ClassRoom

Digital Roots of Perfect Numbers

C⊗MαC

It was claimed in the article by Anant Vyawahare on *Digital Roots* that a perfect number other than 6 has digital root 1 (Property 10 of that article). We now provide a proof of this claim.

But, first things first; let us start by defining the basic motions and related concepts.

Perfect numbers. Many children discover for themselves the following property of the integer 6: the sum of its proper divisors is equal to the number ($1 + 2 + 3 = 6$). Noticing such a property, they may naturally wonder about the existence of more such integers. Two millennia back, the Greeks decided that such a property indicated a kind of perfection, and called such numbers **perfect**. (This is of course the English translation of the word used by the Greeks; other translations could be: *complete*, *ideal*.) So 6 is a perfect number (and it is obviously the smallest perfect number).

Students will naturally ask what we should call numbers which are not perfect, i.e., other than simply calling them imperfect! This line of thinking gives rise to the following definitions.

Keywords: *Perfect number, deficient number, abundant number, Mersenne prime, factor theorem*

Let $d(n)$ denote the sum of the divisors of the positive integer n. We include among the divisors the number n itself (that is why we did not use the word 'proper'). For example, $d(10) = 1 + 2 + 5 + 10 = 18$, and $d(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$. In terms of the d-function, we arrive at the following definitions:

- If $d(n) < 2n$, we say that n is **deficient**.
- If $d(n) = 2n$, we say that n is **perfect**.
- If $d(n) > 2n$, we say that n is **abundant**.

For example:

- 10 is deficient, because $1 + 2 + 5 + 10 < 20$;
- 6 is perfect, because $1 + 2 + 3 + 6 = 12$; and
- 12 is abundant, because $1 + 2 + 3 + 4 + 6 + 12 > 24$.

This categorisation of the natural numbers has considerable antiquity; indeed it goes back to the first century AD! According to Wikipedia: "The natural numbers were first classified as either deficient, perfect or abundant by Nicomachus in his *Introductio Arithmetica* (circa 100)."

Number crunching. Write D, P and A to denote (respectively) the sets of deficient, perfect and abundant numbers. Computer-assisted experimentation (using any computer algebra system, for example, *Mathematica*) yields the following data for the positive integers below 100:

$$\begin{aligned} D = \{&1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19, 21, 22, 23, 25, 26, 27, 29, 31, 32, 33,\\ &34, 35, 37, 38, 39, 41, 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 55, 57, 58, 59, 61, 62, 63,\\ &64, 65, 67, 68, 69, 71, 73, 74, 75, 76, 77, 79, 81, 82, 83, 85, 86, 87, 89, 91, 92, 93, 94,\\ &95, 97, 98, 99, \ldots\}, \end{aligned}$$

$$P = \{6, 28, \ldots\},$$

$$A = \{12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, 96, \ldots\}.$$

Examining these figures, we are struck by the following: there appear to be very few perfect numbers; there appear to be many more deficient numbers than abundant numbers; abundant numbers appear to be all even. But …these being generated by computer experimentation, we must not assume immediately that they are all true; data can deceive us. (Indeed, one of the statements turns out to be incorrect; but we will leave it to you to find out which one!)

Some statements however are easy to conjecture and also easy to prove. For example:

(1) *There exist infinitely many deficient numbers.*

For, any prime p is deficient, since $d(p) = 1 + p < 2p$. Since there are infinitely many primes, there must also be infinitely many deficient numbers.

(2) *There exist infinitely many abundant numbers.*

For, if p is a prime number, then $12p$ is necessarily an abundant number, because

$$d(12p) = p + 2p + 3p + 4p + 6p + 12p = 28p > 24p.$$

Since there are infinitely many primes, there must also be infinitely many abundant numbers.

It is tempting now to conclude: *There exist infinitely many perfect numbers.* But as of today, mathematicians do not know the truth concerning this question!

