Le chiffrement de Rabin

À propos d'un exercice de baccalauréat, spécialité S

Robert Cabane

22 octobre 2018

Cet article est dédié à Michel Mendès France, mathématicien, peintre et ami, décédé le 30 janvier 2018.
Bien que cela n'ait qu'un rapport lointain avec le sujet du présent article, nous invitons le lecteur à découvrir l'arithmétique des nombres premiers sous la houlette de Gérald Tenenbaum et de Michel Mendès France dans un célèbre « Que sais-je ? » [1], ou dans cet ouvrage plus récent et plus complet : Les nombres premiers : entre l'ordre et le chaos [2].

1 Le sujet

L'exercice de spécialité du sujet de baccalauréat (série S) donné à Pondichéry en mai 2018 nous propose d'étudier un système de chiffrement moins connu et naïf que les inévitables chiffrements de Hill et autres. Il s'agit du chiffrement proposé par Michael Rabin [1] en 1979 (l'article originel [3] est librement téléchargeable), reposant sur un système asymétrique à clés publiques et clés secrètes (ou privées).

La proposition de Rabin traite de la communication entre deux personnes, Alice et Bob, qui ne souhaitent pas que leurs échanges puissent être interceptés par autrui (la célèbre espionne Ève). Alice est l'initiatrice de la communication, et elle voudrait recevoir secrètement un message provenant de Bob (pour une communication en sens inverse, on échange les rôles). [2]

Pour ce faire, elle choisit un couple d'entiers (p, q), p et q étant des nombres premiers impairs et distincts [3] (nous verrons plus loin comment « bien » les choisir). Ces deux nombres resteront secrets et seule Alice en aura connaissance ; le couple (p, q) s'appelle la *clé privée* du système. Alice calcule ensuite leur produit $n = pq$ et choisit un entier B compris entre 0 et $n - 1$. Le couple (n, B) forme la *clé publique* du système, qu'Alice transmet (sans précaution particulière) à Bob ; celui-ci va s'en servir pour créer son message, un nombre entier x compris entre 0 et $n-1$, qu'il conserve secrètement : nous appellerons x le *message clair*. Puis Bob calcule

$$(1) \quad y \equiv x(x + B) \bmod n$$

qu'il envoie (publiquement) à Alice ; nous appellerons y le *message chiffré*. Pour accéder au message clair x, Alice doit résoudre la congruence précédente, ce qui peut être singulièrement difficile pour Ève (qui espionne toutes les communications entre Alice et Bob) si l'entier n est très grand mais bien plus aisé pour Alice qui sait factoriser n, grâce au « théorème chinois » que nous allons présenter ci-dessous.

1. Michael Oser Rabin, né le 1er septembre 1931 à Breslau en Allemagne (actuellement Wrocław en Pologne), est un informaticien et logicien israélien. Il a été récipiendaire du prix Turing en 1976. Pour plus de détails sur la vie et les découvertes de M. Rabin, nous invitons le lecteur à consulter la page Wikipedia qui lui est consacrée ainsi que sur celles du prix Turing ou du prix Dan David.

2. Le lecteur pourra trouver un exposé historique captivant de la découverte des cryptosystèmes asymétriques dans le livre de Simon Singh [4] et une présentation plus détaillée dans le chapitre 5 du cours de Gilles Bailly-Maitre [5].

3. En pratique, les nombres premiers choisis seront « grands » (ayant au moins 1024 bits chacun, soit de l'ordre de trois cents chiffres décimaux puisque $\log_{10}(2^{1024}) \approx 308,25$).

La difficulté de factoriser un très grand nombre est actuellement considérée comme fondamentale pour la sécurité des cryptosystèmes de nature arithmétique, et elle est pour l'instant assurée pour des nombres ayant plus de 600 chiffres.

