CHAPITRE 1

Rappels d'arithmétique

1.1 Division euclidienne

On note $\mathbb{N} = \{0, 1, 2, \cdots\}$ l'ensemble des entiers naturels, et $\mathbb{Z}$ représente l'ensemble des entiers relatifs, $\mathbb{Z} = \{\cdots, -1, 0, 1, 2, \cdots\}$.

Théorème 1.1 *Soit $b \in \mathbb{N}^*$ un entier strictement positif, et $a \in \mathbb{Z}$. Alors il existe un unique couple (q, r) d'entiers naturels tel que*

$$a = bq + r, \qquad 0 \leq r < b.$$

q est appelé le `quotient` *et r le* `reste` *de la division de a par b.*

Notation Dans la suite, pour $x \in \mathbb{Z}$, et n entier ≥ 1, on notera souvent $x \bmod n$ le reste de la division de x par n.

Exemple 1.1 :

$$17 = 5 \times 3 + 2 \text{ et } 0 \leq 2 < 5 \quad \text{et} \quad -17 = 5 \times (-4) + 3 \text{ et } 0 \leq 3 < 5$$

donc le quotient de 17 par 5 est 3 avec le reste 2, et le quotient de -17 par 5 est -4 avec le reste 3.

1.2 Congruences

Définition 1.2 *Soit $n > 1$ un entier . On dit que les entiers x et y sont congrus modulo n, et on écrit*

$$x \equiv y \pmod{m},$$

si $y - x$ est un multiple de n.

Théorème 1.3 *La relation de congruence est compatible avec l'addition et la multiplication, c'est à dire que si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors*

$$a + b \equiv a' + b' \pmod{n} \quad \text{et} \quad ab \equiv a'b' \pmod{n}$$

Définition 1.4 *Soit $n > 1$ un entier fixé. Pour tout entier a on note $\overline{a}$ la* `classe de congruence de` *a modulo n, $\overline{a} = \{x \in \mathbb{Z} \ ; \ x \equiv a \pmod{n}\}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de tous les entiers.*

Proposition 1.1 *Pour que $\overline{x} = \overline{y}$ il faut et il suffit que $x \equiv y \pmod{m}$.*

Proposition 1.2 *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n. Plus précisément*

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}.$$

Preuve : Soit r le reste de la division de x par n, $x = qn + r$. On a $x \equiv r \pmod{n}$, et donc $\overline{x} = \overline{r}$. Comme $0 \leq r \leq n-1$, cela montre qu'une classe arbitraire, $\overline{x}$, est égale à l'une des n classes $\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$. □

Définition 1.5 (L'anneau $\mathbb{Z}/n\mathbb{Z}$) *On munit l'ensemble $\mathbb{Z}/n\mathbb{Z}$ d'une addition et d'une multiplication en posant*

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad et \qquad \overline{a}\overline{b} = \overline{ab}.$$

Muni de ces deux opérations $\mathbb{Z}/m\mathbb{Z}$ est un anneau commutatif unitaire. Cela signifie que l'addition et la multiplication sont commutatives et associatives [1] *Il existe un élément neutre $\overline{0}$ pour l'addition et un élément neutre $\overline{1}$ pour la multiplication*

$$\forall x \quad \overline{x} + \overline{0} = \overline{x}, \qquad \overline{1}\,\overline{x} = \overline{x}.$$

Toute classe $\overline{x}$ admet un symétrique $\overline{y} = \overline{-x}$ pour l'addition, c'est à dire une classe y telle que $\overline{x} + \overline{y} = \overline{0}$. Enfin la multiplication est distributive par rapport à l'addition,

$$\forall x, y, z \quad \overline{x}(\overline{y} + \overline{z}) = \overline{x}\,\overline{y} + \overline{x}\,\overline{z}.$$

1.3 Divisibilité. Pgcd, théorème de Bezout

Définition 1.6 *Soient $a, b \in \mathbb{Z}$. On dit que a est un* `multiple` *de b, ou que b est un* `diviseur` *de a s'il existe un entier q tel que $a = bq$. Si $b = 0$ son seul multiple est 0, autrement dit 0 ne divise que 0. Mais 0 est multiple de tout entier donc tout entier divise 0.*

Lemme 1.7 *On ne change pas l'ensemble des diviseurs communs à deux nombres si on ajoute à l'un des deux un multiple de l'autre.*

Preuve : Soient $c = a + mb$. Soit d un diviseur commun à a et b. Puisque b est un multiple de d, mb est encore un multiple de d, et comme a est un multiple de d, $c = a + mb$ est un multiple de d. Réciproquement si d divise b et c, alors il divise $c + mb = a$. □

Théorème et définition 1.8 *Soit a et b deux entiers non tous les deux nuls. Il existe un plus grand entier positif qui est un diviseur commun à a et b. On le note* $\mathrm{pgcd}(a, b)$ *ou (a, b). Les diviseurs communs à a et b sont les diviseurs de (a, b).*

[1] L'opération $\star$ est commutative si $x \star y = y \star x$ et associative si $x \star (y \star z) = (x \star y) \star z$

Preuve : Les diviseurs de x et de $-x$ étant les mêmes on peut supposer, sans nuire à la généralité, que a et b sont positifs ou nuls, et même que $0 \leq b \leq a$. Si $b = 0$, tout entier naturel est un diviseur de b, et les diviseurs communs à a et b sont les diviseurs de a. Le plus grand d'entre eux est a, et il est multiple de tous les autres. Si b est différent de 0 on utilise l'algorithme d'Euclide.

On pose $r_{-1} = a$ et $r_0 = b$, et on effectue la division euclidienne de r_i par r_{i+1}, donnant un quotient q_{i+2} et un reste r_{i+2}. On s'arrête lorsque $r_t = 0$.

$$\begin{array}{lcllll} r_{-1} & = & q_1 r_0 & + & r_1 & 0 < r_1 < r_0 \\ r_0 & = & q_2 r_1 & + & r_2 & 0 < r_2 < r_1 \\ & \vdots & & & & \\ r_{t-3} & = & q_{t-1} r_{t-2} & + & r_{t-1} & 0 < r_{t-1} < r_{t-2} \\ r_{t-2} & = & q_t r_{t-1} & + & r_t & r_t = 0. \end{array}$$

Par le lemme (1.7) les diviseurs communs à a et b sont les diviseurs communs à r_0 et r_1, puis à r_1 et r_2, ... , et enfin les diviseurs communs à r_{t-1} et $r_t = 0$, c'est à dire les diviseurs de r_{t-1}. Il en existe donc un, r_{t-1}, qui est multiple de tous les autres. □

On prouvera en exercice que

Proposition 1.3 *Soit a, b entier non tous les deux nuls.*
- *Pour que $d = (a, b)$ il faut et il suffit qu'il existe a', b' premiers entre eux tels que $a = da'$ et $b = db'$.*
- *Pour tout entier $\lambda > 0$ on a $(\lambda a, \lambda b) = \lambda(a, b)$.*

On laisse aussi en exercie la démonstration du théorème suivant.

Théorème 1.9 *Soit a et b deux entiers non tous les deux nuls. Il existe un plus petit entier $m > 0$ qui soit un multiple de a et de b. Tout autre multiple de a et de b est un multiple de m. On notera* $\mathrm{ppcm}(a, b)$ *cet entier. Le* ppcm *est relié au pgcd par l'égalité* $\mathrm{ppcm}(a, b) = ab/\mathrm{pgcd}(a, b)$.

Théorème 1.10 (Complexité de l'algorithme d'Euclide) *Soit t le nombre de divisions dans l'algorithme d'Euclide pour la recherche du pgcd de a et b. On a toujours*

$$t \leq 2 \left\lceil \frac{\log b}{\log 2} \right\rceil .$$

Preuve : Remarquons qu'après la $(j+2)^{\text{ème}}$ division le dernier reste r_{j+2} est plus petit $r_j/2$. Il suffit pour cela de prouver que $r_2 < r_0/2$. Si $r_1 \leq r_0/2$ alors on $r_2 < r_1 \leq r_0/2$. Si $r_1 > r_0/2$ le quotient q_2 de la division de r_0 par r_1 est 1. Cette division s'écrit $r_0 = 1.r_1 + r_2$, et donc $r_2 = r_0 - r_1 < r_0 - r_0/2 = r_0/2$. Par récurrence sur j, on a $r_{2k} < r_0/2^k = b/2^k$, pour tout entier naturel k. Soit alors $j = \left\lceil \frac{\log b}{\log 2} \right\rceil$, le premier entier tel que $2^j \geq b$. Si $t \geq 2j$, alors $r_{2j} < b/2^j \leq 1$, implique $r_{2j} = 0$, et donc $t = 2j$. □

Théorème 1.11 *Soient a et b deux entiers non tous deux nuls et $d = (a, b)$ leur pgcd. Il existe deux entiers u et v tels que*

$$ua + vb = d.$$

```
gcdext(a,b) =  {
   local(qr,q,r,x,d,t,u);
   if(b==0,
     return([a,1,0]),

     qr = divrem(a,b);
     q=qr[1]; r=qr[2];
     x = gcdext(b,r);
     d = x[1]; t = x[2]; u = x[3];
     return([d,u,(t-q*u)])
     )
}
```

FIG. 1.1 – Une écriture en `pari` de l'algorithme d'Euclide étendu. L'appel gcdext(a,b) rend le triplet [d,u,v]

Preuve : On peut supposer sans nuire à la généralité que $0 \leq b < a$. On raisonne par récurrence sur b. Notons d le pgcd de a et b.

Si $b = 0$ on a $d = a$ et $ua + vb = d$ est satisfaite en choisissant $u = 1$ et $v = 0$. Sinon soit q et r le quotient et le reste de la division euclidienne de a par b.

$$a = bq + r, \quad \text{avec} \quad 0 \leq r < b.$$

Alors, puisque d est aussi le pgcd de r et b, et puisque $r < b$, par hypothèse de récurrence il existe deux entiers t et u tels que

$$tb + ur = d,$$

et cette relation s'écrit encore $tb + u(a - bq) = d$ ou $ua + (t - qu)b$. c'est à dire $d = ua + vb$ en prenant $v = t - qu$. □

La figure 1.3 donne une implémentation en `pari` de cet algorithme, que vous pourrez tester pour vous familiariser avec l'écriture de programmes `pari`. En réalité cet algorihme est l'une des primitives de base de `pari`. Elle est implémentée sous le nom de bezout(a,b).

Définition 1.12 *On dit que a et b sont* `premiers entre eux` *si leur pgcd est* 1.

Théorème 1.13 (Théorème de Bezout) *Pour que a et b soient premiers entre eux il faut et il suffit qu'il existe u et v entiers tels que*

$$ua + vb = 1.$$

Preuve : La condition est nécessaire par le théorème (1.11). Réciproquement, si $ua + vb = 1$, tout diviseur de a et b divise 1. Les diviseurs de a et b sont donc -1 et 1, et le plus grand d'entre eux est 1. □

Théorème 1.14

1. **Lemme de Gauss** *Si d, premier avec a, divise ab, alors d divise b.*
2. *Si a et b premiers entre eux divisent c, alors ab divise c.*

Preuve :

1. Par Bezout il existe u et v tels que $ud + va = 1$. En multipliant par b cela donne

$$udb + vab = b.$$

   d divise le premier membre, donc il divise b.

2. Soit u, v tels que $ua + vb = 1$. On en déduit $uac + vbc = c$. Comme $b \mid c$, $ab \mid ac$. Comme $a \mid c$, $ab \mid bc$. Le produit ab divise donc ac et bc et encore $uac + vbc = c$.

□

1.4 L'équation diophantienne $ax + by = c$

Théorème 1.15 *L'équation aux inconnues entières x et y*

$$ax + by = c, \tag{1.1}$$

avec $a, b, c \in \mathbb{Z}$, a des solutions si et seulement si $(a, b) \mid c$. On les obtient en utilisant l'algorithme d'Euclide étendu.

Preuve : Si (x, y) est une solution et $d = (a, b)$, d divisant a et b, il divise le premier membre de 1.1, donc il divise c ce qui donne la nécessité de la condition. Réciproquement, si d divise c, après division par d des deux membres, l'équation (1.1) devient

$$a'x + b'y = c'$$

avec $(a', b') = 1$. Par Bezout on trouve u et v tels que $a'u + b'v = 1$. Il suffit alors de prendre $x = c'u$ et $y = c'v$. □

1.5 Nombres premiers

Définition 1.16 *On dit que p est un nombre* `premier` *si p est un entier > 1 et si ses seuls diviseurs positifs sont 1 et p. C'est équivalent à dire que p est premier si, et seulement si, il est premier avec tous les entiers k, $1 \leq k < p$.*

Théorème 1.17 *Si p premier divise ab, alors p divise l'un des deux nombres a ou b.*

Théorème 1.18 *Soit $n > 1$. Le plus petit diviseur de n, plus grand que 1 est un nombre premier. On en déduit, par récurrence, que tout entier est un produit de facteurs premiers.*

Théorème 1.19 (Unicité de la décomposition en facteurs premiers) *Tout entier $n > 0$ s'écrit de manière unique comme un produit de facteurs premiers.*

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

où les p_i sont premiers, $p_1 < p_2 < \cdots < p_r$, et les α_i entiers > 0.

Définition 1.20 *Soit n un entier naturel non nul. Pour tout nombre premier p on appelle* `valuation en` p `de` n*, et on note $v_p(n)$ le plus grand entier k tel que p^k divise n, c'est à dire l'exposant de p dans la décomposition en facteurs premiers de n. Autrement dit, par définition des $v_p(n)$,*

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Définition 1.21 *On note $\pi(x)$ le nombre des nombres premiers p jusqu'à x, et $\psi(x)$ la fonction définie par*

$$\psi(x) = \sum_{p^r \leq x} \log p.$$

Le théorème des nombres premiers a été conjecturé dès le début du XVIII$^{\text{e}}$ siècle, et prouvé seulement en 1896 par Hadamard et de la Vallée Poussin.

Théorème 1.22 (Le théorème des nombres premiers) *Lorsque x tend vers l'infini*

$$\pi(x) \sim \frac{x}{\ln x}, \qquad \psi(x) \sim x.$$

1.6 Ordre d'un élément dans groupe fini

Définition 1.23 *Un* `groupe commutatif` *est la donnée de $(G, \star)$ où $\star$ est une loi de composition G, commutative et associative, telle que*

1. *Il existe un élément neutre $e \in G$ tel que, pour tout $x \in G$, $x * e = x$.*
2. *Quel que soit l'élément $x \in G$, il existe un symétrique de x c'est à dire un $y \in G$ tel que $x \star y = e$.*

Définition 1.24 *Un* `sous-groupe` *d'un groupe G est une partie H qui contient l'élément neutre e, stable par composition et par passage au symétrique, c'est à dire telle que, pour tous $x, y \in H$, $x \star y$ est encore un élément de H, ainsi que le symétrique de x.*

Théorème 1.25 *Soit G un groupe fini. Si H est un sous groupe de G, le cardinal de H divise le cardinal de G.*

Théorème et définition 1.26
Soit G un groupe fini et a un élément de G.

1. *Il existe un plus petit entier $\omega \geq 1$ tel que $a^\omega = 1$.*
2. *Les éléments $1, a, a^2, \ldots, a^{\omega-1}$ sont tous distincts, et l'ensemble*

$$G_a = \left\{1, a, a^2, \cdots, a^{\omega-1}\right\}.$$

   est le plus petit sous-groupe de G contenant a.

3. *On a l'équivalence*

$$a^m = 1 \iff \omega \mid m.$$

L'entier ω est appelé `l'ordre de` a.

Preuve :

1. Comme G est fini les $(a^n)_{n\in\mathbb{N}}$ ne sont pas tous distincts. Il existe $0 \leq u < v$ avec $a^u = a^v$. En multipliant les deux termes de cette égalité par l'inverse de a^u, on obtient $a^{v-u} = 1$. Il existe donc au moins un entier $n > 0$ tel que $a^n = 1$. Notons ω le plus petit de ces entiers.
2. Si il existait deux éléments égaux a^i et a^j parmi $a^0, a^1, \cdots, a^{\omega-1}$, on aurait $a^{j-i} = 1$, contredisant la définition de ω. Les éléments $a^0, a^1, \cdots, a^{\omega-1}$ sont donc tous distincts. Soit m arbitraire dans $\mathbb{N}$. En écrivant

$$m = q\omega + r, \quad 0 \leq r < \omega,$$

on obtient $a^m = (a^\omega)^q a^r = a^r \in \left\{a^0, a^1, \cdots, a^{\omega-1}\right\}$. Les a^m, avec $m \geq 0$ sont donc tous dans G_a. Cela prouve en particulier que G_a est stable par la multiplication. Il reste à vérifier que l'inverse d'un élément a^m de G_a est encore dans G_a. Cela est vrai car l'égalité $a^m a^{\omega-m} = a^\omega = 1$, montre que cet inverse est $a^{\omega-m}$. Ainsi G_a est un sous-groupe de G, et il contient a ; c'est évidemment le plus petit car tout sous-groupe de G qui contient a contient les a^n, donc G_a.
3. Soit n un entier naturel. Soient q et r le quotient et le reste de la division de n par ω, $n = \omega q + r$. Alors $a^n = (a^\omega)^q a^r = a^r$. On a donc $a^n = 1$ si et seulement si $a^r = 1$. Vu $0 \leq r < \omega$, $a^r = 1$ si et seulement si $r = 0$.

□

Définition 1.27 *Un groupe G est* `cyclique` *si il existe $a \in G$ tel que le sous-groupe G_a engendré par a soit G tout entier. On dit que a est un* `générateur` *de G.*

Théorème 1.28 (Théorème de Lagrange) *Soit a un élément du groupe fini G de cardinal n. Alors $a^n = 1$.*

Preuve : Par le point (3) du théorème (1.26) cela revient à démontrer que l'ordre ω de a divise le cardinal de G. Or ω est le cardinal du sous-groupe G_a de G engendré par a, et par le théorème (1.25) ce cardinal divise le cardinal de G. □

1.7 Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et la fonction φ d'Euler

Définition 1.29 *L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication est un groupe. On le note $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Théorème 1.30 *Pour que l'élément $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ soit inversible il faut et il suffit que $(a, n) = 1$, et dans ce cas le calcul de l'inverse de $\bar{a}$ se fait à l'aide de l'algorithme d'Euclide étendu, appliqué au couple (a, n).*

Preuve : Si $\bar{a}$ est inversible, il existe $\bar{b}$ tel que $\bar{a}\bar{b} = \bar{1}$. Il existe donc $v \in \mathbb{Z}$ tel que $ab - 1 = vmn$, ou $ba + vn = 1$. Par le théorème de Bezout, a et n sont premiers entre eux. Réciproquement, si a et n sont premiers entre eux, il existe u et v entiers tels que $au + nv = 1$. Cela donne, modulo n, $\overline{au} = \overline{1 - nv} = \bar{1}$. □

Corolaire 1.31 *Pour que l'anneau $\mathbb{Z}/p\mathbb{Z}$ soit un corps il faut et il suffit que p soit premier. On notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, lorsque p est premier.*

Définition 1.32 *Soit n un entier non nul et a premier avec n. Par le théorème (1.30) $\overline{a}$ est un élément du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. On appelle* `ordre de` a `modulo` n *l'ordre de l'élément $\overline{a}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, c'est à dire le plus petit entier $\omega > 0$ tel que $a^\omega \equiv 1 \pmod{n}$.*

Définition 1.33 *On note $\varphi(n)$ le nombre des entiers x premiers avec n tels que $1 \leq x \leq n$, c'est à dire le nombre des éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 1.34 (Théorème d'Euler) *Si $(a, n) = 1$, on a*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Preuve : On applique le théorème de Lagrange (1.28) au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Si $(a, n) = 1$, la classe de a, $\overline{a}$ est un élément du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Ce groupe est, par définition de φ, de cardinal $\varphi(n)$. Par le théorème de Lagrange, $\overline{a}^{\varphi(n)} = \overline{1}$. □

1.8 Le théorème des restes chinois

Lemme 1.35 *On considère le système de congruence*

$$\begin{cases} x & \equiv & a & \pmod{p} \\ x & \equiv & b & \pmod{q} \end{cases}$$

Alors, ou bien ce système n'a pas de solution, ou bien il est équivalent à une unique congruence

$$x \equiv c \pmod{\text{ppcm}(p, q)}.$$

Si p et q sont premiers entre eux il admet toujours une solution.

Preuve : Supposons que ce système admette une solution x_0. Alors x est une solution si et seulement si

$$\begin{cases} x & \equiv & x_0 & \pmod{p} \\ x & \equiv & x_0 & \pmod{q} \end{cases}$$

c'est à dire si et seulement si $x - x_0$ est divisible par a et b c'est à dire est un multiple de $\text{ppcm}(a, b)$.

x est solution de la première congruence si et seulement si $x = a + kp$, avec $k \in \mathbb{Z}$. Pour que x soit solution de la deuxième congruence il faut et il suffit que

$$a + kp \equiv b \pmod{q}$$

c'est à dire que k soit solution de

$$pk \equiv b - a \pmod{q}.$$

Si p, q sont premiers entre eux p est inversible modulo q et cette congruence admet des solutions. □

De ce lemme on déduit imméditement par récurrence le théorème suivant.

