Nombres premiers. Cours

Théorèmes Nombres premiers	
Théorème	C'est le théorème de Gauss appliqué aux nombres premiers. Soient a et b deux entiers relatifs non nuls. Soit p nombre premier. Alors p divise a ou b
Preuve	
Supposons que p ne divise pas a. Alors p et a sont premiers entre eux. Donc d'après le théorème de Gauss p divise b	
Exemple	$7150 = 13 * 550$ donc 13 divise 7150. Mais $7150 = 143 * 50$. 13 ne divise pas 50 donc 13 divise 143
Théorème	Il existe une infinité de nombres premiers.
Preuve	
Supposons qu'il en existe un nombre fini. Soient $p_1, p_2 \dots p_n$ ces nombres. Construisons le nombre $m = p_1 p_2 \dots p_n + 1$ m admet un diviseur premier donc un des $p_1, p_2, \dots . p_n$. Supposons que ce soit p_i Nous avons $m = p_i * M$ De plus $p_1 p_2 \dots p_{i-1} p_i p_{i+1} \dots p_n = p_i * p_1 p_2 \dots p_{i-1} p_{i+1} \dots p_n$ Donc $1 = m - p_1 p_2 \dots p_n = p_i * M - p_i * p_1 p_2 \dots p_{i-1} p_{i+1} \dots p_n = p_i(M - p_1 p_2 \dots p_{i-1} p_{i+1} \dots p_n)$ Nous en sommes arrivés à la conclusion que p_i divise 1. Ce n'est pas possible. L'hypothèse de départ est donc fausse. Le nombre de nombres premiers est donc bien infini.	
Théorème	Tout nombre entier naturel supérieur ou égal à 2 peut se décomposer de manière unique en produit de facteurs premiers. Autrement dit : Pour tout $n \in \mathbb{N}$ et $n \geq 2$ il existe m nombres premiers $p_1, p_2, \dots . p_m$ et m entiers naturels $\alpha_1, \alpha_2, \dots \alpha_m$ tels que $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$
Preuve	
Nous allons montrer dans un premier temps l'existence d'une telle décomposition et dans un deuxième temps l'unicité. L'existence d'une telle décomposition se fait par récurrence. Soit la propriété suivante $P(n)$: n peut se décomposer en produit de facteurs premiers. $P(2)$ est vraie puisque 2 est premier. La récurrence est donc initialisée. Supposons $P(3), P(4) \dots . P(n)$ vraies et montrons $P(n+1)$ Si $n+1$ est premier alors $P(n+1)$ est vérifiée. Supposons $P(n+1)$ non premier. Alors il existe d premier tel que $n+1 = d * D$ $D < n+1$ donc $P(D)$ est vérifiée. D peut s'écrire comme produit de facteurs premiers. il existe m nombres premiers $p_1, p_2, \dots . p_m$ et m entiers naturels $\alpha_1, \alpha_2, \dots \alpha_m$ tels que $D = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$ Il vient $n+1 = d * D = d * {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$ les nombres $d, p_1, p_2, \dots .$ et p_m étant premiers. $P(n+1)$ est donc vérifiée. La propriété est donc vraie quelque soit n. Montrons maintenant l'unicité. Supposons qu'il existe deux décompositions de n $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$ et $n = {q_1}^{\beta_1} {q_2}^{\beta_2} \dots {q_M}^{\beta_M}$ Supposons maintenant qu'un des p_i de la première décomposition ne se retrouve pas dans la liste des q_j Quitte à les réordonner on peut supposer que ce soit p_1 $p_1 \mid {q_1}^{\beta_1} \dots {q_M}^{\beta_M}$; p_1 est premier avec ${q_1}^{\beta_1}$ donc d'après le théorème de Gauss $p_1 \mid {q_2}^{\beta_2} \dots {q_M}^{\beta_M}$ En réitérant le processus : p_1 est premier avec ${q_2}^{\beta_2}$ donc d'après le théorème de Gauss $p_1 \mid {q_3}^{\beta_3} \dots {q_M}^{\beta_M}$ Puis encore et encore nous arrivons à $p_1 \mid {q_M}^{\beta_M}$ ce qui est une contradiction. L'hypothèse de départ est donc invalidée. Tous les p_i sont dans la décomposition des ${q_1}^{\beta_1} {q_2}^{\beta_2} \dots {q_M}^{\beta_M}$ et tous les q_i sont dans la décomposition des ${p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$. Il existe donc $\alpha_1, \alpha_2, \dots \alpha_m$ et $\beta_1, \beta_2, \dots \beta_m$ tels que $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m} = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_m}^{\beta_m}$ $(*)$ Supposons que $\alpha_1 \neq \beta_1$. Nous avons par exemple $\alpha_1 > \beta_1$ En simplifiant $(*)$ par ${p_1}^{\beta_1}$ il vient ${p_1}^{\alpha_1 - \beta_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m} = {p_2}^{\beta_2} \dots {p_m}^{\beta_m}$ Nous en déduisons que p_1 divise ${p_1}^{\alpha_1 - \beta_1} {p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$ donc divise aussi ${p_2}^{\beta_2} \dots {p_m}^{\beta_m}$ ce qui est impossible pour des raisons déjà évoquées plus haut. L'hypothèse de départ est donc invalidée. $\alpha_1 = \beta_1$ et de même $\alpha_i = \beta_i$ quelque soit i. L'unicité de la décomposition est donc démontrée.	
Exemple	$5\,040 = 2^4 \times 3^2 \times 5 \times 7$ et $22\,425 = 3 \times 5^2 \times 13 \times 23$

