Important theorems

Abel Doñate

Contents

1 Fermat's little theorem

If a and p are coprimes, then:

$$a^{p-1} \equiv 1 \ (mod \ p)$$

Proof

Consider the set $S = \{a, 2a, \cdots, (p-1)a\}$.
Now we pick 2 elements of the set, for instance ka, la, with $1 \leq k < l \leq p-1$. We are going to show that necessarily $ka \not\equiv la \ (mod \ p)$. Let's prove it by contradiction:

If we suppose that it is true, then:

$$ka \equiv la \, (mod \, p) \implies p|(l-k)a \implies \begin{cases} p|a & \text{(impossible, they are coprimes)} \\ \text{or} \\ p|(l-k) & \text{(impossible, it is positive and less than } p\text{)} \end{cases}$$

So, it is proven by contradiction.
Thus, the residues of the elements of S must be different from each other, so the set of the elements of S in modulo p is $S_p = \{1, 2, \cdots, p-1\}$, as it has to have the same number of elements that S (the set does not has to be necessarily in order from S).

Now we multiply the elements of S and the elements of S_p. If we consider the residues modulo p of the results, they must be the same, because each element of S_p is the residue of one element of S. Then:

$$a \cdot 2a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1) \ (mod \ p) \implies a^{p-1}(p-1)! = (p-1)! \ (mod \ p)$$

Trivially $(p-1)!$ is coprime with p (they do not share any factor), so we can divide the expression by $(p-1)!$. As desired we end up with

$$a^{p-1} \equiv 1 \ (mod \ p)$$

$\square$

2 Wilson's theorem

Let p any prime. Then it holds:

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

Proof
First we are going to proof two Lemmas.

Lemma 1. If $a^2 \equiv 1 \ (mod\ p)$, then $a \equiv 1 \ (mod\ p)$ or $a \equiv 1 \ (mod\ p)$.
The proof of this lemma is following:

$$a^2 \equiv 1 \ (mod\ p) \implies p|a^2-1 \implies p|(a+1)(a-1) \implies \begin{cases} p|(a+1) \\ \text{or} \\ p|(a-1) \end{cases}$$

so, a must be 1 or -1 in modulo p.

Lemma 2. Every number between 2 and $p-2$ has a unique inverse that is not itself.
The proof is very simple. Using *Lemma 1*, the only numbers that could be its own inverse are 1 and -1. We know that, as every element must have an inverse ($\mathbf{Z_p}$ is a group), the inverse of the remaining elements must be different from themselves.

Now we are ready for the proof. If we take $(p-1)!$, we can split it in this way

$$(p-1)! = 1 \cdot (2 \cdot 3 \cdots (p-3) \cdot (p-2)) \cdot (p-1)$$

Observe that in the middle remains the numbers between 2 and $p-2$. Using *Lemma 2* we can pair the elements in pairs formed by one element and its inverse (that is not itself) so that the product is $1 \ (mod\ p)$. Finally multiplying by 1 and $(p-1)$ gives us

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

as desired.

$\square$