Number Theory

Lakshmy K V

October 5, 2020

Fermat's Little Theorem

Consider the prime $p = 3$. Observe that

$$\begin{aligned} 1^2 &\equiv 1 \bmod 3, \\ 2^2 &\equiv 1 \bmod 3. \end{aligned}$$

Similarly, for the prime $p = 5$, we observe that

$$\begin{aligned} 1^4 &\equiv 1 \bmod 5, \\ 2^4 &\equiv 1 \bmod 5, \\ 3^4 &\equiv 1 \bmod 5, \\ 4^4 &\equiv 1 \bmod 5. \end{aligned}$$

The above congruences are not a coincidence, as the following theorem explains. This theorem is known as Fermat's Little Theorem.

THEOREM 2.15. *Let p be a prime number and let a be an integer co-prime to p. Then,*

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

Proof: Consider the two sets

$$\{1, \ 2, \ 3, \ \cdots, \ (p-1)\}, \qquad \{a, \ 2a, \ 3a, \ \cdots, \ (p-1)a\}.$$

Both have the same cardinality. In the second set,

$$\begin{aligned} ia &\equiv ja \bmod p \\ \implies p &\mid (i-j)a \\ \implies p &\mid (i-j) \\ \implies i &= j, \end{aligned}$$

as $1 \leq i,\ j \leq (p-1)$. Thus each element in the second set is congruent to a unique element of the first set Hence, the product over all the elements of the two sets are congruent modulo p. Hence,

$$\begin{aligned} a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \bmod p \\ \implies \quad (p-1)!a^{p-1} &\equiv (p-1)! \bmod p \\ \implies \quad a^{p-1} &\equiv 1 \bmod p, \end{aligned}$$

as $(p-1)!$ is coprime to p. $\square$

Corollary 2.16. *Let p be a prime and let a be an integer. Then,*

$$a^p \equiv a \ mod\ p.$$

Proof: If a is not coprime to p, then p divides both a and a^p, and

$$a^p \equiv 0 \equiv a \mod p.$$

If a is co-prime to p, then by Fermat's Little Theorem given above, we have

$$a^{p-1} \equiv 1 \mod p \implies a^p \equiv a \mod p. \qquad \square$$

Euler's Theorem

- Euler's theorem generalizes Fermat's theorem to the case where the modulus is composite.
- The key point of the proof of Fermat's theorem was that if p is prime, $\{1, 2, \ldots, p-1\}$ are relatively prime to p.
- This suggests that in the general case, it might be useful to look at the numbers less than the modulus n which are relatively prime to n.

This motivates the following definition.

Definition

The Euler ϕ -function is the function on positive integers defined by $\phi(n) =$ The number of integers in $\{1, 2, \ldots, n-1\}$ which are relatively prime to n.

For example, $\phi(24) = 8$, because there are eight positive integers less than 24 which are relatively prime to 24:

$$1, 5, 7, 11, 13, 17, 19, 23$$

On the other hand, $\phi(11) = 10$, because all of the numbers in $\{1, \ldots, 10\}$ are relatively prime to 11.

Proposition

(a) If p is prime, $\phi(p) = p - 1$.
(b) If p is prime and $n \geq 1$, then $\phi(p^n) = p^n - p^{n-1}$.
(c) $\phi(n)$ counts the elements in $\{1, 2, \ldots, n-1\}$ which are invertible mod n.

Proof.
(a) If p is prime, then all of the numbers $\{1, \ldots, p-1\}$ are relatively prime to p. Hence, $\phi(p) = p - 1$.

(b) There are p^n elements in $\{1, 2, \ldots, p^n\}$. An element of this set is not relatively prime to p if and only if it's divisible by p. The elements of this set which are divisible by p are

$$1 \cdot p, \quad 2 \cdot p, \quad 3 \cdot p, \ldots, p^{n-1} \cdot p.$$

(Note that $p^{n-1} \cdot p = p^n$ is the last element of the set.)
Thus, there are p^{n-1} elements of the set which are divisible by p, i.e. p^{n-1} elements of the set which are not relatively prime to p. Hence, there are $p^n - p^{n-1}$ elements of the set which are relatively prime to p.
(The definition of $\phi(p^n)$ applies to the set $\{1, 2, \ldots, p^n - 1\}$, whereas I just counted the numbers from 1 to p^n . But this isn't a problem, because I counted p^n in the set, but then subtracted it off since it was not relatively prime to p.)

