Si $x = x_1x_2\ldots x_{10}$ est un élément de E, on calcule à partir de x une clé $K(x) = x_{11}x_{12}$ formée de 2 chiffres décimaux. Notons f l'application de E dans F qui à x associe $f(x) = x_1x_2\ldots x_{10}x_{11}x_{12}$ et $C = f(E)$ l'image de E.

b) Quel est le nombre d'éléments de C ?

Si y est un élément de C, on note B_y l'ensemble formé de y ainsi que de tous les éléments obtenus à partir de y en modifiant un (et un seul) chiffre de y.

c) Quel est le nombre d'éléments de B_y ? Montrer qu'il existe au moins deux éléments distincts z_1, z_2 dans C tels que $B_{z_1} \cap B_{z_2} \neq \varnothing$.

Si $t \in B_{z_1} \cap B_{z_2}$, il est impossible de savoir si t provient d'une erreur faite sur z_1 ou d'une erreur faite sur z_2. Cette obstruction montre qu'on ne peut pas réaliser un code correcteur du type de l'exemple précédent avec uniquement des digits décimaux. En essayant de faire ce même calcul sur l'exemple précédent (avec 11 digits), on verra évidemment que cette obstruction n'a pas lieu, mais que « ça passe juste » (pour simplifier un peu le calcul on supposera que pour **toutes** les positions et pas seulement pour la clé, les chiffres peuvent prendre les 11 valeurs 0, 1, …, 9, X).

5. Cryptographie

5.1. Le petit théorème de Fermat

1) Soit p un nombre premier. Montrer que si $1 \leq k \leq p-1$, alors :

$$C_p^k \equiv 0 \quad (p),$$

où les C_p^k sont les coefficients binomiaux.

2) Montrer que $(1+1)^p \equiv 1 + 1\ (p)$. Puis par récurrence trouver une expression de $(1 + 1 + \ldots + 1)^p$. En conclure que pour tout entier a,

$$a^p \equiv a \quad (p)$$

(on pourra distinguer les cas $a = 0$, $a > 0$, $a < 0$).

3) En conclure que si a est premier avec p, alors (petit théorème de Fermat) :

$$a^{p-1} \equiv 1 \quad (p).$$

4) Soit $n = pq$ où p et q sont deux nombres premiers.
Supposons tout d'abord a premier avec n. Montrer que

$$(a^{p-1})^{q-1} \equiv 1 \quad (p),$$

et que

$$(a^{p-1})^{q-1} \equiv 1 \quad (q).$$

En conclure que pour tout $k \geq 0$

$$a^{k(p-1)(q-1)} \equiv 1 \quad (n).$$

Supposons maintenant que $a = lp$ avec $0 < l < q$. Montrer que

$$a^{k(p-1)(q-1)+1} \equiv a \quad (p),$$

et que

$$a^{k(p-1)(q-1)+1} \equiv a \quad (q).$$

En conclure que pour tout k

$$a^{k(p-1)(q-1)} \equiv 1 \quad (n).$$

Montrer que dans tous les cas, pour tout a et tout k on a

$$a^{k(p-1)(q-1)+1} \equiv a \quad (n).$$

5.2. Principe du chiffrement de Rivest, Shamir et Adleman (RSA)

Le chiffrement RSA est certainement le plus connu et le plus utilisé des chiffrements à clé publique. Dans un chiffrement à clé publique, chaque participant X possède une clé publique e_X connue de tous, et une clé privée d_X qu'il ne communique à personne. Si un autre participant veut envoyer un message m à X, il calcule $c = e_X(m)$ (message chiffré grâce à la clé publique de X), et transmet c à X. X peut retrouver m grâce à sa clé privée en calculant $d_X(c)$ qui, par construction des paires de clés publiques-clés privées, redonne m. L'avantage d'un tel système non symétrique (clé de déchiffrement différente de la clé de chiffrement et **incalculable** à partir de celle-ci) est d'éviter d'avoir à échanger avec son correspondant une clé secrète. Le problème bien sûr est de trouver un moyen de réaliser concrètement un tel système. Le système RSA répond à la question.

