Descartes Numbers

William D. Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

Ahmet M. Güloğlu
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
ahmet@math.missouri.edu

C. Wesley Nevans
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
nevans@math.missouri.edu

Filip Saidak
Department of Mathematics and Statistics
University of North Carolina
Greensboro, NC 27402
f_saidak@uncg.edu

Abstract

We call n a *Descartes number* if n is odd and $n = km$ for two integers $k, m > 1$ such that $\sigma(k)(m+1) = 2n$, where σ is the sum of divisors function. In this paper, we show that the only cube-free Descartes number with fewer than seven distinct prime divisors is the number $3^2\,7^2\,11^2\,13^2\,19^2\,61$, which was discovered by Réne Descartes. We also show that if n is a cube-free Descartes number not divisible by 3, then n has over a million distinct prime divisors.

1 Introduction

> *...Mais je pense pouvoir démontrer qu'il n'y en a point de pairs qui soient parfaits, excepté ceux d'Euclide; & qu'il n'y en a point aussi d'impairs, si ce n'est qu'ils soient composés d'un seul nombre premier, multiplié par un carré dont la racine soit composée de plusieurs autres nombres premiers. Mais je ne vois rien qui empêche qu'il ne s'en trouve quelques uns de cette sorte: car, par exemple, si 22021 était nombre premier, en le multipliant par 9018009, qui est un carré dont la racine est composée des nombres premiers 3, 7, 11 & 13, on aurait 198585576189, qui serait nombre parfait...*
>
> – Réne Descartes, *Letter to Mersenne*, November 15, 1638.

Let σ denote the *sum of divisors function*, which is defined by

$$\sigma(n) = \sum_{d\,|\,n} d \qquad (n \geqslant 1),$$

where the sum is taken over the positive divisors d of n. The equivalent formula

$$\sigma(n) = \prod_{p^a\,\|\,n} \frac{p^{a+1}-1}{p-1},$$

where the product is taken over the prime powers p^a that occur in the prime factorization of n, was first discovered by Réne Descartes in 1638.

Recall that an integer $n \geqslant 1$ is said to be a *perfect number* if $\sigma(n) = 2n$. If $2^p - 1$ is a prime number (that is, a *Mersenne prime*), then $n = 2^{p-1}(2^p - 1)$ is a perfect number. This fact was first observed by Euclid (Proposition 36 in Book IX of *Elements*; see [6]), and many of Euclid's successors implicitly assumed that every perfect number has this form. The idea that every *even* perfect number has this form was first proposed by Descartes in the letter to Mersenne quoted above. More than two hundred years later, Euler (in posthumous [4]) published the first proof that Euclid's construction yields all even perfect numbers.

To this day, it is not known whether there exist any *odd* perfect numbers. Descartes believed that such numbers might exist, and he stated (without proof) that every odd perfect number must be of the form $p^a m^2$, where m is an integer, p is a prime number, and $p \equiv a \equiv 1 \pmod 4$. The first rigorous proof of this assertion was given by Euler [3]; however, it is reasonably certain that Descartes himself must have been in possession of such a proof.

Perhaps because of the popularity of Euler's works, Descartes did not receive a great deal of credit for his numerous contributions to the study of perfect numbers (see Dickson [2]). However, the depth of his understanding of the subject should not be underestimated, as is evident from the following example of an odd number $\mathscr{D}$ which he discovered:

$$\mathscr{D} = 3^2\,7^2\,11^2\,13^2\,22021 = 198585576189. \tag{1}$$

The number $\mathscr{D}$ comes "very close to perfection." In fact, as Descartes himself observed, $\mathscr{D}$ would be an odd perfect number if only 22021 were a prime number, since

$$\sigma(3^2\,7^2\,11^2\,13^2)\,(22021+1) = 2\cdot 3^2\,7^2\,11^2\,13^2\,22021 = 2\mathscr{D}. \tag{2}$$

Alas, $22021 = 19^2\,61$ is composite, and the number $\mathscr{D}$ is not perfect.

Inspired by the example (1) and the identity (2), let us call an integer n a *Descartes number* if n is *odd*, and if $n = km$ for two integers $k, m > 1$ such that

$$\sigma(k)(m+1) = 2n. \tag{3}$$

Then $\mathscr{D}$ is a Descartes number, and this is the only currently known example. We remark that if $n = km$ is a Descartes number such that m is prime and $m \nmid k$, then n is an odd perfect number.

