On two occasions I have been asked by members of Parliament,
'Pray, Mr. Babbage, if you put into the machine wrong figures,
will the right answers come out?' I am not able rightly to apprehend
the kind of confusion of ideas that could provoke such a question.
Charles Babbage (1792-1871)

CHAPITRE X

Arithmétique du groupe $\mathbb{Z}_n^\times$

Ce chapitre considère l'anneau quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ et plus particulièrement le groupe multiplicatif $\mathbb{Z}_n^\times$ des éléments inversibles. Ce groupe se révélera très important dans les applications des chapitres suivants, qui s'appuient sur la structure de $\mathbb{Z}_p^\times$ avec p premier. Dans le souci d'une implémentation efficace, ce paragraphe développe quelques algorithmiques spécifiques à cet objet. Le projet discutera les résidus quadratiques et le symbole de Jacobi, dont le calcul est similaire à l'algorithme d'Euclide.

Sommaire

1. Structure du groupe $\mathbb{Z}_n^\times$

On s'intéressera dans la suite à l'anneau $\mathbb{Z}_n$ et plus particulièrement à $\mathbb{Z}_n^\times$, le groupe multiplicatif des éléments inversibles dans $\mathbb{Z}_n$. Le cas d'un nombre premier se révèle le plus important :

Proposition 1.1. *Pour tout nombre naturel n les trois conditions suivantes sont équivalentes :*

(1) *Le nombre n est premier.*

(2) *L'anneau $\mathbb{Z}_n$ est un corps.*

(3) *Le groupe $\mathbb{Z}_n^\times$ est d'ordre $n-1$.*

Exercice/M 1.2. Montrer l'énoncé précédent. Rappeler le théorème de Lagrange sur l'ordre d'un élément (ou d'un sous-groupe) dans un groupe fini donné. En déduire le résultat suivant :

Corollaire 1.3 (Petit théorème de Fermat)**.** *Si p est premier, alors tout $x \in \mathbb{Z}_p^\times$ vérifie $x^{p-1} = 1$. En multipliant par x on obtient la formule $x^p = x$, qui est valable pour tout $x \in \mathbb{Z}_p$. Autrement dit, étant donné un nombre premier p, tout entier $x \in \mathbb{Z}$ vérifie $x^p \equiv x \pmod{p}$.*

Exercice/M 1.4. Vérifier que pour p premier et $x \in \mathbb{Z}_p^\times$ on pourrait calculer l'inverse x^{-1} par la puissance x^{p-2}. Estimer la complexité de ce calcul en utilisant la puissance dichotomique. Cette méthode est-elle plus rapide que l'inversion via Euclide-Bézout ? Est-elle aussi générale et facile à appliquer ?

Étant donné un nombre premier p il existe en général plusieurs groupes abéliens non isomorphes d'ordre $p-1$. (Voir la classification des groupes abéliens finis à la fin du projet IX.) Miraculeusement la structure du groupe $\mathbb{Z}_p^\times$ est toujours la plus simple qui soit :

Théorème 1.5. *Pour tout nombre premier p le groupe multiplicatif $\mathbb{Z}_p^\times$ est cyclique d'ordre $p-1$, c'est-à-dire qu'il existe $g \in \mathbb{Z}_p^\times$ tel que $\mathbb{Z}_p^\times = \langle g \rangle = \{g^1, g^2, \ldots, g^{p-1} = 1\}$. Un tel élément g est appelé un* générateur *de $\mathbb{Z}_p^\times$ ou une* racine primitive *modulo p.*

Exercice/M 1.6. Montrer ce théorème en détaillant l'esquisse suivante :

ESQUISSE DE PREUVE. Comme $\mathbb{Z}_p$ est un corps, le groupe $\mathbb{Z}_p^\times$ est d'ordre $n = p-1$. Soit $n = q_1^{e_1} \cdots q_k^{e_k}$ la décomposition en facteurs premiers. Le polynôme $X^{n/q_i} - 1$ possède au plus n/q_i racines dans le corps $\mathbb{Z}_p$. Il existe alors un élément $z_i \in \mathbb{Z}_p^\times$ tel que $z_i^{n/q_i} \neq 1$. Par conséquent $g_i = (z_i)^{n/q_i^{e_i}}$ est d'ordre $q_i^{e_i}$. Les ordres $q_1^{e_1}, \ldots, q_k^{e_k}$ étant premiers entre eux, on conclut que le produit $g = g_1 \cdots g_k$ est d'ordre $n = q_1^{e_1}, \ldots, q_k^{e_k}$, comme souhaité. □

Exemple 1.7. Vous pouvez vérifier à la main que $\mathbb{Z}_5^\times$ est engendré par 2 (et 3), et que $\mathbb{Z}_7^\times$ est engendré par 3 (et 5). Essayez de trouver des racines primitives pour des nombres premiers suivants.

Remarque 1.8. Soulignons que le théorème assure l'existence d'une racine primitive modulo p sans en expliciter aucune. Effectivement, on ne connaît pas de formule miracle pour trouver une racine primitive de $\mathbb{Z}_p^\times$. En particulier la valeur de la plus petite racine primitive modulo p reste mystérieuse ; il nous ne reste que le tâtonnement par essais successifs. Ceci dit, on traduira dans la suite la preuve d'existence en une méthode efficace pour chercher une racine primitive.

Remarque 1.9. Une fois on a trouvé *une* racine primitive de $\mathbb{Z}_p^\times$ on les connaît toutes : toute racine primitive $g \in \mathbb{Z}_p^\times$ induit un isomorphisme $\phi : \mathbb{Z}_{p-1} \xrightarrow{\sim} \mathbb{Z}_p^\times$, $k \mapsto g^k$, et réciproquement tout tel isomorphisme ϕ correspond au choix d'une racine primitive $g = \phi(1)$. D'un coté $x \in \mathbb{Z}_p^\times$ est une racine primitive ssi x est un générateur du groupe $\mathbb{Z}_p^\times$. De l'autre coté $k \in \mathbb{Z}_{p-1}$ est un générateur ssi k est inversible, c'est-à-dire $k \in \mathbb{Z}_{p-1}^\times$. Ainsi l'isomorphisme ϕ établit une bijection entre $\mathbb{Z}_{p-1}^\times$ et les racines primitives de $\mathbb{Z}_p^\times$.

1.1. Structure du groupe $\mathbb{Z}_n^\times$. Le théorème précédent donne la structure de $\mathbb{Z}_p^\times$ pour p premier. On peut ensuite s'interroger sur la structure de $\mathbb{Z}_n^\times$ pour un entier $n \geq 2$ quelconque. Ce problème se simplifie considérablement en appliquant le théorème des restes chinois : On décompose $n = p_1^{e_1} \cdots p_k^{e_k}$ avec $p_1 < \cdots < p_k$ premiers et $e_1, \ldots, e_k \geq 1$. Le théorème chinois fournit un isomorphisme d'anneaux $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$. On en déduit un isomorphisme de groupes $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{e_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^\times$. (Le détailler.)

