Table des matières

Bulletin AMQ Vol. XLV, n° 3, octobre 2005

Membres du comité de rédaction

Éditorial

Jean-Marie De Koninck
président

En ce début d'automne, nous voilà tous replongés dans la routine de nos activités académiques, la plupart d'entre nous comme enseignants ou comme étudiants. C'est alors qu'il fait bon de se ressourcer et de se divertir "mathématiquement" en parcourant le nouveau Bulletin de l'AMQ. On y trouve, entre autres, un article de Christiane Rousseau sur la cryptographie à clé publique, une entrevue de Bernard Courteau avec Yves Langlois, un article d'André Ross sur la cartographie terrestre et céleste ; et enfin, Robert Bilinski nous parle de livres qu'il a lus dernièrement.

Dans quelques jours débute au Collège Brébeuf le 48^{e} colloque de l'AMQ. La qualité du programme est déjà un gage de son succès. Le Congrès sera également l'occasion d'échanger et de discuter à la fois de mathématiques et de l'avenir de notre Association. Justement, où en est donc celle-ci ? L'an dernier, par manque de ressources financières, l'AMQ a dû temporairement abandonner la version papier de son Bulletin et le mettre en ligne. Néanmoins, le Bulletin sera en version papier pour le numéro du mois de décembre. Pour les numéros qui suivront, ce n'est pas certain.Toutefois, nous serions assurés de pouvoir revenir à une version papier pour chacun des numéros si le membership de l'Association revenait à ce qu'il était dans les bonnes années, et cela pour le grand bonheur de tous ses membres ! C'est pourquoi, une invitation à joindre l'AMQ a été envoyée à des centaines de professeurs des différents niveaux d'enseignement. Mais le contact personnel demeure encore la façon la plus sûre d'influencer quelqu'un. Donc, concrètement, l'idéal serait que chacun des membres actuels fasse un petit effort pour recruter un ou deux nouveaux membres. C'est pourquoi, lors du Congrès du 15 octobre, des formulaires d'abonnement seront disponibles pour ceux et celles qui ont des contacts et qui se sentent capables d'influencer leurs collègues et leurs amis. Autant de petits gestes isolés qui, additionnés, pourraient relancer le membership de l'AMQ et par le fait même assurer sa santé.

AMQ en action

Quelques nouvelles

Le Show Math au Cégep de Sainte-Foy : Une sortie scolaire à ne pas manquer !

Le *Show Math*, une conférence unique de Jean-Marie De Koninck, célèbre professeur au Département de mathématiques et de statistiques de l'Université Laval, fondateur d'*Opération Nez Rouge* et commentateur attitré des compétitions de natation à Radio-Canada, sera présenté **gratuitement à la Salle Albert-Rousseau du Cégep de Sainte-Foy, le 28 octobre à 10 h**, dans le cadre de IMAGINE ! L'événement de l'innovation.

Vous voulez savoir comment trouver la combinaison gagnante du prochain tirage de la Loto 6/49 ou encore, connaître les astuces de plusieurs tours de magie, ou savoir si votre meilleur ami a triché à pile ou face ? Le *Show Math* vous fera découvrir toutes ces réponses et vous convaincra de l'importance des mathématiques dans la vie de tous les jours.
Pour un avant-goût du spectacle, consultez le document vidéo à l'adresse suivante :

`www.cegep-ste-foy.qc.ca/csf/fileadmin/actualites/Videos/showmath-annonce-128.mpg` ou visitez le site : `http ://www.smac.ulaval.ca/showmath/`.

Une invitation du Cégep de Sainte-Foy, fier collaborateur de IMAGINE ! L'événement de l'innovation 27-30 octobre 2005 : `www.imagineinnovation.qc.ca`. Pour toute information, téléphonez à Mme Suzanne Bolduc : (418) 659-6600, poste 3727

Sources : Service des communications du Cégep de Sainte-Foy

Creuse tes méninges

Le Département de mathématiques de l'Université de Sherbrooke organise un concours intitulé **Creuse tes méninges - Défi mathématiques**. Ce concours s'adresse aux jeunes de l'ensemble du Québec qui étudient au cycle secondaire ou collégial. Le concours a le potentiel d'intéresser plus de jeunes aux sciences mathématiques. La date limite d'inscription pour avoir accès à la grande finale est le 15 novembre. Du matériel promotionnel sera présenté au congrès de l'AMQ au Collège Brébeuf.
Vous trouverez tous les renseignements nécessaires à l'adresse suivante :

`http ://www.usherbrooke.ca/jeveux/creuse_maths/index.html`

EMF 2006

Le colloque EMF 2006 aura lieu à l'Université de Sherbrooke du samedi 27 mai (accueil et inscription le vendredi 26 mai) au mercredi 31 mai 2006, avec pour thème central : « *L'enseignement des mathématiques face aux défis de l'école et des communautés* ».

EMF 2006 est organisé en collaboration avec l'Association Mathématique du Québec (AMQ), le Groupe des Responsables en Mathématiques au secondaire (GRMS) et le Groupe des didacticiens et didacticiennes des mathématiques du Québec (GDM).

Les colloques *Espace Mathématique Francophone* (EMF) visent à promouvoir réflexions et échanges au sein de la francophonie sur les de l'enseignement des mathématiques dans nos sociétés actuelles, aux niveaux primaire, secondaire et post-secondaire, ainsi que sur les questions touchant à la formation initiale et continue des enseignants.

Le colloque EMF 2006 sera suivi **du 49^{e} congrès de l'AMQ et du congrès du GRMS**, qui prendront place du mercredi 31 mai 2006 (inscription le mardi 30 mai au soir) au vendredi 2 juin 2006. Il est important de noter que le mercredi 31 mai sera une journée commune EMF, AMQ et GRMS.