One can frame the above as a question rather than a conjecture: *Is there a way of generating as many perfect numbers as one wants?* Long back, the Greeks discovered a partial answer to this question by connecting it with a question about prime numbers. Here is the connection. Within the sequence of prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ \ldots$$

one can identify various subsequences of interest. One which we will be concerned with is the following:

$$3,\ \ 7,\ \ 31,\ \ 127,\ \ 8191,\ \ \ldots.$$

These are the prime numbers which are 1 less than powers of 2:

$$3 = 2^2 - 1, \quad 7 = 2^3 - 1, \quad 31 = 2^5 - 1, \quad 127 = 2^7 - 1, \quad 8191 = 2^{13} - 1, \quad \ldots.$$

Today, such primes are called **Mersenne primes**, after the French mathematician-scientist-theologian Marin Mersenne (1588–1648), because he made a close study of such primes ([1]). But much before Mersenne, the Greeks had identified these primes as being of interest. Indeed, they discovered the following remarkable rule for generating perfect numbers using such prime numbers:

Theorem 1 (Euclid)**.** *If P is a prime number which is 1 less than a power of 2, then the number $P(P+1)/2$ is perfect.*

Let us see how the rule given by this theorem acts.

- $P = 3$ yields the perfect number $3 \times 2 = 6$;
- $P = 7$ yields the perfect number $7 \times 4 = 28$;
- $P = 31$ yields the perfect number $31 \times 16 = 496$;
- $P = 127$ yields the perfect number $127 \times 64 = 8128$;

and so on. (Please check for yourself that the numbers 28 and 496 are perfect.) It may seem now that we have hit upon a perfect recipé for generating infinitely many perfect numbers. But wait, there is a catch! Simply put: we do not know if there are infinitely many Mersenne primes!

Remark. Identifying the precise set of values of n for which the number $2^n - 1$ is prime makes for a fascinating exploration. It is easy to see that n must be prime for $2^n - 1$ to be prime. Indeed, if a is a divisor of n, then $2^a - 1$ is a divisor of $2^n - 1$; for example, $2^3 - 1 = 7$ is a divisor of $2^9 - 1 = 511$.

What complicates the picture is that there are prime values of n for which $2^n - 1$ is not prime! The first such value is 11. Finding the factorisation of $2^{11} - 1 = 2047$ makes for a nice exercise.

Proof of Theorem 1. Proving Theorem 1 is fairly easy. Let $P = 2^n - 1$ be a Mersenne prime (here $n \geq 2$). Then $P(P+1)/2 = 2^{n-1}P$. What are the divisors of the number $2^{n-1}P$? As this number has only two distinct prime factors (2 and P), it is easy to list all its divisors:

$$\begin{cases} 1, & 2, & 2^2, & 2^3, & \ldots, & 2^{n-1}, \\ P, & 2P, & 2^2P, & 2^3P, & \ldots, & 2^{n-1}P. \end{cases}$$

The sum of the divisors is therefore

$$\begin{aligned}&\left(1+2+2^2+\cdots+2^{n-1}\right)+\left(P+2P+2^2P+\cdots+2^{n-1}P\right)\\&=(1+P)\left(1+2+2^2+\cdots+2^{n-1}\right)\\&=(P+1)\left(2^n-1\right)\qquad\text{(by summing the GP)}\\&=(P+1)P,\end{aligned}$$

which is twice the number under study; hence $P(P+1)/2$ is perfect, as claimed. □

How the Greeks stumbled upon this result is not clear. It is noteworthy that they did so and also proved the correctness of the procedure in a pre-algebra age.

Now it is obvious that for $n > 1$, the formula $(2^n - 1)\,2^{n-1}$ will only generate even numbers; hence this rule generates only *even perfect numbers*. A full twenty centuries after the Greeks, the Swiss German mathematician Leonhard Euler (1707–1783) proved a sort of converse to Theorem 1:

Theorem 2 (Euler)**.** *Every even perfect number has the form $P(P+1)/2$ where P is a prime number of the form $2^n - 1$.*

Euler's theorem is rather more challenging to prove than Euclid's; we invite you to find a proof of your own.

Euclid's and Euler's results acting in tandem provide a complete characterisation of the even perfect numbers.

Remark. Nothing has been said till now about *odd perfect numbers*. There is a mystery here. It has been conjectured that there do not exist any odd perfect numbers. However, no proof has been found for this statement, though it is widely believed to be true (all the evidence points in its favour).

Digital root of a perfect number

We are now in a position to prove the statement made in the companion article: *All even perfect numbers other than* 6 *have digital root* 1.

From Theorem 2 we know that every even perfect number has the form $2^{n-1}\,(2^n - 1)$ where n is such that $2^n - 1$ is a prime number.

