Petit Théorème de Fermat

Lemme

Ce théorème débute avec un lemme.

Lemme : Pour $1 < i < p$ avec p premier, $\binom{p}{i}$ est divisible par p

Preuve

Rappelons la définition de $\binom{p}{i}$:

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

$p! = \binom{p}{i} i!(p-i)!$ Donc sachant que p divise $p!$, p divise aussi $\binom{p}{i} i!(p-i)!$

p est premier et $1 < i < p$ donc $p \wedge i!(p-i)! = 1$. ($i!(p-i)!$ est un produit de facteurs tous $< p$)

D'après le théorème de Gauss $p \wedge i!(p-i)! = 1$ implique p divise $\binom{p}{i}$

Théorème

(Petit théorème de Fermat) Soit a un entier relatif et p un nombre premier.

Alors $a^p \equiv a[p]$

De plus si $a \wedge p = 1$ alors $a^{p-1} \equiv 1[p]$

Preuve

- Supposons a entier naturel et démontrons par récurrence sur a que $a^p \equiv a[p]$

- Initialisation : Pour $a = 1$ Nous avons $1^p \equiv 1[p]$

Hérédité : Supposons $a^p \equiv a[p]$

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

Nous avons vu d'après le lemme précédent que pour $1 < i < p$, $p \mid \binom{p}{i}$.

Donc $\binom{p}{i} \equiv 0[p]$.

Il vient $(a+1)^p \equiv \binom{p}{0} a^0 + \binom{p}{p} a^p \equiv 1 + a^p \equiv 1 + a[p]$ (d'après l'hypothèse de récurrence)

L'hérédité est ainsi montrée.

Nous avons donc pour a entier naturel, $a^p \equiv a[p]$

Si a est négatif alors $a = -|a|$

$$a^p \equiv (-|a|)^p \equiv (-1)^p (|a|)^p [p].$$

p étant premier peut être égal à 2 ou à un nombre impair.

S'il est impair $(-1)^p = -1$ donc $a^p \equiv -(|a|)^p \equiv -|a| \equiv a[p]$.

Soit $p = 2$ et dans ce cas quelque soit le signe de a , si a est pair, alors a^2 est pair et si a est impair alors a^2 est impair ce qui implique $a^2 \equiv a[2]$.

Bref dans tous les cas $a^p \equiv a[p]$ aussi pour a négatif ce qui rend la propriété vraie pour a entier relatif.

Il nous reste à démontrer si $a \wedge p = 1$ alors $a^{p-1} \equiv 1[p]$

$a^p \equiv a[p] \Rightarrow a^p - a \equiv 0[p] \Rightarrow a(a^{p-1} - 1) \equiv 0[p] \Rightarrow a(a^{p-1} - 1) = kp$ avec k entier relatif.

Donc $p \mid a(a^{p-1} - 1)$. Si $a \wedge p = 1$ d'après le théorème de Gauss $p \mid (a^{p-1} - 1)$

Donc $a^{p-1} - 1 \equiv 0[p] \Rightarrow a^{p-1} \equiv 1[p]$

Exemple

Nous allons montrer que pour tout n entier naturel non nul, $n^{13} - n$ est divisible par 13; 7; 5; 3 et 2.

- Le petit théorème de Fermat nous dit que 13 étant premier $n^{13} - n \equiv 0[13]$ donc $n^{13} - n$ est divisible par 13.
- $n^{13} - n = n(n^{12} - 1) = n(n^6 - 1)(n^6 + 1) = (n^7 - n)(n^6 + 1)$
7 étant premier $n^7 - n \equiv 0[7]$ donc $n^{13} - n \equiv 0[7]$ donc $n^7 - n$ est divisible par 7.
- $n^{13} - n = n(n^{12} - 1) = n(n^6 - 1)(n^6 + 1) = n(n^3 - 1)(n^3 + 1)(n^6 + 1) =$
 $n(n - 1)(1 + n + n^2)(n + 1)(1 - n + n^2)(n^6 + 1) =$
 $n(n - 1)(n + 1)(1 + n + n^2)(1 - n + n^2)(n^6 + 1)$
Soit n soit $n - 1$ sont pairs donc 2 divise $n^{13} - n$
Soit $n - 1$, soit n , soit $n + 1$ est divisible par 3 donc 3 divise $n^{13} - n$
- Si n est multiple de 5 $n^{13} - n$ est multiple de 5
Si n n'est pas multiple de 5 alors $n^4 \equiv 1(5) \Rightarrow n^6 \equiv n^2(5)$
Donc $n^6 - 1 \equiv n^2 - 1(5)$ et $n^6 + 1 \equiv n^2 + 1(5)$
Donc $n^{13} - n = n(n^6 - 1)(n^6 + 1) \equiv n(n^2 - 1)(n^2 + 1)(5) \equiv n(n^4 - 1)(5) \equiv 0(5)$
Donc 5 est un diviseur de $n^{13} - n$