In this paper, for simplicity, we investigate *cube-free* Descartes numbers n (that is, $p^3 \nmid n$ for every prime p); note that $\mathscr{D}$ is cube-free.

To state our results, recall that a positive integer k is said to be *almost perfect* if $\sigma(k) = 2k - 1$. Every nonnegative power of 2 is almost perfect, and it is generally believed that these are the *only* examples of such integers (see Guy [5]). In particular, it is believed that $k = 1$ is the only *odd* almost perfect number. We remark that if $k > 1$ is an odd almost perfect number, then $n = k\sigma(k)$ is a Descartes number.

Theorem 1. *If n is a cube-free Descartes number which is not divisible by 3, then $n = k\,\sigma(k)$ for some odd almost perfect number k, and n has more than one million distinct prime divisors.*

Theorem 2. *The number $\mathscr{D}$ is the only cube-free Descartes number with fewer than seven distinct prime divisors.*

2 Preparations

We use the following elementary results:

Lemma 3. *Let a and b be integers such that $2a > b \geqslant 1$ and $(2a - b) \mid a$. Then $a = de$ and $b = d(2e - 1)$ for some positive integers d and e.*

Proof. Put $d = \gcd(a, b)$, and write $a = de$, $b = df$, where $\gcd(e, f) = 1$. The hypothesis $(2a - b) \mid a$ implies $(2e - f) \mid e$; therefore, since $2e > f$ we have

$$2e - f = \gcd(2e - f, e) = \gcd(-f, e) = 1,$$

or $f = 2e - 1$ as required. □

Lemma 4. *If p and q are primes such that $p^2 + p + 1 \equiv 0 \pmod{q}$, then $q = 3$ or $q \equiv 1 \pmod 3$. If s is square-free, then the number $\sigma(s^2)$ has no prime divisor $q \equiv 2 \pmod 3$.*

Proof. To prove the first statement, we note that

$$(2p + 1)^2 + 3 = 4p^2 + 4p + 4 \equiv 0 \pmod{q}.$$

If $q \neq 3$, this shows that -3 is a quadratic residue modulo q, which is only possible if $q \equiv 1 \pmod 3$. For a square-free number s we have

$$\sigma(s^2) = \prod_{p \mid s} (p^2 + p + 1), \tag{4}$$

hence the second statement follows from the first. □

Finally, in our proof of Theorem 2 we use the following:

Lemma 5 (Pomerance [7]). *Every odd perfect number has at least seven distinct prime divisors.*

3 Cube-free Descartes numbers

Let n be a Descartes number, and write $n = km$ with odd integers $k, m > 1$ satisfying (3). Then,

$$\sigma(k) \cdot \frac{m+1}{2} = n = km, \tag{5}$$

and therefore,

$$m = \frac{\sigma(k)}{2k - \sigma(k)} = -1 + 2 \cdot \frac{k}{2k - \sigma(k)}. \tag{6}$$

From (5) we deduce that $\sigma(k)$ is odd, hence $k = s^2$ for some integer $s \geqslant 1$. Using (6) together with the fact that $2k - \sigma(k)$ is odd, we also see that $(2k - \sigma(k)) \mid k$; hence, by Lemma 3 we have

$$k = s^2 = de \qquad \text{and} \qquad \sigma(k) = \sigma(s^2) = d(2e-1) \tag{7}$$

for some positive integers d and e. Substituting these expressions into (6), it follows that $m = 2e - 1$, and therefore,

$$\sigma(k) = \sigma(s^2) = dm. \tag{8}$$

Suppose now that n is cube-free. As $s^2 \mid n$, it follows that s is square-free. We claim that $3 \nmid e$. Indeed, if $3 \mid e$, it follows that $m = 2e - 1 \equiv 2 \pmod 3$, hence there is a prime $q \equiv 2 \pmod 3$ dividing m; but this is not possible in view of Lemma 4 since $m \mid \sigma(s^2)$.

Next, we claim that $e \equiv 1 \pmod 3$. Indeed, if a prime $q \equiv 2 \pmod 3$ divides e, then $q \mid s$, and $q^2 \mid s^2 = de$. But q cannot divide d, for otherwise q would divide $\sigma(s^2)$, contradicting Lemma 4. Hence, $q^2 \mid e$, and therefore $q^2 \parallel e$ since e is cube-free. Since $3 \nmid e$, we now see that

$$e = \Bigg(\prod_{\substack{q^a \,\|\, e \\ q \equiv 1 \pmod 3}} q^a \Bigg) \Bigg(\prod_{\substack{q \,|\, e \\ q \equiv 2 \pmod 3}} q^2 \Bigg),$$

and the congruence $e \equiv 1 \pmod 3$ is obvious.