Dans le sujet proposé, on choisissait $p = 3$, $q = 11$, $n = 33$, $B = 13$; on supposait que Bob représentait (encodait) une lettre par son rang alphabétique x (0 à 25), trouvait $y = 3$ puis transmettait ce nombre à Alice. Cela amène à s'intéresser à l'équation $x(x + 13) \equiv 3 \bmod 33$, équivalente à $(x + 23)^2 \equiv 4 \bmod 33$ car :

$$(x + 23)^2 \equiv x^2 + 46x + 100 \equiv x^2 + 13x + 1 \bmod 33$$

2 Le théorème des restes chinois

C'est le moment de signaler l'apparition de ce très célèbre et ancien théorème, délicatement dissimulé dans le sujet du jour. Un article [6] très complet de CultureMath est entièrement consacré à ce sujet.

Théorème 1. *Soient p et q deux nombres premiers entre eux, et $n = pq$. Toute congruence simultanée de la forme*

$$(2) \quad \begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases}$$

admet une solution et une seule $x \in [0, n-1]$.

Preuve algébrique
Le « théorème chinois » a une preuve « abstraite » très simple, basée sur l'observation que l'application

$$\xi : \begin{cases} x \mapsto (x \bmod p, x \bmod q) \\ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \end{cases}$$

est un morphisme de groupes additifs, dont le noyau est lié à la congruence simultanée ($x \equiv 0 \bmod p$, $x \equiv 0 \bmod q$), ayant pour unique solution 0 modulo n puisque p et q sont premiers entre eux. L'injectivité de ξ, jointe à l'observation des cardinaux des deux ensembles, assure sa bijectivité. □

Il est cependant utile de savoir résoudre de manière effective la congruence simultanée (2). On se base pour cela sur la relation de Bézout, c'est-à-dire sur l'existence de deux entiers u et v tels que $up + vq = 1$; le nombre $x = bup + avq$ satisfait alors (2) car $x \equiv avq = a(1 - up) \equiv a \bmod p$, et de même pour q. Il suffit alors de réduire x modulo n pour avoir la « bonne » réponse.

Dans le cas particulier étudié dans l'exercice, la congruence $(x+23)^2 \equiv 4 \bmod 33$ devient équivalente à

$$(3) \quad \begin{cases} (x + 23)^2 \equiv 4 \bmod 3 & \Leftrightarrow (x - 1)^2 \equiv 1 \bmod 3 & \Leftrightarrow x \in \{0, 2\} \bmod 3 \\ (x + 23)^2 \equiv 4 \bmod 11 & \Leftrightarrow (x + 1)^2 \equiv 4 \bmod 11 & \Leftrightarrow x \in \{1, 8\} \bmod 11 \end{cases}$$

(les équivalences situées les plus à droite peuvent être trouvées directement mais reposent aussi sur l'identité remarquable $a^2 - b^2 = (a + b)(a - b)$ dans les corps $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/11\mathbb{Z}$).

On parvient ainsi à quatre congruences simultanées. L'une d'entre elles, par exemple, s'écrit

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 8 \bmod 11 \end{cases}$$

et admet comme solution, grâce au choix de $u = 4$, $v = -1$ dans la relation de Bézout : $x = 8 \times 4 \times 3 - 2 \times 1 \times 11 = 74 \equiv 8 \bmod 33$. Les autres cas se traitent de même et conduisent aux quatre solutions 8, 12, 23 ou 30 modulo 33. Notons déjà que la réponse 30 ne convenait pas pour être le codage d'une lettre comprise entre 0 et 25.

3 L'équation du second degré dans certains anneaux

Le problème du déchiffrement revient donc à résoudre une équation du second degré, de la forme :

$$(4) \quad x^2 + Bx - y = 0,\ (x, y, B) \in (\mathbb{Z}/n\mathbb{Z})^3$$

La résolution de ces équations est enseignée dans certaines classes du lycée, sur le corps des réels et parfois des nombres complexes, mais qu'en est-il lorsque les coefficients et l'inconnue sont dans d'autres ensembles de nombres ? De fait, quand on songe à la formule qui exprime les racines éventuelles de l'équation, il est manifeste que cette formule peut buter sur l'inexistence de racines dans l'ensemble de nombres considéré, voire sur la non-inversibilité du « nombre » 2.

