Section 8

Perfect Numbers

Week 5

We now turn to the fascinating topic of perfect numbers.

A positive integer is said to be **perfect** if and only if it is equal to the sum of its positive divisors excluding itself.

That is, n is **perfect** if $\sigma(n) - n = n$, or equivalently, $\sigma(n) = 2n$.

For example, $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$, and $\sigma(28) = \sigma(2^2)\sigma(7) = 7 \cdot 8 = 56 = 2 \cdot 28$. Perfect numbers were first studied by the Pythagoreans (about 500 BC); they knew of the following four even perfect numbers:

$$\mathrm{P}_1 = 6, \quad \mathrm{P}_2 = 28, \quad \mathrm{P}_3 = 496, \quad \mathrm{P}_4 = 8128.$$

On this evidence they conjectured that

(i) the n^{th} perfect number $\mathbf{P}_n$ contains exactly n digits,

(ii) the even perfect numbers end, alternately, in 6 and 8.

Both conjectures are wrong; there is no perfect number with 5 digits; the next perfect number is $\mathbf{P}_5 = 33,550,336$, and $\mathbf{P}_6 = 8,589,869,056$. Thus $\mathbf{P}_5$ and $\mathbf{P}_6$ are consecutive even perfect numbers ending in 6.

The problem of determining a general form for all perfect numbers dates back to almost the beginning of mathematical time. It was partially solved by Euclid, circa 350 BC, and then the Swiss mathematician Leonhard Euler (1707 – 1783) completed the proof of a beautiful theorem that allows us (in principle) to determine all even perfect numbers. But even today, after nearly *two and a half millennia*, we don't know whether there exist odd perfect numbers or not!

8.1 Euclid's Theorem

Euclid proved a sufficient condition for an integer to be perfect. To prove Euclid's result, recall that if f is a multiplicative function and $(m, n) = 1$, then $f(mn) = f(m)f(n)$. Also recall that σ is a multiplicative function.

Theorem 8.1 (Euclid) *If $2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is perfect.*

Proof.
Let $n = 2^{k-1}(2^k - 1)$. Since $2^k - 1$ is prime, $\sigma(2^k - 1) = 2^k - 1 + 1 = 2^k$. Also, 2^{k-1} is a prime power, so from (7.1),

$$\sigma(2^{k-1}) = 2^k - 1.$$

Now, σ is a multiplicative function and $(2^{k-1}, 2^k - 1) = 1$, hence

$$\sigma(n) = \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)(2^k) = 2n.$$

Thus n is perfect. ■

8.2 Euler's Theorem

About 2000 years after Euclid, Euler proved that all even perfect numbers are of the form given in Euclid's Theorem. Euler's result provides a necessary condition for an even number to be perfect.

Theorem 8.2 (Euler) *If n is an even perfect number, then $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are both prime.*

Concentrate! The proof is cunning!

Proof.
Since n is even, we can write

$$n = 2^e m, \quad \text{where } m \text{ is odd and } e \geq 1. \tag{8.1}$$

We know that $\sigma(2^e) = 2^{e+1} - 1 \neq 2 \cdot 2^e$, so $n \neq 2^e$; that is, $m > 1$.
Since $\sigma(m) \geq 1 + m > m$, we can write

$$\sigma(m) = m + s, \quad \text{where } s > 0. \tag{8.2}$$

Since n is perfect, $2n = \sigma(n)$, so from (8.1),

$$2n = 2^{e+1}m = \sigma(n). \tag{8.3}$$

This is one expression for $\sigma(n)$.

From (8.1) and the multiplicativity of σ,

$$\sigma(n) = \sigma(2^e m) = \sigma(2^e)\sigma(m). \tag{8.4}$$

But $\sigma(2^e) = 2^{e+1} - 1$, thus also using (8.2), (8.4) becomes

$$\sigma(n) = (2^{e+1} - 1)(m + s) = 2^{e+1}m - m + (2^{e+1} - 1)s. \tag{8.5}$$

This is another expression for $\sigma(n)$.

