
FERMAT LITTLE THEOREM AND PERFECT NUMBERS

Denis TRYSTRAM

Maths for Computer Science – MOSIG 1 – 2018

1 Fermat little theorem

Statement:

Let p a prime

$a^p - a$ is divisible by p for any integer a .

Another way to write this theorem is $a^p \equiv a[p]$.

1.1 Classical proof

Before going to the proof, let us first establish a preliminary property on the binomial coefficients when p is prime that is clear while looking at the Pascal triangle in Figure 1: Apart the two extreme coefficients in the prime rows, all coefficients are multiples of p .

Looking from a different perspective (with Pascal triangles modulo primes) evidences the property. We detail it on two particular examples in Figures 2 and 3 (namely, for $p = 5$ and $p = 7$).

Let us compute the powers of $p = 7$ for the first successive integers:

$$1^7 \equiv 1[7]$$

$$2^7 = 128 = 7 \times 18 + 2 \equiv 2[7]$$

$$3^7 = 2187 = 7 \times 312 + 3 \equiv 3[7]$$

$$4^7 = 16384 = 7 \times 2340 + 4 \equiv 4[7]$$

$$5^7 = 78125 = 7 \times 11140 + 5 \equiv 5[7]$$

$$6^7 = 279936 = 7 \times 39990 + 6 \equiv 6[7]$$

This result reflects the core of the Theorem, that is: **the remainders by a prime of a number and its power to the same prime remains the same**. It can be proved more formally by applying the definition:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad (\text{for } 0 < k < p)$$

Thus, $k! \binom{p}{k} = p(p-1) \cdots (p-k+1)$.

p divides the product $k! \binom{p}{k}$ but it has no common divisor with $k!$ since $k < p$, thus, p divides $\binom{p}{k}$.

Proof. The classical proof is obtained by induction on a , applying the Newton binomial decomposition.

- The basis of the induction is straightforward since $1^p \equiv 1[p]$.

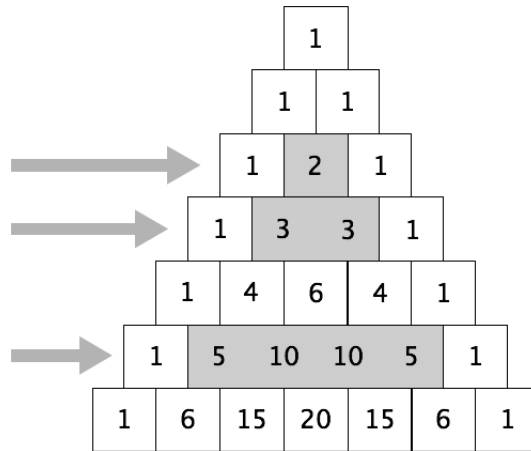


Figure 1: First rows of the Pascal's triangle, which show that the internal elements of the rows corresponding to primes are multiples of this prime.

- Assuming $a^p \equiv a[p]$ holds and let compute $(a + 1)^p$.

$$(a + 1)^p = a^p + 1 + \sum_{1 \leq k \leq p-1} a^k \binom{p}{k}$$

On the first hand, from the preliminary property, all *internal* binomial coefficients are divisible by p , thus, $\sum_{1 \leq k \leq p-1} a^k \binom{p}{k} = a.N.p$

On the second hand, applying the induction hypothesis says there exists an integer N' such that $a^p = a + N'.p$.

$$\text{Then, } (a + 1)^p = a.N.p + 1 + a + N'.p = (a + 1) + p.N''.$$

■

1.2 An alternative combinatorial proof

Consider an alphabet \mathcal{A} with a symbols.

- The number of words of length p built on the alphabet \mathcal{A} is equal to a^p .
- We define the circular permutation c of a word as taking the last symbol of this word and putting it in the first position. More formally:

$$c(\alpha_1 \alpha_2 \cdots \alpha_p) = \alpha_p \alpha_1 \cdots \alpha_{p-1}$$

We also define the *necklace* $\mathcal{N}(\omega)$ associated to a word ω as the set of successive images of ω by c . $\mathcal{N}(\omega) = \omega, c(\omega), c(c(\omega)), \dots$

The size of a necklace is the number of elements in $\mathcal{N}(\omega)$.

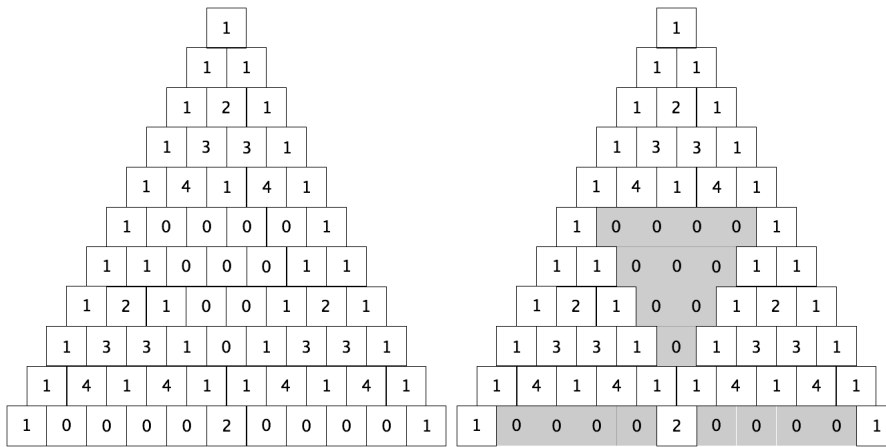


Figure 2: Pascal triangle modulo a prime (here $p = 5$) and its reproducible pattern.

