3.5: Theorems of Fermat, Euler, and Wilson

In this section we present three applications of congruences. The first theorem is Wilson’s theorem which states that 
\((p-1)!+1\) is divisible by \(p\), for \(p\) prime. Next, we present Fermat’s theorem, also known as Fermat’s little theorem which states that \((a^p)\) and \(a\) have the same remainders when divided by \(p\) where \(p \nmid a\). Finally we present Euler’s theorem which is a generalization of Fermat’s theorem and it states that for any positive integer \((m)\) that is relatively prime to an integer \((a)\),

\[a^{\phi(m)} \equiv 1 \pmod{m}\]

where \(\phi\) is Euler’s \((\phi\)-function. We start by proving a theorem about the inverse of integers modulo primes.

**Theorem**

Let \((p)\) be a prime. A positive integer \((m)\) is its own inverse modulo \((p)\) if and only if \((p)\) divides \((m+1)\) or \((p)\) divides \((m-1)\).

Suppose that \((m)\) is its own inverse. Thus \([m.m \equiv 1 \pmod{p}].\) Hence \((p \mid m^2 - 1)\). As a result,

\([p \mid (m-1) \text{ or } p \mid (m+1)]\]

We get that \((m \equiv 1 \pmod{p})\) or \((m \equiv -1 \pmod{p})\).

Conversely, suppose that

\([m \equiv 1 \pmod{p}] \text{ or } [m \equiv -1 \pmod{p}]\]

Thus
\[m^2 \equiv 1 \pmod{p}.\]

Wilson’s Theorem

If \(\ell(p)\) is a prime number, then \(\ell(p)\) divides \(\ell(p-1)!+1\).

When \(\ell(p)=2\), the congruence holds. Now let \(\ell(p)>2\). Using Theorem 26, we see that for each \(\ell(1 \leq m \leq p)\), there is an inverse \(\ell(1 \leq \bar{m} \leq p)\) such that \(\ell(m \bar{m} \equiv 1 \pmod{p})\). Thus by Theorem 28, we see that the only two integers that have their own inverses are \(\ell(1)\) and \(\ell(p-1)\). Hence after coupling the integers from 2 to \(\ell(p-2)\) each with its inverse, we get \(\ell(2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}\). Thus we get \(\ell(1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv (p-1) \pmod{p}\). As a result, we have \(\ell((p-1)! \equiv 1 \pmod{p})\).

Note also that the converse of Wilson’s theorem also holds. The converse tells us whether an integer is prime or not.

If \(\ell(m)\) is a positive integer with \(\ell(m \geq 2)\) such that \(\ell((m-1)!+1 \equiv 0 \pmod{m})\) then \(\ell(m)\) is prime.

Suppose that \(\ell(m)\) has a proper divisor \(\ell(c-1)\) and that \(\ell((m-1)!+1 \equiv 0 \pmod{m})\). That is \(\ell(m=e_1 c_2)\) where \(\ell(1 < e_1 < m)\) and \(\ell(1 < c_2 < m)\). Thus \(\ell(c-1)\) is a divisor of \(\ell((m-1)!+1)\). Also, since \(\ell(m \mid (m-1)!+1)\) we get \(\ell(c_1 \mid (m-1)!+1)\). As a result, by Theorem 4, we get that \(\ell(c_1 \mid (m-1)!+1-(m-1)!))\) which gives that \(\ell(c_1 \mid 1)\). This is a contradiction and hence \(\ell(m)\) is prime.

We now present Fermat’s Theorem or what is also known as Fermat’s Little Theorem. It states that the remainder of \(\ell(a \cdot p-1)\) when divided by a prime \(\ell(p)\) that doesn’t divide \(\ell(a)\) is 1. We then state Euler’s theorem which states that the remainder of \(\ell(a^\ell(\phi(m)))\) when divided by a positive integer \(\ell(m)\) that is relatively prime to \(\ell(a)\) is 1. We prove Euler’s Theorem only because Fermat’s Theorem is nothing but a special case of Euler’s Theorem. This is due to the fact that for a prime number \(\ell(p)\), \(\ell(\phi(p)=p-1)\).