Théorème	Tout nombre entier naturel n dont la décomposition est ${p_1}^{\alpha_1}{p_2}^{\alpha_2}\dots{p_m}^{\alpha_m}$ admet $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$ diviseurs.

Preuve

Pour des raisons déjà évoquées dans les preuves précédentes tout diviseur de ${p_1}^{\alpha_1}{p_2}^{\alpha_2}\dots{p_m}^{\alpha_m}$ est de la forme ${p_1}^{\beta_1}{p_2}^{\beta_2}\dots{p_m}^{\beta_m}$ avec $0 \le \beta_i \le \alpha_i$ quelque soit i entre 1 et m
Chaque β_i pouvant prendre donc α_i+1 valeurs, le nombre de diviseurs de n est égal à $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$

Exemple	Reprenons les décompositions précédentes : $5\,040 = 2^4\times3^2\times5\times7$ et $22\,425 = 3\times5^2\times13\times23$ Le nombre de diviseurs de $5\,040$ est donc égal à $5*3*2*2=60$ Le nombre de diviseurs de $22\,425$ est donc égal à $2*3*2*2=24$
Propriété	Un nombre entier admettant un nombre impair de diviseurs est un carré.

Preuve

Si le produit $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$ est impair cela signifie que chaque (α_i+1) est impair. Donc α_i est pair.
SI tous les α_i sont pairs, cela signifie que n est un degré.

Théorème	C'est le petit théorème de Fermat. Soit p un nombre premier. Soit a un entier naturel alors : $$\boldsymbol{a^p \equiv a\ (p)}$$ Si en plus p ne divise pas a alors : $$\boldsymbol{a^{p-1} \equiv 1\ (p)}$$

Preuve

Commencons pas un lemme : Pour p premier $\binom{k}{p} \equiv 0(p)\ ssi\ 1 \le k \le p-1$
Remarquons que si $k=0$ ou si $k=p$, $\binom{k}{p}=1$
Lorsque $1 \le k \le p-1$; $\binom{k}{p} = \frac{p!(p-k)!}{k!} = p(p-1)\dots(p-k+1)(p-k)!$
Donc $\binom{k}{p} \equiv 0(p)\ ssi\ 1 \le k \le p-1$

Montrons d'abord la première partie tu théorème $a^p \equiv a\ (p)$ par récurrence sur
Par récurrence sur a.
Le cas $a=1$ est évident.
Supposons que la propriété soit vraie à l'ordre a : $a^p \equiv a\ (p)$
Essayons de la démontrer à l'ordre $a+1$:

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

Utilisons maintenant le lemme, $(a+1)^p \equiv a^p + 1^p \equiv a^p + 1(p)$
L'hypothèse de récurrence nous permet d'affirmer que $a^p \equiv a\ (p)$ il vient donc $(a+1)^p \equiv a+1\ (p)$
L'hypothèse de récurrence est donc vérifiée aussi à l'ordre $a+1$
Elle est donc vraie quelque soit a : $\forall a \in \mathbb{N}, a^p \equiv a\ (p)$

$$a^p \equiv a(p) \Rightarrow a(a^{p-1}-1) = 0(p) \Rightarrow p \mid a(a^{p-1}-1)$$

Or p premier donc d'après le théorème de Gauss cela implique : $\begin{Bmatrix} p \mid a \\ ou \\ p \mid (a^{p-1}-1) \end{Bmatrix}$.

Dans le cas où p ne divise pas a nous avons donc $p \mid (a^{p-1}-1) \Rightarrow a^{p-1}-1 \equiv 0(p) \Rightarrow a^{p-1} \equiv 1(p)$

Exemple	17 est premier donc $5^{17} \equiv 5(17)$. De plus 17 ne divise pas 5, donc $5^{16} \equiv 1(17)$