Combining (8.3) and (8.5) gives

$$\begin{aligned} 2^{e+1}m &= 2^{e+1}m - m + (2^{e+1} - 1)s, \\ \text{i.e.} \qquad m &= (2^{e+1} - 1)s. \end{aligned} \tag{8.6}$$

★ This means that $s|m$, and since $e \geq 1$, $2^{e+1} - 1 > 1$ and thus $s < m$.

Now look at (8.2): The sum of all divisors of m is equal to $m + s$. Thus the sum of all divisors of m, excluding m, that is,

♠ the sum of all divisors of m less than m, is equal to s.

From ★, s is a divisor of m and s is less than m, so s is a term of the sum in ♠.

But if s is a term in a sum which sums to s, then s is the **only** term in that sum.

Hence s is the only divisor of m that is less than m, and this is only possible if $s = 1$ because $1|m$ always.

Therefore m is prime, and substituting $s = 1$ in (8.6) we get $m = 2^{e+1} - 1$. The only numbers of this form that can be prime are those in which $e + 1$ is prime, as you had to prove in Assignment 1. Hence $e + 1 = p$, where p is prime, so $n = 2^{p-1}(2^p - 1)$ for some prime p. ■

The results of Euclid and Euler can be combined to provide a characterization of even perfect numbers, that is, a necessary and sufficient condition (or “if and only if” type condition) for an even number to be perfect:

Theorem 8.3 *An even number n is perfect if and only if*

$$n = 2^{p-1}(2^p - 1),$$

where $2^p - 1$ is prime. [If $2^p - 1$ is prime, then p is also prime – Assignment 1.]

8.3 Mersenne Primes

When $2^p - 1$ is prime, it is called a **Mersenne prime**, named after the French monk Marin Mersenne. Let $\mathbf{M}_i$ denote the i'th Mersenne prime, and let $\mathbf{P}_i$ denote the corresponding even perfect number. The first six Mersenne primes and even perfect numbers are given in Table 8.1.

i	prime p	M_i	P_i
1	2	3	$2^1(2^2-1)=6$
2	3	7	$2^2(2^3-1)=28$
3	5	31	$2^4(2^5-1)=496$
4	7	127	$2^6(2^7-1)=8128$
5	13	8191	$2^{12}(2^{13}-1)=33,550,336$
6	17	131,071	$2^{16}(2^{17}-1)=8,589,869,056$

Table 8.1: The first six Mersenne primes and even perfect numbers

The first 47 Mersenne primes and hence the first 47 even perfect numbers are known. Four more Mersenne primes are known, but it is not known whether they are the 48th, 49th, 50th and 51st Mersenne primes because not all candidates inbetween have been eliminated. The first Mersenne prime with over 10 million digits, $\mathbf{M}_{46} = 2^{43,112,609} - 1$, which has 12,978,189 digits and was discovered in 2009, netted the discoverers the *Electronic Frontier Foundation* $\$100,000$ award for the discovery of the first prime with 10 million or more digits. The largest Mersenne prime, which is possibly $\mathbf{M}_{51}$, was discovered on December 7, 2018, and has 24,862,048 decimal digits. When written out, a standard word processor layout (50 lines per page, 75 digits per line) would require 6,629 pages to display it.

Also see http://primes.utm.edu/mersenne/ and http://www.mersenne.org/.

8.4 Last Digits of Perfect Numbers

From $\mathbf{P}_5$ and $\mathbf{P}_6$ we see that it is not true that even perfect numbers end *alternately* in 6 and 8. However, it is true that every even perfect number ends in either 6 or 8, as is proved in the next theorem.

