SECTION A Introduction to Fermat’s Little Theorem

By the end of this section you will be able to
• prove Fermat’s Little Theorem
• apply Fermat’s Little Theorem to congruences

A1 Table of Indices

In this section we evaluate indices in modular arithmetic in a much easier way than in previous sections. However we confine ourselves to a prime modulus. First we develop a table of values and then we will state and prove an important result involving a particular index with a prime modulus.

Example 1

Construct a table of values for the first 5 powers of each non-zero residue modulo 5.

Solution

We work out the powers of the least non-negative residues modulo 5. We have:

\[
\begin{array}{c|c|c|c|c}
 n & 1 & 2 & 3 & 4 \\
 \hline
 n^2 & 1^2 \equiv 1 \pmod{5} & 2^2 \equiv 4 \pmod{5} & 3^2 \equiv 4 \pmod{5} & 4^2 \equiv 1 \pmod{5} \\
 n^3 & 1^3 \equiv 1 \pmod{5} & 2^3 \equiv 3 \pmod{5} & 3^3 \equiv 2 \pmod{5} & 4^3 \equiv 4 \pmod{5} \\
 n^4 & 1^4 \equiv 1 \pmod{5} & 2^4 \equiv 1 \pmod{5} & 3^4 \equiv 1 \pmod{5} & 4^4 \equiv 1 \pmod{5} \\
 n^5 & 1^5 \equiv 1 \pmod{5} & 2^5 \equiv 2 \pmod{5} & 3^5 \equiv 3 \pmod{5} & 4^5 \equiv 4 \pmod{5} \\
\end{array}
\]

TABLE 1

What do you notice about the shaded result?

\[1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod{5}\]

In general \(n^4 \equiv 1 \pmod{5}\) provided that \(n\) is not divisible by 5.

This result is no coincidence but will also work with other prime moduli. For example you would find the following results:

\[1^{12} \equiv 2^{12} \equiv 3^{12} \equiv 4^{12} \equiv 5^{12} \equiv 6^{12} \equiv 7^{12} \equiv 8^{12} \equiv 9^{12} \equiv 10^{12} \equiv 11^{12} \equiv 12^{12} \equiv 1 \pmod{13}\]

This only works if we have a prime modulus and is an example of a general proposition named after the French mathematician Pierre de Fermat, Fermat’s Little Theorem – FLT.

De Fermat was born in France and went to the University of Toulouse where he became a lawyer. As a lawyer he did not perform well as he was interested in mathematics and spent his entire time studying mathematics. He took an interest in pure mathematics rather than its applications.

Fermat is well known for his work in number theory.
Fermat’s Last Theorem is better known than his Little Theorem because it famously took nearly 350 years to prove. Fermat’s Last Theorem states the following:

\[ x^n + y^n = z^n \text{ has no (non-zero) integer solutions for } n \geq 3 \]

Fermat wrote in the margin of his book:

“I have discovered a remarkable proof which this margin is too small to contain.”

This Last Theorem was proved by the British mathematician Andrew Wiles in 1994 and is incredibly complicated.

### A2 Proof of Fermat’s Little Theorem (FLT)

Fermat’s Little Theorem (FLT) is a result which makes evaluating a power of a number to a prime modulus much easier.

Fermat’s Little Theorem states that if \( p \) is prime and \( n \) is any integer such that \( p \) does not divide into \( n \) then

\[ n^{p-1} \equiv 1 \pmod{p} \]

Here are some more numerical examples:

With prime \( p = 11 \) and \( n = 2 \):

\[ 2^{11-1} \equiv 2^{10} \equiv 1024 \equiv 1 \pmod{11} \]

With prime \( p = 7 \) and \( n = 5 \):

\[ 5^{7-1} \equiv 5^6 \equiv 15625 \equiv 1 \pmod{7} \]

With prime \( p = 17 \) and \( n = 15 \):

\[ 15^{17-1} \equiv 15^{16} \equiv (-2)^{16} \pmod{17} \]

\[ \equiv [( -2 )^4]^4 \]

\[ \equiv [ 16 ]^4 \]

\[ \equiv [-1]^4 \equiv 1 \pmod{17} \]

[Because \( 16 \equiv -1 \pmod{17} \)]

Just because this works for these three examples;

\[ 2^{11-1} \equiv 1 \pmod{11} \], \[ 5^{7-1} \equiv 1 \pmod{7} \] and \[ 15^{17-1} \equiv 1 \pmod{17} \]

It does not mean the result is generally true. How can we say that this is always the case? We need to prove this result - Fermat’s Little Theorem; FLT.