(c) $(a, n) = 1$ if and only if $ax \equiv 1 \mod n$ for some x,
so a is relatively prime to n if and only if a is invertible mod n.
Now $\phi(n)$ is the number of elements in $\{1, 2, \ldots, n-1\}$ which are relatively prime to n,
so $\phi(n)$ is also the number of elements in $\{1, 2, \ldots, n-1\}$ which are invertible mod n.

Definition:

A reduced residue system mod n is a set of numbers

$$a_1, a_2, \ldots, a_{\phi(n)}$$

such that:

(a) If $i \neq j$, then $a_i \not\equiv a_j \pmod{n}$. That is, the a's are distinct mod n.

(b) For each i, $(a_i, n) = 1$. That is, all the a's are relatively prime to n.

Thus, a reduced residue system contains exactly one representative for each number relatively prime to n.
Compare this to a complete residue system mod n, which contains exactly one representative to every number mod n.
As an example, $\{1, 5, 7, 11\}$ is a reduced residue system mod 12. So is $\{-11, 17, 31, -1\}$.
On the other hand, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ is a complete residue system mod 12.

Lemma.

Let $\phi(n) = k$, and let $\{a_1, \ldots, a_k\}$ be a reduced residue system mod n.
(a) For all m, $\{a_1 + mn, \ldots, a_k + mn\}$ is a reduced residue system mod n.
(b) If $(m, n) = 1$, $\{ma_1, \ldots, ma_k\}$ is a reduced residue system mod n.

Proof.
(a) This is clear, since $a_i = a_i + mn \mod n$ for all i.
(b) Since $(m, n) = 1$, I may find x such that $mx = 1 \mod n$. Since $(a_i, n) = 1$, so I may find b_i such that $a_i b_i = 1 \mod n$.
Then $(xb_i)(a_i m) = (mx)(a_i b_i) = 1 \mod n$, which proves that $a_i m$ is invertible mod n.
Hence, $(a_i m, n) = 1$ — the ma 's are relatively prime to n.
Now if $ma_i = ma_j \mod n$, then $xma_i = xma_j \mod n$, or $a_i = a_j \mod n$.
Since the a's were distinct mod n, this is only possible of $i = j$. Hence, the ma 's are also distinct mod n.
Therefore, $\{ma_1, \ldots, ma_k\}$ is a reduced residue system mod n.

Corollary:

Let $\phi(n) = k$, and let $\{a_1, \ldots, a_k\}$ be a reduced residue system mod n. Suppose $(s, n) = 1$, and let t be any integer. Then the following is a reduced residue system mod n:

$$\{sa_1 + tn, sa_2 + tn, \ldots, sa_k + tn\}$$

Here are some examples of these results. $\{1, 5\}$ is a reduced residue system mod 6.

Adding $12 = 2 \cdot 6$ to each number, I get $\{13, 17\}$, another reduced residue system mod 6.

Since $(6, 25) = 1$, I may multiply the original system by 25 to obtain $\{25, 125\}$, another reduced residue system.

Finally, $\{25 + 12, 125 + 12\} = \{37, 137\}$ is yet another reduced residue system mod 12.

Euler's theorem

Theorem: Let $n > 0$, $(a, n) = 1$. Then

$$a^{\phi(n)} = 1 \mod n.$$

Remark. If n is prime, then $\phi(n) = n - 1$, and Euler's theorem says $a^{n-1} = 1 \mod n$, which is Fermat's theorem.

Proof. Let $\phi(n) = k$, and let $\{a_1, \ldots, a_k\}$ be a reduced residue system mod n. I may assume that the a_i 's lie in the range $\{1, \ldots, n-1\}$. Since $(a, n) = 1$, $\{aa_1, \ldots, aa_k\}$ is another reduced residue system mod n. Since this is the same set of numbers mod n as the original system, the two systems must have the same product mod n:

$$(aa_1)\cdots(aa_k) = a_1\cdots a_k \mod n, \quad a^k(a_1\cdots a_k) = a_1\cdots a_k \mod n.$$