Vous pourrez obtenir de plus amples informations en visitant le site EMF 2006 :

`http ://emf2006.educ.usherbrooke.ca/`

Décès de Guy-W Richard

Nous avons le regret de vous annoncer que Monsieur Guy-W. Richard est décédé à l'Hôpital Laval, le dimanche 2 octobre 2005, à l'âge de 71 ans. Guy-W Richard, époux de Cécile Roy, a été l'un des pionniers de l'AMQ, il a été l'un des trois demandeurs, avec Lucille Roy et Michel Girard, des lettres patentes qui ont constitué l'AMQ en corporation le 5 mai 1964. L'AMQ l'a nommé membre émérite en 1996. Nous offrons nos plus sincères condoléances à la famille Richard.

Fernand Beaudet
Pour le comité de rédaction

Les dessous de la cryptographie à clé publique

Christiane Rousseau
Université de Montréal

De tout temps l'homme a cherché des moyens de transmettre des messages secrets et a inventé des codes secrets de plus en plus sophistiqués. Historiquement on observe très souvent que les meilleurs codes secrets ont été percés par l'adversaire : ce fut le cas avec le code Enigma utilisé par les Allemands et décodé par les Alliés durant la dernière guerre mondiale. La cryptographie à clé publique, ou code RSA, a été introduite en 1978 [RSA] et est abondamment utilisée sur Internet. Le mode de fonctionnement du système est public. La renommée de ce code est si grande que tout chercheur qui réussirait à le briser obtiendrait une gloire immédiate. Pourtant ce système résiste encore depuis plus de 25 ans !

On commencera par expliquer ce système de cryptographie, basé sur la théorie des nombres, plus particulièrement l'arithmétique $(+, .)$ modulo n, et on montrera pourquoi il fonctionne : c'est la partie élémentaire. La clé du système RSA est un entier n qui est le produit de deux grands nombres premiers p et q. Pour briser le code, il suffit de factoriser n. Le code est encore inviolé parce que les meilleurs ordinateurs ne sont pas capables de factoriser de grands nombres entiers dans un temps raisonnable.

Par contre, il est facile de fabriquer une clé avec un ordinateur, c'est-à-dire de construire deux grands nombres premiers et de les multiplier. La naissance du système RSA a donné naissance à de nombreux algorithmes, surtout probabilistes, parfois déterministes, pour générer de grands nombres premiers et tenter de factoriser de grands nombres entiers. On parlera de ces algorithmes anciens et modernes permettant de construire une clé. Les chercheurs mettent donc toute leur énergie sur un algorithme qui permettrait de factoriser de grands nombres entiers en un temps raisonnable (les informaticiens diront en temps polynomial). Shor a publié en 1997 un tel algorithme mais sur un ordinateur quantique. L'ordinateur quantique n'est plus tout à fait une fiction : on a pu construire en 2003 un

ordinateur quantique factorisant le nombre 15. Comme on le voit, la recherche se poursuit sous nos yeux. On terminera par une brève introduction à l'algorithme de Shor.

Le code RSA est un système à clé publique. Ceci signifie que le fonctionnement du code et la clé sont publics ! Les avantages sont les suivants :

- Il n'y a plus de danger que le code soit connu : il est public ! C'est pourquoi c'est le seul type de code qui puisse fonctionner lorsqu'il y a des millions d'utilisateurs.
- Il est possible de « signer » un message de telle sorte qu'on soit sûr de sa provenance.

L'ingrédient de base est la théorie des nombres, plus particulièrement l'arithmétique $(+, .)$ modulo n. En particulier, on utilise le théorème de Fermat généralisé par Euler.

La méthode fonctionne parce que la théorie et la pratique sont très différentes en théorie des nombres :

- Il est difficile en pratique pour un ordinateur de factoriser un grand nombre ;
- Il est facile en pratique de construire de grands nombres premiers ;
- Il est facile en pratique de décider si un grand nombre est premier.

Définition 1 Soit a, b, n des entiers. On dit que « a est congru à b modulo n » si $n|(a-b)$, i.e. il existe un entier c tel que $a - b = cn$. On note $a \equiv b \pmod{n}$.

1 Le principe du code RSA [RSA] :

- On choisit p et q deux grands nombres premiers (plus de 100 chiffres).
- On calcule $n = pq$. Le nombre n, la "clé", a environ 200 chiffres ou plus. Il est public alors que p et q sont gardés secrets.
- On calcule $\varphi(n)$, où φ est la fonction d'Euler définie comme suit : $\varphi(n)$ est le nombre d'entiers premiers dans $E = \{1, 2, \ldots, n\}$ qui sont relativement premiers avec n. Alors $\varphi(n) = (p-1)(q-1)$.
- Calculer $\varphi(n)$ sans connaître p et q est aussi difficile que de factoriser n.
- On choisit $e \in E$ relativement premier avec $\varphi(n)$, i.e. (Le PGCD de e et $\varphi(n)$ est 1). e est la *clé de cryptage*. Elle est publique et sert à l'expéditeur pour encoder son message.

- Il existe $d \in \{1, \ldots, n\}$ tel que $ed \equiv 1 \pmod{\varphi(n)}$. L'existence de d découle de l'algorithme d'Euclide pour trouver le PGCD de e et $\varphi(n)$. d est la *clé de décryptage*. Elle est secrète et permet au receveur de décoder le message.
- L'expéditeur veut envoyer un message m qui est un nombre de $\{1, 2, \ldots, n\}$ relativement premier avec n.
- Il code $m^e \equiv a \pmod{n}$, i.e. $a \in \{1, \ldots, n\}$ et envoie a.
- Le receveur reçoit a. Pour décoder, il calcule $a^d \pmod{n}$. Le petit théorème de Fermat, généralisé par Euler, assure que $a^d \equiv m \pmod{n}$.

Nous allons montrer toutes les étapes ci-dessus qui requièrent une preuve. Nous aurons alors complètement montré que le code RSA fonctionne.

