PERFECT NUMBERS

Dr. Satyam Sharanam

Guest Faculty

Department of Mathematics

Sabour College, Sabour

T.M. Bhagalpur University, Bhagalpur

Introduction

A number which is equal to the sum of its divisors other than itself is known as a perfect number. For example $p_1 = 6$ is a prefect number because its divisors are 1, 2 and 3 whose sum (1 + 2 + 3) is equal to the number (6) itself. Likewise the second perfect number is $p_2 = 28$ with its divisors 1, 2, 4, 7 and 14. The third and fourth perfect numbers are $p_3 = 496,\ p_4 = 8128.$

For any positive integer n we denote by $\sigma(n)$ the sum of all its positive divisors including 1 and *n*. From this we have the definition that a natural number n is perfect iff $\sigma(n) = 2n.$

The early Greeks conjectured that the perfect numbers end alternately in 6 or 8. This was proved to be false, since the fifth perfect number is $p_5 = 33{,}550{,}336$ which ends in 6, where as the sixth perfect number p_6 = $8{,}589{,}869{,}056$ also ends in 6. The Greeks also believed that first perfect number is of 1 digit, the second one of two digits, the third one of three digits *etc*. But this was also found to be false. In fact, there are no perfect numbers of 5, 6 or 7 digits. There are many solved and unsolved problems related to perfect numbers such as

Conjecture (1) : There are infinitely many perfect numbers.

Open Question : There are no odd perfect numbers. These have not yet been proved or disproved.

Theorem 1: Every perfect number ends in a 6 or in an 8.

Before discussing these problems, we describe the known facts and propositions most of which are given in usual texts on number theory. The proofs are also outlined for sake of completeness, whenever necessary.

Euclid and others :

Euclid made a great contributions to the problem of finding prefect numbers. In the infancy of science the speculation on such perfect numbers enjoyed a certain amount of popularity, which is evidenced by the fact in Euclid's Elements a rule is given for obtaining even perfect, numbers. Euclid's rule amounts to the statement that

Theorem 2. The number $2^{p-1}(2^p-1)$ is a perfect number if 2^p-1 is a prime.

Proof : The divisors of $\{2^{p-1}(2^p-1)\}$ are

$$1, 2, 2^2, ..., 2^{p-1},$$
$$2^p-1, 2(2^p-1), 2^2(2^p-1), ..., 2^{p-2}\left(2^p-1\right)$$

and their sum is

$$1+2+2^2+...+2^{p-1}+(2^p-1)(1+2+...+2^{p-2})$$
$$= \quad 2^p-1+(2^p-1)(2^{p-1}-1)$$
$$= \quad 2^{p-1}(2^p-1)$$

Here we have to show that all even perfect number are necessarily of Euclid's type. This problem amounts to finding for what even n the following equation holds $\sigma(n)=2n.$

Since *n* is supposed to be even, we can set

$$n=2^{p-1}m \quad p>1$$

Where m is odd. Then, since

$$\sigma(n)=(2^p-1)\sigma(m),$$

The condition of the problem is

$$(2^p-1)\sigma(m)=2^p m.$$

Now 2^P and 2^P-1 are relatively prime numbers;

Consequently *m* = $(2^p-1)r$

$\sigma(m)=2^p r$ where *r* is a certain integer. Numbers *r* and *m* are two distinct divisors of *m* and their sum

$$r+(2^p-1)r=2^p r$$

makes up already what should be the sum of all divisors of *m*. Consequently *m* has only two divisors; that is, *m* is prime, which is possible only when *r* = 1 and 2^p-1 is prime. Thus an even perfect number must be of the form $2^{p-1}(2^p-1)$.

Euclid, recognizing that this needed a proof, gave some fundamental underlying theorems and fundamental algorithm, which we shall describe later. We begin with some definitions:

Definitions proper divisor : A divisor of a number other then itself is said to be proper divisor.

Common divisors :

A number which divides several integers is said to be their "common divisor". For example, 2 is a common divisor of 20, 40, 80, 100 also 4 and 5 are such divisors.

Greatest common divisors:

Among the common divisors of a set of numbers, there is one which is the greatest and is called greatest common divisor. If d is the g.c.d of a, b we write $(a, b) = d$. The *g.c.d.* has the following obvious properties.

