

THÉORÈME DE WILSON

L'objectif est de démontrer que : p premier $\Leftrightarrow (p-1)! \equiv -1 [p]$

Lorsque p est premier, on pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (\mathbb{F}_p est donc un corps)

1. a) Comparer les polynômes P et Q de $\mathbb{F}_p[X]$ définis par :

$$P = (X - \bar{1})(X - \bar{2}) \dots (X - \overline{p-1}) \quad \text{et} \quad Q = X^{p-1} - \bar{1}$$

(Pour rechercher les racines de Q , on pourra utiliser le théorème de Fermat)

b) En déduire que : $(p-1)! \equiv -1 [p]$

2. Réciproquement, on suppose maintenant que n est un entier vérifiant : $(n-1)! \equiv -1 [n]$.

a) Démontrer que le produit $\bar{1} \times \bar{2} \times \dots \times \overline{n-1}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

b) En déduire que $\mathbb{Z}/n\mathbb{Z}$ est un corps et conclure.

1. On suppose que p est premier. $\mathbb{F}_p = \{ \bar{0} ; \bar{1} ; \dots ; \overline{p-1} \}$ est donc un corps.

a) Rappelons que dans un corps, un polynôme de degré n a au plus n racines.

Le polynôme P est de degré $p-1$ et possède les $p-1$ racines suivantes :

$$\bar{1} ; \dots ; \overline{p-1}$$

Le polynôme Q est aussi de degré $p-1$ donc possède au plus $p-1$ racines.

Soit $\bar{a} \in \mathbb{F}_p^*$; p ne divise pas a sinon on aurait $a \equiv 0 [p]$, c'est-à-dire $\bar{a} = \bar{0}$ ce qui n'est pas le cas.

Comme p est premier et ne divise pas a , on a d'après le théorème de Fermat :

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

Autrement dit : $\bar{a}^{p-1} = \bar{1}$

Donc \bar{a} est une racine du polynôme Q . Donc Q possède les $p-1$ racines suivantes :

$$\bar{1} ; \dots ; \overline{p-1}$$

Les polynômes P et Q sont de même degré, possèdent les mêmes racines. Et puisqu'ils sont tous deux unitaires, ils sont donc égaux :

$$P = Q$$

b) Si $p = 2$, l'égalité est évidente. Supposons désormais $p \geq 3$.

Nous pouvons identifier les coefficients constants de P et Q . Pour P , c'est :

$$(-1)^{p-1} \bar{1} \times \bar{2} \times \dots \times \overline{p-1}$$

Pour Q , c'est : $-\bar{1}$. Comme p est impair, on a $(-1)^{p-1} = 1$ d'où :

$$\bar{1} \times \bar{2} \times \dots \times \overline{p-1} = -\bar{1}$$

Autrement dit : $(p-1)! \equiv -1 [p]$

2. Réciproquement, soit n un entier vérifiant : $(n-1)! \equiv -1 [n]$.

a) Plaçons nous dans $\mathbb{Z}/n\mathbb{Z}$. Par hypothèse, on a :

$$\bar{1} \times \bar{2} \times \dots \times \overline{n-1} = -\bar{1}$$

Or $-\bar{1}$ est toujours inversible dans $\mathbb{Z}/n\mathbb{Z}$. (En effet : $(-\bar{1}) \times (-\bar{1}) = \bar{1}$, donc $-\bar{1}$ est son propre inverse)

Donc le produit $\bar{1} \times \bar{2} \times \dots \times \overline{n-1}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

b) Il existe donc $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ tel que : $\bar{1} \times \bar{2} \times \dots \times \overline{n-1} \times \bar{k} = \bar{1}$

Chaque facteur $\bar{1}; \bar{2}; \dots; \overline{n-1}$ est donc inversible dans $\mathbb{Z}/n\mathbb{Z}$, ce qui en fait un corps, donc n est premier.

Variante : on peut traiter cette réciproque à l'aide du théorème de Bézout :

Puisque n divise $(n-1)! + 1$, il existe un entier u tel que :

$$(n-1)! + 1 = nu$$

$$nu - (n-1)! = 1$$

Pour tout $k \in \llbracket 1 ; n-1 \rrbracket$, on peut trouver un entier v tel que $kv = (n-1)!$ (puisque k divise $(n-1)!$) d'où :

$$nu - kv = 1$$

D'après le théorème de Bézout, n est donc premier avec tout entier k compris entre 1 et $n-1$ donc n est premier.

Conclusion : on a démontré le théorème de Wilson :

$$p \text{ est premier} \Leftrightarrow (p-1)! \equiv -1 [p]$$