Théorème 1.36 (Le théorème des restes chinois) *Si $q_1, q_2, \ldots, q_r$ sont deux à deux premiers entre eux, le système de congruences*

$$\begin{cases} x & \equiv & a_1 & \pmod{q_1} \\ x & \equiv & a_2 & \pmod{q_2} \\ & \vdots & & \\ x & \equiv & a_r & \pmod{q_r} \end{cases} \tag{1.2}$$

est équivalent à une unique congruence

$$x \equiv a \pmod{q_1 q_2 \ldots q_r}$$

Théorème 1.37 *La fonction d'Euler est une* `fonction arithmétique multiplicative`*, c'est à dire que, pour tout couple (a, b) d'entiers* **premiers entre eux**

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Preuve : Cela résulte du théorème des restes chinois. Considèrons l'application

$$\begin{array}{rccc} \psi & : & \mathbb{Z}/ab\mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & & \overline{x} & \mapsto & (\overline{x}\ ,\ \overline{x}), \end{array}$$

qui à la classe de x modulo ab fait correspondre le couple formé de la classe de x modulo a et de la classe de x modulo b (pour ne pas alourdir l'écriture, on a utilisé la même notation pour représenter les classes modulo ab, modulo a, et modulo b). Pour que ceci définisse bien une application il faut s'assurer que le couple $(\bar{x}, \bar{x}) \in (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ ne dépend que de la classe de x modulo ab, mais pas du représentant x pris dans cette classe. Cela revient à vérifier, ce qui est immédiat, que si y est congru à x modulo ab, alors y est congru à x modulo a, et aussi modulo b. L'élément $\overline{x} \in \mathbb{Z}/ab\mathbb{Z}$ est un antécédent de $(\overline{u}, \overline{v})$ si et seulement si x est solution des deux congruences

$$x \equiv u \pmod{a}, \quad x \equiv v \pmod{b}.$$

Par le théorème des restes chinois, il existe un tel x, unique modulo ab. C'est dire que l'application ψ est une bijection.

Il reste à prouver que l'image par ψ de $(\mathbb{Z}/ab\mathbb{Z})^\times$ est $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. Si x est un élément inversible modulo ab il est encore inversible modulo a et modulo b, car si x_1 est un inverse de x modulo ab, c'est encore un inverse de x modulo a, et aussi modulo b. Ceci démontre l'inclusion

$$\psi\left((\mathbb{Z}/ab\mathbb{Z})^\times\right) \subset (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

Réciproquement soit $(\overline{u}, \overline{v})$ un couple dans $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$, et $\overline{x}$ son unique antécédent. Soit $\overline{u_1}$ et $\overline{v_1}$ les inverses respectifs de $\overline{u}$ et $\overline{v}$ dans $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$. Si $\overline{x_1}$ est l'antécédent de $(\overline{u_1}, \overline{v_1})$, l'entier xx_1 satisfait les congruences

$$xx_1 \equiv uu_1 \equiv 1 \pmod{a}, \quad xx_1 \equiv vv_1 \equiv 1 \pmod{b}.$$

Ce système de congruences admet la solution évidente 1, et par le théorème des restes chinois, cette solution est unique modulo ab. On a donc $xx_1 \equiv 1 \pmod{ab}$, ce qui prouve que $\overline{x}$ est un élément inversible de $\in \mathbb{Z}/ab\mathbb{Z}$. □

Corolaire 1.38 *La fonction d'Euler possède les propriétés suivantes :*

1. *Si p est premier $\varphi(p) = p - 1$.*
2. *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ alors*

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \dots (p_k - 1).$$

3. $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

Preuve : Le point (1) est évident, et (3) résulte immédiatement de (2). Pour montrer (2) on remarque que, les nombres $p_i^{\alpha_i}$ étant deux à deux premiers entre eux, on a, par la proposition précédente

$$\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \varphi\left(p_i^{\alpha_i}\right).$$

Il ne reste plus qu'à démontrer que, pour p premier, et α entier ≥ 1

$$\varphi\left(p^{\alpha}\right) = p^{\alpha - 1}(p - 1).$$

Or $\varphi\left(p^{\alpha}\right)$ est par définition le nombre des entiers n , $0 \leq n < p^{\alpha}$ qui sont premiers avec p. Il en résulte que $p^{\alpha} - \varphi(p^{\alpha})$ est le nombre des entiers $n \leq p^{\alpha}$ qui sont des multiples de p, c'est à dire $p^{\alpha - 1}$. □

Théorème 1.39 *Pour tout entier naturel $n \geq 1$, la fonction d'Euler satisfait l'identité*

$$\sum_{d|n, d>0} \varphi(d) = n.$$

Preuve : Considérons l'ensemble E des fractions

$$\left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \cdots, \frac{n-1}{n}, \frac{n}{n}\right\}.$$

mises sous forme irréductible. Les dénominateurs des fractions irréductibles obtenues sont tous les diviseurs d de n. Pour tout d de n notons E_d le sous-ensemble de E formé des fractions dont le dénominateur est d. Ce sont les fractions de la forme $\frac{a}{d}$ avec $1 \leq a \leq d$ et d premier avec n, il y a en donc $\varphi(d)$. Il en résulte $n = \sum_{d|n} \text{card } E_d = \sum_{d|n} \varphi(d)$.

□

Théorème 1.40 *Soit G un groupe cyclique d'ordre n (noté multiplicativement) et g un générateur de G. Les autres générateurs sont les g^t, avec t premier avec n.*

Plus généralement, soit g un élément d'ordre n d'un groupe G. Pour tout entier naturel e, l'ordre de g^e est $n/(n, e)$, où la notation (a, b) représente le plus grand diviseur commun des entiers a et b.

Preuve : Commençons par démontrer le deuxième point. Soit $d = (n, e)$ le pgcd de n et e. Soient n' et e' définis par

$$n = n'd \text{ et } e = e'd.$$

L'ordre de g^e est le plus petit entier naturel non nul k tel que

$$n \mid ek \text{ ou encore } n' \mid e'k. \tag{1.3}$$

Comme n' et e' sont premiers entre eux, (1.3) est satisfaite si et seulement si k est un multiple de $n' = n/d = n/(n,e)$.

Prouvons maintenant le premier point. On vient de démontrer que l'ordre de g^e est $n/(n,e)$. Dire que g^e est un générateur c'est dire que cet ordre est n, et donc que $(n,e) = 1$. □

Corolaire 1.41 *Le nombre de générateurs d'un groupe cyclique de cardinal n est $\varphi(n)$.*

Preuve : Soit g un générateur arbitraire. Par le théorème précédent, parmi les n éléments de $G = \left\{g^k \ ; \ 0 \leq k \leq n-1\right\}$ les générateurs sont obtenus pour k premier avec n. Par définition de φ, il y en a $\varphi(n)$. □

1.9 Le groupe multiplicatif du corps $\mathbb{Z}/p\mathbb{Z}$

Si p est premier, $\varphi(p) = p-1$ et le théorème d'Euler (1.34) donne imméditament le suivant.

Théorème 1.42 (Théorème de Fermat) *Si p est premier, pour tout entier a non multiple de p,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Remarque : Il résulte immédiatement de (1.42) que tout élément de $\mathbb{F}_p$, y compris l'élément 0, vérifie $a^p \equiv a \pmod{p}$.

Le théorème de Fermat fournit une condition nécessaire de primalité. Soit n un entier dont on veut prouver qu'il n'est pas premier : il suffit de trouver a tel que $(a,n) = 1$ et $a^{p-1} \not\equiv 1 \pmod{n}$.

Le théorème suivant est très important.

Théorème 1.43 (Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique) *Le groupe multiplicatif des éléments non nuls d'un corps fini est un groupe cyclique. En particulier, pour tout premier p, $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique.*

Preuve : Soit q le cardinal de $\mathbb{F}$, et $\mathbb{F}^\times$ le groupe multiplicatif des éléments non nuls de $\mathbb{F}$. Le cardinal de ce groupe est $q-1$. Quel que soit l'élément x de $\mathbb{F}^\times$, l'ordre de x est donc un diviseur de $q-1$. Pour tout diviseur d de $q-1$ notons $\psi(d)$ le nombre des $x \in \mathbb{F}^\times$ dont l'ordre est d. En partitionnant les éléments de l'ensemble $\mathbb{F}^\times$ selon la valeur de leur ordre on obtient l'équation

$$q - 1 = \sum_{d \mid q-1} \psi(d). \tag{1.4}$$

Montrons maintenant que, pour tout diviseur d de $q-1$, si $\psi(d) \neq 0$, alors $\psi(d) = \varphi(d)$, où φ est la fonction d'Euler. Puisque que $\psi(d) > 0$, il existe un élément a d'ordre d dans le groupe $\mathbb{F}^\times$. Puisque a est d'ordre d, les éléments

$$1, a, a^2, \ldots, a^{d-1}$$

sont tous distincts, et vérifient $x^d = 1$. Comme, dans un corps, un polynôme de degré d a au plus d racines, les éléments du corps $\mathbb{F}$ qui vérifient $x^d = 1$, (et particulier les éléments de $\mathbb{F}$ qui sont d'ordre d) sont les éléments du groupe cyclique $A = \{1, a, a^2, \ldots, a^{d-1}\}$. Par le corollaire (1.41) il y en exactement $\varphi(d)$, et l'équation (1.4) s'écrit encore

$$q - 1 = \sum_{d|q-1, \psi(d)\neq 0} \varphi(d).$$

S'il existait une valeur de d pour laquelle $\psi(d) = 0$, on aurait, en utilisant la propostion 1.39,

$$q - 1 = \sum_{d|q-1, \psi(d)\neq 0} \varphi(d) < \sum_{d|q-1} \varphi(d) = q - 1,$$

ce qui est absurde. Quel que soit le diviseur d de $q-1$, on a donc $\psi(d) = \varphi(d)$. En particulier $\psi(q-1) = \varphi(q-1)$, ce qui prouve qu'il existe un élément de $\mathbb{F}^\times$ dont l'ordre est $q - 1$. □

1.10 Les logarithmes discrets

Définition 1.44 (Logarithme discret) *Soit p premier, g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$. Dire que g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ c'est dire que $(\mathbb{Z}/p\mathbb{Z})^\times = \{g^0, g^1, \cdots, g^{p-2}\}$. Si $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, le* `logarithme discret` *de a en base g, noté $\log_g a$ est l'unique entier α tel que*

$$0 \leq \alpha \leq p - 2, \qquad a = g^\alpha.$$

Remarques :

1. Si n est un entier tel que $g^n = a$, le logarithme discret de a en base g est le reste de la division de n par $p - 1$.
2. Si $a \in \mathbb{Z}$ est un entier premier avec p, et g un entier tel que $\overline{g}$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ on appelle encore logarithme discret de a en base g l'unique entier n compris entre 1 et $p - 2$ tel que $a \equiv g^n \pmod p$.

Théorème 1.45 *Soit p premier, et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour tous a et b dans $(\mathbb{Z}/p\mathbb{Z})^\times$ on a*

$$\log_g ab = (\log_g a + \log_g b) \mod (p - 1)$$

Exemple 1.1 :

$p = 7$, et $g = 3$. Le tableau des puissances de g ci-dessous à gauche montre que g est un générateur. On en déduit la table des logarithmes en base g, représentée dans le tableau de droite.

k	0	1	2	3	4	5
g^k	1	3	2	6	4	5

x	1	2	3	4	5	6
$\log_g x$	0	2	1	4	5	3

On vérifie, par exemple, que

$$\log_3 5 = 5, \quad \log_3 6 = 3, \quad \log_3(30 = 2) = 2 = (5 + 3) \mod 6.$$

1.11 Exercices

Les exercices suivants sont faisables à la main. Seuls ceux qui sont suivis de la mention SCF (pour système de calcul formel) seront résolus à la machine, avec l'aide de `Maple`, ou `Pari`, par exemple.

Exercice 1.1
On note $a \div b$ le quotient de la division euclidienne de a par b. Démontrez la propriété d'associativité suivante pour tous b et c non nuls :

$$(a \div b) \div c = a \div (bc).$$

Exercice 1.2
Soit n un entier d'écriture décimale $n = c_k c_{k-1} \cdots c_1 c_0$. Montrer que

$$\begin{array}{rcll} n & \equiv & c_0 + c_1 + \cdots + & c_k & \pmod 9 \\ n & \equiv & c_0 - c_1 + \cdots + & (-1)^k c_k & \pmod{11}. \end{array}$$

Exercice 1.3
Exprimez, si cela est possible, 7 comme une combinaison linéaire à coefficients entiers de 1547 et 560.

Exercice 1.4
Résoudre $24x + 30y + 5z = 10$.

Exercice 1.5 (SCF)
Ecrivez une procedure qui factorise l'entier n en essayant successivement de le diviser par 2 puis pas tous les entiers impairs ≥ 3. Quelle est le temps de calcul de cette procédure dans le pire des cas ? Améliorez la de sorte que le temps de calcul soit, au pire, de l'ordre de $\sqrt{n}$.

Exercice 1.6
Démontrez que pour tout entier n et tout premier p, la valuation en p de $n!$ est donnée par

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor + \cdots$$

Quel est le nombre de zéros consécutifs qui terminent l'écriture décimale du nombre 2005! ?

(SCF) Écrire un programme qui recevant la donnée n affiche la décomposition en facteurs premiers de $n!$.

Exercice 1.7
Résoudre les équations

$$19x \equiv 2 \pmod{140} \qquad \text{et} \qquad 57x \equiv 87 \pmod{105}.$$

Exercice 1.8
Montrer que pout tout entier n, $n^7 - n$ est un multiple de 42, et $n^{13} - n$ un multiple de 455.

Exercice 1.9
Démontrer le théorème de Wilson : *Pour que p soit premier, il faut et il suffit que* $(p-1)! \equiv -1 \pmod{p}$.

Indication pour montrer que la primalité de p implique $(p-1)! \equiv -1 \pmod{p}$: quels sont les éléments de $\mathbb{F}_p$ qui sont leur propre inverse ? Ayant répondu a cette question, vous regrouperez deux par deux les termes du produit $\overline{1} \times \overline{2} \times \overline{3} \cdots \times \overline{(p-1)}$ en associant à chacun son inverse.

Exercice 1.10
Vérifier que les 4 derniers chiffres (en base 10) de 9376^2 sont 9376. Déterminer tous les entiers x, $0 \leq x < 10000$ tels que $x^2 \equiv x \pmod{10000}$?

Exercice 1.11
Résoudre le système de congruences

$$\begin{cases} 2x & \equiv & 3 & \pmod 5 \\ 4x & \equiv & 3 & \pmod 7 \\ 3x & \equiv & 5 & \pmod 8 \end{cases}$$

Exercice 1.12
Résoudre le système de congruences

$$\begin{cases} x & \equiv & a & \pmod 3 \\ x & \equiv & b & \pmod 5 \\ x & \equiv & c & \pmod 7 \end{cases}$$

Exercice 1.13
Soient p, q des entiers non nuls, et a, b des entiers arbitraires. Montrer que le système de congruences

$$\begin{cases} x & \equiv & a & \pmod p \\ x & \equiv & b & \pmod q \end{cases}$$

a des solutions si et seulement si (p, q) divise $b - a$.

Exercice 1.14
Démontrer que le calcul de φ est au moins aussi compliqué que la factorisation des entiers. Considérer pour cela les cas d'un entier $n = pq$, produit de deux nombres premiers. Montrer comment obtenir simplement les deux facteurs p et q à partir de la donnée de n et de $\varphi(n)$.

Exercice 1.15
Dans cet exercice on se propose de démontrer que $\varphi(n)$, le nombre des entiers compris entre 1 et n et premiers avec n, n'est jamais beaucoup plus petit que n. Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $p_1 < p_2 < \dots < p_k$ la décomposition de n en produit de facteurs premiers.

1. Montrer que $k \leq \dfrac{\log n}{\log 2}$.
2. Pour $1 \leq i \leq k$, montrer que $p_i \geq i + 1$.
3. en déduire que $\varphi(n) \geq \dfrac{\log 2}{2} \dfrac{n}{\log n}$.
4. (SCF) Vérifier que pour n variant de 1 à 100, la valeur moyenne du rapport $n/\varphi(n)$ est d'environ 1.91, la plus grande valeur étant 3.75.

Exercice 1.16
11 est premier avec 23. Quel est l'ordre de 11 modulo 23 ?

Exercice 1.17
Quels sont les deux derniers chiffres de 13^{479} ?

Exercice 1.18
Soit p un nombre premier, et q un facteur premier de $2^p - 1$.

1. Que pouvez vous dire de l'ordre de 2 modulo q ?
2. En déduire que $p < q$, et qu'il existe une infinité de nombres premiers.

Exercice 1.19
Soit $A = 2005^{2005}$,

B la somme des chiffres de A,
C la somme des chiffres de B,
D la somme des chiffres de C.

1. Majorer D. Montrer, par exemple, que $D \leq 13$.
2. Quelle est la classe de D modulo 9 ? En déduire la valeur de D.

Exercice 1.20
Soit a un entier impair non multiple de 5.

1. Calculer $(a, 10)$.
2. En déduire qu'il existe un multiple entier de a dont l'écriture décimale ne comporte que des 9.
3. En déduire qu'il existe un multiple entier de a dont l'écriture décimale ne comporte que des 1.

Exercice 1.21 (SCF)
Soit $n = 10^{80} + 1$. Montrer rapidement à l'aide du théorème de Fermat que n n'est pas premier.

Exercice 1.22 (SCF)
Ecrire un programme qui résoud l'équation $ax \equiv b \pmod{m}$ quand elle a des solutions, ou répond qu'elle n'a pas de solutions.

Exercice 1.23
Dans cet exercice on démontre que pour tout premier impair p et $\alpha \geq 2$ le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. Soit g un entier qui est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. Montrer que l'un des deux entiers g, $g+p$ est tel que $x^{p-1} \not\equiv 1 \pmod{p^2}$. Quitte à remplacer g par $g+p$ on supposera dans la suite que $g^{p-1} \neq 1 \pmod{p^2}$.
2. Montrer que l'ordre de g dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est de la forme $(p-1)p^\beta$, avec $0 \leq \beta \leq \alpha - 1$.
3. Montrer que g^{p-1} s'écrit $g^{p-1} = 1 + kp$, avec k non multiple de p.
4. Montrer que pour tout $m \geq 0$, il existe k_m non multiple de p, tel que

$$(1 + kp)^{p^m} = 1 + k_m p^{m+1},$$

et conclure.

CHAPITRE 2

Les carrés dans $(\mathbb{Z}/n\mathbb{Z})^\times$

Dans ce chapitre on s'intéresse à l'ensemble des carrés dans le corps $\mathbb{Z}/p\mathbb{Z}$, mais aussi dans certains anneaux $\mathbb{Z}/n\mathbb{Z}$ avec n non premier. On intoduit le symbole de Legendre qui caractérise les carrés. On introduit aussi le symbole de Jacobi défini sur $\mathbb{Z}/n\mathbb{Z}$ avec n entier impair non nécessairement premier. Le symbole de Jacobi ne permet pas de distinguer les carrés des non-carrés. Il est cependant un outil indispensable pour le calcul des symboles de Legendre. Sans utilisation du symbole de Jacobi il est pratiquement impossible de calculer un symbole de Legendre dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier grand (quelques centaines de chiffres décimaux).

2.1 Carrés et non carrés dans le corps $\mathbb{Z}/p\mathbb{Z}$

Commençons par un exemple simple. Dressons la table des carrés dans $\mathbb{Z}/p\mathbb{Z}$, avec $p = 7$.

x	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	2	2	4	1

Parmi les 6 éléments non nuls, 3 sont des carrés. Les 3 autres ne sont pas des carrés. De plus, chaque carré non nul a deux racines carrées :

$$\sqrt{1} = \pm 1, \quad \sqrt{2} = \pm 3, \quad \sqrt{4} = \pm 2.$$

Théorème 2.1 *Soit $p \neq 2$ premier et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. L'élément $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un carré si et seulement si son logarithme en base g est pair. Parmi les $p-1$ éléments non nuls de $(\mathbb{Z}/p\mathbb{Z})^\times$, la moitié exactement sont des carrés. Chaque carré non nul a 2 racines carrées.*

Preuve : Soit a dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et k son logarithme en base g. Si $k = 2\ell$ est pair $a = (g^\ell)^2$ est un carré. Réciproquement si a est le carré de g^t, $a = g^{2t}$, son logarithme discret est le reste de la division de $2t$ par $p-1$ qui est pair, car $p-1$ est pair. Si a est un carré non nul, $a = b^2$, l'élément $-b$ est une racine du polynôme $x^2 - a$, distincte de la racine b. Le polynôme $x^2 - a$ de $\mathbb{F}_p[x]$ étant de degré 2, il n'admet pas d'autre racine. □

Théorème 2.2 (Le critère d'Euler) *Pour que a premier avec p soit un carré modulo p il faut et il suffit que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Preuve : On calcule dans $\mathbb{Z}/p\mathbb{Z}$. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Si $\overline{a}$ est un carré $\overline{a} = g^{2t}$, on a $\overline{a}^{(p-1)/2} = \overline{a}^{2t\frac{p-1}{2}} = g^{(p-1)t} = 1$. Si $\overline{a} = g^{2t+1}$ n'est pas un carré, on a $\overline{a}^{(p-1)/2} = g^{(p-1)t} g^{(p-1)/2} = 1 \cdot (-1) = -1$. Car $g^{(p-1)/2}$ est une racine de $x^2 - 1 = 0$ différente de 1, c'est donc -1. □

2.2 Symbole de Legendre

Définition 2.3 *Soit $a \in \mathbb{Z}$, et p premier* impair. *On définit le* `symbole de Legendre` *par*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } \overline{a} \text{ est un carré non nul dans } (\mathbb{Z}/p\mathbb{Z})^\times \\ -1 & \text{si } \overline{a} \text{ n'est pas un carré dans } (\mathbb{Z}/p\mathbb{Z})^\times \\ 0 & \text{sinon} \end{cases}$$

Théorème 2.4 *Le symbole de Legendre satisfait les propriétés suivantes : Pour tous a et b entiers, p et q premiers* impairs,

Critère d'Euler : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Périodicité : $\left(\frac{a+\lambda p}{p}\right) = \left(\frac{a}{p}\right)$

Multiplicativité : $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Caractère quadratique de -1 : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Caractère quadratique de 2 : $\left(\frac{2}{p}\right) = \begin{cases} +1 \text{ si } p \equiv \pm 1 \bmod 8 \\ -1 \text{ si } p \equiv \pm 3 \bmod 8 \end{cases}$

Loi de réciprocité quadratique : $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

Nous ne démontrerons pas ce théorème. Les points 1,2,3,4 sont faciles. Le point 5 (caractère quadratique de 2 modulo p), et surtout le point 6, sont plus délicats. La loi de réciprocité quadratique est un résultat remarquable, dû à Gauss, dont il existe de tres nombreuses démonstrations.