Proposition 1 *Si p et q sont deux nombres premiers distincts et $n = pq$, alors $\varphi(n) = (p-1)(q-1)$.*

Preuve Soit $F = \{1, 2, \ldots, n-1\}$. F contient $n-1$ éléments. Pour calculer $\varphi(n)$ on doit compter le nombre d'éléments qui restent dans F une fois qu'on a enlevé tous les nombres qui ne sont pas premiers avec n, soit tous les multiples de $p : p, 2p, \ldots (q-1)p$ et tous les multiples de $q : q, 2q, \ldots (p-1)q$. Il reste donc $(pq-1) - (q-1) - (p-1) = (p-1)(q-1)$ éléments. □

Proposition 2 *Si $e \in E = \{1, \ldots, n\}$ satisfait $(e, \varphi(n)) = 1$, alors il existe $d \in E$ tel que $ed \equiv 1 \ (mod\, \varphi(n))$.*

Preuve Puisque $(e, \varphi(n)) = 1$, alors par l'algorithme d'Euclide il existe deux entiers a et b tels que $1 = ae + b\varphi(n)$. Donc $ae \equiv 1 \pmod{\varphi(n)}$. Soit $d \in E$ le reste de la division de a par $\varphi(n)$ (ceci a du sens même si $a < 0$). Alors $a = q\varphi(n) + d$ avec $d \in E$. On en déduit que $ae \equiv de \equiv 1 \pmod{\varphi(n)}$. □

Théorème d'Euler : Si m est relativement premier avec n, alors $m^{\varphi(n)} \equiv 1 \pmod{n}$. (Fermat a prouvé le théorème quand n est premier.)

Preuve Soit $S = \{a \in N \mid a < n \text{ et } (a, n) = 1\}$. Alors S contient $\varphi(n)$ éléments : $S = \{a_1, \ldots, a_{\varphi(n)}\}$. Soit m tel que $(m, n) = 1$. Multiplions chaque a_i par m et soit b_i le reste de la division de $a_i m$ par n. Alors $a_i m \equiv b_i \pmod{n}$. Comme $(a_i, n) = 1$ et $(m, n) = 1$, alors $(b_i, n) = 1$. Donc $b_i \in S$. De plus, on peut montrer facilement (exercice) que $a_i \neq a_j$

implique que $b_i \neq b_j$. Donc les éléments $b_1, \ldots, b_{\varphi(n)}$ forment une permutation des éléments de S, ce qui implique que $S = \{b_1, \ldots, b_{\varphi(n)}\}$.
D'où

$$\prod_{i=1}^{\varphi(n)} a_i = \prod_{i=1}^{\varphi(n)} b_i.$$

Or $a_i m \equiv b_i \pmod{n}$. Donc $\prod_{i=1}^{\varphi(n)} b_i \equiv m^{\varphi(n)} \prod_{i=1}^{\varphi(n)} a_i \pmod{n}$. Ceci entraîne que n divise $(m^{\varphi(n)} - 1) \prod_{i=1}^{\varphi(n)} a_i$. Comme $(n, a_i) = 1$, alors n divise $m^{\varphi(n)} - 1$. □

Proposition 3 *Le procédé de décodage du code RSA fonctionne et permet de récupérer le message initial.*

Preuve Soit m le message qui est un nombre de $E = \{1, 2, \ldots, n\}$ relativement premier avec n. Pour coder le message, l'expéditeur calcule $a \in E$ tel que $m^e \equiv a \pmod{n}$. Le receveur calcule :

$$a^d \equiv (m^e)^d = m^{ed} = m^{b\varphi(n)+1} = m^{b\varphi(n)}.m = (m^{\varphi(n)})^b.m \equiv 1.m = m \pmod{n}.$$ □

Signature d'un message avec le code RSA : chacun publie sa clé n et sa clé e :

- expéditeur : n_A, e_A publiques, d_A secrète ;
- receveur : n_B, e_B publiques, d_B secrète.

L'expéditeur veut envoyer un message m relativement premier avec n_A et n_B. Il calcule : $m \mapsto m^{d_A} \equiv m_1 \pmod{n_A} \mapsto m_1^{e_B} \equiv m_2 \pmod{n_B}$.
Il envoie m_2.
Pour décoder le message, le receveur fait : $m_2 \mapsto m_2^{d_B} \equiv m_1 \pmod{n_B} \mapsto m_1^{e_A} \equiv m \pmod{n_A}$.

Exemple 1 (Nous avons utilisé Mathematica pour construire l'exemple suivant). Une compagnie veut instaurer un système de commandes sur Internet. Elle instaure donc un cryptage à clé publique pour la transmission du numéro de carte de crédit.
Le numéro de carte de crédit est un numéro de 16 chiffres auquel on ajoute les 4 chiffres qui correspondent à la date d'expiration, soit un nombre de 20 chiffres.
Elle choisit donc p et q deux grands nombres premiers. Nous fonctionnerons dans notre exemple avec des nombres de 25 chiffres, ce qui donne pour n un nombre de 50 chiffres

environ. Dans notre exemple, prenons

$$p = 976095975111111 2041886431$$

et

$$q = 834552399867834125649111 1.$$

Ceci donne

$$n = 814603238530311544121578649434490335599002230148 41$$

$$\varphi(n) = 814603238530311544121578468369652837704469246373 00.$$

La compagnie choisit $e = 45879256903$ et fait calculer d par Mathematica :

$$d = 614249316518661714502675899921801756121674757401 67.$$

A priori on ne peut envoyer que des messages premiers avec n. Ici aucun problème : les seuls diviseurs de n ont 25 chiffres et donc tout nombre de 20 chiffres est relativement premier avec n. Un client a le numéro de carte de crédit : 1234 5678 9098 7654 et la date d'expiration de sa carte est le 01/06.
On doit donc envoyer le message $m = 12345678909876540106$. Le programme d'envoi calcule :

$$m^e \equiv a = 625176510626059110979407460361990023455526694648 5 (\mathrm{mod}\, n).$$

Le nombre a est transmis. À la réception la compagnie calcule :

$$a^d \equiv 12345678909876540106 = m \ (\mathrm{mod}\, n).$$

Dans cet exemple, les entiers p et q choisis ne sont pas assez grands et un ordinateur pourrait factoriser n.

