Identités remarquables et divisibilité

Dans toute la suite a est un entier naturel $\geqslant 2$

$a^2 - 1 = (a-1)(a+1)$ donc $a-1$ et $a+1$ divise a^2-1

$a^3 + 1 = (a+1)(a^2 - a + 1)$

Plus généralement $a-1$ divise $a^n - 1$ pour tout $n \in \mathbb{N}$ avec $n \geqslant 2$ car

$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + ... + a + 1)$

Théorème 1 *Si P est un polynôme en a et si $P(b) = 0$ alors $a - b | P$*

Corollaire : $P = a^n - 1$ a pour racine -1 lorsque n est impair par conséquent $a+1 | a^n + 1$

Théorème 2 *Si k divise n alors $a^k - 1$ divise $a^n - 1$*

Théorème 3 $a^{2^n} - 1 = (a-1) \prod_{k=0}^{n-1} (a^{2^k} + 1)$

Généralisation :

$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + 1) = (a-b) \sum_{k=1}^{k=n} a^{n-k} b^{k-1}$

Donc $a - b$ divise $a^n - b^n$ et

Théorème 4 *Si k divise n alors $a^k - b^k$ divise $a^n - b^n$*

Théorème 5 $a^{2^n} - b^{2^n} = (a-b) \prod_{k=0}^{n-1} (a^{2^k} + b^{2^k})$

Théorème 6 *Etant donnés m et n entiers naturels d'après le Théorème de la division euclidienne il existe q et r entiers naturels uniques tel que $m = nq + r$ avec $0 \leqslant r < n$ et*

$a^m - 1 = (a^n - 1) \sum_{k=1}^{k=q} a^{m-kn} + a^r - 1$

Conséquence : Si $a \geqslant 2$ alors $0 < a^r - 1 < a^n - 1$ et par conséquent $a^r - 1$ est le reste de la division euclidienne de $a^m - 1$ par $a^n - 1$

Théorème 7 $\text{pgcd}(a^m - 1, a^n - 1) = a^{\text{pgcd}(m,n)} - 1$