Considérons donc l'équation (4) dans un anneau commutatif K, et posons $\Delta = B^2 + 4y$. Si l'équation a une racine x dans K, alors $\Delta = 4x^2 + 4Bx + B^2 = (2x + B)^2$, et Δ est un carré d'un élément de K ; en contraposant, on voit que si Δ n'est pas un carré dans K alors (4) n'a pas de solution. C'est ce qui se produit, par exemple, pour la résolution de $x^2 - x - 1 = 0$ dans le corps des rationnels $\mathbb{Q}$, butant sur le fait que $\sqrt{5}$ est un nombre irrationnel [4].

Si au contraire Δ est un carré dans K, on peut poser $\Delta = \delta^2$ et tenter de chercher une racine de la forme $x = s(-B + \delta)$: on calcule un peu

$$\begin{aligned} x^2 + Bx - y &= s^2B^2 + s^2\Delta - 2Bs^2\delta - sB^2 + sB\delta - y \\ &= (2s - 1)\left[sB(B - \delta) + y(2s + 1)\right] \end{aligned}$$

et on voit qu'un « bon choix » serait d'annuler $2s - 1$. Si 2 est inversible dans K, les deux racines usuelles apparaissent ; dans le cas contraire, l'équation peut ne pas avoir de solution comme cela se produit avec $x^2 + x + 1 = 0$ dans $\mathbb{Z}/2\mathbb{Z}$ [5]. Il est donc difficile d'être plus précis sans en savoir plus sur K.

Dans la situation présente, nous avons $K = \mathbb{Z}/n\mathbb{Z}$ avec $n = pq$, p et q premiers impairs et distincts, ce qui nous permet d'aller plus loin, déjà par le fait que 2 est inversible modulo n [6]. En posant $B = 2b$ et $z = b^2 + y$ (discriminant réduit) pour simplifier, l'équation se réécrit sous la forme :

$$(4') \quad x^2 + 2bx - y \equiv 0 \bmod n \Leftrightarrow (x + b)^2 \equiv z \bmod n$$

Le théorème « chinois » nous ramène alors à un système de deux équations du second degré :

$$(5) \quad \begin{cases} (x + b)^2 & \equiv & z \bmod p \\ (x + b)^2 & \equiv & z \bmod q \end{cases}$$

Si z est un carré modulo p et modulo q, on peut continuer ; autrement, il n'y a pas de solution. Posons donc $z \equiv r^2 \bmod p$ et $z \equiv s^2 \bmod q$. Comme $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ sont des corps (p et q étant premiers), on peut appliquer le mécanisme usuel :

$$u^2 = v^2 \Leftrightarrow (u - v)(u + v) = 0 \Leftrightarrow u = \pm v$$

Le système (5) conduit ainsi à

$$(6) \quad \begin{cases} x + b \equiv \pm r \bmod p & \Leftrightarrow x \equiv -b \pm r \bmod p \\ x + b \equiv \pm s \bmod q & \Leftrightarrow x \equiv -b \pm s \bmod q \end{cases}$$

4. Une autre (et jolie) façon de le voir est d'imaginer une solution rationnelle $\frac{p}{q}$ (fraction irréductible), amenant une équation $p^2 - pq = q^2$; cette équation n'a pas de solutions entières parce que q devrait diviser $p(p - q)$ donc aussi $p - q$ puisque p et q sont premiers entre eux, ce qui est de toutes façons contradictoire.

5. Bien que le discriminant soit ici un carré, l'équation n'a pas de solution à cause de la non-inversibilité de 2.

6. Son inverse est $\frac{n+1}{2}$.

soit en général 4 solutions d'après le théorème « chinois », avec des cas particuliers lorsque r ou s est nul, soit quand le discriminant est nul modulo p ou q. Si z est nul modulo p et q, donc modulo n, l'équation (4') a pour unique solution $x = -b$. En fin de compte, l'équation (4) admet 0, 1, 2 ou 4 solutions [7].

