Section 6

Fermat's and Wilson's Theorems

Week 4

Watch out! The work is getting more difficult now.

The aim in this section is to prove two beautiful theorems in number theory, Fermat's Theorem and Wilson's Theorem.

Pierre de Fermat (1601 – 1665) was a lawyer at the provincial parliament in Toulouse, France, and an amateur mathematician. He published almost none of his many mathematical discoveries, but did correspond with other mathematicians about them. Some of his discoveries came to us only because he made notes in the margins of his copy of the work of Diophantus. His son found his copy with the notes and published them so that other mathematicians would be aware of (and be driven crazy by) Fermat's results and claims – more about this later.

John Wilson was a student of the English mathematician Edward Waring, who stated in 1770 that Wilson had discovered a result, now known as "Wilson's Theorem" below. Waring also stated that neither he nor Wilson could prove the result. It was proved in 1771 by Joseph Lagrange, but is nevertheless known as "Wilson's Theorem".

6.1 Fermat's Theorem

Consider the least residue of $a^{10} \pmod{11}$ for $a \neq 0$ a least residue (mod 11):

$$\begin{aligned}
&1^{10} \equiv 1 \pmod{11} \\
&2^{10} \equiv (2^5)^2 \equiv (32)^2 \equiv (-1)^2 \equiv 1 \pmod{11} \\
&3^{10} \equiv (3^2)^5 \equiv (9)^5 \equiv (-2)^5 \equiv -32 \equiv 1 \pmod{11} \\
&4^{10} \equiv (2^{10})^2 \equiv 1 \pmod{11}
\end{aligned}$$

$$\begin{aligned}5^{10} &\equiv (5^2)^5 \equiv 3^5 \equiv 3 \cdot (3^2)^2 \equiv 3 \cdot (-2)^2 \equiv 12 \equiv 1 \pmod{11}\\ 6^{10} &\equiv (-5)^{10} \equiv 5^{10} \equiv 1 \pmod{11}\\ 7^{10} &\equiv (-4)^{10} \equiv 1 \pmod{11},\end{aligned}$$

and so on. This is not a coincidence, but Fermat's Theorem. First a lemma:

Lemma 6.1 *If* $(a, m) = 1$*, then the least residues of*

$$a,\ 2a,\ 3a,\ ...,\ (m-1)a \pmod{m} \tag{6.1}$$

are

$$1,\ 2,\ 3,\ ...,\ m-1 \tag{6.2}$$

in some order.

Proof.
There are $m-1$ numbers in (6.1), none congruent to 0 $\pmod{m}$ because $(a, m) = 1$. Hence each number in (6.1) is congruent, modulo m, to one of the numbers in (6.2).

- We show that no two numbers in (6.1) are congruent $\pmod{m}$; it will follow that their least residues are all distinct, and hence are a permutation of $1, 2, ..., m-1$.

Suppose two of the integers in (6.1) are congruent $\pmod{m}$, that is, suppose

$$ra \equiv sa \pmod{m}.$$

Because $(a, m) = 1$, we may cancel a (Theorem 4.4) and get

$$r \equiv s \pmod{m}.$$

But r and s are least residues $\pmod{m}$ (they range from 1 to $m-1$) and so (using the same argument as in the proof of Lemma 5.3, which I told you to remember – look it up now if you don't) $r = s$. ■

Theorem 6.1 (Fermat's Little Theorem) ***Important!*** *If p is prime and $(a, p) = 1$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof.
If $(a, p) = 1$, then by Lemma 6.1, the least residues $\pmod{p}$ of

$$a,\ 2a,\ ...,\ (p-1)a \tag{6.3}$$

are a permutation of

$$1,\ 2,\ ...,\ p-1. \tag{6.4}$$

Hence the product of the numbers in (6.3) is congruent $\pmod{p}$ to the product of the numbers in (6.4):

$$a \cdot 2a \cdot 3a \ \cdots \ (p-1)a \equiv 1 \cdot 2 \cdot 3 \ \cdots \ (p-1) \pmod{p},$$