Exemple 2.1 :

Calcul de $\left(\frac{31}{71}\right)$. La loi de réciprocité quadratique, puis la périodicité, donnent

$$\left(\frac{31}{71}\right) = (-1)^{15\times 35}\left(\frac{71}{31}\right) = -\left(\frac{9+2\times 31}{31}\right) = -\left(\frac{9}{31}\right) = -1.$$

2.3 Insuffisance du symbole de Legendre

Sachant que le nombre 239 est premier, proposons nous de calculer le symbole de Legendre $\left(\frac{143}{239}\right)$: Pour appliquer la loi de réciprocité quadratique, il faudrait que le symbole de Legendre $\left(\frac{239}{143}\right)$ soit défini donc que 143 soit premier. Ce n'est pas le cas

car $143 = 11 \cdot 13$. Le seul moyen d'avancer dans le calcul est d'utiliser cette factorisation, et la multiplicativité du symbole de Legendre. On écrit

$$\left(\frac{143}{239}\right) = \left(\frac{11}{239}\right)\left(\frac{13}{239}\right).$$

La loi de réciprocité quadratique s'applique maintenant aux deux symboles $\left(\frac{11}{239}\right)$ et $\left(\frac{13}{239}\right)$ car 11 et 13 sont premiers, et cela conduit à

$$\left(\frac{143}{239}\right) = -\left(\frac{239}{11}\right)\left(\frac{239}{13}\right) = -\left(\frac{8}{11}\right)\left(\frac{5}{13}\right) = -\left(\frac{4}{11}\right)\left(\frac{2}{11}\right)\left(\frac{13}{5}\right),$$

puis

$$\left(\frac{143}{239}\right) = -\left(\frac{2}{11}\right)^2\left(\frac{2}{11}\right)\left(\frac{3}{5}\right) = -[1 \cdot (-1) \cdot (-1)] = -1.$$

Le calcul est ici très simple car la factorisation de 143 est évidente. Dans le cas général le calcul du symbole de Legendre $\left(\frac{a}{p}\right)$ lorsque a est non premier nous ramène au problème de la *factorisation* de a qui est un problème difficile. Le symbole de Jacobi supprime cette difficulté.

Définition 2.5 *Soit n un entier positif* impair, *dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Le* `symbole de Jacobi` $\left(\frac{m}{n}\right)$ *est défini par*

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1}\left(\frac{m}{p_2}\right)^{\alpha_2} \dots \left(\frac{m}{p_k}\right)^{\alpha_k}.$$

Théorème 2.6 *Les propriétés essentielles du symbole de Jacobi sont*

1. *L'équation $\left(\frac{a}{n}\right) = 1$ ne caractérise pas les carrés inversibles de $\mathbb{Z}/n\mathbb{Z}$.*
2. *Le symbole de Jacobi ne vérifie pas le critère d'Euler : en général,*
$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}.$$
3. *Périodicité :* $\left(\frac{a+\lambda n}{n}\right) = \left(\frac{a}{n}\right)$
4. *Multiplicativité :* $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
5. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
6. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} +1 \text{ si } n \equiv \pm 1 \bmod 8 \\ -1 \text{ si } n \equiv \pm 3 \bmod 8 \end{cases}$
7. *Loi de réciprocité quadratique :*
Pour tous m et n impairs, $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right)$

Les deux premières propriétés montrent que le symbole de Jacobi n'a a pas de signification mathématique intéressante, contrairement au symbole de Legendre qui permet de reconnaitre les carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Mais c'est un *outil de calcul indispensable*. Reprenons l'exemple du calcul de $\left(\frac{143}{239}\right)$. On commence par appliquer la loi de

réciprocité quadratique, sans se poser la question de la primalité de 143, et on écrit successivement

$$\begin{aligned}\left(\frac{143}{239}\right) &= -\left(\frac{239}{143}\right) = -\left(\frac{96}{143}\right) = -\left(\frac{2^5\cdot 3}{143}\right)\\ &= -\left(\frac{2}{143}\right)^4\left(\frac{2}{143}\right)\left(\frac{3}{143}\right) = -\left(\frac{3}{143}\right)\\ &= \left(\frac{143}{3}\right) = \left(\frac{2}{3}\right) = -1.\end{aligned}$$

Il n'est plus necessaire de factoriser les entiers, sauf pour sortir les facteurs 2 lorsque l'argument figurant au numérateur est pair. On utilise essentiellement la loi de réciprocité, et la périodicité. Le calcul du symbole de Jacobi $\left(\frac{a}{b}\right)$ est semblable au calcul du *pgcd* de a et b par l'algorithme d'Euclide. Le calcul d'un symbole de Legendre en utilisant les symboles de Jacobi ne nécessite que $O(\log b)$ divisions.

2.4 Les carrés dans $(\mathbb{Z}/pq\mathbb{Z})^\times$

Avant de nous intéresser à l'étude des carrés dans $(\mathbb{Z}/n\mathbb{Z})^\times$ pour n entier quelconque, commençons par le cas particulier, d'un entier $n = pq$, produit de 2 nombres premiers distincts, p et q. Ce cas est très fréquent en cryptographie. De nombreux protocoles utilisent un entier n de ce type, avec p et q deux grands nombres premiers. Pour $n = 15 = 3\cdot 5$, la table des carrés des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ est

x	1	2	4	7	8	11	13	14
$x^2 \bmod 15$	1	4	1	4	4	1	4	1

Il n'y a que 2 carrés, 1 et 4, et chacun d'eux a 4 racines carrées :

$$\sqrt{1} = \pm 1, \pm 4, \quad \sqrt{4} = \pm 2, \pm 7.$$

Théorème 2.7 *Soit $n = pq$, avec p, q premiers impairs. Le nombre de carrés inversibles modulo n est $\frac{1}{4}\varphi(n) = \frac{(p-1)(q-1)}{4}$. Chaque carré admet 4 racines carrées distinctes.*

Preuve : Notons C_n l'ensemble des carrés des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$. Soit $a \in \mathbb{C}_n$ et α une racine carrée de a modulo n. Puisque $n = pq$ avec $(p, q) = 1$, on a

$$x^2 \equiv a \pmod{n} \iff x^2 \equiv \alpha^2 \pmod{n} \iff \begin{cases} x \equiv \pm\alpha \pmod{p} \\ x \equiv \pm\alpha \pmod{q} \end{cases}$$

car, dans les corps $\mathbb{Z}/p\mathbb{Z}$ et dans $\mathbb{Z}/q\mathbb{Z}$, α^2 a exactement deux racines carrées qui sont $\pm\alpha$. Et chacun des 4 systèmes chinois admet une unique solution modulo $n = pq$. L'application $(\mathbb{Z}/n\mathbb{Z})^\times \mapsto C_n \ : \ x \to x^2$ est surjective, et, vu le calcul précédent l'image réciproque de tout élément de C_n, est de cardinal 4. Il en résulte

$$|C_n| = \frac{1}{4}\left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \frac{(p-1)(q-1)}{4}.$$

□

2.5 Les carrés dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$

Le théorème précédent ramène l'étude des carrés dans $(\mathbb{Z}/n\mathbb{Z})^\times$ à l'étude des carrés dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, avec p premier, et α entier ≥ 1. Il faut mettre à part le nombre premier 2. Commençons par le cas d'un premier impair.

Théorème 2.8 *Soit p premier* impair, *α entier ≥ 1, et $a \in \mathbb{Z}$, premier avec p, donc aussi avec p^α*

1. *Alors $\overline{a}$ est un carré dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ si et seulement si a est un carré modulo p, c'est à dire si et seulement si le symbole de Legendre de a vérifie $\left(\frac{a}{p}\right) = 1$.*
2. *Chaque carré non nul de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ a exactement 2 racines carrées.*
3. *Si x_1 est une racine carrée de a modulo p, il existe, pour tout entier $n \geq 1$, un entier x_n, unique modulo p^n, qui vérifie*

$$x_n \equiv x_1 \pmod{p}, \qquad x_n^2 \equiv a \pmod{p^n}.$$

Les x_n se construisent par récurrence, en cherchant x_{n+1} sous la forme

$$x_{n+1} = x_n + p^n u$$

où u est une inconnue entière à déterminer.

Preuve : La démonstration est une application de la `méthode de Hensel` qui, partant d'une solution modulo p d'une équation, construit une solution modulo p^α de la même équation. Soit a un carré modulo $\mathbb{Z}^n$. La congruence $a \equiv x^2 \pmod{p^n}$ implique la congruence $a \equiv x^2 \pmod{p}$. Il en résulte que a est aussi un carré modulo p.

Comme l'équation $x^2 \equiv a \pmod{p}$ admet exactement deux solutions, il suffit de démontrer le point 3 pour conclure. Le résultat est vrai pour $n = 1$. Supposons le vrai à l'ordre n. Si x_{n+1} est solution de

$$x_{n+1} \equiv x_1 \pmod{p}, \quad x_{n+1}^2 \equiv a \pmod{p^{n+1}},$$

il est évidemment solution de $x_{n+1} \equiv x_1 \pmod{p}$ et $x_{n+1}^2 \equiv a \pmod{p^n}$, et, par hypothèse de récurrence (unicité modulo p^n), x_{n+1} est de la forme

$$x_{n+1} = x_n + up^n,$$

avec u entier. On a alors

$$x_{n+1}^2 = (x_n + up^n)^2 = x_n^2 + 2x_n up^n + u^2 p^{2n}.$$

puis

$$x_{n+1}^2 \equiv x_n^2 + 2x_n up^n \pmod{p^{n+1}}.$$

Par hypothèse il existe v entier tel que $x_n^2 = a + vp^n$. Pour que $x_{n+1}^2 \equiv a \pmod{p^{n+1}}$ il est donc nécessaire et suffisant que u soit solution de

$$vp^n + 2x_n up^n \equiv 0 \pmod{p^{n+1}}.$$

Après simplification par p^n, il faut et il suffit pour cela que u vérifie

$$v + 2xu \equiv 0 \pmod{p}.$$

Comme p est impair, et x premier avec p, cette équation en u a une solution unique modulo p. Il en résulte l'existence, et l'unicité modulo p^{n+1}, de x_{n+1}. □

Pour $p = 2$ la méthode de Hensel ne fonctionne pas. On a cependant le résultat suivant.

Théorème 2.9

1. *L'unique élément* $\overline{1}$ *de* $(\mathbb{Z}/2\mathbb{Z})^\times$ *est son propre carré.*
2. $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$. *Parmi ces deux éléments l'un est un carré,* $\overline{1}$*, et il admet deux racines carrées,* $\overline{1}$ *et* $\overline{3} = \overline{-1}$.
3. *Soit* $\overline{x} \in (\mathbb{Z}/2^n\mathbb{Z})^\times$*, avec* $n \geq 3$*. Alors* $\overline{a}$ *est un carré si et seulement si* a *est un carré modulo* 8*, c'est à dire si et seulement si* $a \equiv 1 \pmod 8$*. Dans ce cas, chaque carré a exactement* 4 *racines carrées, et exactement un quart des éléments de* $(\mathbb{Z}/2^n\mathbb{Z})^\times$ *sont des carrés.*
4. *Pour* $n \geq 3$*, on calcule les racines carrées de* a *modulo* 2^n*, par récurrence sur* n*, en utilisant la propriété suivante : Soit* x *une racine quarrée de* a *modulo* 2^n*. Alors,*
   (a) *Les autres racines carrées de* a *modulo* 2^n *sont les éléments de l'ensemble* $\{\pm x, \pm(x + 2^{n-1})\}$.
   (b) *Si* x *n'est pas une racine carrée de* a *modulo* 2^{n+1}*,* $x + 2^{n-1}$ *est une racine carrée de* a *modulo* 2^{n+1}.

Preuve : Les points 1 et 2 sont évidents.

Pour $n = 3$ on vérifie immédiatement que dans $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ il n'y a qu'un carré, $\overline{1}$, et dont les 4 racines carrées sont $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

Soit $n \geq 3$, et a premier avec 2^n (c'est à dire impair) qui est un carré modulo 2^n, et x une racine carrée de a modulo 2^n. Il existe λ entier avec

$$x^2 = a + \lambda\, 2^n. \tag{2.1}$$

Remarquons que, puisque a est impair, x aussi est impair.

1. On vérifie immédiatement que les entiers, $\pm x, \pm(x + 2^{n-1})$, deux à deux distincts modulo 2^n sont des racines carrées de a modulo 2^n.
2. Si λ est pair (2.1) montre que x est aussi une racine carrée de a modulo 2^{n+1}. Si λ est impair, $x_1 = x + 2^{n-1}$, qui vérifie

   $$x_1^2 - a = \lambda 2^n + x2^n + 2^{2n-2} = (\lambda + x)2^n + 2^{2n-2}$$

   est une racine de a modulo 2^{n+1}.

Utilisant les points 1 et 2 ci dessus, si $a \equiv 1 \pmod 8$, en partant d'une racine carrée x de a modulo 8, par exemple $x = 1$, on construit, pour tout $n \geq 3$ un ensemble $\{\pm x_n, \pm(x_n + 2^{n-1})\}$ dont les 4 éléments sont des racines de a modulo 2^n. Pour terminer la démonstration il suffit de démontrer que chaque élément du sous-ensemble C_n de $(\mathbb{Z}/2^n\mathbb{Z})^\times$ formé des éléments congrus à 1 modulo 8 admet au plus 4 racines carrées. Considérons l'application surjective

$$\begin{array}{ccc} (\mathbb{Z}/2^n\mathbb{Z})^\times & \to & C_n \\ x & \mapsto & x^2 \end{array}$$

Les images réciproques des éléments de C_n forment une partition de l'ensemble $(\mathbb{Z}/2^n\mathbb{Z})^\times$. On vient de démontrer que chaque classe est de cardinal au moins 4. Le nombre de classes, card $C_n = 2^{n-3}$, est le quart du cardinal de card $(\mathbb{Z}/2^n\mathbb{Z})^\times = 2^{n-1}$. Donc chaque classe a exactement 4 éléments. □

2.6 Les carrés dans $(\mathbb{Z}/n\mathbb{Z})^\times$ avec n quelconque

Théorème 2.10 *Soit n un entier ≥ 2, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers, et soit a un entier premier avec n. Pour que a soit un carré modulo n il faut et il suffit que, pour tout i, $1 \leq i \leq k$, a soit un carré modulo $p_i^{\alpha_i}$.*

Preuve : Dire que $x^2 \equiv a \pmod{n}$ c'est dire que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ divise $x^2 - a$. Commes les nombres $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ sont deux à deux premiers entre eux, c'est dire que $x^2 - a$ est divisible par chacun de ces nombres, autrement dit

$$x^2 \equiv a \pmod{n} \iff \begin{cases} x^2 \equiv a \pmod{p_1^{\alpha_1}} \\ x^2 \equiv a \pmod{p_2^{\alpha_2}} \\ \vdots \\ x^2 \equiv a \pmod{p_k^{\alpha_k}} \end{cases} \tag{2.2}$$

Ceci implique que a est un carré modulo chacun des $p_i^{\alpha_i}$. Réciproquement si a est un carré modulo chacun des $p_i^{\alpha_i}$, il existe, pour chaque i, $1 \leq i \leq k$ un x_i tel que $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$. Par le théorème des restes chinois, il existe un x tel que $x \equiv x_i \pmod{p_i^{\alpha_i}}$ pour tout i. On en déduit que, pour tout i, $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$. C'est dire que x est solution du système figurant à droite de (2.2), et donc de $x^2 \equiv a \pmod{n}$. □

Exercices

Exercice 2.1
7369 et 9283 sont premiers. Calculez de deux manières différentes le symbole de Legendre $\left(\frac{7369}{9283}\right)$:

1. En utilisant uniquement le symbole de Legendre.
2. En utilisant le symbole de Jacobi.

Exercice 2.2
Démontrez que la loi de réciprocité quadratique peut aussi s'écrire, c'était d'ailleurs la forme utilisée pas Gauss,

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

Exercice 2.3
Soit p premier impair. Déterminer $\left(\frac{\frac{p+1}{2}}{p}\right)$ et $\left(\frac{\frac{p-1}{2}}{p}\right)$.

Exercice 2.4
Démontrer, par exemple lorsque $m = 15$, les points 1 et 2 du théorème 2.6 en exhibant un entier a qui n'est pas un carré modulo 15, tel que $\left(\frac{a}{m}\right) = 1$, et en outre $\left(\frac{a}{m}\right) \not\equiv a^{(m-1)/2} \pmod{m}$.

Exercice 2.5
Quels sont les p premiers pour lesquels l'équation $x^2 \equiv 3 \pmod{p}$ admet au moins une solution ?

Exercice 2.6
Montrez que les diviseurs premiers de $4n^2 + 1$ sont de la forme $4k + 1$.

Exercice 2.7
Pour quels p premiers l'équation $x^2 \equiv 5 \pmod{p}$ a-t-elle des solutions ?

Exercice 2.8
Que peut–on dire des diviseurs premiers de $12n^2 - 1$? Et de $12n^2 + 1$?

Exercice 2.9
Résolvez les équations

1. $x^2 \equiv 15 \pmod{77}$.
2. $x^2 + 3\,x + 7 \equiv 0 \pmod{115}$
3. $x^2 + x + 3 \equiv 0 \pmod{125}$.

Exercice 2.10
Soit p premier, et a, b, c entiers, a non multiple de p. Montrer que le nombre de solutions de l'équation $ax^2 + bx + c = 0$ dans le corps $\mathbb{F}_p$ est $1 + \left(\frac{D}{p}\right)$, où $D = b^2 - 4ac$ est le discriminant de $ax^2 + bx + c$.

Exercice 2.11

1. Pour quels p premiers l'équation $x^2 + 6x + 1 = 0 \pmod{p}$ a-t-elle des solutions ?
2. Pour quels p premiers l'équation $x^2 + x + 1 = 0 \pmod{p}$ a-t-elle des solutions ?
3. Mêmes questions en remplaçant dans les deux cas *Pour quels premiers p* par *Pour quels entiers naturels n.*

Exercice 2.12
Soit $f = x^2 + 2x + 9$. Montrer que

1. $f \equiv 0 \pmod 8$ admet deux solutions modulo 8.
2. $f \equiv 0 \pmod{16}$ n'admet pas de solution.

Exercice 2.13
Montrez que si q et $p = 4q + 1$ sont premiers 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 2.14
p est un nombre premier de la forme $4n + 1$. Montrez que $n^n \equiv 1 \pmod p$.

Exercice 2.15
Soit $p = F_n = 2^{2^n} + 1$, avec $n \geq 1$.

1. On suppose p premier.
   (a) Montrez que g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $\left(\frac{g}{p}\right) = -1$.
   (b) Montrez que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. Ici on ne suppose pas p premier, mais seulement que

$$3^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

   Montrez que p est premier. Ce test de primalité pour les nombres de Fermat est le test de Pepin.

Exercice 2.16
Soit a un élément *non nul* de $\mathbb{F}_p$. On se propose de démontrer que, pour $x \in \mathbb{F}_p$, les évènements x *est un carré non nul* et $x + a$ *est un carré non nul* sont à peu près indépendants, c'est à dire que le nombre des $x \in \mathbb{F}_p$ tels que $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$ est environ $\frac{p}{4}$. On note donc A_p le nombre des entiers $x \in \{0, 1, \ldots, p-1\}$ tels que $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$.

1. Dans le cas où $a = 1$ calculer A_7.
2. On pose $S_p = \sum_{x=0}^{p-1} \left[1 + \left(\frac{x}{p}\right)\right]\left[1 + \left(\frac{x+a}{p}\right)\right]$. Montrez que

$$S_p = 4\,A_p + 2 + \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right).$$

3. On est ainsi ramené au calcul de S_p. Montrez que

$$S_p = p + \sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right).$$

4. Pour $1 \leq x \leq p-1$, soit y l'inverse de x modulo p. Montrez que

$$\left(\frac{x(x+a)}{p}\right) = \left(\frac{1+ay}{p}\right).$$

5. En déduire que $S_p = p-1$, puis la valeur de A_p, et enfin l'encadrement

$$\frac{p-5}{4} \leq A_p \leq \frac{p-1}{4}.$$

CHAPITRE 3

Quelques algorithmes 1

On donne ici quelques algorithmes essentiels en arithmétique. L'algorithme des puissances en particulier qui permet de calculer rapidement des expressions comme $a^b \bmod n$ où a, b, n sont des nombres de quelques centaines de chiffres. L'algorithme d'extraction d'une racine carrée dans $\mathbb{Z}/p\mathbb{Z}$ est aussi très utile en cryptographie. On prouve aussi que, lorsque n n'est pas premier, l'extraction des racines carrées modulo n est aussi difficile que la factorisation de n. On termine par le crible d'Eratosthène, toujours utilisé, ne serait-ce que pour construire une table des nombres premiers.