Now each a_i is invertible mod n, so multiplying both sides by $a_1^{-1}\cdots a_k^{-1}$, I get

$$a^k = 1 \mod n, \quad \text{or} \quad a^{\phi(n)} = 1 \mod n.$$

Example

1. $\phi(40) = 16$, and $(9, 40) = 1$. Hence, Euler's theorem says that $9^{16} = 1 \mod 40$.
2. $21^{16} = 1 \mod 40$
3. Reduce $37^{103} \mod 40$ to a number in the range $\{0, 1, \dots 39\}$. Euler's theorem says that $37^{16} = 1 \mod 40$. So

$$37^{103} = 37^{96} \cdot 37^{7} = (37^{16})^{6} \cdot 94931877133 = 1 \cdot 13 = 13 \mod 40.$$

- Solve $15x = 7 \mod 32$.
  Note that $(15, 32) = 1$ and $\phi(32) = 16$. Therefore, $15^{16} = 1 \mod 32$. Multiply the equation by 15^{15} :

  $$x = 7 \cdot 15^{15} \mod 32.$$

  Now

  $$7 \cdot 15^{15} = 105 \cdot 15^{14} = 105 \cdot (15^2)^7 = 105 \cdot 225^7 = 9 \cdot 1^7 = 9 \mod 32.$$

  So the solution is $x = 9 \mod 32$.

Wilson's Theorem

Observe that for the first few primes 3, 5 and 7

$$\begin{aligned} 2! = 2 &\equiv -1 \bmod 3 \\ 4! = 24 &\equiv -1 \bmod 5 \\ 6! = 720 &\equiv -1 \bmod 7 \end{aligned}$$

It is not mere coincidence. This is true for any prime p.

Wilson's Theorem

THEOREM 2.17. *Let p be a prime, Then,*

$$(p-1)! \equiv -1 \ mod\ p.$$

The above theorem is known as Wilson's Theorem. We will later see that the converse of the above theorem is also true.

Wilson's Theorem

Proof: If $1 \leq a \leq p-1$, we know that $ax \equiv 1 \bmod p$ has a solution which is unique modulo p. Thus, each a $(1 \leq a \leq p-1)$ corresponds to a unique element b, $1 \leq b \leq p-1$ such that $ab \equiv 1 \bmod p$. The element b can be thought of as the inverse of a in multiplication modulo p. Now, a will be the inverse of itself modulo p if and only if $a^2 \equiv 1 \bmod p$, i.e.,

$$\begin{array}{rcl} p & | & (a^2-1) \\ \Leftrightarrow p \mid (a-1) & \text{or} & p \mid (a+1) \\ \Leftrightarrow a & \equiv & \pm 1 \bmod p \\ \Leftrightarrow a = 1 & \text{or} & a = p-1. \end{array}$$

In the product $1.2.\cdots.(p-1)$, each factor $a \neq \pm 1$ will have its inverse $b \neq a$ modulo p, so that the product ab will just give 1 modulo p. The remaining factors 1 and $(p-1)$ will multiply to give -1 modulo p. Therefore,

$$1.2.\cdots.(p-1) \equiv 1.(p-1) \equiv -1 \bmod p. \qquad \square$$

Wilson's Theorem

Theorem 2.18. *Let n be a positive integer such that*

$$(n-1)! \equiv -1 \text{ mod } n.$$

Then, n is a prime number.

Proof: Let n be a composite number. Then, $n = ab$ where $2 \leq a,\ b \leq n-1$. If $a \neq b$, both a and b occur as a factor in the product $1 \cdot 2 \cdot \dots \cdot (n-1)$, hence the product is divisible by n, and in this case

$$(n-1)! \equiv 0 \text{ mod } n.$$

If $a = b$, then $n = a^2$. If $2a < n$, then the product $1 \cdot 2 \cdot \dots \cdot (n-1)$ contains both a and $2a$ as factors, and hence $(n-1)!$ is divisible by $a^2 = n$. Again, we have

$$(n-1)! \equiv 0 \text{ mod } n.$$

The remaining case is $n = a^2$ where $2a \geq a^2$. Then, $a = 1$ or 2, and $n = 1$ or $n = 4$. If $n = 4$, we have $3! = 6 = 2$ mod 4. Thus,

$$\begin{aligned}
(n-1)! &\equiv 0 \text{ mod } n \quad \forall \text{ composite number } n > 4. \\
(4-1)! &\equiv 2 \text{ mod } 4 \text{ when } n = 4. \\
(1-0)! &\equiv 0 \text{ mod } 1.
\end{aligned}$$

This concludes the converse. $\square$