

## Nombres premiers. Cours

Nombres premiers	
<b>Définition</b>	Un nombre premier est un entier naturel qui ne possède que deux diviseurs : un et lui-même.
<b>Remarques</b>	<ul style="list-style-type: none"> <li>• 1 n'est pas premier car il ne possède qu'un seul diviseur : lui-même</li> <li>• Les nombres premiers inférieurs à 20 sont 2, 3, 5, 7, 11, 13, 17, 19</li> <li>• A part 2, tous les nombres premiers sont impairs.</li> </ul>
<b>Théorème</b>	Tout entier naturel $n$ tel que $n \geq 2$ admet un diviseur premier $p$
Preuve	
<p>Par récurrence. Soit la propriété <math>P(n)</math> : Tout entier naturel <math>n</math> tel que <math>n \geq 2</math> admet un diviseur premier <math>p</math></p> <p>Pour <math>n = 2</math> alors 2 divise 2 donc oui <math>P(n)</math> est vérifiée, la propriété est initialisée.</p> <p>Supposons <math>P(2), P(3), \dots, P(n)</math>, vraies et montrons que <math>P(n + 1)</math> est aussi vraie.</p> <p>Si <math>n + 1</math> est premier alors c'est fini. En effet <math>n + 1</math> divise <math>n + 1</math> et donc <math>P(n + 1)</math> est aussi vraie.</p> <p>Si <math>n + 1</math> n'est pas premier. Alors il admet un diviseur <math>d</math> tel que <math>1 &lt; d &lt; n + 1</math>. <math>n + 1 = dd'</math></p> <p>Mais <math>P(d)</math> étant vérifiée, il existe un nombre premier <math>p</math> qui divise <math>d</math>. Il divise donc aussi <math>n + 1</math>. <math>P(n + 1)</math> est aussi vraie.</p> <p>Par conséquent tout entier naturel <math>n</math> tel que <math>n \geq 2</math> admet un diviseur premier <math>p</math></p>	
<b>Théorème</b>	Tout entier naturel $n$ non premier tel que $n \geq 2$ admet un diviseur premier $p$ tel que $p \leq \sqrt{n}$
Preuve	
<p>Supposons que tous les diviseurs premiers de <math>n</math> soient strictement supérieurs à <math>\sqrt{n}</math>.</p> <p>Soit <math>p</math> un de ces diviseurs. <math>n = pp'</math></p> <p>Nous avons <math>p' \leq \sqrt{n}</math>. En effet si <math>p' &gt; \sqrt{n}</math> et <math>p &gt; \sqrt{n}</math> alors <math>pp' &gt; n</math> ce qui serait fâcheux puisque <math>n = pp'</math></p> <p>Donc <math>p' \leq \sqrt{n}</math>. D'après le théorème précédent <math>p'</math> admet un diviseur premier <math>m</math>. Ce diviseur est inférieur ou égal à <math>\sqrt{n}</math> ce qui est contradictoire à l'hypothèse de départ.</p>	
<b>Remarque</b>	Le dernier théorème induit dans le crible d'Eratosthène : procédé bien connu pour savoir si un nombre est premier ou non qui permet d'éviter de nombreux calculs inutiles. Prenons un nombre $n$ . Nous élaborons la liste des nombres premiers inférieurs ou égaux à $\sqrt{n}$ . Si tous ces nombres ne divisent pas $n$ , alors $n$ est premier.
<b>Exemple</b>	Nous voulons savoir si le nombre 127 est premier. $\sqrt{127} \approx 11,2$ $\sqrt{127}$ n'est pas divisible par 2, 3, 5, 7, 11. Donc 127 est premier.
<b>Théorème</b>	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 $b$	