3.1 La multiplication du pauvre

L'algorithme suivant permet de multiplier deux nombres pourvu qu'on sache multiplier et diviser par 2. Pour multiplier 37 par 19 on écrit,

19	37
9	74
~~4~~	~~148~~
~~2~~	~~296~~
1	592
$19 \cdot 37$	$= 37 + 74 + 592 = 703$

Dans la colonne de gauche on passe d'une ligne à l'autre en divisant par 2, dans la colonne de droite on multiplie par 2. Puis on raye les lignes dans lesquelles le terme de gauche est pair, et enfin on ajoute les termes de droite dans les lignes non rayées.
Preuve : Les divisions par 2 donnent la décomposition de 19 en base 2. En numérotant les lignes à partir de 0, le coefficient de 2^k dans l'écriture binaire de 19 est 1 si et seulement si la ligne de rang k commence par un nombre impair. On a donc

$$\begin{array}{lllllll} 19 & = & 1 & + & 2 & + & 16 \\ 19 \cdot 37 & = & 1 \cdot 37 & + & 2 \cdot 37 & + & 16 \cdot 37. \end{array}$$

□

Ceci conduit immédiatement à l'algorithme suivant : les valeurs successives de a sont le nombres de la colonne de gauche, le valeurs de y sont les nombres de la colonne de droite, tandis que z cumule les valeurs de y figurant dans les lignes non rayées.

```
Fonction multiplie(A, B)
Var z;
début
    z := 0;
    tant que B > 0 faire
        si B mod 2 = 1 alors z := z + A A := A + A;
        B := B div 2
    fin
    retourner z
fin
```

Algorithme 1 : La multiplication du pauvre

Preuve : Prouvons que cet algorithme, appelé avec les valeurs de départ $A = a$ et $B = b$ se termine en renvoyant ab. Il se termine car à chaque passage dans le corps du `tant que` la valeur entière de B est divisée par 2. Pour vérifier qu'il renvoie ab il suffit de démontrer que, après chaque passage dans le corps de la boucle `tant que`, la quantité $AB + z$ reste inchangée. On exprime ceci en disant que $AB + z$ est un `invariant de la boucle tant que`. En effet supposons démontré que

$$AB + z = \text{ constante.}$$

Quand on entre dans la boucle pour le première fois on a $z = 0$, $A = a$ et $B = b$, donc $AB + z = ab$. Quand on sort de la boucle pour la dernière fois on a toujours $AB + z = ab$, et puisque $B = 0$, $z = ab$.

Il ne reste qu'à vérifier l'invariance de $AB + z$. Soient A_1, B_1, z_1 les valeurs des variables A, B, z en entrant dans la boucle `tant que`, et A_2, B_2, z_2 les valeurs de ces variables en sortant de la boucle. L'instruction `si` se traduit par $z_2 = z_1 + rA_1$, où r est le reste de la division de B_1 par 2. L'instruction suivante se traduit par $A_2 = 2A_1$. La troisième instruction remplace B_2 par son quotient euclidien par 2. On a donc $B_1 = 2B_2 + r$. Il en résulte

$$B_1A_1 + z_1 = (2B_2 + r)A_1 + z_2 - rA_1 = B_2(2A_1) + z_2 = B_2A_2 + z_2.$$

□

3.2 L'algorithme des puissances

C'est un algorithme important qui permet de calculer a^n en $O(\log n)$ opérations, au lieu de n opérations. C'est le même que celui de la multiplication du pauvre dans lequel l'opération d'addition a été remplacée par la multiplication, et l'élément neutre 0 de l'addition remplacé par l'élément neutre 1 de la multiplication. En effet, calculer $a \cdot b$ c'est calculer $a + a + \cdots + a$ où le a est répété b fois, tandis que calculer a^b c'est calculer $a \cdot a \cdot \cdots \cdot a$ où le a est répété b fois.

```
Fonction puissance(A, B)
Var z;
début
    z := 1;
    tant que B > 0 faire
        si B mod 2 = 1 alors z := z · A;
        A := A × A ; B := B/2;
    fin
    retourner z;
fin
```

Algorithme 2 : L'algorithme des puissances

Preuve : La même que pour l'algorithme précédent en démontrant que la valeur de $A^B \cdot z$ est un invariant de la boucle tant que, dont la valeur initiale est a^b et la valeur terminale celle de z. □

3.3 L'exponentiation modulaire

Remplaçant maintenant la multiplication ordinaire par la multiplication modulo n on obtient l'algorithme d'exponentiation modulaire.

```
Fonction PuissanceMod(A, B, n);
Var z;
début
    z := 1;
    tant que B > 0 faire
        si B mod 2 = 1 alors z := z ∗ A mod n;
        A := A ∗ A mod n ; B := B/2;
    fin
    retourner z;
fin
```

Algorithme 3 : L'exponentiation modulaire

Quelle est la complexité de cette procédure, c'est à dire son coût, en fonction de la taille des données ?

On entre dans le corps de la boucle `tant que` autant de fois qu'il faut diviser b par 2 pour atteindre 0. Le nombre de passages dans la boucle tant que est donc $\log_2 b = O(\log b)$. Si on considère que les opérations arithmétiques sur $\mathbb{N}$ se font en temps constant $O(1)$, le coût de cet algorithme est évidemment $O(\log b)$. Si les valeurs de n considérées sont trop grandes pour être mémorisées dans un mot machine, les opérations d'addition et de soustraction sont de coût $O(\log n)$, et la multiplication et la division de coût $O(\log^2 n)$. Dans ce cas, on a

Théorème 3.1 *Le coût de l'exponentiation modulaire est* $O(\log^2 n)(\log b))$. *En particulier le calcul de* $a^n \bmod n$ *est de coût* $O(\log^3 n)$.

Preuve : A chaque passage dans le corps de la boucle `tant que` la multiplication (éventuelle) de y par z, suivie de la réduction modulo n, et la multiplication de y par y suivie de la réduction modulo N sont de coût $O(\log^2 n)$. La division par 2 de l'entier b est $O(\log b)$ est de coût $O(1)$ (si elle est effectuée sans recopie). Chaque passage coûte donc $O(\log^2 n)$, le nombre de passages est $\log_2(b)$. □

Application : un test efficace de non primalité

On a vu dans le premier chapitre que si l'entier n est premier, alors, pour tout entier a premier avec n, on a

$$a^{n-1} \equiv 1 \bmod n.$$

Pour prouver que le nombre impair (donc premier avec 2) n'est pas un nombre premier il suffit de vérifier que 2^{n-1} n'est pas congru à 1 modulo n. On utilise l'algorithme PuissanceMod pour calculer $2^{n-1} \pmod n$,

Exemple 3.2 :

```
> n := 437423879543218906432764213456789097564321567897543211 ;
> PuissanceMod(2,n-1,n)
      = 217032335061865329690807926019318156653702382360731597.
```

$2^{n-1} \neq 1 \pmod n$, donc n n'est pas premier.

3.4 Calcul d'une racine carrée modulo p

Un autre algorithme fondamental en arithmétique est l'algorithme de calcul d'une racine carrée dans le corps $\mathbb{Z}/p\mathbb{Z}$, lorsque p est premier. Commençons par un cas particulièrement simple :

La cas $p = 4k+3$ Dans ce cas la fonction racine carrée se réduit à la fonction monôme

$$x \to x^{\frac{p+1}{4}}.$$

En effet, si $a$est un carré, et $x = a^{\frac{p+1}{4}}$. Alors $x^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \bmod p$, car, a étant un carré, le critère d'Euler donne $1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Le cas général Soit a le nombre dont on recherche la racine carrée. La première chose à faire est de trouver un élément b de $\mathbb{Z}/p\mathbb{Z}$ qui ne soit pas un résidu quadratique c'est à dire pas un carré. On choisit pour cela un b au hasard, et, utilisant le critère d'Euler, on calcule $b^{\frac{p-1}{2}} \pmod p$. Si le résultat est -1 on a gagné, b n'est pas un carré. Sinon on recommence. Comme la moitié des éléments de $\mathbb{Z}/p\mathbb{Z}$ sont des carrés, on a une chance sur 2 de gagner à chaque essai, et on est donc sûr de trouver rapidement un non carré. Remarquons que cet algorithme pour la recherche d'un non carré, entre dans la classe des **algorithmes probabilistes.** Si on est malchanceux il ne terminera jamais ou après un temps extremement long. En pratique il se terminera toujours assez rapidement.

L'entier n non carré modulo p étant ainsi choisi, on s'intéresse alors aux couples d'entiers naturels (e_1, e_2) tels que

$$a^{e_1} b^{e_2} \equiv 1 \bmod p. \tag{3.1}$$

- a étant un carré, le couple $(\frac{p-1}{2}, 0)$ est solution de (3.1) par le critère d'Euler.
- Si (3.1) est vérifié, alors e_2 **est pair**. En effet

$$1 = \left(\frac{a^{e_1} b^{e_2}}{p}\right) = \left(\frac{a}{p}\right)^{e_1} \left(\frac{b}{p}\right)^{e_2} = (-1)^{e_2}.$$

– Si e_1 est impair dans (3.1), alors

$$x = a^{\frac{e_1+1}{2}} b^{\frac{e_2}{2}}$$

est une racine carrée de a. En effet $x^2 = a^{e_1+1}b^{e_2} = aa^{e_1}b^{e_2} = a$.

– Si e_1 est pair on peut remplacer le couple (e'_1, e'_2) par un autre couple ayant la même propriéte, avec $e'_1 = e_1/2$. En effet, considérons

$$u = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}}.$$

Vue la relation (3.1), on a $u^2 = 1$. Donc $u = 1$ ou $u = -1$.

- Si $u = 1$ on obtient encore une équation de la forme (3.1) en remplaçant e_1 par $e_1/2$, et e_2 par $e_2/2$.
- Si $u = -1$ on écrit $1 = -u = u \cdot (-1) = a^{\frac{e_1}{2}} b^{\frac{e_2}{2}} b^{\frac{p-1}{2}}$, et on obtient encore une équation de la forme (3.1) en remplaçant e_1 par $e_1/2$, et e_2 par $(e_2 + p - 1)/2$.

On part donc du couple $(e_1, e_2) = ((p-1)/2, 0)$. Tant que e_1 est pair, on remplace ce couple par un autre couple ayant la même propriété, mais avec e_1 deux fois plus petit. En recommençant l'opération, au plus $\log_2(p-1)$ fois, on est sur d'obtenir un couple dont la première composante e_1 est impaire. Cela donne l'algorithme donné dans la figure Algorithme 4.

Fonction racine(a, p) ;
// a `est un carre modulo` p
Var e_1, e_2, u, r, b : entiers;
début
  $b := 2$;
  tant que $b^{\frac{p-1}{2}} \bmod p = 1$ **faire** $b := b + 1$;
  $e_1 := (p-1)/2$; $e_2 := 0$;
  tant que $e_1 \bmod 2 = 0$ **faire**
    $e_1 := e_1/2$; $e_2 := e_2/2$;
    $u := a^{e_1} \cdot b^{e_2} \bmod p$;
    si $u \neq 1$ **alors** $e_2 := e_2 + (p-1)/2$;
  fin
  $r := a^{\frac{e_1+1}{2}} \cdot b^{\frac{e_2}{2}} \bmod p$;
  retourner r
fin

Algorithme 4 : Calcul d'une racine carrée modulon p

3.5 Racine carrée et factorisation

On montre ici que la problème de l'extraction des des racines carrées dans $(\mathbb{Z}/n\mathbb{Z})^\times$, pour n non premier, est au moins aussi difficile que la factorisation de n. Pour rendre les choses plus claires prenons le cas d'un entier n produit de deux facteurs premiers (la situation la plus courante en cryptographie).

Théorème 3.2 *Soit $N = pq$ un produit de 2 nombres premiers. On suppose que l'on dispose d'un oracle qui répond à la question* Donnez moi une racine carrée de x modulo

N. En posant k questions à cet oracle on peut déterminer la factorisation de N avec une probabilité plus grande que $1 - 1/2^k$.

Preuve : On choisit un entier a au hasard entre 1 et $N-1$. On calcule $y = a^2 \bmod N$. Et on demande à l'oracle de renvoyer une racine carré de y. Par le théorème des restes chinois, les 4 racines carrées de y sont les solutions des 4 systèmes de congruences

$$\begin{cases} x \equiv a \pmod p \\ x \equiv a \pmod q \end{cases} \qquad \begin{cases} x \equiv -a \pmod p \\ x \equiv -a \pmod q \end{cases}$$

$$\begin{cases} x \equiv a \pmod p \\ x \equiv -a \pmod q \end{cases} \qquad \begin{cases} x \equiv -a \pmod p \\ x \equiv a \pmod q \end{cases}$$

Les deux premiers systèmes ont pour solutions évidentes respectives a et $-a$. Soit b une solution du troisième. Alors, modulo N, les racines de y sont les éléments de $\{+a, -a, +b, -b\}$. L'oracle ne sait pas laquelle de ces quatres racine nous avons utilisé pour obtenir le carré y, et il y une chance sur 2 pour que la solution qu'il renvoie soit b ou $-b$, et dans ce cas l'équation

$$a^2 \equiv b^2 \pmod N,$$

qui s'écrit encore

$$(a+b)(a-b) \equiv 0 \pmod N,$$

montre que le produit $N = pq$ divise le produit $(a+b)(a-b)$. Comme b n'est pas égal à $\pm a$ modulo N, N ne divise ni $a+b$ ni $a-b$. Il en résulte que, par exemple, p divise $a+b$ et pas $a-b$, et q divise $a-b$ et pas $a+b$. Le pgcd de N et $a+b$ donne donc le facteur premier p de N. Ainsi chaque fois qu'on pose une question à l'oracle on a une chance sur deux d'en déduire une factorisation de n. □

3.6 Le crible d'Eratosthène

Cet algorithme très simple, donné dans la figure Algorithme 5 construit la table des nombres premiers de l'intervalle $[1, n]$ en temps $O(n \log\log n)$ quasi-linéaire.

```
Procedure eratosthene(Premier, n) ;
//Premier est un tableau de booleens indexe de 1 a n. Le crible
//donne à Premier[n] la valeur VRAI ssi n est premier
Local j, p;
début
    Premier[1] := FAUX;
    pour j de 2 a n faire Premier[j] = VRAI ;
    p := 2 ;
    tant que p <= n/p faire
        pour j de 2 · p à n par p faire  Premier[j] := FAUX;
        répéter p := p + 1 jusqu'à Premier[p];
    fin
fin
```

Algorithme 5 : Le crible d'Eratosthène

Remarque : Des modifications immédiates, qui ne changent pas la complexité en $O(n \log\log n)$, permettent de l'utiliser pour dresser la table donnant pour chaque entier l'ensemble de ses diviseurs premiers, ou sa factorisation. On dit qu'un entier est `friable`, si tous ses facteurs premiers sont petits, plus précisément B-friable, si tous ses facteurs premiers sont inférieurs à B. Le crible d'Eratosthène permet aussi de construire tous les nombres friables de l'intervalle $[1, n]$.

Pour le calcul de la complexité de cet algorithme nous aurons besoin du lemme suivant qui est un résultat élémentaire de la théorie analytique des nombres.

Lemme 3.3 *Soit x un réel ≥ 1. On a*

$$\sum_{p \leq x,\ p \text{ premier}} \frac{1}{p} = \log\log x + O\left(\frac{1}{\log x}\right)$$

Théorème 3.4 *La complexité du crible d'Eratosthène est $O(n \log\log n)$.*

Preuve : La suppression des multiples de chaque nombre premier p est de coût n/p, car il y a n/p multiples de p à rayer entre 1 et n. Le coût total des suppressions des multiples des nombres premiers jusqu'à $\sqrt{n}$ est donc

$$\sum_{p \leq \sqrt{n}} \frac{n}{p} = n \log\log\sqrt{n} \sim n \log\log n.$$

Nous avons négligé le coût total des passages à travers la boucle répéter $p := p + 1$ qui fait passer du nombre premier p à son successeur. Ce coût total est de côut $\sqrt{n}$, car le nombre total d'incrémentations est $\sqrt{n}$. Il est donc négligeable. □

Remarque : On gagne un peu de temps en ne supprimant les multiples de p qu'à partir de p^2 au lieu de $2p$. Car, après le crible par les nombres premiers qui précèdent p, les $p-1$ premiers multiples de p sont déjà rayés. Ceci est intéressant pour les petites valeurs de n, mais ne change pas l'équivalent asymptotique $n \log\log n$, car le temps gagné est de l'ordre de

$$\sum_{p \leq \sqrt{n}} p \leq \frac{\sqrt{n}(\sqrt{n}+1)}{2} \sim \frac{n}{2},$$

négligeable devant $n \log\log\log n$ lorsque n est grand. On gagne aussi un temps non négligeable lorsque n n'est pas très grand en ne criblant pas par 2. Cela est surtout intéressant par ce que cela utilise deux fois moins de mémoire. On peut aussi, c'est un peu plus technique, éviter aussi le crible par les petites valeurs de p, par exemple $p = 2, 3, 5, 7$.

Exercices

Exercice 3.1
(D'après la rubrique de problèmes mathématiques du Monde) Soit $(a_1, a_2, \ldots, a_n)$ une suite finie d'entiers. On définit la fonction f qui à tout entier x associe l'entier y défini de la façon suivante : on multiplie a_1 par x et on ajoute a_2. On multiplie le résultat par x et on ajoute a_3, et ainsi de suite, le calcul se terminant après la multiplication par a_{m-1} suivie de l'ajout de a_m.

On suppose que $f(1) = 2$. Le nombre $f(7)$ est-il un carré parfait ?

Exercice 3.2
Ecrire une procédure qui reçoit un entier B et un entier N, et qui, au moyen d'un crible, détermine tous les entiers B-friables de l'intervalle $[1, N]$, c'est à dire les entiers de cet intervalle dont tous les facteurs premiers sont $\leq B$.

Exercice 3.3
Suite de Fibonacci et algorithme des puissances

Soit la suite de Fibonacci, défine par $u_0 = 0; \quad u_1 = 1; \quad u_{n+2} = u_{n+1} + u_n$.

1. Écrire la procedure Maple

```
fibo0 := proc(n)
 if n <= 1 then n
 else fibo0(n-1) + fibo0(n-2)
 fi
end;
```

   qui est la transcription immédiate de la définition par récurrence de (u_n). Démontrer que le cout $c(n)$ de l'appel `fibo0(n)` est proportionnel à u_n.

2. Vérifier qu'en utilisant l'option `remember`,

```
fibo1 := proc(n) option remember;
 if n <= 1 then n
 else fibo1(n-1) + fibo1(n-2)
 fi
end;
```

   le temps de calcul devient $O(n)$. Qu'observez vous pour de grandes valeurs de n ?

3. Ecrire, en utilisant l'algorithme des puissances, la procédure

```
expm := proc(x,n,Id,multiply)
```

   dont les arguments sont x appartenant à un ensemble muni d'une opération associative notée multiplicativement, `multiply`, dont l'élément neutre est `Id`, et `n` un entier naturel. Cette procédure rend $\mathtt{x}^{\mathtt{n}}$.

4. Soit A la matrice
$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$
   Montrer que, pour tout $n \geq 1$, on a
$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = A^n \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}.$$
   En déduire une procédure `fibo2 := proc(n)` qui calcule u_n avec un nombre d'opérations proportionnel à $\log n$ (le temps de calcul est plus long car les opérations se font sur des entiers de plus en plus grands).

5. Ecrire la procédure `fibo3 := proc(n,p)` qui calcule $u_n \pmod p$ en temps $O(\log n)$.

6. En déduire la valeur de $u_{10^{20}} \pmod{10^{100}}$.

CHAPITRE 4

Cryptographie

La cryptographie s'est longtemps réduite au chiffrement des messages de sorte à les rendre incompréhensibles aux non destinataires. Dans son *Traité de cryptographie militaire* Auguste Kerckhoffs écrivait en 1883 que *La sécurité d'un système cryptographique ne doit pas dépendre de la preservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clef.* Ce principe est un principe de base de la cryptographie moderne. Les algorithmes de chiffrement sont publics. Mais le résultat dépend d'une clef choisie par les utilisateurs, et, sans la connaissance de cette clef, il est pratiquement impossible de décrypter le message chiffré. Rendre publics les algorithmes utilisés est le meilleur moyen de s'assurer de leurs robustesses.

Depuis l'avènement des télécommunications, à l'objectif précédent, la `confidentialité`, s'est greffée la necessité d'assurer l'`authencité` et l'`intégrité` d'un message signé.