4 À la conquête des racines

Le chiffrement de Rabin amène donc à s'interroger sur les carrés (et les racines) dans $\mathbb{Z}/n\mathbb{Z}$ (toujours avec $n = pq$, p et q premiers impairs distincts). Comme on vient de le voir, une classe résiduelle z de $\mathbb{Z}/n\mathbb{Z}$ peut admettre 1, 2, 4 ou 0 racines selon que z mod p (respectivement, z mod q) est nul, ou carré non nul, ou non carré dans $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Z}/q\mathbb{Z}$). Nous allons donc chercher à comprendre davantage comment sont faits les carrés dans $\mathbb{Z}/p\mathbb{Z}$, généralement appelés « résidus quadratiques ». [8] Dans la suite de cette partie, nous ne considérerons que des classes résiduelles de $\mathbb{Z}/p\mathbb{Z}$ (p premier impair), les égalités étant toutes à comprendre avec un modulo p sous-entendu.

En premier lieu, nous avons deux carrés très évidents qui sont $0^2 = 0$ et $1^2 = 1$. Pour aller plus loin, considérons le groupe multiplicatif $G = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ et examinons un peu la fonction « carré », définie sur G par $f(x) = x^2 \bmod p$; f est un morphisme de $(G, \cdot)$ dans lui-même (car $(a \cdot b)^2 = a^2 \cdot b^2$). De plus, si on a $x \neq y$ et $f(x) = f(y)$ alors $x^2 - y^2 = (x - y)(x + y) = 0$, d'où $x = -y$ puisque x et y sont distincts [9]. Les $p - 1$ antécédents par f étant ainsi groupés « deux par deux », on a exactement $\frac{p-1}{2}$ images (les carrés). Notons G^2 l'ensemble de ces carrés.

> Compléments sur G^2
> G^2 est un sous-groupe de G ayant des propriétés intéressantes : c'est un sous-groupe (propre) de G de cardinal maximal (le plus grand diviseur possible de $p - 1$ étant $\frac{p-1}{2}$). Notons aussi qu'il y a, dans G, autant de carrés que de non-carrés.

Nous avons aussi besoin d'un résultat « bien connu ».

Théorème 2 (« petit » théorème de Fermat)**.** *Soit p un nombre premier impair, et x un nombre entier. On a alors $x^p \equiv x \bmod p$; si x n'est pas divisible par p, on a aussi $x^{p-1} \equiv 1 \bmod p$.*

Caractériser les carrés de $\mathbb{Z}/p\mathbb{Z}$ peut se faire de diverses manières. La plus simple consiste à appliquer une puissance :

Théorème 3 (Leonhard Euler)**.** *Soit p un nombre premier impair, et $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$. Alors a est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si*

$$a^{\frac{p-1}{2}} = 1 \tag{7}$$

> Démonstration du théorème
> Cette démonstration est simple et jolie. Si $a = x^2$ (dans $\mathbb{Z}/p\mathbb{Z}$ il va de soi), alors $a^{\frac{p-1}{2}} = x^{p-1} = 1$ en raison du petit théorème de Fermat (a étant est supposé non-nul, $x = a^2$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ et on peut bien diviser par x). Nous savons ainsi que tout carré non nul de $\mathbb{Z}/p\mathbb{Z}$ est racine du polynôme $X^{\frac{p-1}{2}} - 1$; comme il y a exactement $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$, ce polynôme ne peut avoir d'autres racines (à cause de son degré) ; c'est pourquoi toute solution a de (7) est nécessairement un carré, ce qu'il fallait démontrer. □

7. Un intéressant exercice d'arithmétique consiste à étudier le même problème dans $\mathbb{Z}/2p\mathbb{Z}$ ou encore dans $\mathbb{Z}/p^2\mathbb{Z}$ (avec p impair).
8. Le lecteur pourra trouver un exposé assez complet sur les résidus quadratiques dans le cours de Gilles Bailly-Maitre [5], au chapitre 4.
9. On a bien $y \neq -y$ parce que p n'est pas égal à 2.

