Fermat ou Euler ?

PAR PATRICK TELLER

Question 1.

Dans les mathématiques du lycée on trouve le (petit) théorème de Fermat

$\forall p$ premier, $\forall a \in \mathbb{Z}, a^p \equiv a[p]$, *démontré au moyen de la formule du binôme*

Dans les mathématiques du « supérieur » on trouve le théorème d'Euler

$\forall n \in \mathbb{N}^*, \forall a, a \wedge n = 1, a^{\varphi(n)} \equiv 1[n]$, *démontré au moyen du théorème de Lagrange et qui, dans le cas d'un premier p, devient*

$\forall p$ premier, $\forall a \in \mathbb{Z}, a^{p-1} \equiv 1[p]$.

Dit autrement: l'approche « Euler » privilégie la notion d'ordre d'un élément dans un groupe et, par suite ne peut pas s'appliquer à des entiers a qui ne sont pas premiers avec n, alors que l'approche « Fermat » s'applique à tous les entiers a, qu'ils soient premiers ou pas avec n, et annonce une périodicité de la suite des puissances de a, mais ne concerne que le cas où n est premier.

Alors Fermat ou Euler ?

Question 2.

Dans le cadre du cryptage-décryptage RSA on choisit un entier n, produit de deux premiers p et q, et on crypte le message m en l'élevant à la puissance e, modulo n; on le décrypte en élevant le message m^e à la puissance d, choisit tel que $de \equiv 1[\varphi(n)]$; on invoque le théorème d'Euler pour déduire que $m^{\varphi(n)} \equiv 1[n]$ et, par suite, $m^{\mathrm{de}} \equiv m[n]$.

Mais que se passe-t-il si, par mégarde, m n'était pas premier avec n ?

Ce point est rarement précisé dans les présentations de l'algorithme RSA.

1 Le théorème chinois (ou théorème de structure des groupes abéliens finis) et le (petit) théorème de Fermat

Les seuls éléments nécessaires:

Théorème 3.

Soit $n = \prod_{i=1}^{r} p_i^{k_i}$ la factorisation de n en produit de puissances de premiers alors il y a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{k_i}\mathbb{Z}$; en fait ceci est même un isomorphisme d'anneaux (c'est celui-là qui nous importe).

et, plutôt que le théorème d'Euler, nous allons nous contenter de celui de Fermat

Théorème 4.

$\forall p$ premier, $\forall a \in \mathbb{Z}, a^p \equiv a[p]$

2 Le cas « sans carrés »

Définition 5. *Les entiers « sans carrés » (en anglais « square-free »)*

Un entier n sera dit sans carrés » lorsqu'il se factorise $n=\prod_{i=1}^{r} p_i$.

Dans ce cas

Théorème 6. *Le (petit) théorème de Fermat pour les entiers « sans carrés »*

Soit $n=\prod_{i=1}^{r} p_i$ *alors* $\forall a \in \mathbb{Z}, a^n \equiv a[n]$

Démonstration.

Il suffit de raisonner dans chaque anneau $\mathbb{Z}/p_i\mathbb{Z}$ et d'y appliquer le (petit) théorème de Fermat. □

d'où

Théorème 7.

Le principe du cryptage-décryptage RSA est aussi valide lorsque le message $m \in [0, n-1]$ *n'est pas premier avec n.*

Démonstration.

Soient l'exposant de cryptage e et l'exposant de décryptage d, liés par la relation $ed \equiv 1[(p-1)(q-1)]$.

Si m est congru à 0 modulo p alors pour tout k $m^k \equiv 0$[p].

Si m n'est pas congru à 0 modulo p alors dans $\mathbb{Z}/p\mathbb{Z}$ $\bar{m}^{p-1} = \bar{1}$ et par suite $\bar{m}^{ed} = \bar{m}$.

et de même dans $\mathbb{Z}/q\mathbb{Z}$. □

Exemple 8.

Soit n=34, e=5,d=13,$\varphi(34) = 16$

et effectivement

$9^{5.13}$=1061116611996472485436878557527126679911039043304825699818726 49 est congru à 9 modulo(34)

mais si on prend 2 qui n'est pas premier avec 34

$2^{5.13}$=36893488147419103232 est aussi congru à 2 modulo(34).

Question 9.

Que se passe-t-il lorsque n n'est pas « sans carrés » ?

3 Le cas de $\mathbb{Z}/p^m\mathbb{Z}$

Théorème 10. *Les suites géométriques* $(\bar{a}^k)$ *dans* $\mathbb{Z}/p^m\mathbb{Z}$

Soit $\bar{a} \in \mathbb{Z}/p^m\mathbb{Z}$

i) si $a \wedge p = 1$, *la suite* $(\bar{a}^k)$ *est périodique, de période* $\varphi(p^m)$

ii) si $a \wedge p = p^v \neq 1 \quad k \geqslant m - v \Rightarrow \bar{a}^k = \bar{0}$

Immédiat.

4 Le cas de $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{k_i}\mathbb{Z}$

Théorème 11.

Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ et $\overline{a(i)}$ sa classe modulo $p_i^{k_i}$, on notera v(i) l'entier tel que $a \wedge p_i = p_i^v i \neq 1$ et $J = \{i, a \wedge p_i = 1\}$

alors la suite $(\bar{a}^k)_{k > \max(k_i - v_i)}$ est périodique de période le plus petit commun multiple des périodes des $\{\overline{a(i)}^k, i \in J\}$

ou, si on préfère, un diviseur du produit $\prod_{i \in J} \varphi(p_i^{k_i})$

Découle du théorème 8.

(et pourrait s'appeler « petit théorème de Fermat » généralisé)

Exemple 12.

Soit n=300=$2^2.3^1.5^2$

soit a=4=2^2, alors la suite $(\bar{4}^k)_{k > \max(2-2)} = (\bar{4}^k)_{k \geqslant 1}$ est périodique de période le plus petit commun multiple de la période de $\bar{4}$ dans $(\mathbb{Z}/3\mathbb{Z})^*$, c'est à dire 2, et de celle de $\bar{4}$ dans $(\mathbb{Z}/25\mathbb{Z})^*$, c'est à dire 10

comme le confirme le calcul: 1, **4**, 16, 64, 256, 124, 196, 184, 136, 244, 76, **4**, 16, 64, 256, 124, 196, 184, 136, 244, 76, 4, 16, 64, 256, 124, 196, 184, 136, 244, 76, 4 etc..

soit a=6=2×3, alors la suite $(\bar{6}^k)_{k > \max(2-1,1-1)} = (\bar{6}^k)_{k>1}$ est périodique de période le plus petit commun multiple de la période de $\bar{6}$ dans $(\mathbb{Z}/25\mathbb{Z})^*$, c'est à dire 6

comme le confirme le calcul: 1, 6, **36**, 216, 96, 276, 156, **36**, 216, 96, 276, 156, 36, 216, 96, 276, 156, 36, 216, 96, 276, 156, 36, 216, 96, 276, 156, 36, 216, 96, 276, 156]

Réponse.

Le théorème d'Euler a un parfum plus algébrique mais le (petit) théorème de Fermat est plus susceptible d'extension au cas des entiers n quelconques, pas seulement premiers; il affirme une périodicité.

Je vote Fermat

Paris, mars 2017