that is,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}. \tag{6.5}$$

But p is prime, so each number in (6.4) is relatively prime to p, hence p and $(p-1)!$ are relatively prime. Therefore (6.5) is equivalent to

$$a^{p-1} \equiv 1 \pmod{p}$$

as required. ■

Corollary 6.1 *If p is prime, then for all a, $a^p \equiv a \pmod{p}$.*

Corollary 6.2 *If p is prime, $(a,p) = 1$, and t and r are nonnegative integers such that $t \equiv r \pmod{p-1}$, then $a^t \equiv a^r \pmod{p}$.*

Proof.
If $t \equiv r \pmod{p-1}$, then there exists an integer k such that $t = k(p-1)+r$. Hence

$$\begin{aligned} a^t &\equiv a^{k(p-1)+r} \equiv (a^{p-1})^k a^r \equiv 1^k a^r \pmod{p} \quad \text{(Fermat's Theorem)} \\ &\equiv a^r \pmod{p}. \end{aligned}$$

■

Example: Determine the least residues of (i) $3^{16} \pmod{17}$, (ii) $3^{50} \pmod{17}$, (iii) $3^{84} \pmod{85}$.

Solution

(i) Using Fermat's Theorem: 17 is prime and $17 \nmid 3$, hence $3^{16} \equiv 1 \pmod{17}$.

(ii) Since $50 \equiv 2 \pmod{16}$, $3^{50} \equiv 3^2 \equiv 9 \pmod{17}$ by Corollary 6.2.

(iii) Careful: $85 = 5 \cdot 17$ is not prime.

Watch this – you will see such an example again!

We use the Chinese Remainder Theorem:

The system

$$\begin{aligned} x &\equiv 3^{84} \pmod{5} \\ x &\equiv 3^{84} \pmod{17} \end{aligned}$$

has a unique solution (mod 85). Now:

$$\begin{aligned} & x \equiv 3^{84} \equiv 3^{16\cdot 5+4} \equiv 3^4 \equiv 3 \cdot 3^3 \equiv 3 \cdot 10 \equiv 13 \pmod{17}, \\ \text{i.e.} \quad & x = 17r + 13 \qquad \text{for some } r \in \mathbb{Z}. \end{aligned}$$

Substitute into the first congruence and reduce both sides:

$$17r + 13 \equiv \underline{2r+3} \equiv 3^{84} \equiv (3^4)^{21} \equiv \underline{1} \pmod{5},$$

so (from the underlined parts)

$$\begin{aligned} & 2r \equiv -2 \pmod{5}, \\ \text{i.e.} \quad & r \equiv -1 \equiv 4 \pmod{5}, \\ \text{i.e.} \quad & r = 5s + 4 \qquad \text{for some } s \in \mathbb{Z}. \end{aligned}$$

But then

$$x = 17r + 13 = 17(5s+4) + 13 = 85s + 81 \equiv 81 \pmod{85}.$$

The converse of Fermat's Theorem is not necessarily true.

Example: Show that $2^{340} \equiv 1 \pmod{341}$, but $341 = 11 \times 31$ is not prime.

Solution

$x \equiv 2^{340} \equiv (2^{10})^{34} \equiv 1 \pmod{11}$, hence $11|(x-1)$.
Also, $x \equiv 2^{30\cdot 11+10} \equiv 2^{10} \equiv (2^5)^2 \equiv 1 \pmod{31}$, hence $31|(x-1)$.
Since $(11, 31) = 1$, $11 \cdot 31|(x-1)$ and thus $x \equiv 1 \pmod{341}$.

- A **Fermat pseudoprime to a base a**, written psp(a), is an odd composite number n such that $a^{n-1} \equiv 1 \pmod{n}$, i.e., it satisfies Fermat's little theorem for the base a.
- A Fermat pseudoprime to the base 2, written psp(2), is also called a **Poulet number**. There are 21853 Poulet numbers less than 25×10^9.
- If base 3 is used in addition to base 2 to weed out potential composite numbers, only 4709 composite numbers less than 25×10^9 remain.