Euler’s Theorem

If \(\ell(m)\) is a positive integer and \(\ell(a)\) is an integer such that \(\ell((a,m)=1)\), then \(\ell(a^{\phi(m)} \equiv 1 \pmod{m})\)

Note that \(\ell(3^4=81 \equiv 1 \pmod{5})\). Also, \(\ell(2^{\phi(9)}=2^6=64 \equiv 1 \pmod{9})\).

We now present the proof of Euler’s theorem.

Proof

Let \(\ell(k_1,k_2,\ldots,k_{\phi(m)})\) be a reduced residue system modulo \(\ell(m)\). By Theorem 25, the set \(\ell\{a k_1,a k_2,\ldots,a k_{\phi(m)}\}\) also forms a reduced residue system modulo \(\ell(m)\). Thus

\[\ell\{a k_1,a k_2,\ldots,a k_{\phi(m)}\}=a^{\phi(m)} k_1 k_2 \ldots k_{\phi(m)} \equiv k_1 k_2 \ldots k_{\phi(m)} \pmod{m}.\]

Now since \(\ell((k_i m)=1)\) for all \(\ell(1 \leq i \leq \phi(m))\), we have \(\ell((k_1 k_2 \ldots k_{\phi(m)},m)=1)\). Hence by Theorem 22 we can cancel the product of \(\ell(k_i)\)’s on both sides and we get

UC Davis ChemWiki is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.
An immediate consequence of Euler’s Theorem is:

Fermat’s Theorem

If \( p \) is a prime and \( \text{gcd}(a, p) = 1 \), then

\[
[a^{\phi(p)}] \equiv 1 \pmod{p}.
\]

We now present a couple of theorems that are direct consequences of Fermat’s theorem. The first states Fermat’s theorem in a different way. It says that the remainder of \( a^{p-1} \) when divided by \( p \) is the same as the remainder of \( a \) when divided by \( p \). The other theorem determines the inverse of an integer \( a \) modulo \( p \). We now present the two theorems.

If \( \text{gcd}(p, a) = 1 \), then \( a^{p-1} \equiv 1 \pmod{p} \).

If \( \text{gcd}(p, a) = 1 \), by Fermat’s theorem we know that

\[
[a^{p-1}] \equiv 1 \pmod{p}.
\]

Thus, we get

\[
[a^{p}] \equiv a \pmod{p}.
\]

Now if \( \text{gcd}(p, a) = 1 \), we have

\[
[a^{p}] \equiv a \equiv 0 \pmod{p}.
\]

If \( \text{gcd}(p, a) = 1 \), then Fermat’s theorem says that

\[
[a^{p-1}] \equiv 1 \pmod{p}.
\]

Hence

\[
[a^{p-2}] \equiv 1 \pmod{p}.
\]

As a result,

\[
[a^{p-2}] \equiv a^{-1} \pmod{p}.
\]

Exercises

1. Show that \( 10! + 1 \) is divisible by 11.

2. What is the remainder when \( 5!25! \) is divided by 31?

3. What is the remainder when \( 5^{100} \) is divided by 7?

4. Show that if \( \text{gcd}(p, a) = 1 \) is an odd prime, then

\[
[2(p-3)!] \equiv -1 \pmod{p}.
\]

5. Find a reduced residue system modulo \( 2^m \), where \( m \) is a positive integer.

6. Show that if \( \text{gcd}(a_1, a_2, \ldots, a_n, \phi(m)) = 1 \) is a reduced residue system modulo \( m \), then

\[
[a_1 + a_2 + \ldots + a_n] \equiv 0 \pmod{m}.
\]

7. Show that if \( \text{gcd}(a) = 1 \) is an integer such that \( \text{gcd}(a, 3) = 1 \) or such that \( \text{gcd}(a, 9) = 1 \), then

\[
[a^7] \equiv a \pmod{63}.
\]
Contributors

• Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.