**Fermat’s Little Theorem (4.1).**

Let \( n \) be an integer and \( p \) be a prime number which does not divide \( n \). Then

\[ n^{p-1} \equiv 1 \pmod{p} \]

**Proof.**

We examine the first \( p-1 \) positive multiples of \( n \):

\[ n, \ 2n, \ 3n, \ 4n, \ \cdots, \ (p-1)n \]

(*)

Each of these are incongruent modulo \( p \). This means that none of these are congruent to each other modulo \( p \). Why?

Suppose there are two which are congruent to each other:

\[ k \times n \equiv m \times n \pmod{p} \text{ where } 1 \leq k < m \leq p-1 \]

Then by Corollary (3.12) of the last chapter which claims:

If \( a \times c \equiv b \times c \pmod{p} \) and prime \( p \) does not divide into \( c \) then \( a \equiv b \pmod{p} \).
Applying this corollary to \( k \times n \equiv m \times n \pmod{p} \) gives \( k \equiv m \pmod{p} \) which implies \( k - m \) is a multiple of \( p \). This is impossible because from above we have \( 1 \leq k < m \leq p - 1 \). Therefore each of the numbers in the list (*) are incongruent. 

Multiplying these numbers in the list (*) gives 

\[
\begin{align*}
n \times 2n \times 3n \times \cdots \times (p-1) &\equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \times n \times n \times n \times \cdots \times n \\
(p-1)! &\equiv (p-1)! \times n^{p-1} \pmod{p} \\
&= (p-1)! \times n^{p-1} \pmod{p} \\
&= (p-1)! \times n^{p-1} \equiv 1 \times 2 \times 3 \times 4 \times \cdots \times (p-1) \pmod{p} \\
&= (p-1)! \pmod{p}
\end{align*}
\]

Since the numbers in the list (*) are not congruent to each other, so every one of these numbers is congruent to one of \( 1, 2, 3, 4, \ldots, p - 1 \) in some order. This means that we have 

\[
(p-1)! \times n^{p-1} \equiv 1 \times 2 \times 3 \times 4 \times \cdots \times (p-1) \equiv (p-1)! \pmod{p}
\]

Applying the above Corollary (3.12) again to \( n^{p-1} \times (p-1)! \equiv 1 \times (p-1)! \pmod{p} \) with \( c = (p-1)! \) gives: 

\[
n^{p-1} \equiv 1 \pmod{p}
\]

This is our required result.

Fermat’s Little Theorem is useful in simplifying calculations. Why? Because evaluating powers of numbers can be a tedious task so if we have a prime modulus then we want to work with \( n^{p-1} \equiv 1 \pmod{p} \) because \( 1^k \equiv 1 \pmod{p} \) for any natural number \( k \). Working with residue 1 makes evaluation of powers a lot easier.

### A3 Application of Fermat’s Little Theorem

#### Example 2

Find the least non-negative residue \( x \pmod{11} \) in the following congruence 

\[
3^{52} \equiv x \pmod{11}
\]

**Solution**

Since 11 is prime so we can apply FLT:

\[
n^{p-1} \equiv 1 \pmod{p}
\]

With \( n = 3 \) and \( p = 11 \) we have

\[
3^{10} \equiv 1 \pmod{11} \quad (*)
\]

Rewriting the given index of 52 as a multiple of 10 plus remainder:

\[
52 = (5 \times 10) + 2
\]

We have

\[
3^{52} \equiv 3^{(5 \times 10) + 2} = 3^{5 \times 10 \times 2} = 3^{5 \times 10} \times 3^2 \\
= (3^{10})^5 \times 3^2 \\
= (1)^5 \times 9 = 9 \pmod{11}
\]

Hence \( x \equiv 9 \pmod{11} \).
This \( x \equiv 9 \pmod{11} \) means that \( 3^{52} = 6461081889226673298932241 \) divided by 11 leaves remainder 9.

