Simplifying Computations in the Finite Field $\mathbb{F}_p$

Edouard Roberts

June 2025

1 Abstract

The finite field $\mathbb{F}_p$, also denoted $\mathbb{Z}/p\mathbb{Z}$, where $p \in \mathbb{P}$, is a foundational object in modern algebra with widespread applications in number theory and in computer science. Its structure allows for elegant and simplified computations, particularly in the context of modular arithmetic and polynomial identities. One such identity is the simplification of the binomial expansion $(a+b)^p = a^p + b^p$ within the field. This identity is not only algebraically interesting but also closely tied to Fermat's Little Theorem.

The primary goal of this paper is to present a step-by-step derivation and proof of this identity for various small primes, provide a general proof using binomial coefficients and Pascal's Triangle, and ultimately connect it to Fermat's Little Theorem. This paper concludes with a discussion on why this property fails for composite moduli and explore practical motivations in computer science for studying such simplifications in $\mathbb{F}_p$.

The identity states that if $a \in \mathbb{F}_p$, $b \in \mathbb{F}_p$ and $p \in \mathbb{P}$, then in the finite field $\mathbb{F}_p$:

$$(a+b)^p = a^p + b^p$$

2 Clarifications

$\mathbb{P}$ represents the set of all prime numbers.
We define the finite field $\mathbb{F}_p$ as the set of integers modulo p, where $p \in \mathbb{P}$
The elements of $\mathbb{F}_p$ are represented by the equivalence classes $\{\overline{0}, \overline{1}, \overline{2} \ldots, \overline{p-2}, \overline{p-1}\}$.
Since arithmetic is done modulo p, we may use $=$ for equality of elements within the field $\mathbb{F}_p$. The use of $\equiv$ will be used for equivalence when talking about integers modulo p.

3 Proof for small p

Case $p = 2$

Let $p = 2$, then in $\mathbb{F}_2$ we get:

$$(a+b)^2 = a^2 + b^2$$

Proof. Note that:

$$2ab \equiv 0 \mod 2 \qquad \text{(because } 2 \mid 2ab\text{)}$$

So:

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$$

■

Case $p = 3$

Let $p = 3$, then in $\mathbb{F}_3$ we get:

$$(a+b)^3 = a^3 + b^3$$

Proof. Note that:

$$\begin{aligned} 3a^2b &\equiv 0 \mod 3 \qquad \text{(because } 3 \mid 3a^2b\text{)} \\ 3ab^2 &\equiv 0 \mod 3 \qquad \text{(because } 3 \mid 3ab^2\text{)} \end{aligned}$$

So:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3$$

■

Case $p = 5$

Let $p = 5$, then in $\mathbb{F}_5$ we get:

$$(a+b)^5 = a^5 + b^5$$

Proof. Note that:

$$\begin{aligned} 5a^4b &\equiv 0 \mod 5 \qquad \text{(because } 5 \mid 5a^4b\text{)} \\ 10a^3b^2 &\equiv 0 \mod 5 \qquad \text{(because } 5 \mid 10a^3b^2\text{)} \\ 10a^2b^3 &\equiv 0 \mod 5 \qquad \text{(because } 5 \mid 10a^2b^3\text{)} \\ 5ab^4 &\equiv 0 \mod 5 \qquad \text{(because } 5 \mid 5ab^4\text{)} \end{aligned}$$

So:

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 = a^5 + b^5$$

■

4 Pascal's Triangle

In general, we can conjecture that if all the coefficients in the binomial expansion of $(a+b)^p$ are divisible by p then the equality holds. A visual way to see that would be using Pascal's Triangle. If in the p-th row of the Pascal's Triangle, all numbers different then 1 are divisible by p, then the identity holds for that value of p It is easy to see on the following Pascal's Triangle that the rows where the property holds are the rows where p is prime.

$$\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \; 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \; 20 \; 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \; 35 \; 35 \; 21 \quad 7 \quad 1 \\
1 \quad 8 \quad 28 \; 56 \; 70 \; 56 \; 28 \quad 8 \quad 1
\end{array}$$

5 General Proof

We need to prove that: $\forall p \in \mathbb{P}, \forall a \in \mathbb{F}_p$ and $\forall b \in \mathbb{F}_p$ in the field $\mathbb{F}_p$

$$(a+b)^p = a^p + b^p$$

Proof. By the binomial theorem:

$$(a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n} = a^p + b^p + \sum_{n=1}^{p-1} \binom{p}{n} a^n b^{p-n}$$

So we must prove that:

$$\sum_{n=1}^{p-1} \binom{p}{n} a^n b^{p-n} \equiv 0 \mod p$$

Let $j \in \{1, 2, 3, \ldots, p-2, p-1\}$, then:

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} \Leftrightarrow \binom{p}{j} j!(p-j)! = p!$$

Since p appears as a factor in $p!$, we conclude that $p \mid p!$ so p must divide at least one of the terms of the left hand side.
Note that:

$$p \nmid j! \text{ because p > j and p is prime so p doesn't appear in j!}$$

$$p \nmid (p-j)! \text{ because p > p-j and p is prime so p doesn't appear in (p-j)!}$$

Therefore we get that: $\forall j \in \{1, 2, 3, \ldots, p-2, p-1\},\ p|\binom{p}{j}$.
Which proves that all the terms in the $\sum_{n=1}^{p-1} \binom{p}{n} a^n b^{p-n}$ are congruent to 0 modulo p. ■