Theorem 8.4 *Any even perfect number n ends in the digit 6 or 8; that is, either $n \equiv 6 \pmod{10}$ or $n \equiv 8 \pmod{10}$.*

Proof.
By Theorem 8.3, $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is prime. Determining the last digit of n is equivalent to determining the least residue of $n \pmod{10}$. Note that $2^p - 1$ is odd and $2^p - 1 \neq 5$ as there is no integer p such that $2^p = 6$. Therefore the only possible least residues of the odd prime $2^p - 1$, modulo 10, are 1, 3, 7 or 9. [If $2^p - 1 \neq 5$ and $2^p - 1 \equiv 5 \pmod{10}$, then 5 is a proper divisor of $2^p - 1$, which is impossible.]

- If $2^p - 1 \equiv 1 \pmod{10}$, then $2^p \equiv 2 \pmod{10}$ and so, since $p > 1$, $2^{p-1} \equiv 1 \pmod{5}$. This means that $2^{p-1} \equiv 1$ or $6 \pmod{10}$, and obviously the even number 2^{p-1} is not congruent to $1 \pmod{10}$. So $2^{p-1} \equiv 6 \pmod{10}$, from which we get

$$n = 2^{p-1}(2^p - 1) \equiv 6 \cdot 1 \equiv 6 \pmod{10}.$$

- If $2^p - 1 \equiv 7 \pmod{10}$, then $2^p \equiv 8 \pmod{10}$ and so $2^{p-1} \equiv 4 \pmod{5}$. Then $2^{p-1} \equiv 4$ or $9 \pmod{10}$. But the latter case is impossible because 2^{p-1} is even, thus $2^{p-1} \equiv 4 \pmod{10}$. Hence

$$n \equiv 2^{p-1}(2^p - 1) \equiv 4 \cdot 7 \equiv 8 \pmod{10}.$$

- The case $2^p - 1 \equiv 3 \pmod{10}$ is similar.
- If $2^p - 1 \equiv 9 \pmod{10}$, then $2^p \equiv 0 \pmod{10}$ and so $10 | 2^p$. But then $5 | 2^p$, which is impossible since the only prime divisor of 2^p is 2.

Therefore every even perfect number has a last digit equal to 6 or 8. ■

8.5 Other Special Types of Numbers

- The numbers m and n are called an **amicable pair** if and only if $\sigma(m) - m = n$ and $\sigma(n) - n = m$.
- An integer n is called **abundant** if and only if $\sigma(n) - n > n$,
- **deficient** if and only if $\sigma(n) - n < n$, and
- **triangular** if and only if $n = m(m + 1)/2$ for some integer m.

Section 9

Euler's Generalization of Fermat's Theorem

Fermat's Theorem (Theorem 6.1) states that if p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

The purpose of this section is to find out what happens if we use a composite integer m instead of p.

$\boxed{?}$ Is there also some number $f(m)$ such that $a^{f(m)} \equiv 1 \pmod{m}$?

Note that this is impossible if $(a, m) = d > 1$, because then the congruence $a^k \equiv 1 \pmod{m}$ has no solution for any k, as $d \nmid 1$. Consider the tables of powers of $a \pmod{m}$, where $(a, m) = 1$, for $m = 6$, 9 and 10:

$m = 6$	
a	a^2
1	1
5	1

$m = 9$					
a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	$8 \equiv -1$	7	5	1
4	7	1	4	7	1
5	7	$8 \equiv -1$	4	2	1
7	4	1	7	4	1
8	1	$8 \equiv -1$	1	8	1

$m = 10$			
a	a^2	a^3	a^4
1	1	1	1
3	$9 \equiv -1$	7	1
7	$9 \equiv -1$	3	1
9	1	9	1

Evidently,

$$\begin{aligned} a^2 &\equiv 1 \pmod{6} \quad \text{if} \quad (a, 6) = 1, \\ a^6 &\equiv 1 \pmod{9} \quad \text{if} \quad (a, 9) = 1, \\ a^4 &\equiv 1 \pmod{10} \quad \text{if} \quad (a, 10) = 1. \end{aligned}$$

The exponent in each case is equal to the number of positive integers less than m and relatively prime to m.