**Example 3**

Find the remainder when \( 5^{101} \) is divided by 31. (The number \( 5^{101} \) has 70 digits.)

**Solution**

Let \( r \) be the remainder such that

\[
5^{101} \equiv r \pmod{31}
\]

Since 31 is prime we can apply FLT:

\[
n^{p-1} \equiv 1 \pmod{p}
\]

With \( n = 5 \) and \( p = 31 \) we have

\[
5^{30} \equiv 1 \pmod{31}
\]

Rewriting the given index \( 101 = (3 \times 30) + 11 \) in \( 5^{101} \equiv r \pmod{31} \) yields

\[
5^{101} \equiv 5^{(30 \times 3) + 11} \equiv (5^{30})^3 \cdot 5^{11}
\]

\[
\equiv 1^3 \cdot 5^{11} \quad \text{[By (‡)]}
\]

\[
\equiv 5^{11} \pmod{31}
\]

Need to write \( 5^{11} \) as the least non-negative residue modulo 31. Note that

\[
5^3 = 125 = (4 \times 31) + 1 \quad \text{which implies} \quad 5^3 \equiv 1 \pmod{31}
\]

Using this \( 5^3 \equiv 1 \pmod{31} \) in the above result \( 5^{101} \equiv 5^{11} \pmod{31} \) gives

\[
5^{101} \equiv 5^{11}
\]

\[
\equiv 5^{(3 \times 3) + 2} \equiv (5^3)^3 \cdot 5^2 \equiv 1^3 \times 25 \equiv 25 \pmod{31}
\]

We have \( r \equiv 5^{101} \equiv 5^{11} \equiv 25 \pmod{31} \). The remainder after dividing \( 5^{101} \) by 31 is 25.

**Example 4**

Let \( p \) be prime and \( n \) be a non-zero residue modulo \( p \). Show that \( n^{p-2} \) is the multiplicative inverse of \( n \) modulo \( p \).

**Solution**

*What does the multiplicative inverse mean?*

By Definition (3.20) of the last chapter:

\[
ax \equiv 1 \pmod{n} \quad \Rightarrow \quad x \text{ is inverse of } a \pmod{n} \quad \text{provided} \quad \gcd(a, n) = 1
\]

Substituting \( x \equiv n^{p-2} \pmod{p} \) into \( nx \pmod{p} \) gives

\[
nx \equiv n \left( n^{p-2} \right)
\]

\[
\equiv n^{p-1} \quad \text{[Using rules of indices]} \quad \text{By FLT}
\]

We have \( nx \equiv 1 \pmod{p} \) so \( x \equiv n^{p-2} \pmod{p} \) is the inverse of \( n \) modulo \( p \).

\[\blacksquare\]

**Corollary (4.2).**

Let \( n \) be any integer and \( p \) be a prime number. Then
Chapter 4: A Survey of Congruent Results

How is this result different from FLT?
In FLT the prime \( p \) did not divide integer \( n \). This result also applies to the case when \( p \) divides \( n \).

How do we prove this result?
Consider two cases: 1) \( p \) does divide \( n \) 
2) \( p \) does not divide \( n \)

**Case 1** Assume prime \( p \) does divide \( n \), \( p \mid n \), then

\[
\begin{align*}
n & \equiv 0 \pmod{p} \quad \text{implies} \quad n^p \equiv 0^p \equiv 0 \pmod{p}.
\end{align*}
\]
Therefore we have our result \( n^p \equiv n \pmod{p} \).

**Case 2** Assume prime \( p \) does not divide into \( n \). In this case we can use FLT (4.1):

\[
\begin{align*}
n^{p-1} & \equiv 1 \pmod{p}.
\end{align*}
\]

We have \( n^{p-1} \equiv 1 \pmod{p} \). Multiplying this by \( n \) gives

\[
\begin{align*}
n \times n^{p-1} & \equiv (n \times 1) \pmod{p} \\
n^p & \equiv n \pmod{p}
\end{align*}
\]

This is our required result.

We can also use Fermat’s Little Theorem to solve linear congruences.