Le mathématicien Adrien-Marie Legendre [10] a introduit un nouvel outil pour étudier cette question des résidus quadratiques (voir aussi [7]) :

Définition 1 (symbole de Legendre)**.** *Pour tout nombre premier p, et tout entier a, on pose*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si \quad p \mid a \\ 1 & si \quad a \text{ est un carré modulo } p, \text{ et } p \nmid a \\ -1 & sinon \end{cases}$$

Proposition 1. *Pour tout nombre premier impair p, et tout entier a, on a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.*

Ce résultat est déjà démontré lorsque a est nul (modulo p) ou est carré (théorème d'Euler). Dans le cas contraire, la puissance ne peut pas être égale à 1, elle est donc égale à -1 puisque $a^{p-1} = 1$. □

Le symbole de Legendre peut être compris comme l'application $a \mapsto \left(\frac{a}{p}\right)$, allant de G dans $\{1, -1\}$, et morphisme de groupes multiplicatifs comme toute fonction « puissance ».

Le mathématicien, physicien et astronome Carl Friedrich Gauss s'est aussi intéressé à ce problème, en y apportant un théorème très célèbre (qu'il démontra de plusieurs manières, et que nous admettrons, voir par exemple [8]) :

Théorème 4 (loi de réciprocité quadratique)**.** *Soient p et q deux nombres premiers impairs et distincts. On a alors : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.*

Munis de ce résultat, nous pouvons aisément calculer le symbole de Legendre sous réserve de savoir factoriser a. [11] Un exemple : soit à calculer $\left(\frac{99}{103}\right)$. Il vient :

$$\left(\frac{99}{103}\right) = \left(\frac{3}{103}\right)^2 \cdot \left(\frac{11}{103}\right) = 1 \cdot (-1)^{5\times 51}\left(\frac{103}{11}\right) = -\left(\frac{4}{11}\right) = -1$$

(4 est le carré de 2, et cela reste vrai modulo 11).

Maintenant que nous savons détecter les carrés, il reste à savoir calculer les racines. Nous ne le ferons que dans le cas le plus favorable, celui où p est congru à 3 modulo 4.

Proposition 2. *Soit un nombre premier p congru à 3 modulo 4, et a un carré modulo p. Alors $a^{\frac{p+1}{4}}$ est une racine carrée de a modulo p.*

Cette proposition est très simple, car il suffit d'élever au carré :

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} = a$$

d'après le théorème d'Euler. L'hypothèse sert uniquement pour assurer que $\frac{p+1}{4}$ est un nombre entier. □

Les nombres premiers congrus à 3 modulo 4 sont heureusement nombreux, il n'y a donc pas de difficulté pour en trouver d'assez grands (c'est notamment le cas des nombres de Mersenne, de la forme $2^m - 1$, m étant premier).

5 Considérations pratiques

Dans l'usage réel des cryptosystèmes asymétriques, les calculs se font sur des entiers de très grande taille, ce qui est évidemment coûteux en temps de calcul et peut nécessiter des algorithmes spécifiques,

10. Il vécut entre 1752 et 1833. Voir aussi un article d'Image des maths que Michèle Audin et Jean-Pierre Kahane lui ont consacré.

11. En l'absence d'une telle factorisation, et si a est très grand, il vaut mieux utiliser le théorème d'Euler.

notamment pour proposer deux grands nombres premiers et obtenir les termes de la relation de Bézout entre ceux-ci. Dans la même veine, le calcul des puissances se fait grâce à l'algorithme d'exponentiation rapide, qui gagne énormément d'opérations par rapport au produit « simple » (voir par exemple sur Wikipedia en français ou en anglais, plus complet).

6 Peut-on réellement décoder ?

Le déchiffrement du code de Rabin peut ainsi aboutir à quatre réponses possibles pour chaque nombre transmis. Dans l'exemple proposé dans le sujet de Pondichéry 2018, on aboutissait théoriquement à quatre solutions (8, 12, 23 ou 30 modulo 33) ; en tenant compte du fait que la solution 30 ne convient pas pour une lettre codée entre 0 et 25, l'ambiguïté se concentrait entre trois réponses.