Dans ce chapitre on présentera quelques exemples historiques, puis, très brièvement, quelques méthodes actuelles entrant dans la catégorie des chiffrements à clef secrète partagée, avant de s'intéresser à la notion, plus récente, de chiffrement à clef publique. Les procédés de chiffrements à clefs publiques actuellement les plus utilisés reposent sur la difficulté supposée, mais non prouvée, de deux problèmes arithmétiques, la factorisation des grands entiers, et le calcul des logatihmes discrets dans $\mathbb{F}_p$ pour p grand nombre premier.

4.1 Les codages à clef partagée

4.1.1 Substitution alphabétique

La clef est une permutation σ de l'alphabet. Le mot $x = x_1x_2\dots x_n$ est chiffré en le mot $\sigma(x_1)\sigma(x_2)\dots\sigma(x_n)$.

Exemple 4.3 :

Si σ est donneé par le tableau :

$$\sigma = \begin{pmatrix} \text{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \text{N B V C X W M L K J H G F D S Q P O I U Y T R E Z A} \end{pmatrix}$$

Le chiffrement du mot CRYPTOGRAPHIE est le mot VOZQSMOQLKX.

Le `chiffrement de César` est le cas particulier du chiffrement par une permutation circulaire de l'alphabet. Notons σ_1 la permutation circulaire $a \to b, b \to c, \cdots, z \to a$. Si x est la $k^{\text{ème}}$ lettre de l'alphabet le chiffrement de César de clef x est σ_1^k.

Exemple 4.4 :

Avec la clef C, le chiffrement de CRYPTOGRAPHIE est FUBSWRJUDSKLH.

4.1.2 Le chiffrement de Vigenère

Il remonte au XVI$^{\text{ème}}$ siècle. C'est un raffinement du chiffrement de César, longtemps considéré comme indécryptable. C. Babbage a montré comment le décrypter vers 1854. La clef est un mot, par exemple MARC. Les lettres du texte clair sont cryptée en utilisant le chiffre de César avec la clef M pour la première lettre, la clef A pour la seconde lettre, R pour la troisième lettre, C pour la quatrième, M pour la cinquième, et ainsi de suite.

Exemple 4.5 :

Le chiffrement du mot CRYPTOGRAPHIE avec la clef MARC est

	C	R	Y	P	T	O	G	R	A	P	H	I	E
+	M	A	R	C	M	A	R	C	M	A	R	C	M
	P	S	Q	S	G	P	Y	U	N	Q	Z	L	R

4.1.3 Décryptages des codages par substitution

Il est facile de décrypter ce chiffrement en utilisant `l'analyse des fréquences` des caractères. Dans une langue donnée, les 26 lettres de l'alphabet ne sont pas également utilisées. Par exemple dans la langue française, la lettre `E` apparait beacoup plus fréquemment que les autres [1] Voici un tableau des pourcentages de fréquences d'apparition des lettres de l'alphabet dans un texte français, par ordre décroissant :

E	A	S	N	R	T	I	U	L	O
17.8	8.25	8.25	7.25	7.25	7.25	7.25	6.25	5.75	5.75

Connaissant ces fréquences, le déchiffrement d'un message ainsi crypté est un jeu d'enfant. Ceci s'automatise très simplement en utilisant des méthodes basées sur des calculs de corrélations statistiques, et permet aussi de décrypter facilement un code de Vigenère [2]

4.1.4 Le chiffrement de Vernham (1926)

C'est le chiffrement de Vigenère, avec une clef c de longueur infinie, ou au moins aussi longue que tout texte à chiffrer. Ainsi la $k^{\text{ème}}$ lettre du message chiffré est le chiffrement de la $k^{\text{ème}}$ lettre du message clair, par le code de César dont la clef est la $k^{\text{ème}}$ lettre de la clef c. Ce chiffrement est théoriquement parfait, car si les lettres de la

[1] Une exception : le roman de G. Perec, *La disparition*, sans une seule occurence d'un E !

[2] Voir, par exemple, S. Singh *Histoire des codes secrets* J. C Lattès (1999)

clef sont choisies aléatoirement avec équiprobabilité, le message clair correspondant à un message chiffré donné de longueur n est, avec équiprobabilité n'importe quel message de même longueur. Si l'alphabet est l'alphabet $\{0,1\}$, le chiffrement de x par c, est simplement le `ou exclusif` appliqué à x et c, composante par composante.

4.1.5 Procédés modernes à clef symétrique secrète

Ce sont les méthodes actuellement utilisées. Elles sont très rapides. On code facilement quelques mega-octets à la seconde, jusqu'à un giga-octets par seconde. L'inconvénient est que les deux correspondants doivent au préalable se mettre d'accord sur une clef commune. Comment le faire s'ils sont éloignés l'un de l'autre, ne pouvant communiquer que par un canal peu sûr ?

Le message est d'abord converti en une suite de blocs binaires de taille 64 bits, par exemple. Chaque bloc est ensuite chiffré par une fonction qui se calcule rapidement mais s'inverse difficilement. Le procédé DES (Data Encryption Standard) est resté longtemps le standard. Dans ce protocole l'ensemble des clefs est le sous-ensemble de $\{0,1\}^{64}$, formé en concaténant 8 mots de 8 bits chacun de poids pair. Cela donne 56 bits à choisir, soit 2^{56} clefs possibles, soit environ $7 \cdot 10^{16}$. Avec de très gros moyens de calcul on peut essayer toutes les clefs possibles.

IDEA est un renforcement de DES obtenu en utilisant des clefs de 128 bits. Blowfish est un protocole rapide et public. Le nouveau standard actuellement reconnu est le protocole AES (Advanced Encryption Standard) du à Rijndael qui permet d'utiliser au choix, et indépendemment, des clefs et des blocs de 128, 196, ou 256 bits. La commande `ssh` de `OpenSSH` utilise Blowfish ou AES. Pour une liste plus complète, on pourra consulter le site *Cryptographie Tutoriel* à l'adresse `http ://www.uqtr.ca/~delisle/Crypto/`.

4.2 Qu'est ce qu'un chiffrement à clefs publiques ?

Le point faible commun à tous les chiffrements à clef secrète est la nécessité pour les deux correspondants de s'entendre au préalable sur la clef qu'ils vont utiliser. Comment le faire, s'ils sont éloignés l'un de l'autre, ne disposant que d'un unique canal de communication peu sûr ?

Diffie et Hellman ont proposé la construction de sytèmes cryptographiques dans lesquels la clef utilisée pour le chiffrement est publique. Alice, ayant de nombreux correspondants n'a pas besoin de se réunir secrètement avec chacun d'eux pour partager une clef. L'algorithme de chiffrement est une fonction f_A dépendant d'un paramètre A, appelé `la clef de chiffrement`. Alice diffuse un message public disant, *pour m'envoyer un message chiffré, utilisez l'algorithme de chiffrement f avec ma* `clef publique` *A que voici.*

La sécurité du procédé repose sur le fait que, si tout le monde connait l'application f_A, personne n'a la possibilité pratique de l'inverser (certains appellent `fonction trappe` une telle fonction). Alice, et elle seule, dispose d'informations supplémentaires qui permettent de calculer facilement f_A^{-1}. Ces informations constituent `la clef de déchiffrement` d'Alice.

Dans certaines situations, c'est le cas de RSA, l'algorithme de déchiffrement est identique à l'algorithme de chiffrement, mais en y remplaçant le paramètre A, la clef de chiffrement d'Alice, par une autre valeur de ce paramètre, la clef de déchiffrement d'Alice.

L'inconvénient des algorithmes à clef publique actuellement utilisés est leur lenteur. Ils sont plus lents que les algorithmes symétriques d'un facteur de l'ordre de 1000. Les protocoles utilisés en pratique combinent les deux méthodes. Bob commence par utiliser un chiffrement à clef publique, avec la clef publique d'Alice, pour lui envoyer une clef secrète qui servira ensuite au chiffrement du message par une méthode symétrique rapide à clef secrète partagée.

Tous les algorithmes de chiffrement qui suivent agissent sur des entiers. On commence par découper le texte à chiffrer en blocs de caractères de longueurs suffisament petites. Chaque bloc est codé en un entier par un procédé réversible simple. Chacun de ces entiers est crypté par l'algorithme de chiffrement.

4.3 Clefs publiques et Authentification

Si Alice est ma banque, et utilise un protocole à clef publique, n'importe qui, Ève par exemple, peut envoyer un message à Alice disant *Je suis Marc, débitez mon compte de tout son contenu, et virez cette somme sur le compte d'Ève.* Un protocole d'`identification` est un procédé qui permet à Marc d'envoyer un message à Alice, de sorte que celle-ci ait la certitude qu'il provient bien de Marc.

Montrons que tout algorithme de chiffrement à clef publique, fournit de manière canonique un protocole d'identification.

Pour envoyer le message x, Marc envoie à Alice la paire $(f_A(x), f_A f_M^{-1}(m))$, (où f_M est l'application publique de chiffrement utilisée pour s'adresser à Marc, et $m :=$ "Marc"). En utilisant son application de déchiffrement f_A^{-1}, Alice obtient la paire $(x, s) = (x, f_M^{-1}(m))$. Utilisant enfin l'application de chiffrement publique de Marc f_M, Elle calcule $f_M(s) = f_M(f_M^{-1}(m)) =$ "Marc". Et seul Marc peut avoir envoyé ce message, car il est le seul à pouvoir calculer $s = f_M^{-1}$.

4.4 Le chiffrement de Rabin

Ce protocole repose sur le fait que, pour N non premier, calculer une racine carrée dans $\mathbb{Z}/N\mathbb{Z}$ est aussi difficile que de factoriser N.

Clef publique : Alice choisit deux grands nombres premiers p et q, tous deux congrus à 3 modulo 4, puis calcule $N = pq$. Sa clef publique est N.

Chiffrement : Le chiffrement du message x destiné à Alice est $y = x^2 \bmod N$.

Déchiffrement : Alice calcule une fois pour toutes les coefficients de Bezout u et v tels que $up + vq = 1$. Pour déchiffrer le message reçu y, elle doit résoudre

$$x^2 \equiv y \pmod{N}. \tag{4.1}$$

Cette équation est équivalent au système

$$\begin{cases} x^2 \equiv y \pmod{p} \\ x^2 \equiv y \pmod{q}. \end{cases}$$

La racine carrée de y modulo p est $r_1 = y^{(p+1)/4}$ car p est de la forme $4k+3$. De même, la racine carrée de y modulo q est $r_2 = y^{(q+1)/4}$. L'entier x est solution de (4.1) si, et seulement si, il est solution de l'un des 4 systèmes chinois

$$\begin{cases} x \equiv \pm r_1 & (\text{mod } p) \\ x \equiv \pm r_2 & (\text{mod } q). \end{cases}$$

On vérifie immédiatement que vq (resp. up) est solution du système élémentaire

$$\begin{cases} x \equiv 0 & (\text{mod } p) \\ x \equiv 1 & (\text{mod } q) \end{cases} \qquad \left(\text{resp. } \begin{cases} x \equiv 1 & (\text{mod } p) \\ x \equiv 0 & (\text{mod } q) \end{cases}\right)$$

L'équation (4.1) a donc 4 solutions qui sont $x = \pm vqr_1 \pm upr_2$.

Exemple 4.6 :

Alice choisit $p = 11$ et $q = 23$. Sa clef publique est $N = 253$. Le chiffrement du message $x = 158$ est $x^2 \bmod N = 170$. Alice reçoit $y = 170$, calcule $r_1 = y^{(p+1)/4} \bmod p = 4$, et $r_2 = y^{(q+1)/4} \bmod q = 3$. Les coefficients de Bezout pour p et q sont -2 et 1, d'où

$$r_1 = -2 \cdot 11 \cdot 3 \ + \ 1 \cdot 23 \cdot 4 = 26 \qquad r_2 = -2 \cdot 11 \cdot 3 \ - \ 1 \cdot 23 \cdot 4 = 95,$$

et enfin les 4 racines carrées de y sont $26, 95, 158, 227$.

Comment retrouver parmi les 4 racines celle qui est le message envoyé par Alice, 158 dans l'exemple ci-dessus ? Chaque texte chiffré est le chiffrement de 4 textes différents. Si le message clair est un texte ordinaire, parmi les 4 interprétations possibles, seule une a un sens. Mais si le message clair n'est pas un texte, mais, par exemple une liste de valeurs numériques d'apparence aléatoire, aucune des 4 interprétations ne s'impose. Une solution consiste à introduire de la redondance dans le message clair. On choisit un entier k, et on ajoute à la fin de l'écriture binaire de x, une chaine de k bits identique aux k derniers. Parmi les 4 racines carrées de $y = x^2$, x sera reconnu par cette particularité.

Sûreté du chiffrement de Rabin

Par le théorème (3.2), le problème de la recherche d'une racine carrée dans $\mathbb{Z}/N\mathbb{Z}$, lorsque N est un produit de deux facteurs premiers, est aussi difficile que la factorisation de N. Il en résulte que le chiffrement de Rabin, dans la version sans redondance est aussi difficile à casser que de factoriser N. Si on introduit de la redondance cela n'est plus vrai. Car le carré $y = x^2$ n'est plus un carré arbitraire mais le carré d'un entier x possédant une propriété particulière. Il se pourrait que la recherche des racines carrées de tels entiers soit plus simple que l'extraction d'une racine carrée quelconque modulo N, autrement dit, plus simple que la factorisation de N.

Il faut une part aléatoire dans un message chiffré

La pratique de la cryptographie est pleine de dangers. Considérons la situation suivante. Méphisto sait qu'Alice a envoyé le même message x à deux correspondants Bob_1 et Bob_2, dont les cles publiques sont N_1 et N_2. Il a intercepté les deux messages chiffrés $y_1 = x^2 \bmod N_1$ et de $y_2 = x^2 \bmod N_2$. Il résout le sytème chinois, d'inconnue z,

$$\begin{cases} z \equiv y_1 & (\text{mod } N_1) \\ z \equiv y_2 & (\text{mod } N_2) \end{cases}$$

Une solution évidente de ce système est $z = x^2$, et cette solution est dans l'intervalle $[1, N_1N_2]$ car $x < N_1$ et $x < N_2$ (et N_1, N_2 très probablement premiers entre eux. Si d'ailleurs ils ne l'étaient pas, leut pgcd donneait les factorisations de N_1 et N_2). Ève obtient ainsi la valeur de x^2, puis x, car le calcul de la racine carré d'un réel est simple même si ce réel est très grand.

On ne peut pas interdire à Alice d'envoyer le même message à plusieurs correspondants. Pour ce mettre à l'abri de cette attaque tout message est complété par le rajout d'un message aléatoire de longueur fixée.

4.5 Le chiffrement RSA

Cet acronyme provient des noms des trois inventeurs Rivest, Shamir et Adleman (1977).

Clef publique

1. Alice choisit deux grands nombres premiers p et q, Elle calcule le produit $N = pq$. L'ensemble des textes clairs, et l'ensemble des textes chiffrés sont les mêmes, l'ensemble $\{0, 1, 2, \ldots, N-1\}$.
2. Alice calcule $\varphi(N) = (p-1)(q-1)$.
3. Elle choisit un entier e, $3 \leq e < \varphi(N)$ premier avec $\varphi(N)$.

La clef publique d'Alice est le couple (e, N).

Chiffrement Le chiffrement de x est $x^e \bmod N$.

Déchiffrement Alice, connaissant $\varphi(N)$ calcule une fois pour toutes l'inverse d de e modulo $\varphi(N)$. Le couple (d, N) est la clef secrète d'Alice. Montrons que le message clair x est donné par $x = y^d \bmod N$. Puisque $d \equiv e^{-1} \pmod{\varphi(N)}$ il existe un λ tel que $ed = 1 + \lambda\varphi(N)$. Distinguons deux cas :

1. Si x est premier avec N, par le théorème d'Euler $x^{\varphi(N)} \equiv 1 \pmod N$ et donc

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{\lambda\varphi(N)+1} \equiv (x^{\varphi(N)})^\lambda x \equiv 1^\lambda \cdot x \equiv x \pmod N,$$

   car, par le théorème d'Euler, $x^{\varphi(N)} \equiv 1 \pmod N$. Si x est premier avec p et q.
2. Si $x \bmod p = 0$ et $x \bmod q = 0$, c'est que $x = 0$ et dans ce cas, $y = 0$, et $y^d \bmod p = 0 = x$.
3. Sinon, on a, par exemple $x \equiv 0 \pmod p$, et $x \bmod q \neq 0$. Ceci implique, modulo p, $x^e \bmod p = 0$, et donc $y \equiv 0 \pmod p$ et aussi $y^d \equiv 0 \equiv x \pmod p$. Modulo q on a $x^{q-1} \equiv 1 \pmod q$ et donc

$$y^d \equiv x^{ed} \equiv x^{\lambda(p-1)(q-1)} + 1 \equiv (x^{(q-1)})^{\lambda(p-1)} x \equiv x \pmod q.$$

   Les deux congruences $y^d \equiv x \pmod p$ et $y^d \equiv x \pmod q$ donnent $y^d \equiv x \pmod N$.

Exemple 4.7 :

Choisissons $p = 5$ et $q = 11$. Cela donne $N = 55$ et $\varphi(n) = 4 \cdot 10 = 40$. Alice choisit $e = 3$, l'inverse de e modulo 40 est $d = -13 = 27$. Pour envoyer le message

$x = 7$, Bob calcule $y = 7^3 \bmod 55 = 13$. Alice qui reçoit le message chiffré 13 calcule $13^{27} \bmod 55 = 7$. et retrouve ainis le message clair x.

Sûreté du protocole RSA

Elle repose sur deux conjectures.

1. Retrouver l'exposant de déchiffrement d à partir des données publiques N, e est aussi difficile que de factoriser N.
2. La factorisation des entiers est un problème difficile.

En outre, l'exposant d de déchiffrement ne peut pas être choisi arbitrairement.

Théorème 4.1 (Wiener 1990) *Soit $N = pq$ un produit de deux nombres premiers, et e un entier $1 \leq e \leq \varphi(N)$, premier avec $\varphi(N)$. Si l'inverse d de e modulo N est plus petit que $\frac{1}{3}N^{\frac{1}{4}}$ il existe un algorithme qui, à partir de la donnée (N, e) calcule rapidement p, q, et donc aussi d.*

Plus récemment [3] Boneh et Durfee on montré qu'en utilisant l'algorithme LLL, on peut décrypter un message chiffré par RSA si $d \leq N^{0.292}$, et conjecturent que cela puisse être étendu pour $d < N^{0.5}$.

Curieusement, on ne connait pas d'algorithme permettant de factoriser N quand l'exposant public e est petit. Beaucoup d'implémentations de RSA utilisent l'exposant de chiffrement $e = 3$, dont l'avantage est qu'il permet un chiffrement plus rapide. Mais si on fait ce choix, on doit s'interdire d'envoyer un même message a trois correspondants (cf. dans la section (4.4) le pararagraphe sur la nécessité d'introduire une partie aléatoire dans un message chiffré). La encore on se protège en rajoutant à tout message une part d'alea. Cependant, dans ce cas, Coppersmith a montré, utilisant encore LLL, que si cette partie aléatoire est trop courte on peut encore retrouver le message clair envoyé aux trois correspondants.

4.6 Le chiffrement d'El Gamal

Sa sûreté repose sur deux conjectures :

1. Le décryptage du chiffrement de El-Gamal se réduit au problème du calcul du logarithme discret.
2. Le calcul d'un logarithme discret est difficile.

Clef publique Alice choisit un grand nombre premier p et un générateur g du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. Elle choisit aussi un entier a et calcule $A = g^a \pmod p$. Sa clef publique est le triplet (p, g, A).

Chiffrement Pour coder le message x, Bob choisit un entier b arbitraire dans l'ensemble $\{1, 2, \ldots, p-2\}$. Le message chiffré est le couple

$$(u, v) = (g^b \bmod p, xg^{ab} \bmod p) = (g^b \bmod p, xA^b \bmod p).$$

[3] Cryptanalysis of RSA with private key d less than $N^{0.292}$. by D. Boneh and G. Durfee. IEEE Transactions on Information Theory, Vol 46, No. 4, pp. 1339–1349, July 2000.

Déchiffrement Alice recevant le couple (u, v) n'a qu'à calculer vu^{-a} pour retrouver x. En efet, modulo p,

$$vu^{-a} = xg^{ab}(g^b)^{-a} = x.$$

Remarque : Un inconvénient de ce système est que le chiffrement du message x est deux fois plus long que x (ce qui n'est pas génant pour un court message, par exemple une clef qui sera utilisée pour un chiffrement rapide à clef secrète partagée).

Un avantage est que, si ce système nécessite le calcul de deux exponentiations modulaires, pour calculer g^b et A^b, ces deux calculs sont indépendants du message à expédier. On peut donc disposer d'une liste précalculée, rangée dans un dispositif du type carte magnétique. Ceci étant fait, le chiffrement se réduit à une multiplication modulaire.

Remarquons que si Bob choisissait toujours la même valeur pour b, le protocole d'El Gamal serait cassé par une *attaque à texte clair*. Supposons que Ève dispose d'un texte clair x_0 et de son chiffrement $(g^b, v_0) = (g^b, x_0 g^{ab})$. Si elle intercepte le chiffrement de x, $(g^b, v) = (g^b, xg^{ab})$, elle retrouve x en calculant

$$vv_0^{-1}x_0 = xg^{ab}g^{-ab}x_0^{-1}x_0 = x.$$

Exemple 4.8 :

Alice choisit $p = 23$, $g = 7$, $a = 6$. Alors $A = g^a = 7^6 = 4$. La clef publique d'Alice est le triplet $(p, g, A) = (23, 7, 4)$. Pour envoyer le message $x = 7$, Bob choisit $b = 3$. Il envoie donc le couple $(g^b, xA^b) = (7^3, 7 \cdot 4^3) = (21, 11)$. Alice retrouve x en calculant $11.21^{-6} \bmod 23 = 7$.