- For m a positive integer, let $\phi(m)$ denote the number of positive integers less than m and relatively prime to m. We call ϕ **Euler's phi function.**

If p is prime, then $\phi(p) = p - 1$. Thus the following theorem is a generalization of Fermat's Theorem.

Theorem 9.1 (Euler's Theorem) *Suppose that $m \geq 1$ and $(a, m) = 1$. Then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

We require two lemmas to prove Euler's Theorem.

Lemma 9.1 (a) *If $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$.*

Proof.
If $a \equiv b \pmod{m}$, then $a = km + b$ for some integer k, and so by Lemma 1.3, $(a, m) = (b, m) = 1$. ■

Consider the positive integers r_1, r_2, ..., $r_{\phi(9)}$ less than 9 and relative prime to 9, namely 1, 2, 4, 5, 7, 8. Choose a to be any integer relatively prime to 9, say $a = 5$. Then

$$\begin{aligned}
a \cdot 1 &\equiv 5 \pmod{9} \\
a \cdot 2 &\equiv 10 \equiv 1 \pmod{9} \\
a \cdot 4 &\equiv 20 \equiv 2 \pmod{9} \\
a \cdot 5 &\equiv 25 \equiv 7 \pmod{9} \\
a \cdot 7 &\equiv 35 \equiv 8 \pmod{9} \\
a \cdot 8 &\equiv 40 \equiv 4 \pmod{9}.
\end{aligned}$$

Note that for each $i = 1, 2, ..., \phi(9)$, $a \cdot r_i \equiv r_j \pmod{9}$ for some j. This is always the case, as proved in the following lemma.

Lemma 9.1 (b) *If $(a, m) = 1$ and r_1, r_2, ..., $r_{\phi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues $\pmod{m}$ of*

$$ar_1, ar_2, ..., ar_{\phi(m)} \tag{9.1}$$

are a permutation of

$$r_1, r_2, ..., r_{\phi(m)}. \tag{9.2}$$

Proof.
Since there are exactly $\phi(m)$ numbers in (9.1), to prove that their least residues are a permutation of the $\phi(m)$ numbers in (9.2), we must show that the least residues are all different and that the numbers in (9.1) are all relatively prime to m.

Their least residues are all different: Suppose

$$ar_i \equiv ar_j \pmod{m}$$

for some i and j with

$$1 \leq i, j \leq \phi(m) < m. \tag{9.3}$$

Since $(a, m) = 1$, we can cancel a from both sides to get

$$r_i \equiv r_j \pmod{m}.$$

By (9.3) r_i and r_j are least residues $\pmod{m}$, therefore $r_i = r_j$. Thus if $r_i \neq r_j$, then $ar_i \not\equiv ar_j \pmod{m}$ and so the numbers in (9.1) have different least residues.

The least residues of the numbers in (9.1) are all relatively prime to m: Suppose p is a prime common divisor of ar_i and m for some i. Since p is prime,

$$p|a \text{ or } p|r_i.$$

Thus p is a common divisor of a and m, or p is a common divisor of r_i and m. But $(a, m) = 1$ and $(r_i, m) = 1$ (given), so both cases are impossible. Hence $(ar_i, m) = 1$ for each $i = 1, 2, ..., \phi(m)$. By Lemma 9.1(a) their least residues are relatively prime to m. ■

The proof of Euler's Theorem now follows similar to the proof of Fermat's Theorem.

Proof of Euler's Theorem.
From Lemma 9(b) we know that

$$r_1 r_2 ... r_{\phi(m)} \equiv (ar_1)(ar_2)...(ar_{\phi(m)}) \equiv a^{\phi(m)} r_1 r_2 ... r_{\phi(m)} \pmod{m}.$$

Since $r_1, r_2, ..., r_{\phi(m)}$ are relatively prime to m, so is their product. Hence we may cancel to get

$$1 \equiv a^{\phi(m)} \pmod{m}.$$ ■

Example: What is the least residue of $5^{25} \pmod{8}$?

