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 \(m \equiv 1 \pmod{p}\). Hence \(p \mid (m^2 - 1)\). As a result,

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

We get that \((m^2 - 1) \equiv 0 \pmod{p}\) or \((m^2 - 1) \equiv 0 \pmod{p}\).

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

When \(p=2\), the congruence holds. Now let \(p>2\). Using Theorem 26, we see that for each \(0 \leq m \leq p\), there is an inverse \(0 \leq \bar{m} \leq p\) such that \(m\bar{m} \equiv 1 \pmod{p}\). Thus by Theorem 28, we see that the only two integers that have their own inverses are \(1\) and \((p-1)\). Hence after coupling the integers from 2 to \((p-2)\) each with its inverse, we get \(2.3.....(p-2) \equiv 1 \pmod{p}\). Thus we get \([1.2.3.....(p-2)(p-1) \equiv (p-1) \pmod{p}]\) As a result, we have \[((p-1)! \equiv -1 \pmod{p})\].

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

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

Suppose that \((m)\) has a proper divisor \((c_1)\) and that \([\{(m-1)!+1 \equiv 0 \pmod{m}\}]\). That is \((m=ec_2\) where \((1<c_1<\frac{m}{2}\)) and \((1<c_2<\frac{m}{2}\)). Thus \((c_1)\) is a divisor of \((\{(m-1)!\})\). Also, since \((m \text{ is prime})\) we get \([\{c_1 \mid \{(m-1)!+1\}]\). As a result, by Theorem 4, we get that \([\{c_1 \mid \{(m-1)!+1\} \equiv 1 \pmod{c_1}\}]\) which gives that \(c_1 \equiv 1 \pmod{m}\). This is a contradiction and hence \((m)\) is prime.

We now present Fermat's Theorem or what is also known as Fermat's Little Theorem. It states that the remainder of \(a^{(p-1)}\) when divided by a prime \((p)\) that doesn't divide \(a\) is 1. We then state Euler's theorem which states that the remainder of \(a^{\phi(m)}\) when divided by a positive integer \((m)\) that is relatively prime to \((a)\) 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 \((p)\), \((\phi(p)=p-1)\).

Euler's Theorem

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

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

We now present the proof of Euler's theorem.

Proof

Let \((k_1,k_2,...,k_{\phi(m)})\) be a reduced residue system modulo \((m)\). By Theorem 25, the set \([\{ak_1,ak_2,...,ak_{\phi(m)}\}]\) also forms a reduced residue system modulo \((m)\). Thus

\([ak_1k_2...ak_{\phi(m)}=a^{\phi(m)}k_1k_2...k_{\phi(m)} \pmod{m}]\)

Now since \((((k_i,m)=1)\) for all \((i \leq \phi \pmod{\phi(m)})\), we have \(([k_1k_2...k_{\phi(m)},m]=1)\). Hence by Theorem 22 we can cancel the product of \((k_i)\)'s on both sides and we get
\[a^\phi(m) \equiv 1 \pmod{m} \]

An immediate consequence of Euler’s Theorem is:

Fermat’s Theorem

If \( p \) is a prime and \( (a') \) is a positive integer with \( (p' \nmid a') \), then \( [a^{p-1}] \equiv 1 \pmod{p} \).

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 \( (p) \) where \( (p' \nmid a') \).

If \( (p) \) is a prime number and \( (a') \) is a positive integer, then \( (a^{p'}) \equiv a \pmod{p} \).

If \( (p' \nmid a') \), 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 \( (p' \nmid a') \), we have

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

If \( (p) \) is a prime number and \( (a') \) is an integer such that \( (p' \nmid a') \), then \( (a^{p-2}) \) is the inverse of \( (a) \) modulo \( (p) \).

If \( (p' \nmid a') \), then Fermat’s theorem says that \( [a^{p-1}] \equiv 1 \pmod{p} \). Hence \( [a^{p-2}] a \equiv 1 \pmod{p} \). As a result, \( (a^{p-2}) \) is the inverse of \( (a) \) modulo \( (p) \).

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 \( (p) \) 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 \( (a_1, a_2, \ldots, a_{\phi(m)}) \) is a reduced residue system modulo \( (m) \), where \( (m) \) is a positive integer with \( (m \nmid 2^1) \), then \( (a_1 + a_2 + \ldots + a_{\phi(m)}) \equiv 0 \pmod{m} \).
7. Show that if \( (a) \) is an integer such that \( (a) \) is not divisible by 3 or such that \( (a) \) is divisible by 9, then \( (a^7 \equiv a \pmod{63}) \).

Contributors and Attributions

- 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.