Alice choisit deux grands nombres premiers p et q, calcule $n = pq$ ainsi que $(p-1)(q-1)$. Elle choisit un nombre e premier avec $(p-1)(q-1)$ et calcule d et k tels que $ed = k(p-1)(q-1) + 1$. Comment peut-elle mener ce calcul ? Remarque : elle peut trouver un k tel que $0 < k < e$ (pourquoi ?).

Elle rend publics les nombres n et e (c'est sa clé publique) mais pas p, ni q, ni sa clé privée d.

Bob qui veut envoyer à Alice un message numérisé en un nombre $0 \leq x < n$ (si le message est trop long il le découpe en blocs) utilise la clé publique d'Alice pour calculer $y = x^e \bmod n$. Il transmet y à Alice. Alice peut retrouver x grâce à sa clé privée d en calculant $y^d \bmod n$ (montrer qu'on a bien $x = y^d \bmod n$).

On ne sait pas reconstituer la clé privée d d'Alice à partir de sa clé publique (n,e). Bien sûr si on connaissait la décomposition de n en facteurs premiers on pourrait retrouver d en faisant le même calcul que celui qu'a fait Alice pour construire sa paire de clés. La sécurité du système repose sur la difficulté de retrouver p et q connaissant n.

Exemple (non réaliste à cause des nombres minuscules utilisés) :

Alice choisit $p = 263$, $q = 419$. On vérifiera que ces nombres sont premiers. Elle calcule $n = pq$ et $f = (p - 1)(q - 1)$. Constater que f n'est pas divisible par 3. Alice choisit alors $e = 3$. Ainsi sa clé publique est (n,e). On cherche alors d et k tels que

$$3d = kf + 1.$$

Montrer qu'il y a nécessairement une solution avec $k = 1$ ou avec $k = 2$ (revoir le paragraphe 3.1.2 et en particulier la remarque).
Trouver d.

Bob qui dispose de la clé publique d'Alice veut lui envoyer le message $x = 187$. Quel message chiffré lui envoie-t-il ?

Que fait Alice pour retrouver le message clair ? Faire le calcul.

Bibliographie

[1] T.M. Apostol, *Introduction to analytic number theory*. Springer-Verlag, 1976.

[2] L. Chambadal, *Calcul pratique*. Hachette, 1983.

[3] COMAP, *Principles and practice of Mathematics*. Springer-Verlag, 1997.

[4] M. Demazure, *Cours d'algèbre*. Cassini, 1997.

[5] Groupe de travail sur la liaison Lycées-Universités, *Cours et activités en arithmétique pour les classes terminales (2e Éd.)*. IREM de Marseille, 1999.

[6] IREM de Clermont, *Arithmétique en terminale S, enseignement de spécialité*. CRDP de Clermont.

[7] R. Kumanduri, C. Romero, *Number theory with computer applications*. Prentice Hall, 1998.

[8] M. Mignotte, *Mathématiques pour le calcul formel*. Puf, 1989.

L'ARITHMÉTIQUE DANS LES BULLETINS VERTS LES PLUS RÉCENTS

(en tête, numéro du Bulletin en gras, puis pages entre parenthèses)

428 (372-376) *Autour des méthodes de fausse position*, par A. Gazagnes.

(387-389) *Des baguettes pour compter*, par A. Laurent

427 (209-210) *Sur le caractère spectaculaire du théorème de Fermat-Wiles*, par J.-B. Hiriart-Urruty.

(211-214) *De Léonard de Pise à Hilbert : un entier comme somme de deux carrés*, par R. Vidal.