Solution

The integers less than 8 and relatively prime to 8 are 1,3,5,7, so $\phi(8) = 4$. Hence

$$5^{25} \equiv 5 \cdot 5^{4 \cdot 6} \equiv 5 \pmod{8}.$$

The proof of the next corollary to Euler's Theorem is similar to the proof of Corollary 6.2.

Corollary 9.1 *If* $(a, m) = 1$ *and* $t \equiv r \pmod{\phi(m)}$, *then* $a^t \equiv a^r \pmod{m}$.

9.1 Euler's Phi Function

Now we want to determine $\phi(n)$ without listing the integers less than n and relatively prime to n. This will be easy if we can prove that ϕ is multiplicative, and if we can determine $\phi(p^n)$ for a prime number p, without listing them all.

Let $\Phi(n)$ denote the set of least residues of n that are relatively prime to n.

Example: We know, by listing the numbers in $\Phi(27)$, that $\phi(3^3) = 18$. Another way of determining this is to determine $n - |\Phi(n)|$, that is, to count the numbers less than or equal to 27 that are not relatively prime to 27, namely all the multiples of 3:

$$\underline{1} \cdot 3,\ \underline{2} \cdot 3,\ \underline{3} \cdot 3,\ \ldots,\ \underline{9} \cdot 3,$$

a list of $9 = 3^2$ numbers. Hence there are $27 - 9 = 18$ numbers less than (or equal to) 27 that are relatively prime to 27.

Lemma 9.2 *If* p *is prime, then* $\phi(p^n) = p^{n-1}(p-1)$ *for all* $n \in \mathbb{N}$.

Proof.
The positive integers less than or equal to p^n which are not relatively prime to p^n are precisely the multiples of p:

$$1 \cdot p,\ 2 \cdot p,\ \ldots,\ p^{n-1} \cdot p,$$

and there are exactly p^{n-1} of them. Since there are, in total, p^n positive integers less than or equal to p^n, we have

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

■

Corollary to Lemma 9.1(a) *If the least residues* $\pmod{m}$ *of*

$$r_1, r_2, \ldots, r_m$$

are a permutation of $0, 1, \ldots, m-1$, *then they contain exactly* $\phi(m)$ *elements relatively prime to* m.

To prove that ϕ is multiplicative, we must prove that if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Example: Let $m = 4$, $n = 9$, so $mn = 36$. Arrange the integers from 1 to 36 as follows:

$$\overleftrightarrow{\quad\quad n \quad\quad}$$

m	$\boxed{\mathbf{1}}$	$\boxed{\mathbf{5}}$	**9**	$\boxed{\mathbf{13}}$	$\boxed{\mathbf{17}}$	**21**	$\boxed{\mathbf{25}}$	$\boxed{\mathbf{29}}$	**33**
	2	*6*	*10*	*14*	*18*	*22*	*26*	*30*	*34*
	3	$\boxed{\mathbf{7}}$	$\boxed{\mathbf{11}}$	**15**	$\boxed{\mathbf{19}}$	$\boxed{\mathbf{23}}$	**27**	$\boxed{\mathbf{31}}$	$\boxed{\mathbf{35}}$
	4	*8*	*12*	*16*	*20*	*24*	*28*	*32*	*36*

Table 9.1: Integers relatively prime to 36

In the first column, the integers 2 and 4 are not relatively prime to 4, and *none* of the integers in the same rows as 2 and 4 is relatively prime to 36. The integers 1 and 3 are relatively prime to 4, and *some* of the integers in the same rows as 1 and 3 are relatively prime to 36: those in boldface. How many of those are there in each row? Exactly $\phi(9) = 6$. Hence there are $\phi(4)\phi(9) = 12$ integers less than 36 that are relatively prime to 36. This pattern will always occur (if $(m, n) = 1$), and the proof that ϕ is multiplicative depends on this fact.