Exercice/M 1.10. *L'indicateur d'Euler* est la fonction $\varphi : \mathbb{N} \to \mathbb{N}$ définie par $\varphi(n) := |\mathbb{Z}_n^\times|$.
- Montrer que $\varphi(p^e) = (p-1)p^{e-1}$ si p est premier et $e \geq 1$.
- Montrer que $\varphi(ab) = \varphi(a)\varphi(b)$ si a et b sont premiers entre eux.
- Pour $n = p_1^{e_1} \cdots p_k^{e_k}$ conclure que $\varphi(n) = \prod_{i=1}^k (p_i - 1) p_i^{e_i - 1} = n \prod_{i=1}^k (1 - \frac{1}{p_i})$

Comme application montrer le résultat suivant, qui généralise le petit théorème de Fermat :

Corollaire 1.11 (Euler-Lagrange)**.** *L'ordre de tout élément $x \in \mathbb{Z}_n^\times$ divise l'ordre du groupe $\mathbb{Z}_n^\times$, donc $x^{\varphi(n)} = 1$. Autrement dit, tout entier x premier avec n vérifie $x^{\varphi(n)} \equiv 1 \pmod{n}$.*

Exercice/M 1.12. Vérifier que a est un générateur de $(\mathbb{Z}_n, +)$ si et seulement si a est inversible dans $\mathbb{Z}_n$. En déduire que tout groupe cyclique d'ordre n admet exactement $\varphi(n)$ générateurs. En particulier, pour p premier, il existe exactement $\varphi(p-1)$ racines primitives dans $\mathbb{Z}_p^\times$. Si l'on choisit $x \in \mathbb{Z}_p^\times$ de manière aléatoire, quelle est la probabilité de tomber sur une racine primitive ?

Outre l'ordre $\varphi(n)$ on veut connaître la structure précise du groupe $\mathbb{Z}_n^\times$. À nouveau, par le théorème des restes chinois, il suffit de traiter le cas $n = p^e$. Pour le résultat suivant consultez votre cours d'algèbre :

Théorème 1.13. *Si $n = p^e$ est la puissance d'un nombre premier impair $p \geq 3$ à l'exposant $e \geq 2$, alors le groupe $\mathbb{Z}_n^\times$ est cyclique d'ordre $\varphi(p^e) = (p-1)p^{e-1}$. Si g est un générateur de $\mathbb{Z}_p^\times$, alors g ou $g+p$ est un générateur de $\mathbb{Z}_{p^e}^\times$ pour tout $e \geq 2$.*

Pour $p = 2$ la situation est différente : $\mathbb{Z}_2^\times = \{1\}$ est trivial, $\mathbb{Z}_4^\times = \{\pm 1\}$ est cyclique d'ordre 2, mais pour $e \geq 3$, le groupe $\mathbb{Z}_{2^e}^\times$ n'est plus cyclique. Il est le produit directe du sous-groupe $\langle -1 \rangle$ d'ordre 2 et du sous-groupe $\langle 5 \rangle$ d'ordre 2^{e-2}. □

Exercice/M 1.14. Déduire du théorème que $\mathbb{Z}_n^\times$ est cyclique si et seulement si $n = 2, 4, p^e, 2p^e$ avec un nombre premier $p \geq 3$ et $e \geq 1$. *Indication.* — Dans tout autre cas on peut construire un homomorphisme surjectif $\mathbb{Z}_n^\times \to \mathbb{Z}_2 \times \mathbb{Z}_2$. Comme le groupe image n'est pas cyclique, $\mathbb{Z}_n^\times$ ne l'est pas non plus.

1.2. Déterminer l'ordre d'un élément. Comment déterminer efficacement l'ordre de x dans $\mathbb{Z}_m^\times$? Évidemment la méthode naïve consiste à calculer successivement $x^1, x^2, x^3, \ldots$ pour ainsi trouver le plus petit exposant $n \geq 1$ tel que $x^n = 1$ dans $\mathbb{Z}_m$. Ceci est très inefficace lorsque n est grand.

Exemple 1.15. Regardons $m = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1 > 10^{47}$. Il se trouve que m est premier, ce qui permet de déduire $\varphi(m) = m - 1 = 2^{32} \cdot 3^{32} \cdot 5^{32}$. Comment déterminer l'ordre de $\overline{3}$ dans $\mathbb{Z}_m^\times$? Il se trouve que $\mathrm{ord}(\overline{3}) = 2^{26} \cdot 3^{30} \cdot 5^{32}$. Il est donc hors de question d'attaquer cette question par le tâtonnement naïf !

Calculons intelligemment en exploitant notre connaissance du théorème de Lagrange : il nous garantit que l'ordre de x est un diviseur de $\varphi(m)$, ce qui limite considérablement les exposants n à tester ! Supposons connue la décomposition $\varphi(m) = p_1^{m_1} \cdots p_k^{m_k}$ avec $p_1 < \cdots < p_k$ premiers et $m_1, \dots, m_k \geq 1$. L'ordre de $x \in \mathbb{Z}_n^\times$ est donc de la forme $\operatorname{ord}(x) = p_1^{n_1} \cdots p_k^{n_k}$ avec $0 \leq n_i \leq m_i$. Posons $q = \varphi(m)/p_i^{m_i}$ pour un indice $i = 1, \dots, k$. Alors $y = x^q$ est d'ordre $\operatorname{ord}(y) = p_i^{n_i}$. Pour trouver n_i il suffit maintenant de regarder $y, y^{p_1}, y^{p_1^2}, \dots, y^{p_i^{m_i}}$ afin de déterminer le plus petit n_i tel que $y^{p_i^{n_i}} = 1$.

Algorithme X.1 Déterminer l'ordre d'un élément x dans le groupe $\mathbb{Z}_m^\times$

Entrée: un élément $x = \bar{a}$ dans $\mathbb{Z}_m^\times$ et la factorisation $\varphi(m) = p_1^{m_1} \cdots p_k^{m_k}$

Sortie: l'ordre de x dans $\mathbb{Z}_m^\times$, c'est-à-dire le plus petit entier $n \geq 1$ tel que $x^n = 1$

si $\operatorname{pgcd}(a,m) > 1$ **alors retourner** « erreur »
pour i **de** 1 **à** k **faire**
  $q \leftarrow \varphi(m)/p_i^{m_i} = p_1^{m_1} \cdots \widehat{p_i^{m_i}} \cdots p_k^{m_k}$, $y \leftarrow a^q \bmod m$, $n_i \leftarrow 0$
  tant que $y \neq 1$ **faire** $y \leftarrow y^{p_i} \bmod m$, $n_i \leftarrow n_i + 1$
fin pour
retourner $n = p_1^{n_1} \cdots p_k^{n_k}$

Exercice/M 1.16. Prouver que l'algorithme précédent est correct. Pourquoi s'arrête-t-il ? Comment être sûr que dans la $i$ème itération x^q est d'ordre $p_i^{n_i}$? À noter que la spécification exige que $x \in \mathbb{Z}_m^\times$; quel est l'intérêt du test redondant $\operatorname{pgcd}(a,m) > 1$? Est-il coûteux ? Expliquer pourquoi tous les calculs s'effectuent efficacement si l'on utilise la puissance dichotomique modulaire (voir le projet VIII). Montrer ainsi que la complexité est d'ordre $O(k \log(m)^3)$ utilisant la multiplication/division scolaire. Justifier ainsi l'intérêt de cet algorithme vis-à-vis le tâtonnement naïf.

Exercice/P 1.17. Vérifier l'exemple précédent. Puis pour le nombre premier $p = 41! + 1$ déterminer l'ordre de $2, 3, 4, \dots$ dans $\mathbb{Z}_p^\times$. Quelle est la plus petite racine primitive dans $\mathbb{Z}_p^\times$?