Sûreté du chiffrement d'El Gamal

Pour décrypter le chiffrement d'El Gamal, il faut, partant de la donnée de g^a et de g^b calculer g^{ab}. On peut le faire si on sait résoudre le problème du logarithme discret dans $\mathbb{F}_p$. Car, à partir de g^a on calcule a, et à partir de g^b on calcule b, et enfin g^{ab}. On conjecture que le calcul de g^{ab} à partir de g^a etg^b est aussi difficile que le calcul du logarithme discret.

4.7 Le chiffrement de Merkle Hellmann

Merkle et Hellmann ont proposé ce protocole en 1985. C'était une idée séduisante, car les algorithmes de chiffrement, et de déchiffrement sont très rapides. Malheureusement il est facile à casser en utilisant l'algorithme LLL.

Le problème du sac à dos

Expliquons d'abord ce qu'est le `problème du sac à dos`. On se donne k entiers positifs, $c_1, c_2, \ldots, c_k$, et un entier C. Le problème du sac à dos est la recherche d'une solution de l'équation

$$c_1x_1 + c_2x_2 + \cdots + c_kx_k = C,$$

où les inconnues $x_i \in \{0,1\}$. Ce problème est difficile, il est NP-complet. Il existe cependant une classe d'instances de ce problème qui sont très facilement résolubles, la classe des `sacs à dos faciles`.

Définition 4.2 *Une instance* $(c_1, c_2, \ldots, c_n, C)$ *est dite* `facile` *si la suite* $(c_i)_{1\leq i\leq n}$ *est* `super-croissante`*, c'est à dire si elle possède la propriété suivante : Pour tout* i*,* $1 \leq i < n$*,*

$$c_1 + c_2 + \cdots + c_i < c_{i+1}.$$

Dans ce cas la résolution du problème du sac à dos est très simple

Procédure Sac-à-dos-facile(c, C ; **Var** X)
Données : $C \in \mathbb{N}$; $c = (c_1, c_2, \ldots, c_k) \in \mathbb{N}^k$
Résultat : X : tableau de bits
début
  pour i *de* k *à* 1 *par* -1 **faire**
    si $C \geq c_i$ **alors** $X[i] := 1$; $C := C - c_i$ **sinon** $X[i] = 0$
  fin
  si $C = 0$ **alors retourner** X **sinon retourner** ECHEC
fin

Exemple 4.9 :

La suite $(1, 2, 4, \ldots, 2^k)$ est une suite super-croissante.

La clef publique

1. Alice choisit un sac super-croissant, $c = (c_1, c_2, \ldots, c_k)$, et un entier N,

$$N > c_1 + c_2 + \cdots + c_k.$$

2. Elle choisit e premier avec N et calcule $a_i = ec_i \bmod N$, pour $1 \leq i \leq k$. Sa clef publique est $(a_1, a_2, \ldots, a_k)$.

Chiffrement L'application de chiffrement envoie l'ensemble des séquences de k bits sur une partie de l'ensemble $\{0, 1, 2, \ldots, N\}$. Le chiffrement du k-uplet $x = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k) \in \{0,1\}^k$ est l'entier

$$y = \sum_{i=1}^{k} \varepsilon_i, a_i \quad \left(\in \left\{ 0, 1, 2, \ldots, \sum_{i=1}^{k} a_i \right\} \right.$$

Déchiffrement Pour déchiffrer le message y, Alice calcule $d = e^{-1} \pmod N$, puis $z = dy \bmod N$. Comme, modulo N,

$$z = dy \equiv d \sum_{i=1}^{k} \varepsilon_i a_i = d \sum_{i=1}^{k} \varepsilon_i ec_i = \sum_{i=1}^{k} \varepsilon_i dec_i = \sum_{i=1}^{k} \varepsilon_i c_i,$$

avec z et $\sum_{i=1}^{k} \varepsilon_i c_i$ dans $[0, N]$, elle n'a plus qu'à résoudre le problème du sac à dos facile $z = \sum_{i=1}^{k} \varepsilon_i c_i$ pour retrouver $x = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$.

1. Alice et Bob choisissent un grand nombre premier p (quelques centaines de chiffres) et un générateur g du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. Cette conversation est publique.
2. Alice choisit *secrètement un entier* a, Bob un entier b. Alice calcule $A = g^a$ et envoie ce nombre à Bob, sur le canal de communication public. De même, Bob calcule $B = g^b$ et envoie ce nombre à Alice.
3. Alice, qui a reçu B calcule $B^a \bmod p$, et Bob qui a reçu A calcule $A^b \bmod p$. Ces deux nombres sont égaux et leur valeur commune est le secret partagé par Alice et Bob.

FIG. 4.1 – Le protocole de Diffie Hellmann

Exemple 4.10 :

Alice choisit $(c_1, c_2, c_3, c_4) = (3, 7, 15, 30)$, $N = 70$, $e = 27$. Sa clef publique est $(a_1, a_2, a_3, a_4) = (11, 49, 55, 40)$. Le chiffrement du message $x = (0, 1, 0, 1)$ est

$$y = 0 \cdot 11 + 1 \cdot 49 + 0 \cdot 55 + 1 \cdot 40 = 89.$$

Pour déchiffrer y Alice calcule $d = 1/27 \bmod 70 = 13$, puis $z = 13 \cdot 89 \bmod N = 37$, et en résolvant le sac à dos facile

$$37 = \varepsilon_1 \cdot 3 + \varepsilon_2 \cdot 7 + \varepsilon_3 \cdot 15 + \varepsilon_4 \cdot 30,$$

elle retrouve le message $m = (0, 1, 0, 1)$.

4.8 Comment échanger une clef privée sur un canal public ?

Nous avons vu que l'inconvénient commun à tous les protocoles à clef secrète partagée est le problème de l'échange de la clef. Est-il possible d'échanger une clef secrète en utilisant un canal public ? Ce problème a été résolu par Diffie et Hellman en 1976. Leur solution, présentée dans la figure (4.1) repose sur la difficulté du problème du calcul d'un logarithme discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ lorsque p est un grand nombre premier.

Vérifions que $B^a = A^b$.

$$B^a = (g^b)^a = (g^a)^b = A^b.$$

Ève, même connaissant p, g, A et B ne peut pas retrouver $g^{ab} = A^b = B^a$ (dans $(\mathbb{Z}/p\mathbb{Z})^\times$). On ne sait pas comment le faire sans connaitre l'un des deux nombres secrets a ou b. Mais personne n'a prouvé que cela est impossible. Autrement dit, on pense que le protocole de Diffie-Hellmann est sûr, parce qu'on admet, sans preuve, que casser ce protocole est aussi difficile que de calculer les logarithmes discrets dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

4.9 Attaques par interception

Considérons la situation suivante : Alice et Bob, ne se connaissent pas. Imaginons qu' Eve envoie le message suivant à Alice : *Bonjour Alice je suis Bob, voici mon adresse ..., je te propose de chiffrer nos échanges, en utilisant, par exemple, le protocole RSA. Voici la clef publique K_E à utiliser pour chiffrer les messages que tu m'enverras, renvoie moi ta clef publique K_A*. Elle envoie à Bob le message analogue : *Bonjour Bob, je suis Alice, voici mon adresse ..., je te propose de chiffrer nos échanges, en utilisant le protocole RSA. Voici la clef publique K_E à utiliser pour chiffrer les messages que tu m'enverras, renvoie moi ta clef publique K_B*

A partir de là, chaque fois qu'Alice croit envoyer un message à Bob, elle envoie ce message à Eve, chiffré avec K_E, la clef publique d'Eve, qu'elle croit être la clef de Bob. Eve déchiffre le message avec sa clef privée, le chiffre à nouveau avec la vraie clef K_B de Bob, avant de le faire suivre à Bob, qui ne soupçonne pas que le message envoyé par Alice a été intercepté. De même, tout message envoyé par Bob à Alice, est en réalité expédié à Eve, qui le déchiffre et le rechiffre avant de le réexpédier à Alice.

Pour se mettre à l'abri de cette attaque (*the man in the middle attack*) il faut une `autorité certificatrice`.

4.10 Exercices

Exercice 4.1
Un message est écrit avec les 26 lettres de l'alphabet et le caractère blanc. On découpe en tranches de 8 lettres. Chacune de ces tranches est complétée en une tranche de 10 lettres, en rajoutant deux fois la dernière lettre. Dans chaque tranche on remplace la lettre A par 01, B par 02, ..., Z par 26, et le caractère blanc par 27. A chaque tranche est ainsi associée un entier $M < 10^{20}$. On code chacun de ces nombres M par la méthode de Rabin, avec

$$N = 11\,.\,979\,.\,409\,.\,745\,.\,851\,.\,587\,.\,542\,.\,621\,.$$

Décryptez le cryptogramme composé des 2 nombres :

$$586\,.\,252\,.\,050\,.\,213\,.\,245\,.\,505\,.\,607 \qquad 6\,.\,405\,.\,136\,.\,716\,.\,470\,.\,575\,.\,588\,.\,589\,.$$

Exercice 4.2
Un message est écrit avec les 26 lettres de l'alphabet et le caractère blanc. On lui associe un entier M comme dans l'exercice précédent. On code ces nombres M par la méthode RSA avec

$$n = 11\,.\,979\,.\,409\,.\,736\,.\,901\,.\,405\,.\,393\,.\,787, \qquad e = 1\,.\,234\,.\,567.$$

Décryptez le cryptogramme obtenu, composé des 3 nombres :

$$10\,.\,641\,.\,193\,.\,385\,.\,979\,.\,683\,.\,831\,.\,145 \qquad 4\,.\,346\,.\,822\,.\,458\,.\,507\,.\,857\,.\,865\,.\,000$$
$$11\,.\,239\,.\,010\,.\,885\,.\,649\,.\,545\,.\,983\,.\,297$$

Exercice 4.3
Supposons que trois personnes Bob_1, Bob_2, Bob_3 utilisent RSA, avec les clefs publiques respectives $(N_1, 3), (N_2, 3), (N_3, 3)$.

1. On suppose N_1, N_2 et N_3 premiers entre eux deux à deux. En vous inspirant de la fin du paragraphe (4.4) expliquez comment Ève, ayant intercepté les chiffrements m_1, m_2, m_3 d'un même message m envoyé par Alice aux trois personnes Bob_1, Bob_2, Bob_3, est capable de calculer m, en utilisant les données dont elle dispose N_1, N_2, N_3 et m_1, m_2, m_3.
2. Pourquoi N_1, N_2, N_3 sont ils très probablement premiers entre eux deux à deux ?
3. Si N_1, N_2 et N_3 n'étaient pas premiers entre eux, comment pourrait on en déduire un résultat plus fort, la factorisation de deux au moins des N_i ?
4. **Un exemple :** Les clef publiques de Bob_1 de Bob_2 et de Bob_3 sont $(10000000167993271, 3)$, $(10000000077056303, 3)$ et $(10000000761439883, 3)$. Alice envoie le même message m à Bob_1, Bob_2 et Bob_3. Ève intercepte $m_1 = 9010328151653526$, $m_2 = 3715786019602206$, $m_3 = 4712381892400635$. Retouver le message clair m sans factoriser les N_i.

Exercice 4.4
Une autre faute à éviter en utilisant RSA est l'utilisation de clefs publiques (N_1, e_1), (N_2, e_2) avec $N_1 = N_2$. Supposons que les clefs publiques de Bob_1 et Bob_2 sont respectivement (N, e_1) et (N, e_2).

1. Expliquez comment Bob_1, s'il devine que $N_1 = N_2$, déchiffre n'importe quel message adressé à Bob_2.
2. Alice envoie un message identique x à Bob_1 et Bob_2, dont les chiffrements respectifs sont y_1 et y_2. Montrer qu'Eve, supposant que y_1 et y_2 sont les chiffrements d'un même message x, peut retrouver x, par un calcul astucieux.

CHAPITRE 5

Factorisation par la méthode $(p-1)$ de Pollard. Paradoxe des anniversaires et applications

On présente ici quelques algorithmes simples et élégants. Le premier, la méthode $p-1$ de Pollard, permet de factoriser un entier N éventuellement très grand, pourvu, ce qui est exceptionnel, que l'un des facteurs premiers p de N soit tel que $p-1$ n'ait que de tout petits facteurs premiers. Le principe de la méthode est assez général. L'algorithme de factorisation ECM de Lenstra, utilisant les courbes elliptiques, repose sur la même idée. La méthode des pas de bébé et des pas de géant de Shanks est elle aussi importante. Enfin il est important de connaitre le paradoxe des anniversaires. Une application remarquable est la méthode ρ de Pollard qui donne un algorithme probabiliste de factorisation d'un entier non premier n avec un nombre d'opérations de l'ordre de $\mathcal{O}(\sqrt{p})$ où p est le plus petit facteur premier de n, et un coût en espace $\mathcal{O}(1)$. La méthode ρ de Pollard s'adapte au calcul des logarithmes discrets.

5.1 Factorisation par divisions successives

C'est la première méthode qui vient à l'esprit. Pour factoriser n on considère tous les entiers d, $2 \leq d \leq \sqrt{n}$. Si l'un d'eux divise n, on obtient la factorisation $n = n \times (n/d)$, et on continue en remplaçant n par n/d. Si on ne trouve pas de diviseur $d \leq \sqrt{n}$, c'est que n est premier. Cette méthode nécessite $\sqrt{n}$ divisions. Bien sûr, si on dispose d'une table des nombres premiers jusqu'à $\sqrt{n}$, en ne divisant n que par les d premiers, on réduit le nombre de divisons à $2\sqrt{n}/\log n$ le nombre de divisions. Car, par le théorème des nombres premiers, le nombre des entiers premiers dans $[1, \sqrt{n}]$ est équivalent à $\sqrt{n}/\log\sqrt{n} = 2\sqrt{n}/\log n$, quand n tend vers l'infini.

5.2 Factorisation par la méthode $(p-1)$ de Pollard

L'intéret de cette méthode est qu'elle permet de factoriser très rapidement certains grands entiers n bien particuliers, mais inaccessibles aux autres méthodes. Soit n un entier non premier et p une facteur premier de n tel que la décomposition en facteurs premiers de $p-1$

$$p - 1 = \prod_{i=1}^{k} p_i^{\alpha_i}$$

n'utilise que les k plus petits nombres premiers, certains des α_i étant éventuellement nuls.

Pour tout entier naturel non nul $i \leq k$ soit $p_i^{\beta_i}$ la plus grande puissance de p_i qui ne dépasse pas n, et

$$K = \prod_{i=1}^{k} p_i^{\beta_i}.$$

Par exemple, pour $k = 3$ et $n = 6011003$,

$$K_{20} = 2^{22} \times 3^{14} \times 5^9.$$

Pour tout $i \leq k$ on a $p_i^{\alpha_i} \leq p - 1 < n$, et donc, par défintion des β_i on a $p_i^{\alpha_i} \leq p_i^{\beta_i}$. Ainsi K est un multiple de $p - 1$.

Choisissons un entier a premier avec n, et, a fortiori, premier avec p. Par le petit théorème de Fermat, on a $a^{p-1} \equiv 1 \pmod{p}$ et, puisque K est un multiple de $p - 1$, $a^K \equiv 1 \bmod p$. Autrement dit $a^K - 1$ est un multiple de p. On calcule

$$(a^K - 1, n).$$

Ce pgcd est plus grand que 1, car multiple de p. Si ce n'est pas n on a trouvé un diviseur non trivial de n. Sinon on essaie avec une autre valeur de a. Presque à chaque fois le premier choix de a sera bon, car $a^K - 1$ est toujours multiple de p, mais rarement multiple de n.

Pour calculer $\text{pgcd}(a^{K_B} - 1, n)$ on remarque que ce pgcd est inchangé si on remplace a^K par le reste r de sa division par n. Autrement dit on commence par calculer $r = a^K \bmod n$, puis on terminera en calculant $\text{pgcd}(r - 1, N)$. Puis calculer $r = a^K \bmod n$ il est inutile d'expliciter la valeur de K. On commence par calculer $a^{p_1^{\beta_1}} \bmod n$, puis, modulo n, on élève le résultat à la puissance $p_2^{\beta_2}$, et ainsi de suite.

Remarque : **Application à la méhode RSA** Une conséquence pratique importante est que les nombres premiers p et q utilisés pour construire $N = pq$ dans la méthode RSA doivent être tels que $p - 1$ et $q - 1$ admettent chacun au moins un grand facteur premier.

5.3 Calculs de logarithmes discrets : la méthode de Shanks

Rappelons le problème du logarithme discret : Un nombre premier p est donné ainsi qu'un générateur g du groupe multiplicatif cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$. On se donne un élément non nul $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ et on cherche x tel que $g^x = a$.

5.3.1 La méthode naïve

La méthode naive consiste à calculer $g, g^2, g^3, \ldots$ jusqu'à obtenir $g^k = a$. Son cout moyen en temps est $O(p - 1)$.

5.3.2 La méthode des pas de géant et des pas de bébé

Dans cette méthode, dûe à Shanks, on échange du temps contre de la mémoire. Au prix d'un encombrement mémoire en $O(\sqrt{p})$, le calcul se fait en $O(\sqrt{p})$ au lieu de $O(p)$. Cela donne un algorithme utilisable pour des valeurs de p jusqu'à 10^{20}. Soit

$m = \lceil \sqrt{p-1} \rceil$, le plus petit entier supérieur ou égal à $\sqrt{p-1}$. On écrit le nombre x cherché sous la forme

$$x = qm + r, \quad 0 \leq r < m.$$

Comme $x < p-1$ et $m \geq \sqrt{p-1}$, le quotient q ne dépasse pas $\sqrt{p-1}$. Rechercher x tel que $g^x = a$, c'est donc rechercher q et r vérifiant

$$0 \leq r < m, \quad 0 \leq q \leq \sqrt{p-1}, \quad g^{qm+r} \equiv a \pmod{p},$$

ou encore $0 \leq r < m, \quad 0 \leq q \leq \sqrt{p-1}, \quad (g^m)^q \equiv ag^{-r} \pmod{p}$. D'abord on calcule (les pas de bébé) l'ensemble B

$$B = \{ag^{-r} \bmod p \ : \ 0 \leq r < m\}.$$

Puis (les pas de géant) on calcule $u = g^m \bmod p$, puis pour $q = 0, 1, 2, \ldots, m-1$, on calcule u^k jusqu'à ce qu'on obtienne q tel que $u^q \equiv g^{qm} \equiv ag^{-r} \pmod{p}$.

Quand on calcule une valeur $y = u^q \bmod m$, on doit non seulement répondre à la question *cette valeur appartient-elle à l'ensemble B ?* , mais en outre, en cas de réponse affirmative, il faut répondre à la deuxième question *quelle est la valeur r telle que $y = ag^{-r} \bmod p$?*

Ceci correspond exactement à la définition de la structure de donnée appelée *dictionnaire* ou encore *table associative.*

Définition 5.1 *Soit E et F deux ensembles. Le premier, E est appelée l'ensemble des entrées, le second F, l'ensemble des informations. Un* `dictionnaire à entrées dans` E `et informations dans` F *est un triplet $\mathcal{D} = (D, F, f)$ où $\mathcal{D}$ est une partie finie de E et f une application $f \ : \ \mathcal{D} \longrightarrow F$ (quand $D = \emptyset$, on dit que f est le dictionnaire vide).*

1. *L'ensemble D est l'ensemble des mots, ou des entrées du dictionnaire.*
2. *L'opération de* `consultation`, `cherche`$(x, \mathcal{D})$ *renvoie ECHEC si x n'est pas dans D, et renvoie $y = f(x)$ si $x \in D$.*
3. *Pour $x \in E \setminus D$ et $y \in F$, l'opération d'*`insertion`, `insere`$(\mathcal{D}, x, y)$ *renvoie le dictionnaire obtenu en prolongeant f à l'ensemble $D' = D \cup \{x\}$, par $f(x) = y$.*

Avec ces définitions l'algorithme de Shanks s'écrit

```
Fonction logdiscret(p, g, a : entiers);
Var D : dictionnaire d'entiers à informations entières,
m, u, q, v, r : entiers;
début
    D := dictionnaire vide;
    m := ⌈√(p − 1)⌉;
    q := 0;
    pour r de 0 à m − 1 faire insere(D, ag^{−r} mod p, r);
    u := g^m mod p ; v := 1;
    tant que (r := cherche(v, D)) = ECHEC faire
        q := q + 1 ; v := vu (mod p)
    fin
    retourner qm+ r;
fin
```

Algorithme 6 : L'algorithme des pas de bébé et de géant

Le coût (en temps) de cette procédure est $O(\sqrt{p-1})$, *pourvu que l'operation d'insertion dans le dictionnaire, et l'opération de consultation soient de coût constant* $O(1)$. Nous n'expliquerons pas ici comment implémenter un dictionnaire en respectant ces contraintes. La technique la plus courante est celle des *tables de hachage*.

La structure de dictionnaire est l'une des primitives de Maple (sous le nom de `table`). L'implémentation de la méthode des pas de bébé et des pas de géant est donc immédiate.