(I) $(a, b) = (b, a)$ (Commutative Law)

(II) $a(b, c) = \{(a, b)c\}$ (Associative Law)

(III) $(ac, bc) = c(a, b)$ (Distributive Law)

(IV) $(a, 1) = (1, a) : (a, 0) = (0, a) = | a |$

Prime Number

The integers which are divisible by 1 and itself, is called prime number.

Example- 1,3,5,7,11…………………..

Composite Number

An integer which is not prime is called composite Number.

Example- 2,4,6,8……………………..

Relatively prime or co–prime:

Two numbers a and b are called co–prime or relatively prime if their g.c.d is 1 In such a case we write $(a, b) = 1$. Thus, 10, 21 are relatively prime and we write $(10, 21) = 1$, since g.c.d of 10 and 21 is 1.

Division Algorithm : Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying a

$$a = qb + r \qquad 0 \le x < b$$

The integers q and r are called, respectively, the quotient and reminder in the division of a by b.

The result is true for any integer $b \neq 0$ provided b is replaced by $| b |$.

In the above q and r are unique. To see this, suppose that

$$a = qb + r \quad 0 \le r < |b|$$

and

$$a = q'b + r' \quad 0 \le r' < |b|$$

On subtraction we have

$$b(q - q') + r - r' = 0$$

This implies $r' - r = b(q - q')$ whence *b* divides $r' - r$. But r' and *r* are numerically less than *b*. Hence $r = r'$ and then $q = q'$ (since $b \neq 0$).

The above result is due to Euclid. We rewrite this result as

Theorem 3. (Euclid's Theorem) :

If *a* and *b* are integers with $b \neq 0$, then exist unique integers *q* and *r* such that

$$a = bq + r \qquad 0 \leq r < |b|$$

Euclid's algorithm:

The Euclidean algorithm may be described as follows : We apply the division algorithm to *a* and *b* to get

$$a = bq_1 + r_1 \text{ where } 0 \leq r_1 < b$$

If $r_1 > 0$ there exist q_2 and r_2 such that

$$b = r_1 q_2 + r_2 \text{ where } 0 \leq r_2 < r_1$$

If $r_2 > 0$, there exist q_3 and r_3 such that

$$r_1 = r_2 q_3 + r_3 \text{ where } 0 \leq r_3 \leq r_2$$

This process may be continued as long as the remainder r_1 does not vanish, which must happen after a finite number of stepts, since a decreasing sequence of numbers cannot continue indefinitely. Therefore we shall obtain an r_n that is zero.

Thus the last step in the above process

$$r_{n-2} = r_{n-1} q_n + 0, r_n = 0$$

Now each $r_i, (1 \leq i \leq n-1)$ is positive so that $r_{n-1} > 0$. Proceeding from bottom to top we see that r_{n-1} divides $r_{n-2}, r_{n-3}, \ldots, r_{2,} r_1,$ *b* and *a*. Proceeding from top to bottom we see that it divides both *a* and *b*. It divides $r_1, r_2, \ldots r_{n-2}$ and r_{n-1}. Then since r_{n-1} divides each of *a*, *b* and conversely, since any common divisor of *a* and *b* divides r_{n-1} it follows that r_{n-1} is the *g*, *c*, *d* of *a*, *b*.

It must be remarked that Euclidean algorithm is simple and efficient.

Theorem 4 (Euclid) : If *d* = (*a*, *b*) there is a linear combination of *a* and *b* with integer coefficients *x* and *y* such that

$$d = ax + by$$

Proof : By taking the steps of the Euclid's algorithm and using the principle of mathematical induction, we shall first establish that there exist integers x_i and y_i such that

$$ax_i + by_i = r_i \tag{1}$$

for $i = 1, 2, 3, ..., n-1$

When $i = 1,$ let $x_i = 1$ and $y_i = -q_i$

Now assume that integer solutions of (1) have been found for all *i* less than or equal to *k*. we know that