Remarque 1.18. L'algorithme précédent s'applique plus généralement à un groupe G quelconque pourvu que l'on sache préalablement assurer $x^m = 1$ et factoriser $m = p_1^{m_1} \cdots p_k^{m_k}$. Si G est fini alors $m = |G|$ convient. L'algorithme s'applique même à des groupes infinis, dans quel cas il faut assurer $x^m = 1$ par un autre moyen pour pouvoir satisfaire l'hypothèse de l'algorithme.

Remarque 1.19. Afin d'être efficace, l'algorithme précédent suppose que l'on sache factoriser l'exposant en question. Ceci peut être facile dans certains cas, mais en général la factorisation est une tâche très dure ! C'est pour cette raison que nous l'avons placée ici parmi les *hypothèses* de l'algorithme : il faut d'abord résoudre le problème de factorisation avant de l'appliquer. Ainsi la factorisation d'entiers reste un problème à part ; nous le discuterons dans le chapitre suivant.

2. Algorithmes probabilistes

2.1. Recherche d'une racine carrée de -1 modulo p. Étant donné un nombre premier p on se propose de trouver une racine carrée de -1 dans $\mathbb{Z}_p^\times$. Le développement qui suit est une application exemplaire de nos connaissances sur la structure de $\mathbb{Z}_p^\times$. L'algorithme efficace qui en découle nous servira plus tard, dans le projet XII, dans un tout autre contexte.

Exercice/M 2.1. Montrer que $\mathbb{Z}_p^\times$ contient une racine carrée de -1 si et seulement si $4 \mid p - 1$.

Désormais soit $p = 4k + 1$ un nombre premier. On cherche une racine $y \in \mathbb{Z}_p^\times$ du polynôme $X^2 + 1$: il en existe exactement deux, notons-les y et $-y$. Pensons à un nombre p gigantesque, comme $10^{100} + 949$. *Comment trouver deux aiguilles dans une telle botte de foin ?*

Exercice/P 2.2. Écrire une fonction qui prend comme paramètre un nombre premier $p = 4k + 1$ et cherche le plus petit entier $y = 2, 3, \dots$ tel que $y^2 \equiv -1 \pmod{p}$.

Remarque. — Il sera instructif de faire afficher chaque essai par `cout << '.'`. Comme la deuxième racine est $p - y$, il suffit d'en trouver la première. Si l'on n'en trouve pas dans $y \in [\![2, 2k]\!]$, la fonction peut

renvoyer 0 pour signaler l'erreur : dans ce cas p ne peut être premier. (La conclusion réciproque est fausse : 25 n'est pas premier, mais il existe bien des racines carrées de -1 modulo 25. Les expliciter.)

Exemple 2.3. Tester votre fonction sur 5, 13, 17, 29, 37, ... puis sur des nombres plus grands :

$$1009,\ 10^6+33,\ 10^9+9,\ 10^{15}+37,\ 10^{30}+57,\ 10^{50}+577,\ 10^{100}+949.$$

Jusqu'où peut-on aller ? Convainquez-vous que la valeur de y en fonction de p semble aléatoire. De manière heuristique, quel est le nombre moyen d'itérations nécessaires pour trouver y ?

Peut-on trouver une méthode plus efficace ? Bien sûr ! Rappelons que $\mathbb{Z}_p^\times$ est cyclique d'ordre $4k$. Pour tout $x \in \mathbb{Z}_p^\times$ la puissance $y = x^k$ vérifie alors $y^4 = 1$. En particulier $z = y^2$ vérifie $z^2 = 1$, et dans un corps ceci implique soit $z = 1$ soit $z = -1$. Dans le cas favorable $z = -1$ on a trouvé avec y une des deux racines carrées de -1 modulo p. Ceci motive l'algorithme suivant :

Algorithme X.2 Trouver une racine carrée de -1 modulo p

Entrée: un nombre premier p de la forme $p = 4k+1$
Sortie: un entier y tel que $y^2 \equiv -1$ modulo p.

répéter
  choisir un entier $x \in [\![2, p-2]\!]$ de manière aléatoire
  calculer $y \leftarrow x^k \bmod p$, puis $z \leftarrow y^2 \bmod p$
jusqu'à $z \neq 1$
si $z = p-1$ **alors retourner** y **sinon retourner** « erreur : p n'est pas premier »

Exercice/M 2.4. Justifier l'algorithme précédent ; en particulier expliquer pourquoi on peut espérer de trouver rapidement un élément x qui convient. *Indication.* — Soient $\pm y$ les deux racines carrées de -1 modulo $p = 4k+1$. Vérifier que l'application $h\colon x \mapsto x^k$ définie un homomorphisme surjectif $h\colon \mathbb{Z}_p^\times \to \{\pm 1, \pm y\}$, le noyau étant le sous-groupe des éléments dont l'ordre divise k. Montrer ainsi que pour la moitié des éléments $x \in \mathbb{Z}_p^\times$ on tombe sur une des racines $\pm y$ cherchée.

Remarque. — Quand on appelle l'algorithme pour un nombre premier p, comme exigé par la spécification, alors on a toujours $z = p-1$ au test final. Bien que redondante, quel pourrait être l'intérêt pratique d'une telle mesure de précaution ? Est-elle coûteuse ? Vaut-il mieux la supprimer ou la garder en place ?

Exercice/P 2.5. Écrire une fonction efficace qui prend comme paramètre un nombre premier $p = 4k+1$ et qui renvoie un entier $y \in [\![2, p-2]\!]$ vérifiant $y^2 \equiv -1$ modulo p.

Remarque. — Veiller à implémenter une puissance efficace. Comme avant il sera instructif de faire afficher chaque essai par `cout << '.'`. Justifier que votre fonction travaille correctement et motiver son intérêt. Vérifier empiriquement votre prévision sur les exemples ci-dessus.

Remarque. — Dans la pratique on remplace souvent le choix aléatoire de x par des essais successifs $x = 2, 3, \ldots$. Quels avantages (pragmatiques) et inconvénients (théoriques) voyez vous dans cette variante ?

Exercice/M 2.6. Essayons de déterminer la complexité asymptotique des deux méthodes :

(1) Supposons que la première méthode nécessite k itérations en moyenne. (Ce nombre correspond-il à vos expériences ? Vous pouvez le justifier sous l'hypothèse que y parcourt l'intervalle de manière aléatoire.) Chaque test calcule $y \mapsto y^2$ en effectuant une multiplication modulo p. La complexité moyenne est donc d'ordre $\Theta(p \ln(p)^2)$.

(2) Supposons que la deuxième méthode nécessite 2 itérations en moyenne. (Vous pouvez le justifier rigoureusement si vous voulez. Ce nombre correspond-il à vos expériences ?) Chaque test effectue une puissance dichotomique $y \mapsto y^k$, ce qui nécessite entre $\log_2 k$ et $2\log_2 k$ multiplications modulo p. La complexité moyenne est donc d'ordre $\Theta(\ln(p)^3)$.

Vérifier ces affirmations et comparer les prévisions aux expériences.

2.2. Recherche d'un élément d'ordre q^e modulo p. Le paragraphe précédent a présenté une méthode efficace pour trouver un élément d'ordre 4 dans $\mathbb{Z}_p^\times$. On étendra aisément cette approche aux éléments d'ordre q^e avec q premier.

