Crypto: Un peu de théorie des nombres

Hiver 2019

Le reste de la division

$3 \cdot 5 \bmod 5 = 0$
$12 \bmod 4 = 0$
$5 \bmod 13 = 5$
$17 \bmod 7 = 3$
$8 \bmod 3 = (5 \bmod 3) + (3 \bmod 3) \bmod 3 = 2$

- **Thme (unicité des quotients et restes):** Pour a et $b>0$ des entiers naturels, il n'y a qu'un seul couple d'entiers naturels k et $r<b$ tel que $a=k\cdot b+r$.
- ***Preuve.*** Montrons en premier lieu qu'un tel couple existe. Choisissons k tel que $k\cdot b \le a < (k+1)\cdot b$. C'est toujours possible de trouver un tel entier naturel k. Nous avons alors $a=k\cdot b+r$ avec $r<b$ puisque $r=a-k\cdot b<(k+1)\cdot b-k\cdot b=b$.

  Montrons maintenant que ce couple (k,r) est unique. Supposons au contraire qu'il existe $(k',r')\neq(k,r)$ tel que $a=k'\cdot b+r'=k\cdot b+r$ avec $r'<b$ et $r<b$. En conséquence $(k-k')\cdot b=r'-r$. Trois cas sont maintenant possibles:

  1) si $k=k'$ alors $r'-r=0$. Donc, $r'=r$ et $(k',r')=(k,r)$ pour une contradiction.

  2) si $k>k'$ alors $b \le (k-k')\cdot b=r'-r \le r'<b$. Donc, $b \le r'$ pour une contradiction.

  3) si $k<k'$ alors $b \le (k'-k)\cdot b=r-r' \le r$. Donc, $b \le r$ pour une contradiction. ■
- **Défn:** Pour a et $b>0$ des entiers naturels, la *division entière* de a par b, notée $\lfloor a/b \rfloor$, est l'entier naturel k tel que $a=k\cdot b+r$ avec $0 \le r<b$. Le terme r, noté $a \bmod b$, est appelé le *reste de la division* de a par b et k est son *quotient*. Lorsque $r=0$ nous dirons que b *divise* a.

Le reste de la division entière d′une somme

- Dans une expression arithmétique avec des +,· et mod, l'opération mod est de moindre priorité.
- **Lemme M:** $\forall x,y \in \mathbf{N}\ \forall b \in \mathbf{N}^*$,

$$(x+y) \bmod b = ((x \bmod b) + (y \bmod b)) \bmod b.$$

Il est facile de vérifier que $(a \bmod b) \bmod b = a \bmod b$.

- ***Preuve.*** Posons, $x=k\cdot b+r$, $r<b$ et $y=k'\cdot b+r'$,$r'<b$ promis par le théorème d'**unicité des quotients et restes**. Nous avons, $x+y \bmod b = ((k+k')\cdot b+r+r') \bmod b$. De la même façon, $r+r'=k''\cdot b+r''$, $r''<b$ (i.e. $r''= r+r' \bmod b$) et donc $x+y=(k+k'+k'')\cdot b+r''$, par le théorème d'**unicité des quotients et restes**, $x+y \bmod b=r''= r+r' \bmod b$ comme nous devions le montrer. ■

Preuve classique par contradiction

- **Thme E(Euclide):** Pour p un nombre premier, a et b des entiers naturels, si p divise $a \cdot b$ alors p divise a ou p divise b.
- ***Preuve.*** Nous prouvons le cas $b>1$, car autrement le théorème est trivialement vrai. Supposons pour une contradiction que p divise $a \cdot b$, mais p ne divise ni a ni b. Pour a et p fixés, choisissons le b minimum qui satisfait ces conditions. Le **Thme d'unicité des quotients et restes** nous indique que $a=k \cdot p+r$ et $b=k' \cdot p+r'$ avec $1 \le r<p$ et $1 \le r'<p$. Puisque p divise $a \cdot b=a \cdot k' \cdot p+a \cdot r'$ alors p divise $a \cdot r'$, puisque par le **Lemme M**,

$$0=a \cdot b \bmod p = (a \cdot k' \cdot p \bmod p + a \cdot r' \bmod p) \bmod p = a \cdot r' \bmod p.$$