2 La construction de grands nombres premiers

Nous avons affirmé qu'il est facile de construire de grands nombres premiers. Cela vient du théorème des nombres premiers qui donne la distribution asymptotique des nombres premiers. Pour construire un nombre premier de 100 chiffres, i.e. un élément de $E =$

$\{1, \ldots, 10^{100}\}$, on génère au hasard des nombres entiers de 100 chiffres et on teste s'ils sont premiers. Nous énonçons sans preuve le théorème des nombres premiers. Sa preuve est d'un niveau très avancé.

Théorème des nombres premiers : Si on choisit n au hasard dans $E = \{1, \ldots, N\}$ alors

$$\text{Prob}(n \text{ premier}) \approx \frac{\frac{N}{\ln N}}{N} = \frac{1}{\ln N}.$$

Proposition 4 *On génère au hasard des nombres impairs dans $E = \{1, \ldots, 10^{100}\}$ et on teste s'ils sont premiers. Alors, après en moyenne 115 essais, on trouve un nombre premier.*

Preuve Si $N = 10^{100}$, alors $\text{Prob}(n \text{ premier}) \approx \frac{1}{\ln 10^{100}} = \frac{1}{100 \ln 10} \approx \frac{1}{230}$. Comme un entier sur deux est impair, alors $\text{Prob}(n \text{ premier si } n \text{ impair}) \approx \frac{1}{115}$. Soit X le nombre d'essais nécessaires avant d'obtenir un nombre premier. Alors X est une variable aléatoire géométrique de paramètre $p = \frac{1}{115}$. Son espérance est donc $E(X) = \frac{1}{p} = 115$. □

Pour que la méthode fonctionne, il faut qu'il existe un moyen rapide de tester si un nombre entier n est premier, qui soit plus simple que de factoriser n. On va donc discuter de la « taille » d'un algorithme.

Taille d'un algorithme appliqué à un entier n de m chiffres. On a alors $n \approx 10^m$.

1. Les algorithmes pour factoriser n fonctionnent en *temps exponentiel* par rapport à la « taille » m de n. L'algorithme classique demande de tester si les nombres $2, 3, \ldots, d \leq \sqrt{n}$ sont des diviseurs de n. Le nombre de tests est donc de l'ordre de $10^{\frac{m}{2}}$. Il existe de bien meilleurs algorithmes mais pas au point de menacer le code RSA.
2. Pour être utilisable en pratique, un algorithme doit fonctionner en *temps polynomial* : Cm^r avec r entier.
3. Il existe depuis longtemps des *algorithmes probabilistes* pour décider en temps polynomial si un nombre est premier. Un tel algorithme ne peut affirmer avec certitude qu'un nombre est premier. Il permet d'affirmer qu'avec une très grande probabilité le nombre est premier.
4. Un tout nouvel algorithme déterministe (appelé algorithme AKS) pour décider en temps polynomial si un nombre est premier vient d'être annoncé en 2003 par Agrawal, Kayal et Saxena ([AKS] et [B]). Ce résultat a eu un grand retentissement, mais

cet algorithme est moins rapide que les algorithmes probabilistes. C'est donc une percée théorique, mais les informaticiens continuent de lui préférer les algorithmes probabilistes.

Un algorithme probabiliste pour tester si n est premier :
Le principe sous-jacent est que n laisse ses « empreintes » partout, si bien que, si n n'est pas premier, au moins la moitié des nombres de l'ensemble $E = \{1, \ldots, n\}$ savent que n n'est pas premier. Le test utilise le symbole de Jacobi. Le symbole de Jacobi est une fonction $J(a, b)$ définie sur les couples d'entiers (a, b) à valeurs dans $\{-1, 1\}$. Nous donnerons sa définition ci-dessous mais celle-ci est sans intérêt, si ce n'est qu'il est facile pour un ordinateur de calculer $J(a, b)$ même si a et b sont grands.

Théorème :

1. Si n est premier, alors

$$(*) \qquad (a, n) = 1 \quad \text{et} \qquad J(a, n) \equiv a^{\frac{n-1}{2}} (\mathrm{mod}\, n).$$

   Si a satisfait $(*)$, on dit que a « passe le test ».

2. Si n n'est pas premier, alors moins de la moitié des éléments $a \in E$ premiers avec n satisfont $(*)$. Si a relativement premier avec n ne satisfait pas $(*)$, on dit que a «échoue le test».

Preuve Nous ne ferons pas la preuve de 1. Nous ne dirons qu'un mot sur la preuve de 2 pour montrer l'élégance d'un argument algébrique. Soit $S = \{a \in E \mid (a, n) = 1\}$. Alors si on définit sur S la multiplication modulo n, S devient un groupe pour cette multiplication. Soit $F \subset S$ le sous-ensemble des éléments de S qui vérifient $(*)$. Alors F est un sous-groupe de S. Soit $|F|$ le nombre d'éléments de F et $|S|$ le nombre d'éléments de S. Le théorème de Lagrange en théorie des groupes affirme que $|F|$ divise $|S|$. Alors $|F| \leq \frac{|S|}{2} \leq \frac{|E|}{2}$ dès que S a un élément qui ne vérifie pas $(*)$. □

Algorithme :

1. On choisit a_1 au hasard et on vérifie si $(*)$ est satisfaite. Si oui, a_1 a passé le test. Sinon on sait que n n'est pas premier et on arrête. **Mais on n'a pas identifié de facteur de n !**

2. On choisit a_2 au hasard et on vérifie si $(*)$ est satisfaite. Si oui, a_2 a passé le test. Sinon on sait que n n'est pas premier et on arrête.
3. ...
4. Si $a_1, \ldots, a_k$ réussissent le test avec k assez grand, on sait que n a une très grande chance d'être premier. En effet, si n n'est pas premier, chacun des a_i a au moins une chance sur deux d'échouer le test.

