CTD17: MD.

Nombres premiers

Définit°:

Un entier $p>1$ est dit premier si tous ses diviseurs sont ± 1; $\pm p$.

Notat°:

L'ensemble des nombres premiers se note $\mathcal{P}$

Exercice 4.21. Prouver qu'il y a une infinité de nombres premiers.

On suppose que $\mathcal{P}$ est fini, càd $\mathcal{P}=\{p_1;p_2;\dots;p_n\}$

Alors, le nombre $p=p_1p_2\dots p_n$ est divisible par tous les éléments de $\mathcal{P}$.

Regardons le nombre $P=p_1p_2\dots p_n+1$.

Alors, P n'est divisible par aucun élément $p_i\in\mathcal{P}$ car $p_i\geq 2$.

Donc P n'admet que P et 1 comme diviseurs, donc P est premier.

Or, $P\notin\mathcal{P}$. Contradict° ! Donc $\mathcal{P}$ n'est pas fini.

Exercice 4.22. Soit p un nombre premier. Montrer que, pour tout entier k avec $1<k<p$, on a $\binom{p}{k}\equiv 0 \mod p$. En déduire que si a et b sont deux entiers, on a $(a+b)^p\equiv a^p+b^p \mod p$.

$$\binom{p}{k}=\frac{p!}{(p-k)!\,k!} \quad . \quad p!=(p-k)!\,k!\binom{p}{k}$$

$$\Rightarrow p\mid(p-k)!\,k!\binom{p}{k},$$

Comme $k<p$, $p\nmid 1\dots k$

Donc $p\nmid k!$ Donc $PGCD(p,k!)=1$

pareil pour $p\nmid(p-k)!$

Donc $p\mid\binom{p}{k}$

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

$$\Rightarrow (a+b)^p \equiv a^p + \cancel{\binom{p}{1} a^{p-1}} b + \dots + \cancel{\binom{p}{k-1} a^{p-k+1}} b^{p-1} + b^p \mod p$$

$$\equiv a^p + b^p \mod p.$$

Θm de Gauss tout $n \in \mathbb{N}$, $n \geqslant 1$ se factorise de manière unique.

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_m^{\alpha_n}$$