For any integer t, we have $3 \mid (t^2 + t + 1)$ if and only if $t \equiv 1 \pmod 3$, and in this case, $t^2 + t + 1 \equiv 3 \pmod 9$. Therefore, observing that $n = e\,\sigma(s^2)$, we deduce from (4):

$$\#\big\{p \ : \ p \mid s \text{ and } p \equiv 1 \pmod 3\big\} = v_3(\sigma(s^2)) = v_3(e\,\sigma(s^2)) = v_3(n). \tag{9}$$

Here, v_3 denotes the standard 3-*adic valuation*, and we have used the fact that $3 \nmid e$ to derive the second equality.

4 Proof of Theorem 1

We continue to use the notation of the previous section. In particular, n is a cube-free Descartes number. In what follows, we assume that $3 \nmid n$.

Since d divides n, we have $3 \nmid d$. By (9), we also see that d is not divisible by any prime $p \equiv 1 \pmod 3$. Finally, since $d \mid \sigma(s^2)$, Lemma 4 shows that d is not divisible by any prime $q \equiv 2 \pmod 3$. Therefore, $d = 1$. Now we have $n = k\sigma(k)$ by (5) and (8), and $\sigma(k) = 2k - 1$ by (7). Since k is odd, this proves the first assertion of Theorem 1.

As $k = s^2$ and $\sigma(k) = 2k - 1$, for every prime q dividing $\sigma(s^2)$ we have $2s^2 \equiv 1 \pmod q$, and thus $q \equiv \pm 1 \pmod 8$ (since 2 is a quadratic residue modulo q). Consequently, if p is any prime dividing s, then $p^2 + p + 1$ is composed of primes $q \equiv \pm 1 \pmod 8$; this implies that $p \equiv 5$ or $7 \pmod 8$. Also, $p \neq 3$ since we are assuming that $3 \nmid n$, and $p \not\equiv 1 \pmod 3$ by (9). We have therefore shown that every prime divisor of s lies in the set

$$\mathcal{P} = \big\{p \ : \ p \equiv 5 \text{ or } 23 \pmod{24}\big\}.$$

Let $p_1 < p_2 < p_3 < \cdots$ denote the primes in $\mathcal{P}$. Now, assuming that s has at most one million distinct prime divisors, we derive that

$$\frac{\sigma(s^2)}{s^2} = \prod_{p \mid s} \left(\frac{p^2 + p + 1}{p^2}\right) \leqslant \prod_{j=1}^{10^6} \left(\frac{p_j^2 + p_j + 1}{p_j^2}\right) < 1.995.$$

On the other hand, noting that $s \neq 1$ (since $s^2 = k > 1$), we have $s \geqslant 100$ since the equation $\sigma(s^2) = 2s^2 - 1$ has no solutions in the range $1 < s < 100$. Therefore,

$$\frac{\sigma(s^2)}{s^2} = 2 - \frac{1}{s^2} \geqslant 1.9999.$$

This contradiction, together with the fact that $n = s^2\,\sigma(s^2)$, implies the second assertion of Theorem 1, and this completes the proof.

5 Proof of Theorem 2

We continue to use the notation of Section 3. In what follows, we assume that n is a cube-free Descartes number such that $3 \mid n$ and $\omega(n) \leqslant 6$, where $\omega(n)$ denotes the number of distinct prime factors of n.

Since $m = 2e - 1 \equiv 1 \pmod 3$, and $(m+1)/2$ is odd by (5), we have

$$m \equiv 1 \pmod{12}. \tag{10}$$

Since $3 \mid n$ it follows that $3 \mid k = s^2$, thus $3^2 \mid k \mid n$; as n is cube-free, this means that $3^2 \,\|\, n$, and by (9) we see that

$$\#\big\{p \;:\; p \mid k \text{ and } p \equiv 1 \pmod 3\big\} = 2. \tag{11}$$

Since $n = km$ is cube-free and $k = s^2$, it is clear that $\gcd(k, m) = 1$. The number m cannot be prime, for otherwise the equation $\sigma(k)(m+1) = 2km$ implies n is an odd perfect number, and by Lemma 5 it has at least *seven* distinct prime divisors. Since $m \mid \sigma(s^2)$, Lemma 4 shows that m is not divisible by any prime $q \equiv 2 \pmod 3$; hence, from (10) it follows that $m \geqslant 49$. On the other hand, it must also be the case that $\omega(k) \geqslant 4$, for otherwise

$$\frac{\sigma(k)}{k} \leqslant \frac{\sigma(3^2\,7^2\,13^2)}{3^2\,7^2\,13^2} < \frac{2m}{m+1}$$

for any $m \geqslant 49$. We therefore have two distinct cases to consider:

(*A*) $m = p^2$ for some prime p, and $\omega(k) = 4$ or 5;

(*B*) $\omega(m) = 2$ and $\omega(k) = 4$.

Lemma 6. $5 \nmid k$.

Proof. Suppose on the contrary that $5 \mid k$, and write $k = s^2 = 3^2\,5^2\,\ell^2$ with some square-free integer ℓ. Then,

$$13 \cdot 31\, \sigma(\ell^2)(m+1) = 2 \cdot 3^2\,5^2\,\ell^2 m. \tag{12}$$

Since $5 \nmid \sigma(\ell^2)$ by Lemma 4, it follows that $5^2 \mid (m+1)$; using (10) and the Chinese Remainder Theorem we deduce that

$$m \equiv 49 \pmod{300}. \tag{13}$$

It cannot be the case that $(13 \cdot 31) \mid \ell$, for otherwise

$$\frac{\sigma(k)}{k} \geqslant \frac{\sigma(3^2\,5^2\,13^2\,31^2)}{3^2\,5^2\,13^2\,31^2} > 2 > \frac{2m}{m+1}.$$

Hence, by (12) we see that $13 \mid m$ or $31 \mid m$. But this is already impossible in case (A) as neither 13^2 nor 31^2 is congruent to 49 (mod 300); thus, we can assume that (B) holds for the rest of the proof.

Note that m is not divisible by *both* 13 and 31 since m is cube-free, $\omega(m) = 2$, and

$$13^\alpha\, 31^\beta \not\equiv 49 \pmod{300} \qquad (1 \leqslant \alpha, \beta \leqslant 2).$$

Suppose that $13 \mid m$. Then $m \equiv 949 \pmod{3900}$ by (13) and the Chinese Remainder Theorem. Also, from (12) it follows that $31 \mid \ell$ (since $31 \nmid m$), and thus $k = 3^2\, 5^2\, 31^2\, q^2$ for some prime q. However, since $m \geqslant 949$ we have

$$\frac{2 \cdot 949}{950} \leqslant \frac{2m}{m+1} = \frac{\sigma(k)}{k} = \frac{\sigma(3^2\, 5^2\, 31^2)}{3^2\, 5^2\, 31^2}\, \frac{(q^2+q+1)}{q^2} < 2,$$

and it is easy to see that there is no integer q for which both inequalities are satisfied. This shows that $13 \nmid m$. By a similar argument, one also sees that $31 \nmid m$, and we obtain the desired contradiction for case (B). $\square$

On the other hand, we can now see that $7 \mid k$, for otherwise the inequality

$$\frac{2m}{m+1} = \frac{\sigma(k)}{k} \leqslant \frac{\sigma(3^2\, 11^2\, 13^2\, 17^2\, 19^2)}{3^2\, 11^2\, 13^2\, 17^2\, 19^2}$$

is not possible for any $m \geqslant 49$. Let us write $k = s^2 = 3^2\, 7^2\, \ell^2$ with some square-free integer ℓ; then,

$$13 \cdot 19\, \sigma(\ell^2)(m+1) = 2 \cdot 3 \cdot 7^2\, \ell^2 m. \tag{14}$$

We observe that $(13 \cdot 19) \nmid \ell$, for otherwise we have $3^2\, 7^2\, 13^2\, 19^2 \mid k$, and this contradicts (11). Hence, by (14) it follows that $13 \mid m$ or $19 \mid m$.

In case (A), these observations imply that $m = 13^2$ or 19^2. However, if $m = 13^2$, then $5 \mid (m+1)$, and from (14) we deduce that $5 \mid k$, which contradicts Lemma 6. On the other hand, if $m = 19^2$, then $181 \mid (m+1)$, and from (14) we conclude that $3^2\, 7^2\, 13^2\, 181^2 \mid k$, which contradicts (11). Hence, we can assume that (B) holds from now on.