Remarque : On voit donc que l'algorithme permet d'affirmer avec certitude que n n'est pas premier dès qu'un des a_k a échoué le test. Par contre il ne permet jamais d'affirmer que n est premier : on peut seulement conclure que n est presque sûrement premier. C'est le propre d'un algorithme probabiliste.

Que veut dire «k assez grand» ? C'est un exercice avec la formule de Bayes. Nous nous contenterons de donner le résultat sans faire les calculs. Soit p_k la probabilité que n soit premier sachant que $a_1, \ldots, a_k$ ont passé le test. Si n a 100 chiffres, i.e. est de l'ordre des 10^{100}, alors :

$$p_{15} \geq 0,996533$$

$$p_{35} \geq 0,9999999967.$$

Définition du symbole de Jacobi $J(a,n)$ pour n impair :

$$J(a,n) = \begin{cases} 1 & a = 1 \\ J\left(\frac{a}{2}, n\right)(-1)^{\frac{n^2-1}{8}} & a \text{ pair} \\ J(n \pmod a, a)(-1)^{\frac{(a-1)(n-1)}{4}} & a \text{ impair} \end{cases}$$

où $n \pmod a$ désigne le reste de la division de n par a.
On voit donc que le calcul de $J(a,n)$ se fait par itération successive. Son calcul est facile à programmer et le calcul se fait en temps polynomial.

Exemple : prenons $a = 130$ et $n = 207$. Alors

$$J(130,207) = J(65,207)(-1)^{\frac{42848}{8}} = J(65,207)(-1)^{5356} = J(65,207) = J(12,65)(-1)^{\frac{64\times 206}{4}}$$
$$= J(12,65) = J(6,65)(-1)^{\frac{4224}{8}} = J(6,65)(-1)^{528} = J(6,65) = J(3,65)(-1)^{528} = J(3,65)$$
$$= J(2,3)(-1)^{\frac{2\times 64}{4}} = J(2,3) = J(1,3)(-1)^{\frac{8}{8}} = -J(1,3) = -1$$

Ce calcul peut sembler long et fastidieux. Mais ce qui est important c'est que pour un ordinateur c'est un calcul simple.

Pour vérifier si a passe le test, on doit aussi calculer $a^{\frac{n-1}{2}} \pmod{n}$, soit $130^{103} \pmod{207}$. On doit être plus astucieux que de demander à l'ordinateur de calculer 130^{103} et de le réduire ensuite modulo 207. Pour cela on décompose 103 en puissances de 2 :

$$103 = 64 + 32 + 4 + 2 + 1 = 1 + 2^1 + 2^2 + 2^5 + 2^6.$$

On calcule :

$$\begin{aligned}
130^2 &= 16900 \equiv 133 \pmod{207} \\
130^4 &= (130^2)^2 \equiv 133^2 = 17689 \equiv 94 \pmod{207} \\
130^8 &= (130^4)^2 \equiv 94^2 = 8836 \equiv 142 \pmod{207} \\
130^{16} &= (130^8)^2 \equiv 142^2 = 20164 \equiv 85 \pmod{207} \\
130^{32} &= (130^{16})^2 \equiv 85^2 = 7225 \equiv 187 \pmod{207} \\
130^{64} &= (130^{32})^2 \equiv 187^2 = 34969 \equiv 193 \pmod{207}
\end{aligned}$$

Finalement

$$\begin{aligned}
130^{103} &= 130^{64} \times 130^{32} \times 130^4 \times 130^2 \times 130^1 \\
&\equiv 193 \times 187 \times 94 \times 133 \times 130 \equiv 67 \pmod{207}
\end{aligned}$$

On voit que $J(130, 207)$ n'est pas congru à $130^{\frac{207-1}{2}}$. On en conclut que 207 n'est pas premier. Ici c'était facile à voir : $207 = 3^2 \cdot 23$.

Discussion de la valeur du code RSA : Le code a été introduit en 1978. Il a stimulé les chercheurs à trouver de meilleurs algorithmes pour factoriser de grands nombres entiers mais sans succès : la méthode tient toujours si l'entier n est assez grand. En 1978, on évaluait à 74 ans le temps pour factoriser un nombre de 100 chiffres, à $3,8 \times 10^9$ années le temps pour factoriser un nombre de 200 chiffres et à $4,2 \times 10^{25}$ années le temps pour factoriser un nombre de 500 chiffres. Une clé de 100 chiffres est donc vulnérable maintenant. C'est d'ailleurs ce qui est arrivé avec la clé de 100 chiffres du système bancaire européen, laquelle a été factorisée par un particulier au début de l'an 2000. Mais, même en tenant compte de l'augmentation de la puissance des ordinateurs et du fait qu'on peut en mettre beaucoup

en parallèle, une clé de 200 chiffres tient encore le coup tant qu'on n'a pas de meilleur algorithme de factorisation.