$$r_{k-1} = r_k q_{k-1} + r_{k+1} \qquad (2)$$

Now, by induction

$$(ax_{k-1} + by_{k-1}) - (ax_k + by_k)q_{k+1} = r_{k+1} \qquad (3)$$

This can be written as

$$(x_{x-1} - x_k q_{k+1})a + (y_{k+1} - y_k a_{k+1})b = r_{k+1} \qquad (4)$$

Hence $x_{k+1} = x_{k-1} - x_k q_{k+1}$ and $y_{k+1} = y_{k-1} - y_k q_{k+1}$ are solutions of equation (1) when *i* = *k* + 1. The equation (1) is established for *i* = 1, 2, 3, …, $n-1$, by the mathematical induction. In particular if $i = n-1$ then we have

$$ax_{n-1} + by_{n-1} = r_{n-1} = g.c.d\,(a, b).$$

Corollary (1) : In order that there exist integers *x* and *y* satisfying the equation

$$ax + by = c \qquad (5)$$

it is necessary and sufficient that $d \mid c$ where $d = (a,b)$.

Proof : Let *a* = *ed* and *b* = *fd*, then we have

$$c = edx + fdy = d(ex + fy)$$

Thus $d \mid c$

On the other hand if $d \mid c$, let *kd* = *c*. Then by equation (5) there exist *x*' and *y*' such that

$$ax' + by' = d$$

Hence $a(x'k) + b(y'k) = dk = c$

Writing $x'k = x$ and $y'k = y$

The result follows

Corollary (2) : If (*a*, *c*) = (*b*, *c*) = 1 then (*ab*, *c*) = 1

Proof : Since (*a*, *c*) = 1 we have

$$ax_1 + cy_1 = 1 \qquad (6)$$

Similarly

$$bx_2 + cy_2 = 1 \qquad (7)$$

Multiplying the equations (6) and (7) we have

$$abX + cY = 1$$

Where $X = x_1, x_2, Y = x_1 y_2 a + x_2 y_1 b + y_1 y_2 c$

Then any common divisor of *ab* and *c* must divide 1, and therefore (*ab*, *c*) = 1.

Remark : By the theorem (4) we know that if (*a*, *b*) = 1 then *ax* + *by* = 1 for some integers *x* and *y*. this finds application in the solution of the Diophantine equation $ax + by = c$. A Diophantine equation is one which is to be solved in integers, and is so named in honour of the Greek mathematician Diophantas who lived in Alexondria about 250 A.D.

We now prove

Theorem 5 (Euclid) : If *a* and *b* are integers, *p* is a prime, *p/ab* and *p*†*a* then $p \mid b$

Proof : If *p*†*a* then $(a, p) = 1.$

Hence $p \mid b$

Corollary (3) : If $p \mid a_1 \, a_2 ... a_n,$ then there exists some *i* such that $p \mid a_i$

Proof : We proceed by mathematical induction. This assertion is true for $n = 1$. We assume that the assertion is true for n less than or equal to k. Then for $n = k + 1$ we have the relation

$$p \mid (a_1 a_2 ... a_k) a_{k+1}$$

Now either $p \mid a_{k+1} \; or \; p \mid a_1 a_2 ... a_k$

In the latter case $p \mid a_i$ for some $i (1 \le i \le k)$, by the induction hypothesis.

Corollary (4) : If $p, q_1, q_2, ..., q_n$ are all prime

and $p \mid q_1 q_2 ... q_n$ then $p = q_k$ for some *k* where $1 \le k \le n.$

Proof: we know that if then $p \mid q_1 q_2 ... q_n$ then $p \mid q_k$ for some *k* with $1 \le k \le n.$ Being a prime, q_k is not divisible by any positive integer other than 1 and itself. Since *p* > 1 we conclude that $p = q_k$

References :

1. Jr. Peter Magis and W.L. Mc Daniel: A new result concerning the structure of odd perfect numbers, proc, Amer. Math 506; vol. 32, No.1 (1972).
2. H. Griffin: Elementary theory of numbers, McGraw–Hill Book Company, Inc, New York (1954).
3. H. Griffin: Elementary theory of numbers Mc Grow-Hill Book Company, inc, New York (1954)
4. J.V. Uspensky and M.A. Healslet: Elementary Number theory Mc Grow-Hill Book, Company, Inc. New York and London (1939)