Algorithme X.3 Trouver un élément $y \in \mathbb{Z}_p^\times$ d'ordre q^e

Entrée: deux nombres premiers p et q et un exposant $e \geq 1$ tel que $p-1 = q^e r$
Sortie: un entier $y \in [\![1, p-1]\!]$ représentant un élément d'ordre q^e dans $\mathbb{Z}_p^\times$

répéter
  choisir $x \in [\![1, p-1]\!]$ de manière aléatoire
  calculer $y \leftarrow x^r \bmod p$, puis $z \leftarrow y^{q^{e-1}} \bmod p$
jusqu'à $z \neq 1$
si $z^q \equiv 1 \pmod p$ **alors retourner** y **sinon retourner** « erreur : p n'est pas premier »

Exercice/M 2.7. La preuve de cet algorithme suit exactement la démonstration précédente : Soit p un nombre premier. Vérifier que l'application $h\colon x \mapsto x^r$ définit un homomorphisme $h\colon \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$. Le noyau $\ker(h)$ est le sous-groupe des éléments dont l'ordre divise r.

Supposons que g est un générateur de $\mathbb{Z}_p^\times$ et que $p-1 = q^e r$. Alors $\ker(h)$ est cyclique d'ordre r, engendré par g^{q^e}. L'image $\mathrm{im}(h)$ est le sous-groupe des éléments dont l'ordre divise q^k ; il est cyclique d'ordre q^e, engendré par g^r. En particulier $\mathrm{im}(h)$ contient exactement $(q-1)q^{e-1}$ éléments d'ordre q^k.

Montrer qu'avec probabilité $1 - \frac{1}{q}$ le choix de x mène à un élément y d'ordre q^k. En déduire que l'algorithme précédent est correct, et justifier l'intérêt de cette approche.

Exercice/P 2.8. Écrire une fonction efficace qui implémente l'algorithme ci-dessus. Comme toujours, il faut veiller à utiliser une puissance efficace.

Remarque. — Quand on appelle l'algorithme pour un nombre premier p, comme exigé par la spécification, alors on a toujours $z^q = 1$ au test final. Bien que redondante, quel pourrait être l'intérêt pratique d'une telle mesure de précaution ? Est-elle coûteuse ? Vaut-il mieux la supprimer ou la garder en place ?

Remarque. — Dans la pratique on remplace souvent le choix aléatoire de x par des essais successifs $x = 2, 3, \ldots$. Quels avantages (pragmatiques) et inconvénients (théoriques) voyez vous dans cette variante ?

Exemple 2.9. Trouver un élément d'ordre 41 modulo $p = 41! + 1$. Vous pouvez vérifier aisément la factorisation $41! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41$. Si vous voulez, essayez de trouver un élément d'ordre 1024, puis un élément d'ordre 81. Comment en fabriquer un élément d'ordre $3400704 = 2^{10} \cdot 3^4 \cdot 41$? On discutera plus bas la généralisation évidente : produire un élément $g \in \mathbb{Z}_{41!+1}^\times$ d'ordre 41! c'est-à-dire une racine primitive.

2.3. Recherche d'une racine primitive modulo p. Reprenons le théorème 1.5 qui assure l'existence d'une racine primitive modulo p sans en expliciter aucune. Heureusement nous sommes en mesure de remédier à ce défaut, non par une formule close, mais par un algorithme efficace.

D'après le théorème, $\mathbb{Z}_p^\times$ est un groupe cyclique d'ordre $n = p-1$. On pourrait donc parcourir $g = 2, 3, \ldots$ en calculant chaque fois l'ordre de g dans $\mathbb{Z}_p^\times$. Soulignons que ceci est trop coûteux avec la méthode naïve, mais tout à fait faisable avec l'algorithme efficace X.1, qui découle du théorème de Lagrange. Voici une version peaufinée pour la question restreinte :

Algorithme X.4 Déterminer si g est un générateur de $\mathbb{Z}_p^\times$

Entrée: Un entier g, un nombre premier p, et la factorisation $p-1 = q_1^{e_1} \cdots q_k^{e_k}$
Sortie: le message « g est un générateur » si et seulement si g est un générateur de $\mathbb{Z}_p^\times$.

pour i **de** 1 **à** k **faire**
  calculer $y \leftarrow g^{(p-1)/q_i} \bmod p$.
  si $y = 1$ **alors retourner** « g n'est pas un générateur »
  si $(y^{q_i} \bmod p) \neq 1$ **alors retourner** « erreur : p n'est pas premier »
fin pour
retourner « g est un générateur »

Exercice/M 2.10. Montrer que l'algorithme ci-dessus est correct.

Remarque. — Selon la spécification p est premier ; en déduire que l'on a toujours $(y^{q_i} \bmod p) = 1$. Ce test est donc redondant quand on assure d'avance que p est premier. Quel pourrait être l'intérêt pratique d'une telle mesure de précaution ? Est-elle coûteuse ? Vaut-il mieux la supprimer ou la garder en place ?

Exercice/M 2.11. Si l'on choisit $g \in \mathbb{Z}_p^\times$ de manière aléatoire, quelle est la probabilité de tomber sur une racine primitive ? En déduire une méthode efficace pour trouver une racine primitive. Comment en trouver la plus petite ? Heuristiquement pourquoi peut-on espérer de la trouver rapidement ?

Exercice/M 2.12. On peut faire légèrement mieux si l'on veut trouver *une* racine primitive, n'importe laquelle. Étant donné la factorisation $p-1 = q_1^{e_1} \cdots q_k^{e_k}$ on sait déjà trouver des éléments $g_1, \ldots, g_k$ d'ordre $q_1^{e_1}, \ldots, q_k^{e_k}$ respectivement (voir l'algorithme X.3 plus haut). Montrer que $g = g_1 \cdots g_k$ est d'ordre $p-1$, c'est donc une racine primitive comme souhaité. Voyez-vous l'avantage par rapport à l'approche précédente ? Déterminer la probabilité de succès et le nombre moyen d'itérations.

☞ *Remarque.* — Cette méthode est la version algorithmique de notre preuve du théorème 1.5 ci-dessus. Ainsi se ferme le cercle d'idées autour de la structure de $\mathbb{Z}_p^\times$.

Exercice/P 2.13. Montrer que $\overline{2}$ est une racine primitive modulo $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$. Puis trouver une racine primitive g modulo $p = 41! + 1$. Est-ce que ces questions sont abordables par une recherche naïve ? Par quelle méthode pensez-vous y parvenir le plus facilement ? Après avoir trouvé un élément $g \in \mathbb{Z}_p$ d'ordre $p-1$ peut-on conclure que p est premier ? Félicitations, vous venez de découvrir une preuve de primalité ! Contemplez ce bel exploit. Nous y reviendrons au chapitre suivant.

Tout problème mathématique pourrait, en principe, être directement résolu par une énumération exhaustive. Mais il existe des problèmes d'énumération qui peuvent actuellement être résolus en quelques minutes, alors que sans méthode toute une vie humaine n'y suffirait pas.
Ernst Mach, *Populär-wissenschaftliche Vorlesungen*, 1896

PROJET X

Résidus quadratiques et symbole de Jacobi

Sommaire

1. Le symbole de Jacobi

Étant donné un entier impair $n \geq 3$, on dit que $a \in \mathbb{Z}$ est un *résidu quadratique* ou *carré modulo n* s'il existe $r \in \mathbb{Z}$ tel que $r^2 \equiv a \pmod{n}$. Dans ce cas on appelle r une *racine carrée* de a modulo n. Ce projet étudie les résidus quadratiques modulo n. Voici la première méthode qui vient à l'esprit :

Exercice/P 1.1. Écrire une fonction `bool est_carre( Integer a, Integer n )` qui teste par des essais successifs pour $r \in [\![0, \frac{n-1}{2}]\!]$ si $a \equiv r^2 \pmod{n}$. Elle renvoie `true` si a est un résidu quadratique modulo n et `false` sinon. Cette méthode est-elle praticable pour $a = 2$ et $n = 1009$? pour $n = 10^9 + 7$? pour $n = 10^{18} + 3$? pour $n = 10^{56} + 3$? (On développera des méthodes plus efficaces dans la suite.)