Où en est-on par rapport aux évaluations de 1978 ? Les améliorations sont de deux ordres : la puissance des ordinateurs et de meilleurs algorithmes. La loi de Moore (du nom de Gordon Moore, cofondateur d'Intel) prédisait en 1965 que la densité des transistors doublerait tous les 18 mois à 2 ans, et elle s'est révélée étonnamment exacte. Quel est le lien avec la vitesse de calcul ? Les précisions suivantes viennent de Paul Rousseau travaillant chez TSMC : la vitesse des transistors augmente d'un facteur 1,4 tous les 2-3 ans. En fait les compagnies annoncent que la vitesse de l'horloge d'un circuit est multipliée par 2, mais le circuit fait moins de travail par cycle, donc ce facteur est artificiel. La vraie mesure est la capacité de faire du « vrai travail ». Pour un algorithme de factorisation où le travail peut être fait en parallèle, l'augmentation de la capacité de travail est de l'ordre de 2,8, soit 1,4 par transistor et un facteur 2 dû à l'augmentation du nombre de transistors. Il s'est écoulé 27 ans depuis 1978. Si l'on prend des générations ayant en moyenne 2,5 années, cela donne 10,8 générations, soit un facteur de 67500, inférieur à 10^5.

L'amélioration au niveau des algorithmes est non moins spectaculaire. Déjà Gauss au 19$^{\text{e}}$ siècle avait qualifié le problème pratique de la factorisation de grands nombres premiers de problème fondamental en théorie des nombres. Les algorithmes les plus importants sont :

- le crible quadratique de Pomerance ;
- la méthode des courbes elliptiques de Lenstra ;
- le crible des corps de nombres de Pollard, Adleman, Bulher, Lenstra et Pomerance.

En 1996, on factorisait des nombres de 130 chiffres. Un bon article sur le sujet est l'article de Carl Pomerance [P]. L'auteure n'exclut pas de faire un prochain article sur le sujet. Malgré toutes ces améliorations, le code RSA n'est pas encore menacé et une clé de 200 chiffres est encore suffisante.

La méthode de cryptage-décryptage pour le code RSA est longue et fastidieuse. La cryptographie à clés publiques n'est donc pas utilisée pour transmettre de longs textes et on lui préfère d'autres méthodes, surtout quand le texte transmis n'a pas besoin d'être tenu secret longtemps. Pour de plus longs textes, on va parfois préférer un algorithme à clé symétrique, par exemple le DES (Data Encryption System), i.e. l'expéditeur et le receveur ont la même clé. Ils peuvent utiliser le code RSA pour se transmettre la clé.

Application du code RSA :

- envoyer un numéro de carte de crédit sur la toile ;
- coder des NIP dans les systèmes bancaires.

Pour casser le code, on pense en général qu'il faut pouvoir factoriser la clé en temps polynomial. Rien ne prouve cependant qu'il ne puisse exister un autre algorithme fonctionnant en temps polynomial et permettant de retrouver le message m à partir de l'information publique (n, e, m^e) sans pour autant factoriser n. Un algorithme polynomial permettant de factoriser la clé existe, mais sur un ordinateur quantique. Nous allons discuter brièvement cet algorithme.

3 L'algorithme de Shor pour factoriser de grands nombres

Avant de discuter cet algorithme, on va commencer par se convaincre que les raffinements de l'algorithme classique de factorisation ne permettent pas de diminuer significativement le temps de factorisation. On considère un nombre n de 200 chiffres, i.e. un nombre de l'ordre de 10^{200}. L'algorithme classique consiste à chercher s'il existe un diviseur $d \leq \sqrt{n}$. On doit donc faire environ 10^{100} essais. Essayons quelques astuces :

- Si on se limite aux nombres d impairs, on a $m_1 = \frac{10^{100}}{2}$ tests à faire.
- Si on se limite à des grands diviseurs (des nombres de 100 chiffres), alors on a $m_2 = \frac{9}{10} m_1$ tests à faire (exercice).
- Si on met en parallèle un milliard d'ordinateurs, on a $m_3 = 10^{-9} m_2$ tests à faire sur chaque ordinateur.
- Si chacun des milliards d'ordinateurs est un super-ordinateur de 5000 processeurs pouvant faire 5000 opérations en parallèle (c'est la puissance maximum des super-ordinateurs en 2004), on limite le nombre d'opérations successives à faire sur chaque processeur à $m_4 = \frac{m_3}{5000}$.
- Avec ces tests, on aurait encore $m_5 \geq 10^{86}$ opérations sucessives à faire.
- Et supposons qu'on arrive tout juste à s'approcher avec d'autres astuces d'une factorisation de la clé, alors il suffirait d'allonger la clé de quelques dizaines de chiffres pour voir nos efforts anéantis.

On voit donc que pour factoriser des grands nombres il nous faut absolument un meilleur algorithme. L'algorithme de Shor a été introduit en 1997 et permet de factoriser des nombres entiers.

- Cet algorithme fonctionne en temps exponentiel sur un ordinateur classique.
- Il fonctionne en temps polynomial sur un ordinateur quantique.

C'est un algorithme probabiliste : si n n'est pas premier, l'algorithme a une très grande probabilité de trouver un diviseur d de n. L'algorithme ne permet donc pas de décider avec certitude si n est premier. Par contre, dès qu'on a trouvé un diviseur d de n, on sait que n n'est pas premier. Nous nous contenterons de donner les grandes lignes de cet algorithme, sans en montrer tous les détails.

Le principe de l'algorithme de Shor ([K & al] et [S]) :

Première étape : **On cherche un entier r tel que $n \mid r^2 - 1$, mais ni $r-1$ ni $r+1$ ne sont divisibles par n.**

En effet : $r^2 - 1 \equiv 0 \pmod{n}$, ce qui implique que $(r-1)(r+1) = mn$ pour un entier m. Alors si p est un facteur premier de n, nécessairement $p \mid r-1$ ou $p \mid r+1$. Si $p \mid r-1$, alors $(r-1, n) = d > 1$. Donc d est un diviseur de n. De même si $p \mid r+1$.