6 A Proof of a Restricted Form of Fermat's Little Theorem

Using the aforementioned identity, we can prove a restricted form Fermat's Little Theorem which states that:
Let $p \in \mathbb{P}$, and $a \in \mathbb{F}_p$ such that $0 \leq a < p$, then:

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

Intuitively, we can observe it for small a's.
Note that we will be using the identity $(a+b)^p = a^p + b^p$ and that in the equation of a greater a's we may use results found for smaller a's
For $a = 0$, we get:

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

For $a = 1$, we get:

$$a^p = 1^p = 1 \equiv 1 \mod p$$

For $a = 2$, we get:

$$a^p = 2^p = (1+1)^p = 1^p + 1^p = 1 + 1 = 2 \equiv 2 \mod p$$

For $a = 3$, we get:

$$a^p = 3^p = (2+1)^p = 2^p + 1^p = 2 + 1 = 3 \equiv 3 \mod p$$

Proof. We proceed by induction on a.
Base case: Let $a = 0$. Then clearly:

$$0^p = 0 \equiv 0 \mod p$$

So the theorem holds for $a = 0$.
Induction: Suppose the statement holds $\forall a \in \{0, 1, 2, \dots, n-1, n\}$, where $n < p$.
We want to prove it holds for $a = n + 1$
By the binomial identity valid in $\mathbb{F}_p$, we have:

$$(n+1)^p \equiv n^p + 1^p \mod p$$

Using the inductive hypothesis $a^p \equiv a \mod p$, and noting that $1^p = 1$, we get:

$$(n+1)^p \equiv n + 1 \mod p$$

Thus, the theorem also holds for $a = n + 1$.
By induction, the statement holds $\forall a \in \{0, 1, 2, \dots, p-2, p-1\}$.

■

So for all elements of the field, Fermat's Little Theorems holds.

7 Generalising the identity for more terms

With the identity $(a+b)^p = a^p + b^p$, we have proven that exponentiation distributes over the addition of 2 terms in the field. We might now consider if the identity holds for additional terms. In the same way that multiplication distributes over addition in the reals, can we conjecture that exponentiation distributes over addition in the field $\mathbb{F}_p$.
We can prove that it works for 5 terms using the associative property of addition and by repeating the application of the identity for 2 terms.
Let $a \in \mathbb{F}_p$, $b \in \mathbb{F}_p$, $c \in \mathbb{F}_p$, $d \in \mathbb{F}_p$ and $e \in \mathbb{F}_p$, then in the field $\mathbb{F}_p$:

$$\begin{aligned}(a+b+c+d+e)^p &= (a+(b+c+d+e))^p = a^p + (b+c+d+e)^p \\ &= a^p + (b+(c+d+e))^p = a^p + b^p + (c+d+e)^p \\ &= a^p + b^p + (c+(d+e))^p = a^p + b^p + c^p + (d+e)^p \\ &= a^p + b^p + c^p + d^p + e^p\end{aligned}$$

Proof. We prove by induction on n in the following: For integer terms $x_1, x_2, \dots, x_n$ in $\mathbb{F}_p$,

$$\left(\sum_{i=1}^{n} x_i\right)^p = \sum_{i=1}^{n} x_i^p$$

Base Case: For $n=1$, then, trivially:

$$(x_1)^p = x_1^p$$

Induction: Let the identity be true for n=k, ergo:

$$\left(\sum_{i=1}^{k} x_i\right)^p = \left(\sum_{i=1}^{k} x_i^p\right)$$

We must prove that it holds true for $k+1$.

$$\left(\sum_{i=1}^{k+1} x_i\right)^p = \left(x_{k+1} + \sum_{i=1}^{k} x_i\right)^p = x_{k+1}^p + \left(\sum_{i=1}^{k} x_i\right)^p = x_{k+1}^p + \sum_{i=1}^{k} x_i^p$$

■

Using Fermat's Little Theorem which we proved previously for all elements of the field, we are left with this final version of the identity, which states that for any number of integer terms called $x_1, x_2, \dots, x_n$, in the field $\mathbb{F}_p$:

$$\left(\sum_{i=1}^{n} x_i\right)^p = \sum_{i=1}^{n} x_i^p = \sum_{i=1}^{n} x_i$$

8 Further Considerations

Naturally, one might ask why does it only work if p is prime? In cases were p is composite, we can easily see, via Pascal's Triangle, that p doesn't divide all the binomial coefficients. One might consider a connection with the fact that if p isn't prime then instead of a field, we get a ring. This is due to the loss of the multiplicative inverse property.

9 Practical Applications

Simplifying computations in finite fields, more particularly in $\mathbb{F}_p$ has many practical implications in computer science. In cryptography, for example, computations in $\mathbb{F}_p$ are used for encryption algorithm such as ECC. ECC is considered the standard in cryptography and protects the banking information of billions of people and also the secrets of many governments. Simplifying calculations in $\mathbb{F}_p$ could help data encryption or decryption. It is also used for error correction such as Reed–Solomon codes, which are used in digital formats like CDs, DVDs, and Blu-Rays.

10 Acknowledgements

In February 2025, I encountered a variant of this problem on MathStackExchange and then I wrote this proof. After the fact, I found many variants of this proof, most using the binomial theorem but others using cyclic operators. When I first tried to prove it, I had to try some cases and then I made a connection with the binomial theorem via Pascal's triangle. I then independently found a proof of a restricted Fermat's Little Theorem and thought to generalise to more than 2 terms. The following link is of the original post on MathStackExchange that inspired my interest in this identity: https://math.stackexchange.com/questions/3867463/in-the-ring-mathbbz-p-p-is-prime-abp-apbp-proof.