1.1. Le symbole de Legendre. Soit $p \geq 3$ un nombre premier. Pour $a \in \mathbb{Z}$ on note $\bar{a} \in \mathbb{Z}_p$ sa classe modulo p. On définit alors le *symbole de Legendre* de a modulo p par

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & \text{si } \bar{a} \in \mathbb{Z}_p^\times \text{ est un carré,} \\ -1 & \text{si } \bar{a} \in \mathbb{Z}_p^\times \text{ n'est pas un carré,} \\ 0 & \text{si } \bar{a} = 0. \end{cases}$$

Exercice/M 1.2. Afin d'avoir des exemples concrets, déterminer $\left(\frac{5}{7}\right)$ et $\left(\frac{7}{5}\right)$, puis $\left(\frac{7}{11}\right)$ et $\left(\frac{11}{7}\right)$.

Exercice/M 1.3. Rappelons que $\mathbb{Z}_p$ est un corps et que $\mathbb{Z}_p^\times$ est un groupe cyclique d'ordre $p-1$. Il existe alors une racine primitive g d'ordre $p-1$, c'est-à-dire $\mathbb{Z}_p^\times = \{g, g^2, g^3, \ldots, g^{p-1} = 1\}$.

(1) En fonction de g caractériser les carrés et les non-carrés dans $\mathbb{Z}_p^\times$. Déterminer $g^{\frac{p-1}{2}} \in \mathbb{Z}_p$.

(2) En déduire le critère d'Euler, dont l'énoncé ne fait plus intervenir la racine primitive : Pour tout $a \in \mathbb{Z}$ on a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(3) En déduire la multiplicativité $\left(\frac{a_1 a_2}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)$ ainsi que $\left(\frac{1}{p}\right) = 1$.

Exercice/P 1.4. Écrire une fonction efficace `int legendre( Integer a, Integer p )` qui calcule la puissance $e = a^{\frac{p-1}{2}} \bmod p$ puis renvoie ± 1 si $e \equiv \pm 1$, et renvoie 0 dans tout autre cas. (Pour effectuer ce calcul on suppose que $p \geq 3$ est impair. Si jamais $e \not\equiv \pm 1$ la fonction signale l'erreur en renvoyant 0.)

Exercice 1.5. Combien d'itérations faut-il pour évaluer `legendre(a,p)` ? Cette méthode est-elle praticable pour les exemples de l'exercice 1.1 ? (Attention aux hypothèses différentes.) Êtes-vous contents de la performance ? Justifier l'intérêt de cette méthode vis-à-vis la méthode naïve utilisée en exercice 1.1.

1.2. La loi de réciprocité quadratique. Dans la suite on aura besoin d'une formule importante, dont on admettra la preuve. Il s'agit de la célèbre *loi de réciprocité quadratique* de Gauss :

Théorème 1.6. *Soient p,q deux nombres premiers impairs distincts. Alors on a la formule de réciprocité*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\cdot\varepsilon(p,q) \quad \textit{avec} \quad \varepsilon(p,q) := \begin{cases} +1 & \textit{si } p\equiv 1 \textit{ ou } q\equiv 1 \pmod 4, \\ -1 & \textit{si } p\equiv 3 \textit{ et } q\equiv 3 \pmod 4. \end{cases}$$

Pour le cas exceptionnel $q=2$ on a la formule complémentaire :

$$\left(\frac{2}{p}\right) = \delta(p) \quad \textit{avec} \quad \delta(p) := \begin{cases} +1 & \textit{si } p\equiv \pm 1 \pmod 8, \\ -1 & \textit{si } p\equiv \pm 3 \pmod 8. \end{cases}$$

Exercice/M 1.7. Déterminer $\left(\frac{5}{7}\right)$ et $\left(\frac{7}{5}\right)$ comme en exercice 1.2. Que vaut $\varepsilon(5,7)$?
Vérifier la réciprocité dans ce cas particulier. Même exercice avec $\left(\frac{7}{11}\right)$ et $\left(\frac{11}{7}\right)$ et $\varepsilon(7,11)$.

Exercice/M 1.8. Vérifier la formule complémentaire pour $\left(\frac{2}{3}\right)$ et $\left(\frac{2}{5}\right)$ puis $\left(\frac{2}{7}\right)$ et $\left(\frac{2}{17}\right)$.

1.3. Le symbole de Jacobi. Le symbole de Legendre $\left(\frac{a}{p}\right)$ n'est défini que pour les nombres premiers $p\geq 3$. On l'étend aux nombres composés par multiplicativité : pour $b\geq 1$ impair on définit le *symbole de Jacobi* par $\left(\frac{a}{b}\right) := \prod_i \left(\frac{a}{p_i}\right)$ où $b=\prod_i p_i$ est la décomposition de b en facteurs premiers p_i. À noter que

$$\left(\frac{a}{1}\right) = 1 \qquad \text{et} \qquad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right).$$

Exercice/M 1.9. Dans l'objectif d'un calcul efficace, justifier les règles de calcul suivantes :

① $\left(\frac{a}{b}\right) = 0$ si et seulement si $\operatorname{pgcd}(a,b)>1$

② $\left(\frac{1}{b}\right) = 1$ et $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$

③ $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$ si $a\equiv a' \pmod b$

④ $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)\cdot\varepsilon(a,b)$ si a est impair

⑤ $\left(\frac{2}{b}\right) = \delta(b)$

Ici on sous-entend que ε et δ sont définis par les formules ci-dessus pour des nombres impairs quelconques. Pour prouver ces règles il faut passer par la décomposition en facteurs premiers : pour ⑤ montrer d'abord que δ est multiplicatif, et pour ④ que ε est multiplicatif en chaque argument.

Exercice/M 1.10. Calculer à la main la valeur de $\left(\frac{71}{83}\right)$ en utilisant les règles ci-dessus. Vous pouvez ensuite comparer votre résultat avec celui de `legendre(71,83)`, car 83 est premier.

Exercice/M 1.11. Soit $a=13\,353\,839$ et admettons que $p=64a+3$ est premier. Existe-t-il une solution $x,y\in\mathbb{Z}$ à l'équation $x^2+yp=4a$? Même question pour l'équation $x^2+yp=8a$. *Remarque.* — Tout le calcul est faisable à la main ! Vous pouvez ensuite comparer avec `legendre`.