Dans un langage de programmation ne disposant pas de la notion de table associative, comme par exemple `pari` une implémentation relativement simple et efficace de la structure de dictionnaire peut se faire de la manière suivante (à condition de ne pas mêler les opérations d'insertion dans le dictionnaire, et les opérations de consultation, c'est à dire de construire d'abord le dictionnaire en insérant toutes les définitions, puis une fois ceci réalisé, en ne faisant plus des consultations). On supposera que l'ensemble E des entrées possibles est un ensemble totalement ordonné.

Un dictionnaire de taille n est implémenté comme un tableau T de n éléments qui sont les couples $(u, f(u))$ pour $u \in D$. Les éléments de ce tableau sont rangés par valeurs croissantes de u.

Pendant la phase de construction du dictionnaire on ne se préoccupe pas de ranger les couples (u, v) de T par ordre croissant des valeurs de u. Chaque nouveau couple (u, v) est inséré en fin de tableau. Quand le dernier élémen a été ajoute et, à ce moment seulement, on trie le tableau T par valeurs croissantes de u, au moyen d'une procédure de tri rapide. On sait que ceci coûte $n \log n$ comparaisons ou permutations d'éléments de T. Une fois ce tri terminé on a constitué un dictionnaire de taille n en $n \log n$ opérations, soit un coût moyen de $\log n$ opérations par insertion.

Ensuite la consultation dans le dictionnaire, à la recherche d'une définition de l'entrée u se fait par dichotomie, c'est à dire en au plus $\log n$ opérations de comparaison.

En procédant ainsi vous pouvez écrire en `pari` la méthode des pas de bébé et de géant, avec un coût $\sqrt{p}\log(p)$ au lieu de $\sqrt{p}$.

5.4 Le paradoxe des anniversaires

Soit E un ensemble de cardinal n. On se donne un entier k et on tire successivement, avec remise, et avec chaque fois la probabilité uniforme, un élément de E. Cela définit une suite $(x_1, x_2, \ldots, x_k)$ d'éléments de E. Quelle est la probabilité p_k de l'évenement *tous les* x_i sont distincts ?

Toutes les suites de longueur k, $(x_1, x_2, \ldots, x_k)$ ont la même probabilité d'occurence. Il y en a n^k. Pour construire une suite injective, on a n choix pour x_1, $n-1$ choix pour x_2, etc.... Cela donne la probabilité

$$p_k = \frac{1}{n^k} \prod_{i=1}^{k-1} (n-i) = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right).$$

La fonction exponentielle étant convexe, on a, pour tout x réel, $1+x \leq e^x$. Il en résulte que

$$p_k \leq \prod_{i=1}^{k-1} e^{-\frac{i}{n}} = e^{-\frac{k(k-1)}{2n}}. \tag{5.1}$$

Théorème 5.2 *Si* $k \geq \frac{1}{2}\big(1+\sqrt{1+8n\ln 2}\big) \approx 1.17\sqrt{n}$, *on a* $p_k < 1/2$. *Autrement dit, si on tire au hasard, avec remise, avec probabilité uniforme, un peu plus de* $\sqrt{n}$ *éléments dans un ensemble de cardinal* n, *la probailité d'obtenir au moins deux fois le même élément est plus grande que* $1/2$.

Preuve : Pour que p_k soit plus petit que $1/2$, il faut et il suffit que $\log p_k < \log(1/2)$. Pour cela, vue la majoration (5.1), il suffit que

$$-\frac{k(k-1)}{2n} \leq -\log 2,$$

soit

$$k \geq \frac{1}{2}\big(1+\sqrt{1+8n\ln 2}\big) \approx 1.17\sqrt{n}.$$

□

Application : Prenant $n = 365$, et $k = 23$, si 23 personnes sont réunies dans une salle la probabilité que deux au moins d'entre elles aient leur anniversaire le même jour, est plus grande que $1/2$.

5.4.1 Application à la factorisation : méthode ρ de Pollard

Considérons maintenant N non premier et p un facteur premier de N. Soit b entier arbitraire, et $f_b : [0, n-1] \to [0, n-1]$ l'appplication définie par $x \mapsto (x^2+b) \bmod p$. On choisit $x_1 \in [0, n-1]$, arbitraire, et on considérons la suite (x_n) définie par son premier terme x_1 et la relation de récurrence $x_{n+1} = f(x_n)$. Les valeurs de cette suite sont effectivement calculables une fois donnés b et x_1. Considérons aussi la suite (y_n) définie par $y_n = x_n \bmod p$. Cette suite est bien définie mais nous ne pouvons pas expliciter les y_n, car nous ne connaissons pas p. Faisons l'hypothèse que la suite (y_n) se comporte comme une suite aléatoire prenant ses valeurs dans $[0, p-1]$ avec la probabilité uniforme. L'expérience montre que cela est en général assez bien vérifié. Alors, par le paradoxe des anniversaires, pour deux entiers i et j, $1 \leq i \leq j$, j proche de $\sqrt{p}$, $y_i = y_j$.

Or la connaisance d'un tel couple (i, j) donne très probablement une factorisation de n. En effet l'égalité $y_i = y_j$ égalité implique la congruence $x_i \equiv x_j \pmod p$. Le pgcd $(x_j - x_i, N)$ est un multiple de p, et donc non réduit à 1.

Comment déterminer efficacement un tel couple (i, j) ? Soit y_{n_0} le premier des y_i qui apparait plus d'une fois dans les valeurs de la suite $(y_n)_n$, et soit n_1, le plus petit entier $> n_0$ tel que $y_{n_1} = y_{n_0}$. La suite $(y_n)_{n \geq n_0}$ est périodique de période $T = n_1 - n_0$. De plus, par le paradoxe des anniversaires, n_1 est de taille environ $\sqrt{p}$. Soit enfin 2^K la plus petite puissance de 2 qui dépasse n_1. Puisque, à partir de $2^K \geq n_0$ la suite (y_n) est périodique de période T on a $y_{2^K} = y_{2^K+T}$, c'est à dire que le couple $(i, j) = (2^K, 2^K + T)$ est solution de $y_i = y_j$. De plus, puisque $T = n_1 - n_0 \leq 2^K$ on a $2^K + T \leq 2^{K+1}$. Ainsi, pour K suffisament grand, l'intervalle $[2^K, 2^{K+1}]$ contient un entier j tel que $y_{2^K} = y_j$. Ceci donne l'algorithme suivant :

```
Fonction rhoPollardFactorise(N, x_1, b : entiers)
Var x, u, d : entier;
début
    u := x_1 ; x := x_1 ; d := 1;
    répéter
        pour j de d + 1 à 2d faire
            x := (x^2 + b) mod N;
            si pgcd((x − u, N) > 1) alors
                retourner pgcd(x − u, N)
            fin
        fin
        u := x ; d := 2d ;
    jusqu'à l'infini;
fin
```

Algorithme 7 : Factorisation de N par la méthode ρ de Pollard

La variables x reçoit les valeurs successives de $x_n \bmod N$, en mémorisant au passage la valeur de x_n dans u, chaque fois que n est une puissance de 2. Pour chaque valeur de x on calcule $\text{pgcd}(x-u, N)$, qui est en général 1. Lorsque $d = 2^K$, pour la valeur $j = T$, $u = x_{2^K}$ et $x = x_{2^K+T}$, et le pgcd $(x-u, N)$ est un diviseur de N, autre que 1. Si ce diviseur est N, l'algorithme a échoué, on recommence avec une autre valeur initiale x_1 ou une autre fonction d'itération, en changeant la valeur de b. Ce cas d'échec est très rare car $x_j - x_{2^K}$ a beaucoup plus de chances d'être multiple de p sans être multiple de N que d'être multiple de N.

Ainsi cette méthode a toute chance de nous fournir une factorisation de N avec un nombre d'opérations de l'ordre de $\sqrt{p}$, qui, dans tous les cas est plus petit que $N^{1/4}$, parfois beaucoup plus petit, si p est beaucoup plus petit que $\sqrt{N}$.

5.4.2 Application au calcul du logarithme discret

Le paradoxe des anniversiares conduit aussi à un algorithme de calcul du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$, plus généralement dans n'importe quel groupe cyclique G de cardinal n, en temps $O(\sqrt{n})$ et en espace $O(1)$. Soit G un groupe cyclique d'ordre n, de générateur g, et a un élément de G que l'on cherche à écrire sous la forme $a = g^\alpha$. On partitionne l'ensemble G en trois parties

$$G = G_1 \cup G_2 \cup G_3.$$

On considère l'application $f : G \to G$ définie par

$$f(u) = \begin{cases} gu & \text{si} \quad u \in G_1 \\ u^2 & \text{si} \quad u \in G_2 \\ au & \text{si} \quad u \in G_3 \end{cases}$$

On choisit un élément $x_1 \in \{1, 2, \ldots, n\}$, $y_1 = 0$, et on considère la suite récurrente (β_i) définie par

$$\beta_1 = g^{x_1}, \quad \beta_{i+1} = f(\beta_i).$$

Pour tout $i \geq 1$, il existe des entiers x_i, et y_i tels $\beta_i = g^{x_i} a^{y_i}$ et vérifiant

$$x_{i+1} = \begin{cases} (x_i + 1) \bmod n & \text{si} \quad \beta_i \in G_1 \\ 2x_i \bmod n & \text{si} \quad \beta_i \in G_2 \\ x_i & \text{si} \quad \beta_i \in G_3 \end{cases}$$

et

$$y_{i+1} = \begin{cases} y_1 & \text{si} \quad \beta_i \in G_1 \\ 2y_i \bmod n & \text{si} \quad \beta_1 \in G_2 \\ (y_i + 1) \bmod n & \text{si} \quad \beta_i \in G_3 \end{cases}$$

La suite (β_i) prenant ses valeurs dans le groupe fini G, il existe deux indices distincts i et j tels que $\beta_i = \beta_j$ c'est à dire

$$g^{x_i} a^{y_i} = g^{x_j} a^{y_j}.$$

Si nous disposons d'un tel couple (i, j) nous pouvons calculer α de la manière suivante. Puisque

$$g^{x_i - x_j} = a^{y_j - y_i} = g^{\alpha(y_j - y_i)},$$

α est solution de la congruence

$$\alpha(y_j - y_i) \equiv x_i - x_j \pmod{n}. \tag{5.2}$$

Si $y_j - y_i$ est premier avec n l'équation (5.2) détermine entièrement α modulo n. Sinon, si $d = (y_j - y_i, n)$ est plus grand que 1, cette équation en l'inconnue α admet d solutions modulo n. Il suffit d'essayer les d solutions.

Pour obtenir un couple (i, j) tel que $\beta_i = \beta_j$, sans utiliser de mémoire, on procède comme dans le cas de la factorisation. Soit n_0 le plus petit entier tel qu'il existe j, $j > n_0$, avec $\beta_{n_0} = \beta_j$, et soit n_1 le plus petit de ces j. Si la suite $(\beta_n)_n$ étaitune suite aléatoire, par le paradoxe des anniversaires, n_1 serait de l'ordre de grandeur de $\sqrt{n}$. L'expérience montre que cela est vérifié bien que (β_n) ne soit pas aléatoire.

Si $T = n_1 - n_0$, à partir de l'indice n_0, la suite $(\beta_n)_n$ est périodique de période T. Soit 2^K la première puissance de 2 telle que $2^K \geq n_1$. Alors, puisque $T = n_1 - n_0 \leq n_1 \leq 2^K$,

$$\beta_{2^K} = \beta_{2^K + T}, \quad \text{et} \quad 2^K + T \leq 2^{K+1}.$$

Pour $n = 0, 1, 2, 3, \ldots$, on calcule (β_n, x_n, y_n), en conservant au passage le triplet $(\beta_d, x_d, y_d) = (\beta_n, x_n, y_n)$, chaque fois que $n = d = 2^k$ est une puissance de 2. Après chaque calcul d'une valeur (β_n, x_n, y_n), cette valeur est comparée au triplet (β_d, x_d, y_d), d étant la dernière puissance de 2 inférieur à n. Si ces deux triplets ont la même première composante $\beta_d = \beta_n$, on obtient l'équation $x_d - x_n = \alpha(y_n - y_d) \pmod{n}$, d'où on déduit la valeur de α.

Exemple 5.1 :

On choisit $p = 103$, et on veut calculer le logarithme discret de $a = 10$ en base $g = 5$. Pour construire la suite des (β_i) on choisit

$$G_1 = \{1, \ldots, 34\}, \quad G_2 = \{35, \ldots, 68\} \text{ et } G_3 = \{69, \ldots, 102\} \text{ et } x_1 = 2.$$

Cela donne $[\beta_1, x_1, y_1] = [25, 2, 0]$. Le tableau suivant donne les valeurs (β_d, x_d, y_d), pour $d = 1, 2, 4, 8$.

d	β_d	x_d	y_{dj}
1	25	2	0
2	22	3	0
4	35	5	0
8	62	11	2

Pour $n = 10$ on obtient le triplet $(\beta_{10}, x_{10}, y_{10}) = (62, 23, 4)$. L'égalité $\beta_{10} = \beta_8$ donne l'équation $g^{11}a^2 = g^{23}a^4$, soit $g^{12}a^2 = 1$. Remplaçant a par g^α, et cela donne l'équation $g^{12+2\alpha} = 1$, soit $2\alpha \equiv -12 \pmod{102}$ soit

$$\alpha \equiv -6 \pmod{51}.$$

α est donc l'une des 2 valeurs $45, 97$. On vérifie que $5^{45} \equiv 10 \pmod{103}$.

5.5 Exercices

Exercice 5.1
Ecrire en Maple la procédure `pmoins1 := proc(N,B)` qui essaie de factoriser l'entier N au moyen de la méthode $p-1$ de Pollard en espérant que N admette un diviseur premier tel les facteurs premiers de $p-1$ soient majorés par B. Puis factoriser

```
N = 536598073612914384251090186279917836286620295442 49\
    396452035817474423290853286439934795299454737340 74\
    095423205484492406140302428885978232270314999189 57\
    67836182646541829
```

Quelle est la plus petite valeur du paramètre B permettant de factoriser N ?

Exercice 5.2
Un autre point de vue sur le paradoxe des anniversaires

N et n sont deux entiers > 0. On dispose d'une urne contenant N boules numérotées de 1 à N. On tire n fois de suite une boule avec remise après chaque tirage. On note x_i le numéro de la boule obtenue au tirage numéro i. On obtient ainsi une suite $(x_1, x_2, \cdots, x_n)$ d'entiers de $\{1, 2, \ldots, N\}$. Soit X le nombre des couples $(i, j), 1 \leq i < j \leq n$ tels que $x_i = x_j$. On se propose d'étudier la variable aléatoire X. On utilisera pour cela les variables aléatoires $X_{i,j}$, définies pour $1 \leq i < j \leq n$, par

$$X_{i,j} = \begin{cases} 1 & \text{si } x_i = x_j \\ 0 & \text{sinon.} \end{cases}$$

1. Exprimer X en fonction des $X_{i,j}$.
2. (a) En déduire l'espérance de X, $E(X)$.
   (b) Combien vaut $E(X)$ lorsque $n = N$? Lorsque $N = 365$ et $n = 40$?
   (c) Comment choisir n (en fonction de N) pour que $E(X) \geq 1$?
3. (a) Les variables $(X_{i,j})_{1 \leq i < j \leq n}$ sont elles indépendantes ?
   (b) Démontrer qu'elles sont deux à deux indépendantes.
   (c) En admettant que la variance d'une somme de variables 2 à 2 indépendantes est la somme de leurs variances, exprimer simplement la variance de X en fonction de n et N.

4. On rappelle la formule de Tchebychev : $P(|Y - E(Y)| \geq \lambda) \leq \frac{V(Y)}{\lambda^2}$, où Y est une variable aléatoire d'espérance finie $E(Y)$, de variance finie $V(Y)$, et λ un réel positif quelconque. Montrer que

$$P(X = 0) \leq \frac{V(X)}{E(X)^2}.$$

En déduire que si $n(n-1) \geq 4(N-1)$ soit, approximativent, $n \geq 2\sqrt{N}$, la probabilité de l'évènement $X > 0$ est plus grande que $1/2$.

Exercice 5.3

Une application du paradoxe des anniversaires. Une `fonction de hachage cryptographique` est une fonction définie sur un ensemble E de grand cardinal, éventuellement infini, à valeurs dans un ensemble de petit cardinal fini K.

La fonction f est `fortement résistante aux collisions` si la construction d'un couple $(x, y) \in E \times E$ tel que $x \neq y$ et $f(x) = f(y)$ est pratiquement impossible (un tel couple est appelé une collision de f).

Soit f une fonction de hachage à valeurs dans $\{1, 2, \ldots, 2^{64}\}$. Expliquer comment fabriquer en un temps raisonnable une collision (x, y) de f.

Exercice 5.4

Factoriser par la méthode ρ de Pollard $n = 6359931032400308378413700370799 49$.

Exercice 5.5

On admet que $p = 100000000000031$ est premier et que $g = 19$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Calculer à l'aide de la méthode ρ de Pollard le logarithme discret de 10 en base 19, c'est à dire le plus petit entier $x \geq 0$ tel que $19^x \equiv 10 \pmod{p}$.

CHAPITRE 6

Tests de primalité

Les chapitres précédents ont mis en évidence l'importance des nombres premiers en cryptographie, et donc la necessité de savoir construire rapidement de grands nombres premiers.

Agrawal, Kayal et Saxena on prouvé en 2002 que le problème de la primalité est de complexité polynomiale, c'est à dire qu'il existe un algorithme qui répond à la question *n est il premier ,* en un temps majoré dans tous les cas, par un polynôme en $\log n$. Pour le moment cet algorithme ne permet pas, en pratique, de tester le primalité d'entiers au dela de quelques centaines de chiffres décimaux. Il existe depuis quelques décennies des algorithmes qui répondent assez rapidement à la question *n est il premier ?*, dont on ne sait pas prouver que le temps de calcul est polynomial, mais qui sont, à l'heure actuelle, plus efficaces que l'algorithme de Agrawal, Kayal et Saxena. Ils permettent de tester la primalité de nombres de quelques milliers de chiffres décimaux (en quelques dizaines de jours de calcul).

Dans ce chapitre on présente un théorème très élémentaire, le théorème de Lucas, qui permet de construire de grands nombres premiers p, ainsi qu'un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$.

On s'intéressera aux nombres de Carmichael. L'existence d'une infinité de ces nombres (1994) assure l'impossibilité de tester la primalité en ne s'appuyant que sur le théorème de Fermat.

On présentera ensuite les tests probabilistes de primalité de Solovay-Strassen et de Miller-Rabin. Ces tests sont des algorithme qui, recevant l'entier n, répondent ou bien *n est non premier*, et dans ce cas la réponse est toujours exacte, ou bien *n est très probablement premier*. Plus précisément on se donne un entier N arbitrairement grand. On peut rendre aussi faible que l'on veut la probabilité de l'événement *l'entier n tiré au hasard avec équiprobabilité dans l'intervalla $[1, N]$ a été declaré premier apres application du test de Miller-Rabin alors qu'il n'est pas premier* . Ces tests sont beaucoup plus rapides que les tests exacts, et ce sont eux que l'on utilise pour fabriquer rapidement de grands nombre premiers.

6.1 Le théorème de Lucas

Le théorème de Lucas fournit une condition suffisante simple de primalité, mais il ne s'applique qu'à une petite classe d'entiers, les entiers n pour lesquels il est possible

d'expliciter la factorisation de $n-1$.

Théorème 6.1 (Le théorème de Lucas) *Soit a et $n \geq 2$ deux entiers tels que*

$$a^{n-1} \equiv 1 \pmod{n},$$

et, pour tout diviseur premier q de $n-1$

$$a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}.$$

Alors n est premier, et a est un générateur du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

Preuve : Soit $\bar{a}$ la classe de a modulo n. L'hypothèse $\bar{a}^{n-1} = 1$, montre que $\bar{a}$ est un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ (son inverse est inverse $\bar{a}^{n-2}$). Il suffit de démontrer que l'ordre de $\bar{a}$ est $n-1$. En effet, si ceci est vrai, les $n-1$ éléments $\bar{a}, \bar{a}^2, \bar{a}^3, \ldots, \bar{a}^{n-1}$ sont non nuls, deux à deux distincts, et inversibles. Ce sont donc tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$, et ainsi $\mathbb{Z}/nZ$ est un corps, et n est premier. De plus $\bar{a}$ est un générateur du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

Soit donc ω l'ordre de $\bar{a}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Montrons que $\omega = n-1$. Puisque $\bar{a}^{n-1} = 1$, ω est un diviseur de $n-1$. Si ω était un diviseur strict de $n-1$, et il existerait un diviseur premier q de $n-1$, tel que $\omega \mid \frac{n-1}{q}$ ce qui impliquerait $\bar{a}^{\frac{n-1}{q}} = 1$, contredisant l'hypothèse. □

Introduisons la fonction `lucas(p,a)` : $\mathbb{N} \times \mathbb{N} \to \{-1, 0, 1\}$ qui prend la valeur

$$\begin{cases} -1 & \text{si } a^{p-1} \neq 1 \pmod{p} \\ 1 & \text{si } a^{p-1} = 1 \text{ et } a^{(p-1)/q} \neq 1 \pmod{p}, \text{ pour tout diviseur premier de } p-1 \\ 0 & \text{sinon} \end{cases}$$

- Lorsque `lucas(p,a)`$= 1$ on peut affirmer, grâce au théorème de Lucas, que p est premier et de plus que a est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.
- Lorsque `lucas(p,a)`$= -1$ on peut affirmer, par le petit théorème de Fermat, que p n'est pas premier.
- Lorsque `lucas(p,a)`$= 0$ on peut seulement en conclure que : ou bien p n'est pas premier, ou bien p est premier mais a n'est pas un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Cette fonction n'est, en pratique, calculable que si l'on connait la factorisation de $p-1$. La figure 6.1 donne le script `pari` de la fonction `lucas(p,a,ldivp1)` qui calcule $lucas(p,a)$ au moyen de la donnée supplémentaire de la liste `ldivp1` des facteurs premiers de $p-1$.

