Fermat little theorem

Statement:

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

A combinatorial proof

The idea is to build an adequate set and to count its elements. Consider the set obtained by all the words of length p coded on the alphabet $\mathcal{A}$ with a symbols (p is prime).

- 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 by taking the last symbol of this word, putting it in the first position and shifting all the others to the right. 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 the successive images of ω by c, namely, $\mathcal{N}(\omega) = \omega, c(\omega), c(c(\omega)), \cdots$.

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

  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.

  As p is prime, the size of a necklace with at least 2 different symbols is exactly p.

  Fig. **??** depicts all the necklaces of size $p = 3$ on the alphabet $\{A, B, C\}$. Indeed, it is easy to prove this by contradiction using the definition of primes that have no divisors lower than themselves.

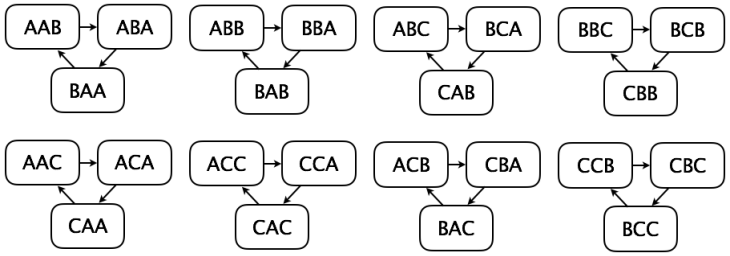

Figure 1: 8 groups of necklaces of size $p = 3$ (for $a = 3$).

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 (see Fig. **??**).

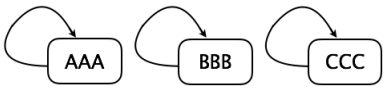

Figure 2: The 3 necklaces composed of the the same symbol ($a = 3$)

The proof of Fermat little theorem with combinatorial arguments is a direct consequence of the previous properties since the number of necklaces of size p is equal to $a^p - a$ (both terms are multiple of p).