1.4. Une implémentation efficace. Après ces préparations, on se propose d'implémenter le calcul du symbole de Jacobi. À noter que sa définition utilise la décomposition en facteurs premiers, opération très coûteuse pour les grands entiers. Fort heureusement la loi de réciprocité permet un calcul efficace :

Exercice/P 1.12. Écrire une fonction `int jacobi( Integer a, Integer b )` qui calcule le symbole de Jacobi $\left(\frac{a}{b}\right)$ par une méthode similaire à l'algorithme d'Euclide, en utilisant les règles ①,②,③,④,⑤ ci-dessus. (Une version récursive sera plus facile à écrire, une version itérative sera légèrement plus efficace.) Une fois la fonction est construite, essayer de prouver la terminaison, puis la correction du calcul. La tester sur les exemples précédents (exercices 1.7, 1.8, 1.10, 1.11) afin de trouver d'éventuelles erreurs. Dans ces tests il sera instructif d'afficher les étapes intermédiaires.

2. Deux applications aux tests de primalité

Comme applications nous établissons le critère de primalité de Pépin, fait sur mesure pour les nombres de Fermat, puis le test probabiliste de Solovay-Strassen, qui s'applique à un entier quelconque.

2.1. Nombres de Fermat et le critère de Pépin. Fermat conjectura que $F_n = 2^{2^n}+1$ est premier pour tout n. Effectivement $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ sont tous premiers. Mais déjà Euler trouva la décomposition $F_5 = 4294967297 = 641 \cdot 6700417$. On constate que $641 = 5 \cdot 2^7 + 1$ et $6700417 = 52347 \cdot 2^7 + 1$. Ceci n'est pas un hasard :

Exercice/M 2.1. Si un nombre premier p divise F_n avec $n \geq 2$, alors $p = k \cdot 2^{n+2} + 1$ avec $k \in \mathbb{N}$. *Indication.* — En supposant $p \mid F_n$ calculer 2^{2^n} mod p, et en déduire l'ordre de 2 dans $\mathbb{Z}_p^\times$. Pour $n \geq 2$ on a $p \equiv 1 \pmod 8$, ce qui permet de déterminer $\left(\frac{2}{p}\right)$. En déduire qu'il existe $x \in \mathbb{Z}_p^\times$ d'ordre 2^{n+2}.

Exercice/P 2.2. Implémenter cette observation pour trouver un facteur $k \cdot 2^{n+2} + 1$ de F_n, au moins dans les cas $n = 5, 6, 9, 10, 11, 12, 15, 16, 18, 19, 23, 30$, puis tester d'autres indices n. *Indication.* — À noter que p est petit tandis que F_n est très grand. Pour tester si p divise F_n il n'est donc pas une bonne idée de calculer F_n dans $\mathbb{Z}$. Il est plus efficace de fixer d'abord p puis de calculer $F_n = 2^{2^n}+1$ modulo p via une puissance dichotomique modulaire. Ceci garantit que tous les calculs intermédiaires restent bornés par p.

Dans les cas restants $n = 7, 8, 13, 14, 17, 20, 21, 22, 24, \ldots$ on ne trouve pas de petits facteurs, et il est certainement trop coûteux de tester *tous* les candidats possibles. On développera dans la suite une méthode efficace pour déterminer néanmoins si F_n est premier ou composé. (On a déjà utilisé ce critère, dit de Pépin, dans le projet VIII.)

Exercice/M 2.3. Commençons par un critère suffisant. Soit $N = 2^k + 1$ et supposons que $a \in \mathbb{Z}_N$ vérifie $a^{2^{k-1}} = -1$. Montrer que $a \in \mathbb{Z}_N^\times$ et déterminer son ordre. Conclure que N est premier.

Exercice/M 2.4. Calculer $\left(\frac{F_n}{3}\right)$ puis $\left(\frac{3}{F_n}\right)$ par réciprocité. En déduire le critère de Pépin : Pour $n \geq 1$ le nombre F_n est premier si et seulement si $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

Exercice/P 2.5. En déduire une fonction `bool pepin(int n)` qui renvoie `true` si F_n est premier et `false` sinon. (Vous pouvez réutiliser la fonction `legendre` de l'exercice 1.4.) Jusqu'à quelle valeur de n pouvez-vous déterminer la nature de F_n ?

— ∗ —

Remarque historique. — Mis à part les cinq premiers cas, on ignore s'il existe d'autres nombres premiers parmi les nombres de Fermat. Bien que très particulière, cette question a attiré beaucoup d'attention ; elle apparaît d'ailleurs dans le problème classique de la construction des polygones réguliers à la règle et au compas.

Pour tout $5 \leq n \leq 30$ on sait que F_n est composé : pour certains F_n on connaît un ou plusieurs petits facteurs, pour d'autres on sait que F_n est composé grâce au critère de Pépin, sans pour autant connaître de facteurs. Les cas les plus durs et les plus récents sont F_{14} en 1964, F_{20} en 1988, F_{22} en 1995, et F_{24} en 2003, tous résolus par le critère de Pépin. Vous pouvez vous convaincre que le nombre F_{24} a 2^{24} bits, c'est-à-dire environ 5 million de décimales. En 2003 le test de Pépin pour F_{24} nécessitait environ 200 jours de calcul.

Actuellement, en 2006, le plus petit nombre de Fermat dont la nature reste inconnue est F_{33}. Malgré ces difficultés, on peut dire qu'il est raisonnablement facile de déterminer si F_n est premier ou composé, au moins pour $n \leq 32$. Pourtant il est extrêmement dur de trouver la décomposition de F_n en facteurs premiers, même pour n aussi petit que 9 ou 10 ou 11 : leurs factorisations ont été trouvées entre 1988 et 1995, nécessitant chaque fois quelques mois de calcul. On ignore actuellement la factorisation complète de F_n pour $n \geq 12$.

Ces exemples laissent déjà imaginer que la factorisation des grands entiers présente des difficultés considérables, ce qui en fait davantage un domaine intéressant. Pour savoir plus sur l'approche algorithmique aux nombres premiers, vous pouvez consulter le livre récent de R. Crandall et C. Pomerance [**15**] ou l'incontournable P. Ribenboim [**14**].

2.2. Test de primalité d'après Solovay et Strassen. L'étude précédente est très spécifique aux nombres de Fermat $F_k = 2^{2^k}+1$. Pour un entier impair n quelconque on ne sait pas prédire la forme de ses facteurs, et il n'existe pas de critère simple de primalité non plus. En particulier on ne sait pas prédire quels nombres $a \in [\![1,n[\![$ vont témoigner que n est composé ou certifier que n est premier. Voici l'observation clé :

Théorème 2.6 (R. Solovay et V. Strassen, 1977)**.** *Pour tout entier impair n l'ensemble*

$$G_n = \left\{ \bar{a} \in \mathbb{Z}_n \;\middle|\; 0 \neq \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n} \right\}$$

est un sous-groupe de $\mathbb{Z}_n^\times$. On a $G_n = \mathbb{Z}_n^\times$ si et seulement si n est premier. Si n est composé, alors G_n est d'indice ≥ 2 dans $\mathbb{Z}_n^\times$, et on a donc la majoration $|G_n| \leq \frac{n-1}{2}$.