**Example 5**
Solve the linear congruence \( 31x \equiv 5 \pmod{37} \).

**Solution**
Since 37 is prime and \( 37 \nmid 31 \) so applying FLT we have

\[
31^{36} \equiv 1 \pmod{37}
\]

Note that \( 31 \equiv -6 \pmod{37} \). Therefore

\[
31^{36} \equiv (-6)^{36} \equiv 1 \pmod{37}
\]

We can rewrite the index 36 as 35 plus 1 so that we have

\[
(-6)^{36} \equiv (-6)^{1+35} \equiv (-6)(-6)^{35} \equiv 1 \pmod{37}
\]

**What does \((-6)(-6)^{35} \equiv 1 \pmod{37}\) mean?**

The multiplicative inverse of \(-6\) modulo 37 is \((-6)^{35}\) modulo 37 because by (3.20) of the last chapter we have:

\[
ax \equiv 1 \pmod{n} \Rightarrow x \text{ is the inverse of } a \text{ provided } \gcd(a, n) = 1
\]

We can find this inverse by evaluating \((-6)^{35}\) modulo 37:

\[
\begin{align*}
(-6)^2 & \equiv 36 \equiv -1 \pmod{37} \quad \text{implies} \\
(-6)^{35} & \equiv (-6)^{34}(-6) \equiv (-1)^{34}(-6)(-1)^{17}(-6) \equiv 6 \pmod{37}
\end{align*}
\]

So the inverse of \(-6\) modulo 37 is 6 modulo 37. Multiplying both sides of the given equation by 6 yields

\[
6 \times 31x \equiv 6 \times 5 \equiv 30 \pmod{37}
\]
Therefore our solution is $x \equiv 30 \pmod{37}$.

You are asked to do this in the exercises.

Additionally, FLT is used for testing whether a given number is composite because

$$n^{m-1} \neq 1 \pmod{m} \; \text{then} \; m \; \text{is composite}$$

For example $5^{1000} \equiv 716 \pmod{1001}$ therefore 1001 is composite. Actually

$$1001 = 7 \times 11 \times 13$$

**A4 Pseudoprimes**

*Is the converse of FLT true?*

This means we need to check that if $n^{m-1} \equiv 1 \pmod{m}$ then $m$ is prime. Let $m = 561$ and $n = 2$ then by evaluation we find that

$$2^{560} \equiv 1 \pmod{561}$$

However $561 = 3 \times 11 \times 17$ which means 561 is composite. The converse of FLT does *not* hold, that means

$$n^{m-1} \equiv 1 \pmod{m} \; \text{does not imply} \; m \; \text{is prime}$$

We call numbers like 561 a pseudoprime.

Another pseudoprime is 341 which is composite because $341 = 11 \times 31$. However

$$2^{340} \equiv 1 \pmod{341}$$

There is a difference between the pseudoprime 341 and 561. Examine the following results for 341:

$$3^{340} \equiv 56 \pmod{341}, \quad 5^{340} \equiv 67 \pmod{341}, \quad 7^{340} \equiv 56 \pmod{341}, \quad 23^{340} \equiv 1 \pmod{341}$$

These do *not always* give $n^{m-1} \equiv 1 \pmod{m}$.

However for 561 this result works for every base number $n$ provided 561 does *not* divide into $n$. Hence $n^{560} \equiv 1 \pmod{561}$ provided 561 does *not* divide $n$. The number 561 is called a **Carmichael number**. These are composite numbers $m$ such that to every base $n$ we have $n^{m-1} \equiv 1 \pmod{m}$ provided $m \nmid n$.

Carmichael numbers are very rare. The smallest being 561. There are only 2,163 Carmichael numbers in the first 25 billion natural numbers. However in 1994 it was proved that there are an infinite number of Carmichael numbers. (Alford, W. R.; Granville, A.; and Pomerance, C. "There are Infinitely Many Carmichael Numbers." *Ann. Math.* **139**, 703-722, 1994.)

The existence of Carmichael numbers prevents FLT being used to test primality.

We will revisit pseudoprimes in section (4.3).

**SUMMARY**

FLT (4.1). Let $n$ be an integer and $p$ be a prime number which does *not* divide $n$. Then

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

We can use this result to simplify powers of prime moduli.