Now if n is even, $2^n - 1$ is a multiple of 3 (this may be established using induction; please do so); and $2^n - 1 > 3$ for $n > 2$. Hence if $n > 2$ and is even, $2^n - 1$ is not a prime number. Expressing this statement in a negative way, we infer that if $n > 2$ and $2^n - 1$ is a prime number, then n is odd.

The claim that all even perfect numbers other than 6 have digital root 1 is implied by the following result, which actually establishes a much stronger statement.

Theorem 3. *If n is odd, then $2^{n-1}\,(2^n - 1)$ leaves remainder* 1 *under division by* 9.

For example, for $n = 3$, $2^{n-1}\,(2^n - 1) = 2^2\,(2^3 - 1) = 28 = (9 \times 3) + 1$; and for $n = 9$, $2^{n-1}\,(2^n - 1) = 2^8\,(2^9 - 1) = 130816 = (9 \times 14535) + 1$.

Proof of Theorem 3. The statement of the theorem can be rewritten thus:

If n is odd, then $2^{2n-1} - 2^{n-1} - 1$ is divisible by 9.

Multiplication by 2 has no effect on divisibility by 9; so we may express this as:

If n is odd, then $4^n - 2^n - 2$ is divisible by 9.

We offer two proofs of this statement. The first one runs along lines which should be very familiar to class 11 and 12 students.

First proof. Let $f(n) = 4^n - 2^n - 2$; then $f(1) = 0$ and $f(3) = 54$. So $f(1)$ and $f(3)$ are multiples of 9. To prove the theorem, it suffices to show that $f(n+2) - f(n)$ is divisible by 9 for all odd positive integers n. Now we have:

$$\begin{aligned} f(n+2) - f(n) &= 4^{n+2} - 4^n - 2^{n+2} + 2^n \\ &= 16 \cdot 4^n - 4^n - 4 \cdot 2^n + 2^n = 15 \cdot 4^n - 3 \cdot 2^n \\ &= 3 \cdot 2^n \left(5 \cdot 2^n - 1\right). \end{aligned}$$

Therefore, to prove that $f(n+2) - f(n)$ is divisible by 9 for all odd positive integers n, it suffices to show that $5 \cdot 2^n - 1$ is divisible by 3 for all odd positive integers n. But:

$$5 \cdot 2^n - 1 = 3 \cdot 2^n + 2 \cdot 2^n - 1 = 3 \cdot 2^n + 2^{n+1} - 1.$$

Hence it suffices to show that $2^{n+1} - 1$ is divisible by 3 for all odd positive integers n. But this is easily seen to be true, for if n is odd, then $n + 1$ is even, and we have already noted earlier that if m is even, then $2^m - 1$ is divisible by 3.

Traversing the chain of reasoning in the reverse direction, we see that we have shown that $2^{n-1}\left(2^n - 1\right)$ leaves remainder 1 under division by 9 for all odd n. □

Second proof. Noting that $4^n - 2^n - 2$ is of the form $x^2 - x - 2$ (with the substitution $x = 2^n$), and this polynomial factorizes conveniently as $x^2 - x - 2 = (x-2)(x+1)$, we get:

$$4^n - 2^n - 2 = \left(2^n - 2\right)\left(2^n + 1\right).$$

Since n is an odd positive integer, $n - 1$ is an even nonnegative integer; therefore $2^{n-1} - 1$ is a multiple of 3, say $2^{n-1} - 1 = 3a$ where a is an integer. Hence $2^{n-1} = 3a + 1$, and so

$$2^n = 6a + 2 = 3b + 2$$

where b is another integer ($b = 2a$). From this we get $2^n - 2 = 3b$ and $2^n + 1 = 3b + 3$. So both $2^n - 2$ and $2^n + 1$ are multiples of 3, implying that their product is a multiple of 9. Therefore $4^n - 2^n - 2$ is a multiple of 9. □

References

1. Marin Mersenne, https://en.wikipedia.org/wiki/Marin_Mersenne

The COMMUNITY MATHEMATICS CENTRE (CoMaC) is an outreach arm of Rishi Valley Education Centre (AP) and Sahyadri School (KFI). It holds workshops in the teaching of mathematics and undertakes preparation of teaching materials for State Governments and NGOs. CoMaC may be contacted at shailesh.shirali@gmail.com.