DÉMONSTRATION. L'observation que G_n est un sous-groupe se vérifie aisément. (Le détailler.) En plus on a déjà établi le critère d'Euler dans l'exercice 1.3 : si n est premier, alors $G_n = \mathbb{Z}_n^\times$. Il reste à montrer que $G_n \neq \mathbb{Z}_n^\times$ pour n composé. Supposons que n se décompose en $n = p^e q$ avec p premier, $e \geq 1$, et $p \nmid q$. Le théorème chinois nous donne l'isomorphisme d'anneaux $\Phi\colon \mathbb{Z}_n \xrightarrow{\sim} \mathbb{Z}_{p^e} \times \mathbb{Z}_q$. Il existe $g \in \mathbb{Z}$ tel que $\bar{g} \in \mathbb{Z}_{p^e}$ soit une racine primitive, c'est-à-dire un générateur du groupe cyclique $\mathbb{Z}_{p^e}^\times$ d'ordre $(p-1)p^{e-1}$. Soit $a \in \mathbb{Z}$ tel que $\Phi(\bar{a}) = (\bar{g}, \bar{1})$. Par construction on a $\bar{a} \in \mathbb{Z}_n^\times$ et nous affirmons que $\bar{a} \notin G_n$.

Supposons d'abord que $e = 1$; dans ce cas on a $n = pq$ avec p premier et un cofacteur $q \geq 3$. On trouve $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)\left(\frac{1}{q}\right) = -1$, mais $\Phi(\bar{a}^{\frac{n-1}{2}}) = (\bar{g}^{\frac{n-1}{2}}, \bar{1}) \neq (-\bar{1}, -\bar{1})$, donc $\bar{a}^{\frac{n-1}{2}} \neq -\bar{1}$.

Supposons enfin que $n = p^e q$ avec $e \geq 2$. Si l'on avait $\bar{a}^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) = \pm 1$, alors $\bar{a}^{n-1} = \bar{1}$ et $\Phi(\bar{a}^{n-1}) = (\bar{g}^{n-1}, \bar{1}) = (\bar{1}, \bar{1})$. Ceci voudrait dire que $\operatorname{ord}(\bar{g}) = (p-1)p^{e-1}$ divise $n-1$, on aurait donc que $p \mid n-1$, ce qui est impossible. Donc $\bar{a}^{\frac{n-1}{2}} \neq \pm\bar{1}$, et on conclut que $a \notin G_n$. □

On ne sait pas grand chose sur G_n outre la majoration de son cardinal. D'autre part, pour tout $a \in \mathbb{Z}_n$ donné, il est facile de tester si $a \in G_n$: il suffit de comparer $\left(\frac{a}{n}\right)$ et $a^{\frac{n-1}{2}}$. Heureusement nous disposons de deux méthodes efficaces : la réciprocité quadratique pour calculer $\left(\frac{a}{n}\right)$, et la puissance dichotomique modulaire pour calculer $a^{\frac{n-1}{2}}$ modulo n. Ceci donne lieu à un test de primalité : on choisit $a \in [\![1,n[\![$ de manière aléatoire. Si $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}$, alors n est composé. Si $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}$, alors n est possiblement premier, donc on répète le test.

Exercice/M 2.7. *Argument probabiliste.* — Si n est premier, alors il passe le test pour tout a. Si n est composé, alors un élément a choisit au hasard le témoignera avec probabilité $\geq \frac{1}{2}$; la probabilité d'échec est $\leq \frac{1}{2}$. Après t tests indépendants la probabilité d'échec tombe à $\leq 2^{-t}$. Ainsi l'itération de t tests trouve avec probabilité $\geq 1 - 2^{-t}$ un témoin a vérifiant $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}$. Vérifier ces affirmations.

Conclusion réciproque ? — Si après quelques tests de Solovay-Strassen la réponse est « composé » alors n est composé : on a effectivement trouvé une preuve, sous forme d'un témoin a. Si la réponse après 100 tests est toujours « possiblement premier » alors on voudrait conclure que n est premier, mais il reste une probabilité d'erreur majorée par $2^{-100} < 10^{-30}$. Quelle conclusion vous semble justifiée ?

Exercice/P 2.8. Écrire une fonction `Integer cherche_temoin( Integer n, int t=100 )` qui effectue au plus `t` tests de Solovay-Strassen. Elle renvoie le premier témoin trouvé, ou 0 si aucun témoin n'a été trouvé. Comme application, trouver le plus petit nombre premier de la forme $10^{100}+k$ avec $k \geq 0$. Est-il raisonnable de tester la primalité par la méthode naïve (c'est-à-dire via des divisions successives) ? Justifier ainsi l'intérêt du test probabiliste de Solovay-Strassen.

— ∗ —

Remarque historique. — Publié en 1977, le test de Solovay-Strassen fut le premier test probabiliste de primalité, et il est vite devenu un exemple phare de l'approche probabiliste. On peut même dire qu'il a déclenché l'étude approfondie des algorithmes probalistes, auparavant considérés comme heuristiques, non rigoureux et mathématiquement inintéressants. Dans le chapitre XI nous discuterons son successeur, le test de Miller-Rabin, qui est plus facile à implémenter et plus performant. Si le caractère probabiliste vous gêne, on discutera aussi une alternative déterministe, bien que moins rapide.

3. Une preuve de la réciprocité

Nul n'est censé ignorer la loi
(de la reciprocité quadratique).

3.1. Un théorème peu plausible ? La réciprocité quadratique établit un lien remarquable et plutôt inattendu : pourquoi la propriété de q d'être un carré modulo p serait-elle liée à la propriété de p d'être un carré modulo q ? A priori le « monde modulo p » et le « monde modulo q » n'ont rien en commun — n'est-ce pas l'affirmation du théorème chinois ?

Pourtant, après avoir calculé suffisamment d'exemples, on constate une certaine régularité. Avouons toutefois que la réciprocité est loin d'être évidente : même en rétrospective, en contemplant la formule ci-dessus, qui aurait deviné le facteur $\varepsilon(p,q) = (-1)^{(p-1)(q-1)/4}$?

Historiquement la réciprocité fut conjecturée par Euler, puis formulée explicitement par Legendre, mais sa preuve restait incomplète. La première preuve fut trouvée par Gauss en 1796, à l'âge de 19 ans, qui publierait six preuves différentes dans les années suivantes. On en compte plus de deux cents variantes publiées aujourd'hui, soit à peu près une par an. On trouve une liste chronologique assez complète sur le site de Franz Lemmermeyer, `www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`

Les exercices suivants présentent une des preuves les plus élémentaires, découverte par G. Zolotarev en 1872, qui ne repose que sur les *permutations* et leur *signature*.

3.2. Quelques préparatifs. Commençons par une révision de quelques jolis résultats.

Exercice/M 3.1. Tout d'abord, rappelons les propriétés essentielles de la signature :

(1) Rappeler la définition, construction, et unicité de la signature $\operatorname{sign}_X : \operatorname{Sym}(X) \to \{\pm 1\}$. Quelle est la signature d'une transposition (i,j) ? D'un cycle $(i_1, i_2, \dots, i_\ell)$ de longueur ℓ ?

(2) Supposons X ordonné. Quel est le rapport entre la signature d'une permutation $\sigma : X \to X$ et les inversions, c'est-à-dire les paires $(i,j) \in X \times X$ telles que $i < j$ mais $\sigma(i) > \sigma(j)$?

(3) Si $X \subset Y$, expliquer comment on peut construire naturellement un homomorphisme de groupes injectif $\iota : \operatorname{Sym}(X) \hookrightarrow \operatorname{Sym}(Y)$. A-t-on $\operatorname{sign}_X = \operatorname{sign}_Y \circ \iota$?

(4) Supposons X décomposé en $X = A \cup B$ avec $A \cap B = \emptyset$. Si une permutation $\sigma : X \to X$ vérifie $\sigma(A) = A$ et $\sigma(B) = B$, a-t-on $\operatorname{sign}_X(\sigma) = \operatorname{sign}_A(\sigma|_A) \cdot \operatorname{sign}_B(\sigma|_B)$?

