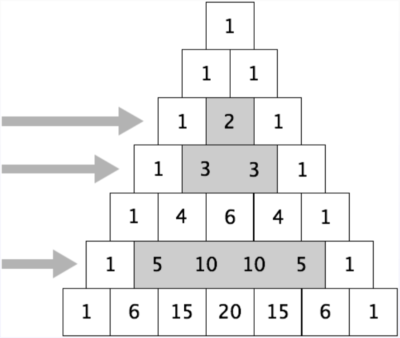
Training Lecture 5 – Maths for Computer Science
Proving the little Fermat Theorem

Denis TRYSTRAM
MoSIG1

nov. 2019

A preliminary property

Draw the first rows of Pascal's triangle and focus on rows corresponding to prime numbers.



Guess a property of the internal elements of such rows.

Looking at the first rows of the Pascal's triangle shows that **the internal elements of the rows corresponding to primes are multiple of this prime** (in the previous figure: row 2, 3 and 5).

Showing the same from another perspective...

Draw the Pascal's triangle modulo primes.

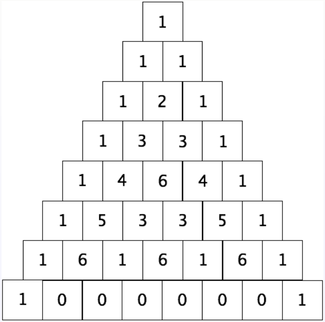


Figure: Example of Pascal triangle modulo a prime for $p = 7$

Proof of the statement

As the meaning of the internal elements of the Pascal's triangle is $\binom{p}{k}$ we prove formally that it is a multiple of p...

...by simply applying the definition:
$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ (for $0 < k < p$)

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

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

Coming back to the central result...

Let us start by some observations:

$1^7 \equiv 1[7]$
$2^7 = 128 = 7 \times 18 + 2 \equiv 2[7]$
$3^7 = 2187 = 7 \times 312 + 3 \equiv 3[7]$
$4^7 = 16384 = 7 \times 2340 + 4 \equiv 4[7]$
$5^7 = 78125 = 7 \times 11140 + 5 \equiv 5[7]$
$6^7 = 279936 = 7 \times 39990 + 6 \equiv 6[7]$

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

Little Fermat Theorem

The proof is by induction on a (for a given p).
Let assume this property is true up to a, and compute $(a+1)^p$ and apply the Newton binomial decomposition:

- The basis of the induction is straightforward since $1^p \equiv 1[p]$.
- $(a+1)^p = a^p + 1 + \Sigma_{1 \leq k \leq p-1} a^k \binom{p}{k}$

  On the first hand, from the preliminary property, all *internal* binomial coefficients are divisible by p
  thus, $\Sigma_{1 \leq k \leq p-1} a^k \binom{p}{k} = a.N.p$
  On the second hand, applying the induction hypothesis says there exists an integer N' such that $a^p = a + N'.p$.
  Then, $(a+1)^p = a + 1 + (a.N + N').p$.