Application 1 : calcul d'un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$

Soit p un entier dont on sait qu'il est premier. Si on connait la factorisation de $p-1$ le théorème de Lucas permet de calculer rapidement un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Il suffit de calculer $lucas(p,a)$ pour $a = 2, 3, 5, 6, 7, \ldots$ jusqu'à ce que la réponse soit positive. Le nombre de générateurs d'un groupe cyclique d'ordre n est $\varphi(n)$ et ce nombre n'est pas beaucoup plus petit que n. On peut donc espérer obtenir ainsi rapidement un générateur.

En particulier, lorsque p est un nombre premier de Sophie Germain, c'est à dire de la forme $p = 2q+1$ avec q premier impair, $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $2q$ et donc $\varphi(p-1) = \varphi(2q) = q-1$. Autrement dit, environ la moitié des éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont des générateurs.

```
lucas(p,a,ldivp1) =
{// ldivp1 est la liste des diviseurs premiers de p-1
 local(A = Mod(a,p));
 if (lift(A^(p-1)) != 1, return(-1));
 for (j=1,length(ldivp1),
    if (lift(A^((n-1)/lst[j])) == 1, return(0))
 );
 return(1);
}
```

FIG. 6.1 – Calcul de la fonction testlucas(p,a)

```
bigprime(n) =
{/* primedivs(n)(à écrire) rend la liste des diviseurs premiers de n
 On utilise la procedure de concatenation de listes predefinie concat
 et la procedure de tri listsort dont le deuxième argument 1
 provoque la suppression des doublons. */

 local(lpn = primedivs(n),lpk);
  for (k=1,2000,
  lpk = listsort(concat(lpn,primedivs(k)),1);
  for(a=2,100,
    lucasres = lucas(k*n+1,a,lpk);
    if (lucasres <0,break,
    if (lucasres==1,return([k*n+1,a,k])))
    )
  )
}
```

FIG. 6.2 – Construction d'un nombre premier p de la forme p=kn+1 et d'un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, lorsque n est un produit de petits facteurs premiers. L'appel bigprime(n) rend le triplet [p,a,k] où p est un (en général le plus petit) nombre premier de la forme p=kn+1 et a le plus petit générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Application 2 : construction de grands nombres premiers

A l'aide du théorème de Lucas il est facile de construire un couple (p, a) formé d'un grand nombre premier p et d'un générateur a de $(\mathbb{Z}/p\mathbb{Z})^\times$. Puisqu'on ne sait calculer $lucas(a, p)$ que connaissant la factorisation de $p-1$ il faut considérer des grands entiers p tels que $p-1$ soit facilement factorisable.

On part d'un grand entier n facile à factoriser, par exemple $n = 3^{200}$. Pour $k = 1, 2, \ldots$ nous calculons $p = kn+1$. Puisque k est petit la liste lpk des facteurs premiers de $p-1 = kn$ est très facile à calculer. On calcule alors `lucas(p,a,lpk)` pour $a = 2, 3, 4, \ldots$ jusqu'à obtenir la valeur 1. Si pour une valeur de a on obtient -1 on sait que p n'est pas premier et on passe à la valeur suivante de k et donc de p. En général (les exceptions étant les nombres de Carmichael), lorsque p n'est pas premier, la fonction `lucatest(p,a)` rend presque tout de suite la valeur -1. La figure 6.1 donne un script `pari` qui définit la fonction `bigprime`.

Remarque :

- Cette fonction n'est utilisable que si votre procdure `primedivs(n)` aboutit c'est à dire que si n est un entier se factorisant tres facilement.
- On obtient donc ainsi des nombres premiers p tels que $p-1 = kn$ soit un produit de petits facteurs premiers. En utilsant la méthode de factorisation $p-1$ de Pollard les nombres $N = pq$ obtenus en utilisant de tels nombres premiers sont faciles à factoriser et ne peuvent pas être utilisés en cryptographie.

6.2 Insuffisance du théorème de Fermat pour tester la primalité

On rappelle le théorème de Fermat qui donne une condition nécessaire simple de primalité.

Théorème 6.2 (Théorème de Fermat) *Pour que p soit premier, il est nécessaire que, pour tout a,*

$$(a,p) = 1 \implies a^{(p-1)} \equiv 1 \pmod{p}.$$

Exemple 6.1 :

Soit $p = 4348278997$. On vérifie rapidement à l'aide de l'algorithme des puissances que

$$2^{p-1} = 1791392699 \pmod{p}.$$

On en déduit que n n'est pas premier.

Considérons un autre exemple, $n = 341$ et $a = 2$: on a

$$2^{340} \equiv 1 \pmod{341}.$$

Pourtant $341 = 11 \times 31$ n'est pas premier. Ceci nous conduit aux définitions suivantes.

Définition 6.3 *Soit a et p deux entiers ≥ 1. On dit que p est* `pseudo-premier en base` *a si*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Vu le théorème de Fermat, tout nombre premier est pseudo premier en base a pour tout a tel que $(a,p) = 1$.

Définition 6.4 *L'entier a est un* `faux témoin de primalité` *pour l'entier n, au sens de Fermat, si n est* non premier *et pseudo-premier en base a.*

Ainsi l'entier 2 est un faux témoin de primalité au sens de Fermat pour $n = 341$. On pourrait penser que chaque fois que n est un entier non premier, les faux témoins de primalité de n, sont rares, c'est à dire que, pour la plupart des a vérifiant $(a,n) = 1$, on a

$$a^{n-1} \neq 1 \bmod n,$$

et espérer bâtir ainsi un test de primalité. C'est faux. $561 = 3 \times 11 \times 17$ n'est pas premier, et (démontrez le en exercice) tous les entiers a premiers avec n sont des faux témoins de primalite,

$$\forall a, \quad (a,n) = 1 \implies a^{560} \equiv 1 \bmod 561.$$

Définition 6.5 *On appelle* `nombre de Camichael` *un entier* p non premier *qui est pseudo-premier en base* a *pour tous les entiers* a *premiers avec* p.

Le plus petit nombre de Carmichael est 561.

Théorème 6.6 (Alford, Granville, Pomerance 1994) *Il existe une infinité de nombres de Carmichael.*

L'existence d'une infinité de nombres de Carmichael empêche de construire un test de primalité n'utilisant que le théorème de Fermat.

6.3 Les critères d'Euler et de Miller-Rabin

Le critère d'Euler permet de rémedier à cette situation. Rappelons l'énoncé :

Proposition 6.1 (Critère d'Euler) *Pour que* p *soit premier, il est nécessaire que, pour tout* a *tel que* $(a,p)=1$ *on ait*

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

La définition suivante est l'analogue de (6.3)

Définition 6.7 *Soit* n *un entier impair. On dit que* n *est* `pseudo premier eulérien en base` a *si* $(a,n)=1$, *et*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Vu le critère d'Euler, tout nombre premier p *est pseudo premier eulérien en base* a *pour tout* a *tel que* $(a,p)=1$.

Exemple 6.2 :

Tout nombre pseudo-premier eulérien en base a est pseudo premier en base a, car, en élevant au carré la relation $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right)$ on obtient $a^{n-1} \equiv 1 \pmod{n}$. Mais la réciproque est fausse car $p=341$ est pseudo premier en base 2 (cf. l'exemple précédent), mais n'est pas pseudo premier eulérien en base 2. En effet

$$\left(\frac{2}{341}\right) = -1 \qquad \text{et} \qquad 2^{170} = 1 \bmod 341.$$

Définition 6.8 *On dit que* a *est un* `faux témoin de primalité de` n `au sens d'Euler`, *si* n *est non premier et pseudo premier eulérien en base* a.

Exemple 6.3 :

Le nombre de Carmichael $n = 561 = 3 \times 11 \times 17$ n'est pas premier. Mais il pseudo-premier eulérien en base 2 car

$$2^{280} \equiv 1 \pmod{561} = \left(\frac{2}{561}\right).$$

2 est donc un faux témoin de primalité de 561 au sens d'Euler. Mais $a = 5$, (premier avec 561) n'est pas un faux témoin de primalité au sens d'Euler car

$$5^{280} \equiv 67 \pmod{561} \neq \left(\frac{5}{561}\right).$$

Pour la pseudo-primalité au sens d'Euler, il n'existe pas d'analgues des nombres de Carmichael. Quel que soit l'entier impair n non premier, il existe $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui n'est pas un faux témoins de primalité de n au sens d'Euler. Mieux le nombre des faux témoins est toujours relativement petit.

Théorème 6.9 *Si n est non premier, le nombre des a, $1 \leq a \leq n-1$ tels que*

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

est plus petit que $\frac{1}{2}\varphi(n)$. Autrement dit, si n est non premier et si on choisit a au hasard, avec équiprobabilité dans $(\mathbb{Z}/n\mathbb{Z})^\times$, la probabilité pour que a soit un faux témoin de primalité au sens d'Euler est plus petite que $1/2$.

Preuve : Les faux témoins de primalité de n sont les éléments de l'ensemble G,

$$G = \{a \mid 1 \leq a \leq n-1, \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\}.$$

Par multiplicativité du symbôle de Jacobi, cet ensemble est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$. Son cardinal est donc un diviseur du cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$, et il suffit de démontrer que G n'est pas $(\mathbb{Z}/n\mathbb{Z})^\times$ tout entier, pour prouver que card $G \leq \varphi(n)/2$. Distinguons deux cas :

1. Si n est divisible par le carré d'un nombre premier p, $n = p^\alpha q$, avec $\alpha \geq 2$ et $(p, q) = 1$. Dans ce cas on considère l'élément

   $$a = 1 + p^{\alpha-1}q.$$

   Vu $a \equiv 1 \pmod{p}$, $a \equiv 1 \pmod{q}$, et la défintion du symbôle de Jacobi, on a d'une part

   $$\left(\frac{a}{n}\right) = \left(\frac{1}{p}\right)^\alpha \left(\frac{1}{q}\right) = 1 \times 1 = 1.$$

   D'autre part, par la formule du binôme, et en utilisant $2(\alpha - 1) \geq \alpha$,

   $$a^{\frac{n-1}{2}} \equiv 1 + \frac{n-1}{2} p^{\alpha-1} q \pmod{p^\alpha}.$$

   La plus grande puissance de p qui divise $a^{\frac{n-1}{2}} - 1$ est donc $p^{\alpha-1}$, il en résulte que $a^{\frac{n-1}{2}} - 1$ n'est pas multiple de n et $a \notin G$.

2. Si n est sans facteur carré. Il est le produit de k nombres premiers distincts $n = q_1 q_2 \dots q_k$, $k \geq 2$. Choisissons u qui n'est pas un carré modulo q_1, puis, par le théorème des restes chinois, un entier a qui satisfait

   $$a \equiv u \pmod{q_1}, \quad a \equiv 1 \pmod{q_i}, \quad 2 \leq i \leq k.$$

Par définition du symbôle de Jacobi,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\left(\frac{a}{q_3}\right)\cdots = (-1)\times 1\times 1\cdots = -1.$$

D'autre part, de $a \equiv 1 \pmod{q_2}$ on déduit

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{q_2}.$$

ce qui exclut $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, car $q_2 \mid n$.

□

Définition 6.10 (Le test de primalité de Solovay-Strassen) *Le test de Solovay Strassen pour l'entier n est le test suivant : on tire au hasard, avec équiprobabilité, un entier a entre 1 et $n-1$. Si*

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n,$$

autrement dit, si n est pseudo-premier en base a, le test a réussi, sinon il a échoué.

Théorème 6.11 *N est un entier fixé. Soit n un entier, choisi avec la probabilité uniforme parmi les entiers $1 \leq n \leq N$. On effectue au plus r fois le test de Solovay Strassen à l'entier n. Si tous les résultats sont positifs, la probabilité de l'évenement n* n'est pas premier *est inférieure à*

$$\frac{N}{\pi(N)}\frac{1}{2^r} \sim \frac{\ln N}{2^r}. \tag{6.1}$$

Preuve : Soit A l'évènement *n n'est pas premier*, et S l'évènement *n passe r fois avec succès le test de Solovay-Strassen*. On veut majorer la probabilité conditionelle $P(A \mid S)$. En utilisant la définition d'une probabilité conditionelle, et le fait que les évènements A et $\bar{A}$ forment un système complet d'évènements,

$$P(A \mid S) = \frac{P(A \cap S)}{P(S)} = \frac{P(S \mid A)\,P(A)}{P(S \cap A) + P(S \cap \bar{A})}$$

En utilisant encore la définiton de la probabilité conditionelle pour transformer le dénominateur,

$$P(A \mid S) = \frac{P(S \mid A)\,P(A)}{P(A)\,P(S \mid A) + P(\bar{A})\,P(S \mid \bar{A})}.$$

Si $\bar{A}$ est vrai, c'est à dire si n est premier, pour tout choix de a, le couple (a, n) passe avec succès le test de Solovay-Strasses ; autrement dit la probabilité conditionelle $P(S \mid \bar{A})$ est 1. D'où

$$P(A \mid S) = \frac{P(S \mid A)\,P(A)}{P(A)\,P(S \mid A) + P(\bar{A})}.$$

En majorant le numérateur et minorant le dénominateur cela donne

$$P(A \mid S) \leq \frac{P(S \mid A)}{P(\bar{A})}.$$

Par le théorème (6.9) $P(S \mid A) \leq 2^{-r}$. Enfin, l'évènement $\bar{A}$, est l'évènement *l'entier tiré n est premier*. Sa probabilité est $\pi(N)/N$. □

Le test de Miller-Rabin

Le test de Miller Rabin est similaire au test de Solovay Strassen, mais plus fort en ce sens qu'on qu'il permet de remplacer la constante 2^r au dénominateur de (6.1) par la constante 4^r. On introduit une nouvelle condition nécessaire de primalité. Soit p premier impair. On définit q et s par

$$p - 1 = 2^s q$$

avec q impair. Considérons l'identité polynomiale

$$Y^{2^s} - 1 = (Y-1)(Y+1)(Y^2+1)\dots(Y^{2^{s-1}}+1).$$

Soit maintenant a premier avec p. Posons $y = a^q$. Alors, par le théorème de Fermat, dans le corps $\mathbb{Z}/p\mathbb{Z}$,

$$0 = a^{p-1} - 1 = a^{q2^s} - 1 = y^{2^s} - 1 = (y-1)(y+1)(y^2+1)\dots(y^{2^{s-1}}+1)$$

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps l'un des éléments de ce produit est nul. Autrement dit on a démontré le

Théorème 6.12 *Pour que le nombre impair p, $p-1 = 2^s q$ avec q impair, soit premier, il est nécessaire que, pour tout a premier avec p, on ait*

- *Soit $a^q = 1$*
- *Soit il existe k, $1 \le k \le s-1$ tel que $(a^q)^{2^k} = -1$.*

Définition 6.13 *Soit n impair, $n = 1+2^s q$, avec q impair. On dit que n est* `pseudo-premier fort en base` *a si*

$$a^q = 1 \text{ ou si il existe } k, \quad \text{tel que} \quad 0 \le k \le s-1, \quad a^{q2^k} = -1.$$

Définition 6.14 *On dit que a est un* `faux témoin de primalité de` *n au* `sens de Miller-Rabin` *si n est non premier, mais pseudo-premier fort en base a.*

Exemple 6.4 :

$n = 25 = 5 \times 5$ n'est pas premier. Vérifions qu'il est pseudo-premier fort en base $a = 7$. On a $n - 1 = 24 = 2^s \times q$, avec $s = 2$ et $q = 3$.

On calcule d'abord $y = 7^q \equiv 18 =\equiv -7 \pmod{n}$. Ce nombre est différent de 1 modulo n. Il n'est pas non plus congru à -1 modulo n. En élévant une fois y au carré, on obtient $y^2 \equiv 49 \equiv -1 \pmod{25}$, ce qui établit la pseudo-primalité forte de 25 en base 7.

Théorème 6.15 *Si n est un entier composé distinct de 9 alors le nombre des entiers a, $1 \le a \le n-1$ tel que p soit pseudo premier fort en base a est plus petit que $\dfrac{\varphi(n)}{4}$. Autrement dit, si n est impair non premier, et si on choisit un entier $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ avec la probabilité uniforme, la probabilité de l'évenement n* est pseudo-premier fort en base *a est au plus* $1/4$.

Définition 6.16 (Test de Miller Rabin) *Le test de Miller Rabin pour l'entier n est le test suivant : on tire au hasard, avec équiprobabilité, un entier a entre 1 et $n-1$. Si n est pseudo-premier fort en base a, le test a réussi, sinon il a échoué.*

Le théorème suivant se démontre de la même manière que le théorème (6.11).

Théorème 6.17 *Soit N fixé. On choisit n avec la probabilité uniforme parmi les entiers $1 \leq n \leq N$. Si n est pseudo-premier fort en base a pour r valeurs de a tirées au hasard avec équiprobabilité dans $(\mathbb{Z}/n\mathbb{Z})^\times$, alors la probabilité que n ne soit pas premier est inférieure à $\dfrac{N}{\pi(N)}\dfrac{1}{4^r} \sim \dfrac{\ln N}{4^r}$.*

Exercices

Exercice 6.1

1. Ecrire la fonction `pari primedivs(n)` qui rend la liste des diviseurs premiers de l'entier `n`.
2. Application. En lançant `bigprime`(10^{1000}) donner un nombre premier p dont l'écriture décimale contient plus de 1000 chiffres, et un générateur g de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 6.2

Démontrer que $n = 561$ est un nombre de Carmichael.

Exercice 6.3

Soit m entier tel que $6m+1$, $12m+1$, $18m+1$ soient premiers. Démontrer que $n = (6m+1)(12m+1)(18m+1)$ est un nombre de Carmichael.

Exercice 6.4

Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ un nombre de Carmichael.

1. Démontrer que 2^α n'est pas un nombre de Carmichael (on vérifiera que 3 est premier avec 2^α, et $3^{2^{\alpha-1}} \neq 1 \pmod{2^\alpha}$).
2. Montrer que n admet au moins un facteur premier impair p. Soit g un entier, générateur du groupe cyclique $\mathbb{F}_p^\star$. Démontrer qu'il existe a tel que
$$a \equiv g \pmod{p}, \quad \text{et } a \equiv 1 \pmod{q},$$
pour tout facteur premier q de n, autre que p.
3. En déduire que $p-1$ est un diviseur de $n-1$.
4. En considérant le symbole de Legendre $\left(\frac{a}{p}\right)$ démontrer que n est impair.
5. On suppose que, pour un diviseur premier p de n, la plus grande puissance de p qui divise n est p^α, avec $\alpha \geq 2$. Montrer qu'il existe un entier a, premier avec n qui est un générateur du groupe cyclique $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. En déduire que n est un produit de facteurs premiers distincts.
6. Montrer que n est un nombre de Carmichael si et seulement si
   (a) n est impair, sans facteurs carrés.
   (b) Pour tout diviseur premier p de n, $p-1$ divise $n-1$.

Exercice 6.5

1. Déterminer tous les nombres non premiers et pseudo-premiers en base 2 plus petits que 10000.
2. Déterminer tous les nombres non premiesr et pseudo-premiers eulériens en base 2 plus petits que 10000.
3. Déterminer tous les nombres non premiers qui sont pseudo-premiers en base 2 et en base 3, plus petits que 10000.
4. Déterminer tous les nombres de Carmichael plus petits que 10000.

Exercice 6.6

1. Ecrire la procédure PARI `PetitFact(n)` qui rend 1 si l'entier n est divisible par un petit nombre premier. Vous pourrez pour cela précalculer la constante $Pk = \prod_{i=1}^{k} p_i$, et tester si le pgcd de n et Pk est plus grand que 1. Vous choisirez une valeur arbitraire de k, par exemple $k = 100$, quitte à la modifier plus tard, après quelques expériences.
2. On dira qu'un entier p est *pseudo-premier* s'il est pseudo-premier fort en base a pour 100 valeurs de a tirées au hasard. Ecrire la procedure `NextPseudoPrime(m)` qui calcule le plus petit pseudo-premier qui majore m. On partira de m supposé impair, et testera les valeurs $p = m, m+2, m+4, \ldots$ jusqu'à obtenir un pseudo-premier. On gagnera du temps en utilisant la procedure `PetitFact` pour éliminer immédiatement les p divisibles par un petit facteur premier.
3. Ecrire la procedure `RandPseudoPrime(l)` qui rend un nombre pseudo-premier aléatoire d'environ `l` bits en base 2.
4. Ecrire la procedure `RsaTriple(l)` qui rend un triplet $[N, e, d]$ où N est un nombre d'environ `l` bits en base 2, qui est de la forme $N = pq$ avec p et q premiers de taille `l/2`, e un entier aléatoire premier avec $\varphi(N)$, et d inverse de e modulo $\varphi(N)$.

Exercice 6.7

Démontrer que n est premier si et seulement si $(X+1)^n \equiv X+1 \pmod{n}$. Ce théorème est à la base du test de primalité AKS.