(suite page 99)

La division simple à l'aide de l'abaque de Gerbert(*)

D'après Bernelin (élève de Gerbert d'Aurillac) Libre d'Abaque
trad. Bakkouche, B., CIHSO, Toulouse, 1999, p. 35-37(**)

Michel Guillemot

On appelle « simple » la division dont nous nous apprêtons à parler maintenant, parce qu'on propose un diviseur à un chiffre, mais qu'on place au-dessus un dividende à un ou plusieurs chiffres. Divisons donc 668 par le diviseur 6 de la façon suivante : plaçons dans le premier tracé de l'unité le diviseur 6 et au-dessous de lui la différence 4, pour qu'ils arrivent au total de 10 ; plaçons un 6 du dividende dans le second tracé des centaines, l'autre dans le second aussi des dizaines, et 8 dans le second des unités. Au-dessous d'eux, plaçons ces mêmes nombres aussi dans le troisième tracé, selon la première façon, pour que ces nombres étant pris pour la dénomination et les premiers d'entre eux restant à leur place, on puisse plus facilement retenir quel nombre est proposé pour dividende.

Il s'agit de diviser 668 par 6. Pour des raisons typographiques, nous limitons l'abaque à un damier comportant trois colonnes et quatre rangées.

		6 4
6	6	8
6	6	8

diviseur
différence : $10 - 6 = 4$
dividende
dividende

Puisque donc le diviseur, ajouté à la différence, atteint la seconde colonne, c'est à dire les dizaines, y occupant la place de la première unité, prends le nombre 6 en entier du troisième tracé des centaines et place-le en seconde position pour la dénomination totale dans le quatrième tracé des dizaines.

		6 4
6	6	8
	6	8
	6	

quotient partiel q_1 (dénomination)

on obtient un premier quotient partiel : 60

$$\frac{668}{6} > \frac{600}{10} = 60$$

(*) Cf. Article sur Gerbert, Bulletin n° 431, pages 831-832.
(**) En vente à la Régionale APMEP de Toulouse, 200 F avec port.

Multiplie par ce nombre la différence du diviseur de cette façon : 6 fois 4, 24, c'est-à-dire 2 dans le troisième tracé des centaines, mais 4 dans le même des dizaines [...]

		6 4
6	6	8
2	6 **4**	8
	6	

$4q_1 = 4 \times 6 = 24$

$$\frac{668}{6} = 60 + \frac{68}{6} + \frac{240}{6}$$

De nouveau, prends le 2 des centaines et, comme auparavant, place-le pour en faire la dénomination ; multiplie-le par la différence du diviseur de cette façon 2 fois 4, 8 avec les autres dans le troisième des dizaines.

		6 4
6	6	8
	6 4 **8**	8
	6 **2**	

d
$r = 10 - d$

D

de manière générale

(1) $\dfrac{\mathrm{D}}{d} = \dfrac{a \cdot 10^{n+1} + b}{d} = a \cdot 10^n + \dfrac{ar + b}{d}$

Si tu les additionnes, c'est-à-dire 6, 4 et 8, tu auras un nombre qui compte 18 unités, c'est-à-dire 1 dans le troisième tracé des centaines, mais 8 dans le troisième tracé des dizaines.

		6 4
6	6	8
1	**8**	8
	6 2	

De même, prends l'unité des centaines et place-la aussi, de la façon précédente, en seconde position pour en faire la dénomination ; multiplie-la par la différence du diviseur de cette façon : une fois 4, 4, dans le troisième tracé des dizaines.

		6 4
6	6	8
	8 **4**	8
	6 2 **1**	

d'après (1)

ar

$a \cdot 10^n$

Si tu additionnes ce nombre au 8 restant, tu obtiendras le nombre 12, c'est à dire 1 dans le troisième nombre des centaines et 2 dans le troisième aussi des dizaines.

		6 4
6	6	8
1	**2**	8
	6 2 1	

Encore une fois, prend le 1 des centaines et place-le pour la dénomination ; multiplie-le par la différence du diviseur, de cette façon : 1 fois 4, 4, dans le troisième des dizaines.

		6 4	d'après (1)
6	6	8	
	2 **4**	8	*ar*
	6 2 1 **1**		$a \cdot 10^n$

Si tu additionnes ce chiffre au 2 restant, tu auras le nombre 6 dans le troisième aussi.

