## Note sur le théorème de Fermat

Etudiant les diviseurs des nombres de la forme $a^p - a$, j'ai été amené incidemment à énoncer un théorème, qui me paraît inédit, et qui généralise le théorème de Fermat.

Je rappellerai d'abord le théorème de Fermat en question :

Théorème de Fermat : $p$ étant un nombre premier et $a$ un nombre quelconque, on a la congruence :

$$a^p - a \equiv 0 \pmod{p}.$$

Si, de plus, $a$ n'est pas divisible par $p$, on a : $a^{p-1} - 1 \equiv 0 \pmod{p}$.

Cela étant, soit $p$ et $a$ deux entiers quelconques, $q$ un diviseur de $p - 1$, on a en posant : $p - 1 = qd$ :

$$a^{p-1} - 1 = a^{qd} - 1 = (a^d)^{(q+1)-1} - 1.$$

Supposons alors que $q + 1$ soit premier et que $a$, donc $a^d$, ne soit pas divisible par $q + 1$ le théorème de Fermat donne :

$$(a^d)^{(q+1)-1} - 1 \equiv 0 \ [\text{mod. } (q+1)]$$

c'est-à-dire : $$a^{p-1} - 1 \equiv 0 \ [\text{mod. } (q+1)].$$

Si $a$ est divisible par $q + 1$, on a évidemment :

$$a^p - a \equiv 0 \ [\text{mod. } (q+1)],$$

A condition que $q + 1$ soit premier, on a donc dans tous les cas :

$$a^p - a \equiv 0 \ [\text{mod. } (q+1)].$$

D'où le théorème annoncé.

Théorème : $p$ et $a$ étant deux entiers quelconques, si $q$ est un diviseur de $p - 1$ tel que $q + 1$ soit premier, on a la congruence :

$$a^p - a \equiv 0 \ [\text{mod. } (q+1)].$$

Si, de plus, $a$ n'est pas divisible par $q + 1$, on a :

$$a^{p-1} - 1 \equiv 0 \ [\text{mod. } (q+1)].$$

*Exemple :* $p = 25$, $p - 1 = 24$, $q = 1, 2, 3, 4, 6, 8, 12, 24$, d'où les valeurs de $q + 1$ premières : 2, 3, 5, 7, 13. On a donc :

$$a^{25} - a \equiv 0 \text{ (mod. : } 2.3.5.7.13) \text{ quel que soit } a.$$

*Cas particulier :* p *est un nombre de Fermat,* c'est-à-dire de la forme : $p = 2^{2^m} + 1$.

On a alors : $p - 1 = 2^{2^m}$ et tous les diviseurs de $p - 1$ sont de la forme $q = 2^h$, donc $q + 1 = 2^h + 1$. Or, on sait qu'une condition nécessaire (mais non suffisante) pour que $2^h + 1$ soit premier est que $h = 2^k$ ; les nombres $q + 1$ qui sont premiers sont donc de la forme $2^{2^k} + 1$ et par suite sont eux-mêmes des nombres de Fermat. Donc :

(Théorème) : Si $p$ est un nombre de Fermat (premier ou non) et $a$ un entier quelconque, le nombre $a^p - a$ est divisible par tous les nombres de Fermat premiers et inférieurs à $p$.

Combes A.,

*Professeur au Lycée Pasteur.*