(5) Soit $\Phi : X \xrightarrow{\sim} Y$ une bijection. Expliquer comment construire de manière naturelle un isomorphisme de groupes $\Phi_* : \operatorname{Sym}(X) \xrightarrow{\sim} \operatorname{Sym}(Y)$. A-t-on $\operatorname{sign}_X = \operatorname{sign}_Y \circ \Phi_*$?

$$\begin{array}{ccc} \operatorname{Sym}(X) & \xrightarrow[\cong]{\Phi_*} & \operatorname{Sym}(Y) \\ & {\scriptstyle \operatorname{sign}_X} \searrow \quad \swarrow {\scriptstyle \operatorname{sign}_Y} & \\ & \{\pm 1\} & \end{array}$$

(6) Si $\sigma : X \xrightarrow{\sim} X$ et $\tau : Y \xrightarrow{\sim} Y$ sont deux permutations, déterminer le signe de la permutation produit $\sigma \times \tau : X \times Y \xrightarrow{\sim} X \times Y$ définie par $(x,y) \mapsto (\sigma(x), \tau(y))$.

Exercice/M 3.2. Considérons ensuite l'ensemble $X = \mathbb{Z}_p$ pour un nombre premier impair $p \geq 3$. On se propose de calculer la signature de l'application affine $\alpha : \mathbb{Z}_p \to \mathbb{Z}_p$, $x \mapsto qx + r$ avec $q \in \mathbb{Z}_p^\times$ et $r \in \mathbb{Z}_p$.

(1) Décomposer $\sigma : x \mapsto x+1$ en cycles et en déduire $\operatorname{sign}(\sigma)$.

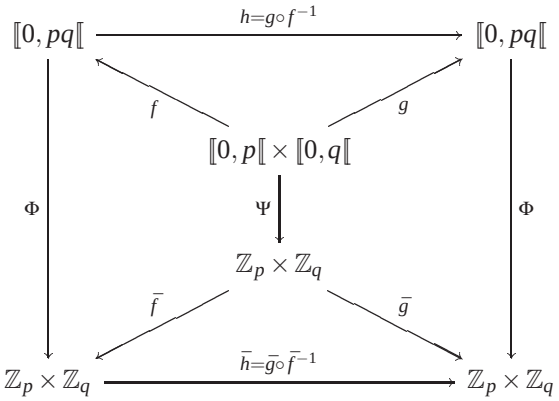
(2) Rappeler la structure du groupe multiplicatif $\mathbb{Z}_p^\times$.

(3) Pour une racine primitive g de $\mathbb{Z}_p^\times$, décomposer $\rho : x \mapsto gx$ en cycles et en déduire $\operatorname{sign}(\rho)$.

(4) Dans le cas général on a $q = g^k$, donc $\alpha = \sigma^r \rho^k$. En déduire $\operatorname{sign}(x \mapsto qx + r)$.

(5) En conclusion, exprimer $\operatorname{sign}(x \mapsto qx + r)$ par le symbole de Legendre.

3.3. La preuve de Zolotarev. Considérons deux nombres premiers impairs distincts $p, q \geq 3$. Pour l'intervalle $[\![0, pq[\![$ deux systèmes de numération mixte $f, g\colon [\![0, p[\![\times [\![0, q[\![\xrightarrow{\sim} [\![0, pq[\![$ viennent à l'esprit : d'une part $f(x,y) = x + py$, d'autre part $g(x,y) = qx + y$. Tous les deux sont des bijections, leur inverse étant donnée par la division euclidienne par p et par q respectivement. La composition $h = g \circ f^{-1}$ envoie $x + py$ sur $qx + y$. C'est la première ligne du diagramme suivant :



Par construction, h est une permutation. L'astuce de Zolotarev consiste à calculer la signature de h de deux manières différentes, pour en déduire la loi de réciprocité quadratique.

Exercice 3.3. On va d'abord exprimer $\operatorname{sign}(h)$ à l'aide des symboles de Legendre calculés ci-dessus. Pour cela on identifie $[\![0, p[\![\times [\![0, q[\![$ avec $\mathbb{Z}_p \times \mathbb{Z}_q$ via l'application $\Psi(x,y) = (\pi_p(x), \pi_q(y))$. L'application $\Phi\colon [\![0, pq[\![\xrightarrow{\sim} \mathbb{Z}_p \times \mathbb{Z}_q$ donnée par $\Phi(z) = (\pi_p(z), \pi_q(z))$ est une bijection par le théorème chinois. Ainsi nos fonctions f et g se traduisent en deux applications $\bar{f}\colon (\bar{x}, \bar{y}) \mapsto (\bar{x}, \overline{py + x})$ et $\bar{g}\colon (\bar{x}, \bar{y}) \mapsto (\overline{qx + y}, \bar{y})$ définies par les conditions que $\Phi \circ f = \bar{f} \circ \Psi$ et $\Phi \circ g = \bar{g} \circ \Psi$. Ceci se résume en disant que le diagramme précédent commute.

(1) Exprimer les signatures $\operatorname{sign}(\bar{f})$ et $\operatorname{sign}(\bar{g})$ par des symboles de Legendre.

(2) Expliquer pourquoi on a l'égalité $\operatorname{sign}(\bar{g} \circ \bar{f}^{-1}) = \operatorname{sign}(g \circ f^{-1})$.

Exercice 3.4. Ensuite on calcule $\operatorname{sign}(h)$ en comptant le nombre des inversions.

(1) Vérifier que

$$\begin{aligned} x + py < x' + py' \quad &\Longleftrightarrow \quad y < y' \text{ ou } (y = y' \text{ et } x < x'), \\ qx + y > qx' + y' \quad &\Longleftrightarrow \quad x > x' \text{ ou } (x = x' \text{ et } y > y'). \end{aligned}$$

(2) En déduire que $z = x + py$ et $z' = x' + py'$ vérifient $z < z'$ et $h(z) > h(z')$ si et seulement si $x > x'$ et $y < y'$. Compter le nombres des telles inversions, puis en déduire la signature de h.

(3) Établir la loi de réciprocité en mettant toutes les informations ensemble.

Exercice/M 3.5 (Question bonus)**.** Si vous voulez, vous pouvez réfléchir aux questions suivantes :

(1) Où utilise-t-on la primalité de p et q dans la preuve précédente ?

(2) A-t-on $\operatorname{sign}\left(\begin{smallmatrix} \mathbb{Z}_p \to \mathbb{Z}_p \\ x \mapsto qx + r \end{smallmatrix}\right) = \left(\frac{q}{p}\right)$ pour tout $p \geq 3$ impair ? (Symbole de Jacobi)

(3) Peut-on généraliser les arguments en supposant seulement que $\operatorname{pgcd}(p, q) = 1$?

(4) Comment calculer $\left(\frac{-1}{p}\right)$? Puis $\left(\frac{2}{p}\right)$? *Indication.* — On peut tenter la récurrence suivante :

$$\left(\frac{2}{m+2}\right) = \left(\frac{-m}{m+2}\right) = \pm\left(\frac{m}{m+2}\right) = \pm\left(\frac{m+2}{m}\right) = \pm\left(\frac{2}{m}\right).$$

(5) Comment généraliser $\left(\frac{q}{p}\right)$ et ce développement à p pair ? (Symbole de Kronecker)