- Adding base 5 leaves 2552, and base 7 leaves only 1770 composite numbers, all of which are greater than 10,000.

The following table gives the first few Fermat pseudoprimes to some small bases a.

Base a	psp(a)
2	341, 561, 645, 1105, 1387, 1729, 1905, ...
3	91, 121, 286, 671, 703, 949, 1105, 1541, 1729, ...
4	15, 85, 91, 341, 435, 451, 561, 645, 703, ...
5	124, 217, 561, 781, 1541, 1729, 1891, ...

Table 6.1 Fermat pseudoprimes

Example: Show that $a^{560} \equiv 1 \pmod{561}$ for every integer a such that $(a, 561) = 1$.

Solution

- We cannot apply Fermat's Theorem to 561 because 561 is not prime: $561 = 3 \cdot 11 \cdot 17$.
- To show that $a^{560} \equiv 1 \pmod{561}$ whenever $(a, 561) = 1$, it is sufficient to show that $a^{560} \equiv 1$ (mod 3, 11 and 17), for then 3, 11 and 17 all divide $a^{560} - 1$, from which it follows that $561 = 3 \cdot 11 \cdot 17$ divides $a^{560} - 1$, that is, $a^{560} \equiv 1 \pmod{561}$.
- If $(a, 561) = 1$, then $(a, 3) = (a, 11) = (a, 17) = 1$, so we may apply Fermat's Theorem to 3, 11 and 17:

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{aligned}$$

  and the result follows.

★ A composite integer m such that $a^{m-1} \equiv 1 \pmod{m}$ for all a such that $(a, m) = 1$ is called a **Carmichael number**. There are infinitely many of them.

6.2 Wilson's Theorem

Look at the least residues of $(n-1)!$ modulo n for $n = 2, ..., 11$:

$$\begin{aligned}
1! &\equiv 1 \equiv -1 \pmod{2}\\
2! &\equiv 2 \equiv -1 \pmod{3}\\
3! &\equiv 6 \equiv 2 \pmod{4}\\
4! &\equiv 4 \cdot 6 \equiv 4 \equiv -1 \pmod{5}\\
5! &\equiv 5 \cdot 4 \cdot 6 \equiv 0 \pmod{6}\\
6! &\equiv (-1)(-2)(-3) \cdot 3 \cdot 2 \equiv -36 \equiv -1 \pmod{7}\\
7! &\equiv k \cdot 4 \cdot 2 \equiv 0 \pmod{8}\\
8! &\equiv k \cdot 6 \cdot 3 \equiv 0 \pmod{9}\\
9! &\equiv k \cdot 5 \cdot 2 \equiv 0 \pmod{10}\\
10! &\equiv (-1)(-2)\cdots(-5)5 \cdot 4 \cdot \cdots \cdot 2 \equiv -(5!)^2 \equiv -(-1)^2 \equiv -1 \pmod{11}.
\end{aligned}$$

Note that if n is prime, then $(n-1)! \equiv -1 \pmod{n}$, $3! \equiv 2 \pmod{4}$, and if n is not prime and $n > 4$, then $(n-1)! \equiv 0 \pmod{n}$. This is Wilson's Theorem. First, two lemmas:

Lemma 6.2 *If p is prime, then $x^2 \equiv 1 \pmod{p}$ has exactly two solutions: 1 and $p-1$.*

Proof.
Obviously $1^2 \equiv 1 \pmod{p}$ and $(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$, so both these numbers are solutions of the congruence.
Let r be any solution. Then $r^2 \equiv 1 \pmod{p}$, so $p|(r^2-1)$, that is,

$$p|(r-1)(r+1)$$

and so, since p is prime, $p|(r-1)$ or $p|(r+1)$. This means that

$$r \equiv 1 \pmod{p} \quad \text{or} \quad r \equiv -1 \equiv p-1 \pmod{p}.$$

Since r is a least residue $\pmod{p}$ it follows that $r = 1$ or $r = p-1$. ■

This is analogous to the fact that $x^2 = 1$ is satisfied if and only if $x = 1$ or $x = -1$ (but only holds if p is prime).