=0

De plus, p ne divise ni r'(puisque $r'<p$) ni a(par hypothèse). La minimalité de b implique donc $b \le r'<p$. Par **Thme d'unicité des quotients et restes,** posons $p=m \cdot b+s$ avec $1 \le s<b$, car p ne divise pas b. Alors, $a \cdot p=m \cdot a \cdot b+a \cdot s$ et p divise $a \cdot s=a \cdot p-m \cdot a \cdot b$ puisqu'il divise $a \cdot p$ et $m \cdot a \cdot b$ sans diviser a et sans diviser s. Ceci contredit que b soit minimum puisque $s<b$. ■

Le théorème fondamental de l′arithmétique

- Le théorème fondamental de l'arithmétique énonce que chaque entier naturel peut être représenté d'une façon unique par un produit de puissance de nombres premiers.
- **Défn:** Les nombres premiers qui apparaissent dans la représentation de l'entier naturel *n* sont appelés *facteurs premiers* de *n*. *Factoriser n* signifie trouver ses facteurs premiers.

et sa preuve (I)

- **Thme (fondamental de l'arithmétique):** Pour $n>1$ un entier naturel, il existe un seul entier naturel $k>0$ et un seul ensemble $\{(p_1, e_1),(p_2,e_2),\ldots,(p_k,e_k)\}$ où chaque p_i est un nombre premier et chaque $e_i>0$ est un entier naturel pour lequel

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_k^{e_k}.$$

- ***Preuve.*** En premier, nous prouvons l'existence par induction mathématique généralisée. Considérons le prédicat $P(n)$= "*chaque entier $n>1$ est ou bien premier ou le produit de nombres premiers*".

base *($n=2$):* *2* est premier.

pas d'induction: Supposons $P(j)$ pour $2\leq j<n$, montrons $P(n)$. Si n est premier alors il n'y a rien à prouver. Si n est composé alors $n=a\cdot b$ pour $2\leq a\leq b<n$. Par hypothèse d'induction, $a=p_1\cdot p_2\cdot\ldots\cdot p_l$ et $b=q_1\cdot q_2\cdot\ldots\cdot q_m$ et $n=a\cdot b=p_1\cdot p_2\cdot\ldots\cdot p_l\cdot q_1\cdot q_2\cdot\ldots\cdot q_m$ est un produit de nombres premiers. Ceci établit que chaque entier supérieur à *1* peut être exprimé comme le produit de nombres premiers.

et sa preuve (II)

- ***Preuve(suite).*** Nous montrons maintenant l'unicité de la décomposition. Supposons pour $n>1$ que

$$n=p_1 \cdot p_2 \cdot \ldots \cdot p_l = q_1 \cdot q_2 \cdot \ldots \cdot q_{l'}$$

Nous montrons que les q_i sont un réarrangement des p_i. Notons que p_1 divise s, par le **Thme E** p_1 divise au moins un des q_j. Ceci est impossible à moins que $p_1=q_j$, car q_j est premier. Renommons q_j comme q_1 est q_1 comme q_j. Nous divisons maintenant s par p_1. Nous avons alors

$$n/p_1=p_2 \cdot \ldots \cdot p_l = q_2 \cdot q_3 \cdot \ldots \cdot q_{l'}.$$

Le même argument montre que $p_2=q_2$, ensuite $p_3=q_3$, ..., $p_l=q_l$. Nous avons $l'=l$, car si $l'>l$ nous aurions

$$n/p_1 \cdot p_2 \cdot \ldots \cdot p_l = 1 = q_{l+1} \cdot q_{l+2} \cdot \ldots \cdot q_{l'}$$

ce qui est impossible à résoudre. Même chose si $l>l'$. ■

Encore une preuve classique par contradiction

- **Thme(Euclide):** $|\mathbf{P}|=\infty$.
- ***Preuve.*** Supposons pour une contradiction que l'ensemble des nombres premiers est de taille finie $\mathbf{P}=\{p_1,p_2,\ldots,p_n\}$. Considérons maintenant l'entier naturel $w=p_1\cdot p_2\cdot\ldots\cdot p_n+1$. Si w est premier alors nous obtenons une contradiction, car $w\notin\mathbf{P}$. Si w n'est pas premier alors par le théorème fondamental de l'arithmétique, il doit être divisible par un nombre premier $q\in\{p_1,p_2,\ldots,p_n\}$. Impossible, car le reste de la division $w/p_i = 1$ pour chaque $1\leq i\leq n$. L'ensemble $\mathbf{P}$ ne contient donc pas tous les nombres premiers, car il ne contient pas q. Contradiction, $\mathbf{P}$ ne peut pas être de taille finie. ■