The size of a necklace is always bounded by p since in the worst case, the circular permutation shift all the symbols before coming back to the original position.

If p is prime, the size of a necklace with at least 2 different symbols is p . This result comes by contradiction from the definition of primes that have no divisors lower than them.

Moreover, it is easy to see that the number of necklaces of size 1 is equal to a (there are the words where the symbols are all the same).

The proof of Fermat's little theorem with combinatorial arguments is a direct consequence of the previous properties since the number of necklaces of size p is equal to $a^p - a$.

2 Perfect numbers: Definitions

A perfect number (PN in short) is a number which is equal to the sum of its proper divisors.

For instance, the first perfect numbers are the following:

- 6, which has 3 proper divisors, namely, 1, 2 and 3.
 $1 + 2 + 3 = 6$.
- 28 whose 5 proper divisors are: 1, 2, 4, 7 and 14.
 $1 + 2 + 4 + 7 + 14 = 28$.
- 496 has 9 proper divisors, namely, 1, 2, 4, 8, 16, 31, 62, 124 and 248.

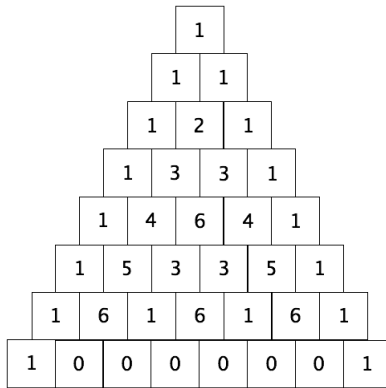


Figure 3: Pascal triangle modulo a prime ($p = 7$)

$$1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496.$$

A *Mersenne number* is a prime which has the following expression: $2^\alpha - 1$ for some given integer α .

For instance, $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$ are primes while $15 = 2^4 - 1$ is not prime... Obviously, there exist primes which are not Mersenne's numbers (like 5, 13, etc.).

Property 1.

$2^\alpha - 1$ is only prime if α is prime.

The proof is a direct consequence of the little Fermat theorem (proved in the last section).

The objective of the next section is to study some characterizations of perfect numbers.

Notice that it remains several open questions related to perfect numbers like the existence of odd PN or if there are an infinite number of such numbers.

3 Properties

We are now going to prove the main result:

Theorem (characterization of PN).

Let consider a prime α .

Let denote by PN_α the number obtained by the following expression: $2^{\alpha-1}(2^\alpha - 1)$ where $2^\alpha - 1$ is a prime.

PN_α is a perfect number and all the perfect numbers have this form.

Proof.

The list of factors F_i (for $0 \leq i \leq \alpha - 1$) of $2^{\alpha-1}$ is: $F_0 = 1, F_1 = 2, F_2 = 4, \dots, F_{\alpha-1} = 2^{\alpha-1}$.

The other factors of PN_α are obtained by: $F_i \cdot (2^\alpha - 1)$ for $i < \alpha - 1$.

Summing up all these factors, we obtain:

$$\begin{aligned} & \Sigma_{i=0, \alpha-1} 2^i + \Sigma_{i=0, \alpha-2} 2^i (2^\alpha - 1) \\ &= 2^{\alpha-1} + \Sigma_{i=0, \alpha-2} 2^i (1 + 2^\alpha - 1) \\ &= 2^{\alpha-1} + 2^\alpha (2^{\alpha-1} - 1) \\ &= 2^{\alpha-1} (1 + 2 \cdot 2^{\alpha-1} - 2) \\ &= 2^{\alpha-1} (2^\alpha - 1). \end{aligned}$$

This property was proved by Euclide in *Principae IX-36*.

Property 3.

The last digit of any perfect number (in usual decimal notation) is 6 or 8.

Property 4 (coding by the binary representation).

Give the binary representation of NP_3 and NP_5 .

Deduce the binary representation of NP_α .

$$PN_\alpha = (11\dots10\dots0)_2 \text{ (}\alpha \text{ times 1 followed by } \alpha - 1 \text{ times 0)}.$$

Property 5 (link with triangular numbers Δ_n).

It is easy to remark that $6 = \Delta_3$, verify that 28 is a triangular number.

Show more generally that $PN_\alpha = \Delta_{2^{\alpha-1}}$.

Proof.

The proof is straightforward by using the basic expression $\Delta_n = \frac{n(n+1)}{2}$ for $n = \alpha - 1$.

$$\Delta_{2^{\alpha-1}} = \frac{(2^\alpha - 1)(2^\alpha)}{2} = \frac{(2^\alpha - 1)(2^\alpha)}{2} = (2^\alpha - 1)2^{\alpha-1}$$