod{4(\alpha + 2)})\].

Theorem 2 reproduces, for \( \alpha = 1 \), Theorem 1 except for the fact that its second congruence does not contain \( n \).
Note 2 (factors of \( n \) related to \( \pi \)). We can research factors of \( n \), in addition to the method of the Note 1, considering Theorem 2:

- If \( \pi \not\equiv 1 \pmod{4(\alpha+2)} \) and \( \alpha+2 \) is prime, then it holds the first congruence of the thesis, so that \((\alpha+2)^2 \mid n\).

Finally, the most extended form of Toucard’s theorem is the alternative:

**Theorem 3.** \((n \equiv 9 \pmod{36}) \quad XOR \quad (n \equiv \pi \equiv 1 \pmod{12})\).

Theorem 3 has a non-trivial corollary:

**Theorem 4.** If \( \pi \equiv 1 \pmod{12} \), then \( 3 \nmid n \).

We apply the previous considerations to the following two examples.

**Example 1.** Let it be \( n = 13^9M^2 \). Thus, \( 7^2 \mid n \) from Note 7, \( 11^2 \mid n \) from Note 2 and \( 3 \nmid n \) from Theorem 4.

**Example 2.** Let it be \( n = 5M^2 \). The methods described in Notes 1 and 2 lead to the same result that \( 9 \mid n \).

## 2 The proofs

We warn that a line numbered to the right, regardless of content, is generically indicated as equation.

### 2.1 Proof of Theorem 1

**Proof.** Also synthesizing the simpler proofs of Touchard’s theorem given by Satyanarayana [4], Raghavachari [3] and Holdener [2], we prove the following two statements contained in Equations (2) and (3):

\[\text{if } 3 \mid n, \text{ then } n \equiv 9 \pmod{36} \quad (2)\]

In fact, \( 9 \mid \pi \) so \( 9 \mid M^2 \Rightarrow n = \pi^9N^2 = (4k + 1)9 \equiv 9 \pmod{36} \).

\[\text{if } 3 \nmid n, \text{ then } n \equiv \pi \equiv 1 \pmod{12} \quad (3)\]

In fact, \( \pi \not= 12k + 5 \) (otherwise \( 3 \mid n \), see Equation (11)), so \( \pi \equiv 1 \pmod{12} \). Since \( M \equiv 1 \pmod{6} \) or \( M \equiv 5 \pmod{6} \), it follows \( M^2 \equiv 1 \pmod{6} \). Thus, being also \( M^2 \equiv 1 \pmod{4} \), it results \( M^2 \equiv 1 \pmod{12} \) and, therefore, \( n \equiv 1 \pmod{12} \).

Combining the statements in Equations (2) and (3), it follows the proof. \( \square \)
2.2 Proof of Theorem 2

We need the following result due to Starni [5]:

**Statement 3.** If \( \gcd(\pi - 1, \alpha + 2) = 1 \) and \( \alpha + 2 \) is prime, then \( (\alpha + 2) \mid M^2 \).

Now we are able to prove Theorem 2.

**Proof.** There are two cases:

- **Case 1** \( \gcd(\pi - 1, \alpha + 2) = 1 \).
  
  We obtain from Statement 3:
  
  \[
  n = \pi^\alpha(\alpha + 2)^2 N^2 = (\alpha + 2)^2(4k + 1).
  \]
  
  It follows the first congruence of the thesis.

- **Case 2** \( \gcd(\pi - 1, \alpha + 2) > 1 \), i.e., \( \gcd(\pi - 1, \alpha + 2) = \alpha + 2 \).
  
  We have
  
  \[
  \pi - 1 = k(\alpha + 2) \implies \pi \equiv 1 \pmod{\alpha + 2}.
  \]
  
  Since \( \pi \equiv 1 \pmod{4} \), it follows the second congruence of the thesis.

\[
\square
\]

2.3 Proof of Theorem 3

**Proof.** The system of the two congruences in Theorem 1 does not have solution because \( \gcd(36, 12) = 12 \mid (9 - 1) \). Thus, the logical connective OR may be replaced by XOR.

\[
\square
\]

2.4 Proof of Theorem 4

**Proof.** Theorem 3 states that:

\[
\pi \equiv 1 \pmod{12} \implies n \neq 9 \pmod{36}
\]

The contrapositive formulation of the statement in Equation 2 is

\[
n \neq 9 \pmod{36} \implies 3 \nmid n
\]

Thus, from the transitive property of the logical implication, it follows the proof.

\[
\square
\]
References

[1] L. E. Dickson, *History of the theory of numbers*, vol. 1, Dover, New York, (2005).

[2] J. A. Holdener, A theorem of Touchard on the form of odd perfect numbers, *American Mathematical Monthly* 109 (7) (2002), 661-663.

[3] M. Raghavachari, On the form of odd perfect numbers, *Math. Student* 34 (1966), 85-89.

[4] M. Satyanarayana, Odd perfect numbers, *Math. Student* 27 (1959), 17-18.

[5] P. Starni, Odd perfect numbers: a divisor related to the Euler’s factor, *J. Number Theory* 44 (1993), 58-59.

[6] J. Touchard, On prime numbers and perfect numbers, *Scripta Mathematica* 19 (1953), 35-39.