If $(a, p) = 1$, then $ax \equiv 1 \pmod{p}$ has exactly one solution, say this is a'. It is for congruence what the reciprocal is for equality, since $aa' \equiv a'a \equiv 1 \pmod{p}$. For example, for $p = 11$ we have

a	1	2	3	4	5	6	7	8	9	10
a'	1	6	4	3	9	2	8	7	5	10

.

Note that there are no duplications in the second line. This is true in general, as is shown in the next lemma.

Lemma 6.3 *Let p be an odd prime and let a' be the solution of $ax \equiv 1 \pmod{p}$, for $a = 1, 2, ..., p-1$. Then*

(i) $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$;

(ii) $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $a = p - 1$.

Proof.
(i) If $a' \equiv b' \pmod{p}$, then

$$b \equiv 1 \cdot b \equiv aa'b \equiv ab'b \equiv a \pmod{p}.$$

Conversely, if $a \equiv b \pmod{p}$, then

$$b' \equiv b' \cdot 1 \equiv b'aa' \equiv b'ba' \equiv a' \pmod{p}.$$

(ii) It follows from $1 \cdot 1 \equiv 1 \pmod{p}$ and $(p-1)(p-1) \equiv (-1)^2 \equiv 1 \pmod{p}$ that $1' \equiv 1 \pmod{p}$ and $(p-1)' \equiv p - 1 \pmod{p}$.

Conversely, if $a \equiv a' \pmod{p}$, then

$$1 \equiv aa' \equiv a^2 \pmod{p},$$

which we know from Lemma 6.2 is only possible if $a = 1$ or $a = p - 1$. ■

Theorem 6.2 (Wilson's Theorem) ***Important!*** *The integer p is prime if and only if*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof.
Suppose p is prime. If $p = 2$ the result is obvious, so assume p is odd. By Lemma 6.3 we can arrange the $p - 3$ numbers

$$2,\ 3,\ ...,\ p-2$$

as $(p-3)/2$ pairs such that each pair consists of an integer a and its associated integer a', which is different from a, such that $aa' \equiv 1 \pmod{p}$. Since the product of the two integers in each pair is congruent to $1 \pmod{p}$, it follows that

$$2 \cdot 3 \cdot \cdots \cdot (p-2) \equiv 1 \pmod{p},$$

hence

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}.$$

Conversely, suppose that for some integer n,

$$(n-1)! \equiv -1 \pmod{n}. \tag{6.6}$$

We must prove that n is prime. Suppose $n = ab$ for some positive integers a, b such that $a \neq n$. From (6.6) we have

$$n|((n-1)!+1)$$

and since $a|n$ we have

$$a|((n-1)!+1). \tag{6.7}$$

But since $a \leq n-1$ it follows that a is one of the factors of $(n-1)!$. Thus

$$a|(n-1)! \tag{6.8}$$

But (6.7) and (6.8) imply that $a|1$, so $a = 1$. Therefore the only positive divisors of n are 1 and n, thus n is a prime. ■

Section 7

The Divisors of an Integer

In this section two functions are introduced: Let

$d(n)$ denote the **number of positive divisors** of the positive integer n,

$\sigma(n)$ denote the **sum of the positive divisors** of n.

Then

$$d(n) = \sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n) = \sum_{d|n} d.$$

▲ Our aim is to determine $d(n)$ and $\sigma(n)$ for the positive integer n with prime-power decomposition $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$.

