Résultats d'arithmétique.

Petit théorème de Fermat.

Monier MPSI 4.4.50 p114

Soit p premier, montrer que $\forall n \in \mathbb{Z} \quad n^p \equiv n \, [p]$

En déduire $\forall n \in \mathbb{Z} \quad (p \nmid n \Rightarrow n^{p-1} \equiv 1 \, [p])$

Lemme : Soit p premier, $k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$

pour $k \in [\![1, p-1]\!]$ $\quad \binom{p}{k} = \dfrac{p(p-1)(p-2)\dots(p-k)}{k!} = \dfrac{p}{k} \dfrac{(p-1)\dots(p-k)}{(k-1)!}$

d'où $\binom{p}{k} = \dfrac{p}{k}\binom{p-1}{k-1}$

$k\binom{p}{k} = p\binom{p-1}{k-1}$ et $p \nmid k$ $(p \wedge k = 1)$

donc $p \mid \binom{p}{k}$ (théorème de Gauss)

1) Montrons le résultat par récurrence sur n.

$$\forall n \in \mathbb{N} \quad n^p \equiv n \, [p] \qquad ①$$

La propriété est évidente pour $n = 0$

Supposons-la vraie pour un $n \in \mathbb{N}$.

$$(n+1)^p \equiv n^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} n^k}_{p \mid \binom{p}{k}} + 1$$

$$\equiv n^p + 1 \underset{(rec)}{\equiv} n + 1 \, [p]$$

2) Soit $n \in \mathbb{Z}_-$.

Si p est impair $\quad n^p = -(-n)^p \underset{①}{\equiv} -(-n) = n$

Si $p = 2 \quad n^2 = (-n)^2 \underset{[2]}{\equiv} -n \underset{[2]}{\equiv} n$.

b) Soit $n \in \mathbb{Z}$ tq $p \nmid n$ comme p est premier, on a $n \wedge p = 1$

On peut simplifier dans la relation de congruence par n

$$n^p \equiv n [p] \Rightarrow n^{p-1} \equiv 1 [p]$$

Théorème de Wilson. Merci DPS 4.4 GT p115

a) Soit p premier. Montrer dans l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$

$$X^{p-1} - \bar{1} = \prod_{k=1}^{p-1} (X - \bar{k})$$

En déduire le théorème de Wilson

Si p premier alors $(p-1)! \equiv -1 [p]$

b) Réciproquement, montrer par tout n que si $(n-1)! \equiv -1 (n)$ alors n est premier

Déf

a) D'après le th de Fermat

$$\forall y \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \quad y^{p-1} = \bar{1} \quad (\text{mod Wilson } p)$$

Le polynôme $X^{p-1} - \bar{1}$, de $\mathbb{Z}/p\mathbb{Z}[X]$ est de degré $p-1$

et admet $\bar{1}, \bar{2}, \dots, \overline{p-1}$ pour zéros 2 à 2 distincts

donc $X^{p-1} - \bar{1} = \prod_{k=1}^{p-1} (X - \bar{k})$

En remplaçant X par 0, on obtient $-\bar{1} \equiv \prod_{k=1}^{p-1} (-\bar{k}) = (-1)^{p-1} (p-1)! \; [p]$

Si p est impair alors $(p-1)! \equiv -1 (p)$

Si p est pair $(p-1)! = 1 \equiv -1 (2)$

donc $(p-1)! \equiv -1 [p]$

b) Supposons n composé. Il existe $a \in \mathbb{N}^*$ tq $2 \leq a \leq n-1$ et $a | n$

alors $a | (n-1)!$ et $a | n$ donc $(n-1)! \not\equiv -1 (n)$