Exemple : Si $n = 65, r = 14$, alors $r^2 = 196 = 3 \times 65 + 1 \equiv 1 \pmod{65}$. $r - 1 = 13$ est un diviseur de 65. Par contre, si on prend $s = 64 \equiv -1 \pmod{65}$, alors $s^2 \equiv (-1)^2 = 1 \pmod{65}$. On voit que $s+1 = 65$ est divisible par 65. Donc s ne nous est d'aucun secours pour trouver un diviseur propre de 65.

Deuxième étape : **Comment trouver r ?**
On prend a au hasard dans $E = \{1, \ldots, n\}$ et on calcule les puissances de a : $a, a^2, a^3, \ldots$ que l'on réduit modulo n : $a^k \equiv a_k \pmod{n}$ avec $a_k \in E$.

- Si $(a, n) = d$, on a trouvé un diviseur de n.
- Si $(a, n) = 1$, comme E est fini, il existe k et l tels que $a_k = a_l$. On peut supposer $k > l$. Alors $a_{k-l} \equiv a^{k-l} \equiv 1 \pmod{n}$.
- Donc il existe s minimum tel que $a^s \equiv 1 \pmod{n}$. Ce nombre s est appelé l'*ordre* de a. On a $s \leq n$.

- Si s est pair : $s = 2m$, on prend $r \equiv a^m \pmod{n}$ avec $r \in E$. Alors $r^2 \equiv a^{2m} = a^s \equiv 1 \pmod{n}$.
- Si ni $r-1$, ni $r+1$ ne sont divisibles par n, on a terminé par la première étape.

Sinon on recommence avec un $a' \neq a$ choisi au hasard dans E.
On peut montrer qu'il y a beaucoup de $a \in E$ d'ordre impair qui font l'affaire, donc c'est un bon algorithme.

Rapidité de l'algorithme : la seule partie de l'algorithme qui ne s'effectue pas en temps polynomial est de calculer l'ordre de a. Un algorithme simpliste consiste à calculer tous les a_k jusqu'au premier qui est égal à 1. Le nombre d'opérations est de l'ordre de n, donc l'algorithme est exponentiel. C'est pour cette seule partie de l'algorithme qu'un ordinateur quantique prend la relève.

Calcul de l'ordre de a modulo n avec un ordinateur quantique (nous nous contenterons de donner quelques idées) : on écrit les nombres en base 2. Si n s'écrit avec m chiffres dans $\{0,1\}$, alors $n \leq 2^m$. On écrira les entiers k en base 2 : $k = [j_{m-1}j_{m-2}\dots j_0] = j_{m-1}2^{m-1} + j_{m-2}2^{m-2} + \dots + j_0 2^0$. Pour calculer l'ordre de a, on voudrait pouvoir calculer a^k pour tous les $k \in E$ simultanément, c'est-à-dire pour tous les $[j_{m-1}, \dots, j_0] \in \{0,1\}^m$. Se donner k revient donc à se donner m bits dans $\{0,1\}$. Essayer tous les $k \in E$ c'est essayer toutes les possibilités $j_i = 0$, et $j_i = 1$, pour $i = 0, \dots, m-1$, soit 2^m possibilités. C'est là que l'ordinateur quantique vient à la rescousse. On remplace les bits classiques $j_{m-1}, \dots, j_0$ par des bits quantiques.

Les bits quantiques Un bit quantique a la propriété de pouvoir se mettre dans un état superposé. Il est dans l'état $|0\rangle$ avec probabilité $|\alpha|^2$ et dans l'état $|1\rangle$ avec probabilité $|\beta|^2$ où $|\alpha|^2 + |\beta|^2 = 1$. ($\alpha$ est l'« amplitude » de $|0\rangle$ et β est l'« amplitude » de $|1\rangle$. Ce sont tous deux des nombres complexes.) En mécanique quantique, on dira que son état est $\alpha|0\rangle + \beta|1\rangle$. Pour se donner une analogie, pensons à un sou : il a probabilité 1/2 de tomber sur pile et 1/2 de tomber sur face. Avant le lancer, notre sou est donc dans un état superposé. Par contre, quand on le lance, on observe soit pile, soit face. C'est la même chose avec un bit quantique. Si on le mesure, on obtient 0 avec probabilité $|\alpha|^2$ et 1 avec probabilité $|\beta|^2$.

Le grand parallélisme d'un ordinateur quantique Si on met tous les bits $j_{m-1}, \ldots, j_0$ dans un état superposé en même temps, alors, en calculant $a^{|k\rangle} \pmod n$ où $|k\rangle$ est une superposition de tous les $k \in E$, on fait le calcul de a^k pour tous les $k \in E$ simultanément ! Comme le calcul quantique est linéaire et réversible, on peut voir $a^{|k\rangle} \pmod n$ comme un superposition de tous les $a_k \equiv a^k \pmod n$, chacun étant lié à la valeur de $k \in E$ associée. Toute l'information qui nous est nécessaire se trouve maintenant dans cet état, mais on ne peut y accéder sans le mesurer. En le mesurant, on ne mesure qu'une seule valeur $k \in E$, soit un $m-$tuplet $(j_{m-1}, \ldots, j_0)$. La mesure d'un état quantique est un processus aléatoire qui suit une distribution de probabilité dictée par les amplitudes de la superposition. Il faut donc user d'ingéniosité pour augmenter nos chances de lire un k qui nous intéresse. En particulier on utilise les probabilités conditionnelles et on mesure k sous la condition que $a^k \equiv 1 \pmod n$. On a un peu triché dans cette présentation et ce n'est pas aussi simple que cela, mais les grandes idées sont là.

Remarque : On a déjà montré dans la section précédente qu'il n'est pas difficile pour un ordinateur de calculer $a^k \pmod n$. En effet, si $k = j_{m-1}2^{m-1} + j_{m-2}2^{m-2} + \ldots + j_0 2^0$, alors $a^k = \prod_{j_i=1} a^{2^i}$. Il suffit donc de calculer les a^{2^i} modulo n, pour $i = 0, \ldots, m-1$. Ce calcul se fait de proche en proche :

- $a^2 \equiv a_1 \pmod n$ avec $a_1 \in E$;
- $a^4 \equiv (a_1)^2 \equiv a_2 \pmod n$ avec $a_2 \in E$;
- ...
- $a^{2^{m-1}} \equiv (a_{m-2})^2 \equiv a_{m-1} \pmod n$ avec $a_{m-1} \in E$.

