

# Pense Bête pour la crypto

Laure Gonnord

9 février 2009

THÉORÈME 1 (GAUSS) *Si  $n \mid ab$  et  $n \wedge a = 1$  alors  $n \mid b$*

THÉORÈME 2 (BEZOUT) *Soient  $p$  et  $q$  premiers entre deux (pas forcément premiers). Alors :*

$$\exists u, v, \quad pu + qv = 1$$

*et c'est constructif.*

On peut utiliser Bezout pour calculer l'inverse modulo  $p$  d'un entier.

Dans un corps il n'y a pas de diviseur de 0, donc, comme  $(\mathbb{Z}/p\mathbb{Z}^*, \times)$  est un corps :

PROPOSITION 1 *Pour tout  $x, y \in \mathbb{Z}/p\mathbb{Z}, xy = 0 \Rightarrow (x = 0 \text{ ou } y = 0)$ .*

THÉORÈME 3 (CHINOIS) *Pour  $p$  et  $q$  premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Remarque : Pour  $p$  et  $q$  premiers entre eux, cela fournit un algo pour passer de  $(x[p], x[q])$  à  $x[pq]$  (dans le sens non trivial, considérer  $(x_1, x_2) \mapsto x_1qv + x_2pu$ ).

PROPOSITION 2 (CRITÈRE D'EULER)  *$x \neq 0$  est un carré  $\Leftrightarrow x^{\frac{p-1}{2}} = 1[p]$*

DÉFINITION 1 — Symbole de Legendre

Si  $p$  est un nombre premier et  $a$  un entier, alors le symbole de Legendre  $\left(\frac{a}{p}\right)$  vaut :

- 0 si  $p$  divise  $a$
- 1 si  $a$  est un résidu quadratique modulo  $p$  (ce qui signifie qu'il existe un entier  $k$  tel que  $k^2 = a \pmod{p}$ )
- -1 si  $a$  n'est pas un résidu quadratique modulo  $p$ .

PROPOSITION 3 (LEGENDRE)

1.  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$  (le symbole de Legendre est donc une fonction complètement multiplicative par rapport à son argument supérieur).
2. Si  $a = b \pmod{p}$ , alors  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
3.  $\left(\frac{1}{p}\right) = 1$  car 1 est le carré de lui-même

4.  $\left(\frac{-1}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)} = \begin{cases} 1 & \text{si } p \equiv 1[4] \\ -1 & \text{si } p \equiv 3[4] \end{cases}$ . Ceci est une conséquence directe du critère d'Euler.
5.  $\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)} = 1$  si  $p = 1$  ou  $7(\text{mod } 8)$  et  $-1$  si  $p = 3$  ou  $5(\text{mod } 8)$
6.  $\left(\frac{a}{2}\right) = 1$  si  $a$  est impair et 0 sinon.

PROPOSITION 4 (LOI DE RÉCIPROCITÉ QUADRATIQUE) *Si  $q$  est un nombre premier impair alors :*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

DÉFINITION 2 — Fonction indicatrice d'Euler

L'indicatrice d'Euler  $\varphi$  est la fonction de l'ensemble des entiers strictement positifs dans lui-même, qui à  $n$  associe le nombre d'entiers positifs inférieurs à  $n$  et premiers avec  $n$ .

$$\varphi(8) = \text{Card}\{1, 3, 5, 7\} = 4$$

THÉORÈME 4 (THÉORÈME D'EULER) *Soit  $n$  un entier naturel et  $a$  un entier premier avec  $n$ , alors*

$$a^{\varphi(n)} \equiv 1[n]$$

où  $\varphi$  est la fonction indicatrice d'Euler

Quelques règles de calcul :

- $\varphi(2^k) = 2^{k-1}$
- $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$
- $\varphi(\prod p_i^{\alpha_i}) = \prod \varphi(p_i^{\alpha_i})$

THÉORÈME 5 (CRITÈRE D'EULER SAUCE LEGENDRE) *Ce qui s'écrit également, en utilisant le symbole de Legendre, de la façon suivante :*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$$