Theorem 9.2 *ϕ is multiplicative.*

Proof.
Suppose $(m, n) = 1$. We want to prove that $\phi(mn) = \phi(m)\phi(n)$.
Write the numbers $1, 2, ..., mn$ as follows:

$$\begin{array}{ccccccc} 1 & m+1 & 2m+1 & & \cdots & & (n-1)m+1 \\ 2 & m+2 & 2m+2 & & \cdots & & (n-1)m+2 \\ \vdots & \vdots & \vdots & & \cdots & & \vdots \\ r & m+r & 2m+r & \cdots & km+r & \cdots & (n-1)m+r \\ \vdots & \vdots & \vdots & & \cdots & & \vdots \\ m & 2m & 3m & & \cdots & & mn \end{array} . \tag{9.4}$$

Suppose that for some $r \in \{1, 2, ..., m\}$, $(m, r) = d > 1$.

- Then no element in the r^{th} row of (9.4) is relatively prime to mn, because we have $d|m$, $d|r$, and therefore $d|mn$ and $d|(km + r)$ for any integer k.

So if we are looking for integers that are relatively prime to mn, we will not find any except in rows whose first element is relatively prime to m.

- There are $\phi(m)$ such rows.
- If we can show that each of these $\phi(m)$ rows contains $\phi(n)$ elements relatively prime to mn, then we will have shown that (9.4) contains $\phi(m)\phi(n)$ integers relatively prime to mn, that is, that $\phi(mn) = \phi(m)\phi(n)$.

Hence suppose $(r, m) = 1$. The r^{th} row of (9.4) is

$$r \quad m+r \quad 2m+r \quad \cdots \quad km+r \quad \cdots \quad (n-1)m+r \ . \tag{9.5}$$

- We now show that the least residues of the numbers in (9.5) are a permutation of

$$0, 1, 2, ..., n-1. \tag{9.6}$$

To do this, all we have to show is that no two numbers in (9.5) are congruent (mod n), because (9.5) and (9.6) both contain n elements. Suppose

$$km + r \equiv jm + r \pmod{n},$$

where $0 \leq k < n$, $0 \leq j < n$. Then

$$km \equiv jm \pmod{n}$$

and since $(m, n) = 1$, we may cancel m to get $k \equiv j \pmod{m}$. But k and j are both least residues (mod n), so $k = j$ and therefore $km + r = jm + r$.

Thus the least residues of the numbers in (9.5) are a permutation of the numbers in (9.6).

Therefore the numbers in (9.5) contain as many numbers relatively prime to n as (9.6) does, namely $\phi(n)$.

These $\phi(n)$ numbers are precisely the numbers in (9.5) that are relatively prime to mn:

Since r is relatively prime to m, and all the numbers in (9.5) are congruent to r (mod m), it follows that **all** numbers in (9.5) are relatively prime to m.

Hence (9.5) contains exactly $\phi(n)$ numbers relatively prime to mn, which is what we wanted to show. ■

The next result now follows easily.

Theorem 9.3 *If n has prime-power decomposition*

$$n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k},$$

then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1)...p_k^{e_k-1}(p_k - 1).$$

This formula can also be written as

$$\phi(n) = p_1^{e_1}\left(\frac{p_1-1}{p_1}\right)p_2^{e_2}\left(\frac{p_2-1}{p_2}\right)...p_k^{e_k}\left(\frac{p_k-1}{p_k}\right)$$

$$= n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)...\left(\frac{p_k-1}{p_k}\right).$$

Example

Find the least residue of $19^{26} \pmod{36}$.

Since $36 = 2^2 3^2$, $\phi(36) = 36 \times \frac{1}{2} \times \frac{2}{3} = 12$. Since $26 \equiv 2 \pmod{12}$,

$$19^{26} \equiv 19^2 \equiv 1 \pmod{36}.$$