Nous pouvons cependant reprendre l'exemple avec des valeurs plus grandes de p et q, comme $p = 19$ et $q = 23$, d'où $n = 437$; cela revient à agrandir l'espace de représentation au prix d'une moindre compacité du codage. Choisissons aussi $B = 100$. Si Bob souhaite envoyer la lettre « C », il choisit le nombre $x = 2$ en tant que message clair, et calcule donc $y = x(x+B) = 204$ qu'il envoie comme message chiffré à Alice. Celle-ci reformule le problème en termes de carrés : $(x + 50)^2 = 204 + 50^2 = 2704 \equiv 82 \bmod 437$. Comme elle connaît la factorisation de n, elle transforme cette congruence en deux congruences plus simples :

$$\begin{cases} (x+50)^2 \equiv 82 \bmod 19 & \Leftrightarrow (x-7)^2 \equiv 6 \bmod 19 \equiv 25 \bmod 19 \\ (x+50)^2 \equiv 82 \bmod 23 & \Leftrightarrow (x+4)^2 \equiv 13 \bmod 23 \equiv 36 \bmod 23 \end{cases}$$

soit :

$$\begin{cases} (x+50)^2 \equiv 82 \bmod 19 & \Leftrightarrow x \in \{2, 12\} \bmod 19 \\ (x+50)^2 \equiv 82 \bmod 23 & \Leftrightarrow x \in \{2, 13\} \bmod 23 \end{cases}$$

Les 4 solutions cherchées sont donc décrites par les congruences suivantes :

$$\begin{cases} x \equiv 2 \bmod 19 \\ x \equiv 2 \bmod 23 \end{cases}, \begin{cases} x \equiv 12 \bmod 19 \\ x \equiv 2 \bmod 23 \end{cases}, \begin{cases} x \equiv 2 \bmod 19 \\ x \equiv 13 \bmod 23 \end{cases}, \begin{cases} x \equiv 12 \bmod 19 \\ x \equiv 13 \bmod 23 \end{cases}$$

On les résout comme précédemment, trouvant les solutions (modulo 437) :

$$x \in \{2,\ 278,\ 59,\ 335\}$$

Seule la première solution convient (comme codage d'une lettre, compris entre 0 et 25) ; c'est ainsi que l'ambiguïté peut être (théoriquement) traitée et le message clair bien déterminé.

En pratique, les caractères du flux d'entrée sont combinés entre eux puis recodés sous la forme d'un (grand) entier compris entre 0 et $n - 1$ (tout se faisant en binaire) ; et on ajoute un certain nombre de bits « de contrôle » pour lever l'ambiguïté (ce qui revient à faire usage d'un code correcteur d'erreurs).

Références

[1] G. Tenenbaum et M. Mendès France, *Les nombres premiers*, ser. Que sais-je ? PUF, 1997. 1

[2] G. Tenenbaum et M. Mendès-France, *Les nombres premiers : entre l'ordre et le chaos*, 2nd ed., ser. UniverSciences (Paris). Dunod, 2014, http://www.iecl.univ-lorraine.fr/~Gerald.Tenenbaum/LNP-D/indexLNP.html. 1

[3] M. O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, *MIT Laboratory for Computer Science, MIT/LCS/TR-212*, janvier 1979, http://www.dtic.mil/dtic/tr/fulltext/u2/a078415.pdf. 1

[4] S. Singh, *L'Histoire des codes secrets*. J.-C. Lattès, 1999, trad. Catherine Coqueret. 1

[5] G. Bailly-Maitre, *Cours de théorie des nombres et Cryptologie*, 2005, http://perso.univ-lr.fr/gbailly/cours.html. 1, 4

[6] D. Daumas, M. Guillemot, O. Keller, R. Mizrahi, et M. Spiesser, Le théorème des restes chinois, *CultureMath*, juin 2011, http://culturemath.ens.fr/content/le-th%C3%A9or%C3%A8me-des-restes-chinois. 2

[7] Legendre symbol, https://en.wikipedia.org/wiki/Legendre_symbol. 5

[8] J.-P. Serre, *Cours d'arithmétique*. PUF, 1995, https://www.puf.com/content/Cours_darithm%C3%A9tique. 5