		6 4
6	6	8
	6	8
	6 2 1 1	

Prends donc de même ce nombre de sa place, et place-le en seconde position, dans le quatrième tracé de l'unité, pour la dénomination, multiplie-le par la différence du diviseur de cette façon : 6 fois 4, 24, c'est-à-dire 2 dans le troisième des dizaines, 4 dans le même des unités [...]

		6 4	d'après (1)
6	6	8	
	2	8 **4**	*ar*
	6 2 1 1	**6**	$a \cdot 10^n$

De même prends le 2 des dizaines et place-le en seconde position pour la dénomination : multiplie par la différence du diviseur de cette façon : 2 fois 4, 8, dans la troisième des unités.

		6 4
6	6	8
		8 4 **8**
	6 2 1 1	6 **2**

d'après (1)

ar

$a \cdot 10^n$

Si tu l'additionnes aux deux nombres restants, c'est-à-dire 8 et 4, tu auras 20, c'est-à-dire 2 dans le troisième tracé des dizaines.

		6 4
6	6	8
	2	
	6 2 1 1	6 2

il n'y a pas de signe numérique pour 0 : c'est le vide

Prends-le de sa place, place-le en seconde position, comme précédemment, pour la dénomination ; multiplie-le par la différence du diviseur de cette façon : 2 fois 4, 8, dans le troisième des unités.

		6 4
6	6	8
		8
	6 2 1 1	6 2 **2**

d'après (1)

ar

$a \cdot 10^n$

Parce que donc tu ne peux continuer à placer en seconde position, sans plus t'occuper de la différence, compare le diviseur au dividende pour savoir lequel des deux – du diviseur ou du dividende – est considéré comme le plus grand. Mais le dividende est supérieur au diviseur de 2 ; il te reste donc, des nombres additionnés auparavant, à accorder aux dénominations le 1 des unités et à replacer le reste des dividendes, 2 dans le troisième tracé des unités aussi.

		6 4
6	6	8
		2
	6 2 1 1	6 2 2 **1**

$b - d$

(2) $\frac{b}{d} = 1 + \frac{b-d}{d}$ si $b > d$

Cela fait, il faut voir la valeur à laquelle arrivent les dénominations ajoutées ensemble, de façon à conclure que c'est par leur quantité que le diviseur divise les dividendes. De fait, si tu ajoutes les 6 et deux 2 à 1, tu auras un 1 avec les autres dénominations des dizaines et tu placeras l'autre dans le même tracé des unités.

		6 4
6	6	8
		2
	6 2 1 **1**	**1**

		6 4
6	6	8
		2
	6 2 1 **1**	1

Si tu ajoutes 6, 2 et deux 1 à l'unité restante, tu placeras un 1 dans le quatrième des centaines, tu ramèneras l'autre dans la quatrième aussi des dizaines. Concluons donc que 668 est divisé cent onze fois par le diviseur 6, reste 2 précisément.
Remarque. Ici, Bernelin joue habilement en déplaçant un jeton marqué 1.

		6 4	diviseur différence : $10 - 6 = 4$
6	6	8	dividende
		2	reste de la division
1	**1**	1	quotient

$668 = 6 \times 111 + 2$

L'ARITHMÉTIQUE DANS LES BULLETINS VERTS LES PLUS RÉCENTS

(suite de la page 94)

426 (78-88) *Les critères de divisibilité en Inde*, par C. Morice-Singh.

421 (219-232) *Codage et cryptage*, par D.-J. Mercier.

417 (459-463) *Le carré de tout nombre premier (sauf 2 et 5) est somme de 3 carrés non nuls*, par J.-P. Brévan.

408 (568-581) *Cryptographie classique et cryptographie publique à clé révélée*, par D.-J. Mercier.

403 (173-182) *Pell-Fermat toujours d'actualité*, par Ch. Jeanbreau et Ch. Notari.

398-399 (531-550 et 675-685) *Commentaires des histoires de numérations du Ifrah*.

- De plus, signalons dans le **415** (173-192), *L'algèbre et la correction des erreurs*, par D.-J. Mercier