7.1 Number of Divisors of an Integer

If p is prime, the only divisors of p are 1 and p, and the only divisors of p^t are 1, p, p^2, ..., p^t. Thus $d(p) = 2$ and, more generally, $d(p^t) = t + 1$. It is easy to determine $d(n)$ using elementary counting principles:

A positive integer d is a divisor of n if and only $d = p_1^{f_1} p_2^{f_2} ... p_k^{f_k}$, where $0 \leq f_i \leq e_i$ for each i. So, when "constructing" a divisor d of n, we have any choice from 0 to e_1 (inclusive of 0 and e_1), thus $e_1 + 1$ choices, for powers of p_1. For each such choice, we have $e_2 + 1$ choices for powers of p_2, and so on, ending with $e_k + 1$ choices of powers of p_k, thus

$$(e_1 + 1)(e_2 + 1)...(e_k + 1)$$

choices of divisors of n. This proves the following theorem.

Theorem 7.1 *If $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, then*

$$d(n) = d(p_1^{e_1}) d(p_2^{e_2}) ... d(p_k^{e_k}) = (e_1 + 1)(e_2 + 1)...(e_k + 1).$$

7.2 Sum of Divisors of an Integer

Now consider the sum of the divisors of an integer. If p is prime, then its only divisors are 1 and p , hence $\sigma(p) = p + 1$. The divisors of p^2 are 1, p and p^2, so $\sigma(p^2) = 1 + p + p^2$.

In general, the divisors of p^n are 1, p, p^2, ..., p^n. Sum this geometric sequence: See Ass. 1, Q2.

$$1 + p + p^2 + ... + p^n = \sum_{i=0}^{n} p^i = \frac{p^{n+1} - 1}{p - 1},$$

hence

$$\sigma(p^n) = \frac{p^{n+1} - 1}{p - 1}. \tag{7.1}$$

In particular, $\sigma(2^n) = 2^{n+1} - 1$.

If p and q are distinct primes, then $\sigma(pq) = 1 + p + q + pq = (1 + p)(1 + q)$. In general, to calculate $\sigma(p^e q^f)$, we note that the $(e + 1)(f + 1)$ divisors of $p^e q^f$ are

$$\begin{array}{lllll} 1 & p & p^2 & \cdots & p^e \\ q & pq & p^2q & \cdots & p^eq \\ q^2 & pq^2 & p^2q^2 & \cdots & p^eq^2 \\ & & \vdots & & \\ q^f & pq^f & p^2q^f & \cdots & p^eq^f \end{array}.$$

Adding across each row we get

$$\begin{aligned} \sigma(p^e q^f) &= (1 + p + p^2 + ... + p^e) \\ &+ q(1 + p + p^2 + ... + p^e) \\ &+ q^2(1 + p + p^2 + ... + p^e) \\ &+ ... \\ &+ q^f(1 + p + p^2 + ... + p^e) \\ &= (1 + p + p^2 + ... + p^e)(1 + q + q^2 + ... + q^f) \\ &= \frac{(p^{e+1} - 1)(q^{f+1} - 1)}{(p - 1)(q - 1)}. \end{aligned}$$

This forms the basis step as well as the method for the induction step of a proof of the following result.

Theorem 7.2 *If $p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ is the prime-power decomposition of n, then*

$$\begin{aligned} \sigma(n) &= \sigma(p_1^{e_1})\sigma(p_2^{e_2})...\sigma(p_k^{e_k}) \\ &= \frac{(p_1^{e_1+1} - 1)(p_2^{e_2+1} - 1)...(p_k^{e_k+1} - 1)}{(p_1 - 1)(p_2 - 1)...(p_k - 1)}. \end{aligned}$$

Both d and σ are examples of **multiplicative functions**.

A function $f : \mathbb{N} \to \mathbb{N}$ is said to be **multiplicative** if and only if

$$f(mn) = f(m)f(n) \qquad \text{whenever} \qquad (m, n) = 1.$$

From Theorems 7.1 and 7.2 we have:

Theorem 7.3 *d is multiplicative.*

Theorem 7.4 *σ is multiplicative.*

If we know the value of a multiplicative function f for all prime-powers, then we can find the value of f for all $n \in \mathbb{N}$.

Theorem 7.5 *If f is a multiplicative function and $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, then*

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) ... f(p_k^{e_k}).$$