Suppose first that $(13 \cdot 19) \mid m$. Since m is cube-free, $\omega(m) = 2$, and $m \equiv 1 \pmod{12}$, it follows that $m = 13 \cdot 19^2$ or $13^2\, 19^2$. If $m = 13^2\, 19^2$, then $5 \mid (m+1)$, and (14) leads to the conclusion that $5 \mid k$, which contradicts what we have already shown. On the other hand, if $m = 13 \cdot 19^2$, then (14) implies

$$2347\,\sigma(\ell^2) = 3 \cdot 7^2\,19\,\ell^2.$$

Writing $\ell = 2347q$ for some prime q, this relation becomes

$$397 \cdot 661\,(q^2 + q + 1) = 7 \cdot 19 \cdot 2347\,q^2,$$

which does not have an integer solution q. Therefore, $(13 \cdot 19) \nmid m$.

Next, suppose that $19 \mid \ell$ and $13 \mid m$, and write $\ell = 19q$ for some prime q; note that (11) implies $q \equiv 2 \pmod 3$. From (14) we deduce that

$$13 \cdot 127\,(q^2 + q + 1)(m + 1) = 2 \cdot 7^2\,19\,q^2 m. \tag{15}$$

Since $q \equiv 2 \pmod 3$, it follows that $(13 \cdot 127) \mid m$. As m is cube-free, $\omega(m) = 2$, and $m \equiv 1 \pmod{12}$, we must have $m = 13 \cdot 127^2$ or $13^2\,127^2$. However, if $m = 13 \cdot 127^2$ then (15) becomes

$$17 \cdot 881\,(q^2 + q + 1) = 7 \cdot 19 \cdot 127\,q^2,$$

and if $m = 13^2\,127^2$ we have

$$397 \cdot 3433\,(q^2 + q + 1) = 7^2\,13 \cdot 19 \cdot 127\,q^2,$$

and neither equation has an integer solution q.

Finally, we are reduced to the case that $13 \mid \ell$ and $19 \mid m$. Write $\ell = 13q$ for some prime q, and note that (11) implies that $q \equiv 2 \pmod 3$ as before. From (14) it follows that

$$19 \cdot 61\,(q^2 + q + 1)(m + 1) = 2 \cdot 7^2\,13\,q^2 m. \tag{16}$$

Since $q \equiv 2 \pmod 3$, we have $(19 \cdot 61) \mid m$. As m is cube-free, $\omega(m) = 2$, and $m \equiv 1 \pmod{12}$, we must have $m = 19^2\,61$ or $19^2\,61^2$. If $m = 19^2\,61^2$ then (16) implies

$$337 \cdot 1993\,(q^2 + q + 1) = 7^2\,13 \cdot 19 \cdot 61\,q^2,$$

which has no integer solution q. On the other hand, if $m = 19^2\,61$, then (16) becomes

$$11^2\,(q^2 + q + 1) = 7 \cdot 19\,q^2,$$

which implies that $q = 11$. In this case, we see that

$$n = 3^2\,7^2\,11^2\,13^2\,19^2\,61 = \mathscr{D},$$

and this completes the proof of Theorem 2.

6 Acknowledgements

The authors wish to thank the referee for several helpful remarks.

References

[1] R. Descartes (1596–1650), *Œuvres de Descartes*, publiées par Charles Adam & Paul Tannery sous les auspices du Ministère de l'instruction publique, Paris, L. Cerf, 1898.

[2] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1 (pp. 3–50), 1st ed., Carnegie Inst., Washington, 1919.

[3] L. Euler, 'Tractatus de numerorum doctrina capita sedecim, quae supersunt,' *Commentationes Arithmeticae* **2** (1849) p. 514; reprinted in *Opera Posthuma, 1*, pp. 14–15, 1862.

[4] L. Euler, 'De numeris amicabilibus,' *Commentationes Arithmeticae* **2** (1849) p. 630 (written in 1747); reprinted in *Opera Posthuma, 1*, p. 88, 1862.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, (§B2, pp. 45–53) 2nd ed., Springer-Verlag, New York, 1994.

[6] T. L. Heath, *The Thirteen Books of Euclid's Elements*, University Press, Cambridge, 1908; 2nd ed. reprinted by Dover, New York, 1956.

[7] C. Pomerance, 'Odd perfect numbers are divisible by at least seven distinct primes,' *Acta Arithmetica* **25** (1973) pp. 265–300.