Finalement $a^k \equiv \prod_{j_i=1} a_i \pmod n$.

Où en est-on avec l'ordinateur quantique ? Isaac Chuang et ses collègues du centre de recherche Almaden d'IBM ont pu construire un ordinateur quantique avec 7 bits quantiques simultanément dans un état superposé, lequel a permis de factoriser le nombre 15. Leur technique ne se généralise pas à un grand nombre de bits quantiques. Mais la recherche se poursuit sur d'autres techniques...

Remerciements Je tiens à remercier Isabelle Ascah-Coallier qui m'a intéressée à l'ordinateur quantique et Valérie Poulin qui m'a aidée à comprendre son fonctionnement.

Références

[AKS] M. Agrawal, N. Kayal and N. Saxena, *Primes is in P*, prépublication sur le site de Manindra Agrawal à www.cse.iitk.ac.in

[B] F. Bornemann, *Primes is in P*, Notices of the American Mathematical Society, (2003), **50** No 5, page 545-552.

[K & al] E. Knill, R. Laflamme, H. Barnum, D. Dalvit, J. Dziarmaga, J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola and W. H. Zurek, *Introduction to quantum Information Processing*, 2002.

[RSA] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of the ACM, (1978), **21** No. 2, 120-126.

[P] C. Pomerance, *A tale of two sieves*, Notices of the American Mathematical Society, (1996), **43** No. 12, 1473-1485.

[S] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Computation, **26** (1997), 1484-1509.

Applications

Bernard Courteau

Une vie à résoudre des problèmes : entrevue avec Yves Langlois

Bulletin AMQ — Bonjour et merci de nous recevoir dans ce bel édifice de Bell au 1050 Beaver Hall.

Yves Langlois — C'est l'un des plus vieux édifices de Montréal, un édifice art déco, construit de 1927 à 1929 pour abriter le siège social de la compagnie Bell.

Bulletin AMQ — C'est mon quartier aussi, parce que je suis allé au Collège Ste-Marie pour mes études. C'était au coin de Bleury et Dorchester, qui est devenu René-Lévesque.

Yves Langlois — C'est toujours là !

Bulletin AMQ — Le Gésu est toujours là, mais le collège a été démoli.

Yves Langlois — Je me souviens quand j'étais en secondaire V. On allait voir des pièces de théâtre au Gésu. On avait un très bon prof de français, Jacques Laurin.

Bulletin AMQ — Tu as fait tes études pas loin d'ici ?

Yves Langlois — J'ai fait ma première année de primaire dans une école publique et puis je suis allé chez les sœurs à partir de ma 2^{e} année. Donc j'étais pensionnaire. C'était à l'école St-Enfant-Jésus du Mile-End, au coin de St-Dominique et St-Joseph. J'étais pensionnaire à la

semaine. Ensuite pour le secondaire, je suis allé au Séminaire de Terrebonne toujours comme pensionnaire. J'ai fait les deux premières années du cours classique, mais le cours classique s'est désagrégé avant que je puisse me rendre en Versification. Donc j'ai fait Éléments latins et Syntaxe. Ensuite c'est devenu secondaire (I, II, III, IV) et c'est devenu aussi moitié externe, moitié pensionnaire. Dans mes deux premières années, on ne sortait que trois fois par année : à l'Action de Grâce, à Noël et à Pâques, et nos parents venaient nous visiter le dimanche. C'était assez sérieux. J'ai fait du latin, mais pas de grec, parce qu'on commençait le grec en Méthode, mais quand je suis arrivé en Méthode, c'est devenu le secondaire III et tout le programme avait été changé... C'était en 1967-1968.

Bulletin AMQ — Tu as vécu de grands bouleversements.

Yves Langlois — Oui, j'ai vécu la fin d'une époque. J'ai fait jusqu'à mon secondaire IV à Terrebonne puis je suis revenu à Montréal pour faire mon secondaire V et ensuite je suis allé au Cégep Ahuntsic en sciences pures. Le cadre du programme c'était biologie, mathématiques, physique et chimie. On avait aussi les cours de philosophie, les cours de français, quelques cours de langue.

Bulletin AMQ — Première question : d'où vient ta passion des mathématiques ?

Yves Langlois — C'est venu tranquillement. J'ai toujours détesté l'école ; pour moi l'école était une source de stress. Même à l'université, même quand j'étais en mathématiques, je détestais l'école surtout à cause des examens. Je ne peux pas dire que c'est la passion des mathématiques qui m'a amené à faire des mathématiques. C'était plus un choix parmi d'autres. Évidemment je suis allé en sciences parce que j'avais beaucoup plus de facilité en sciences et puis, après le cégep, il fallait bien que je décide. C'était soit la physique soit les mathématiques. Je trouvais que les mathématiques, c'était plus « pur », et comme je ne savais pas ce que je voulais faire, je me disais : en mathématiques ça m'ouvre des portes, c'est plus général, c'est plus « basic ». Je me disais aussi que, de toute façon, la physique, c'était beaucoup de mathématiques. À un moment donné, la physique ça devient des mathématiques. Donc je me suis dit : je vais aller en mathématiques et si je veux faire de la physique après, j'aurai déjà ma base de mathématiques.

C'était ça un peu mon cheminement logique, mais mon goût des mathématiques c'était

aussi les problèmes, car j'aime les problèmes. J'ai appris à aimer les mathématiques, même si je n'aimais pas le système d'enseignement ou le processus de cours et d'examens. Probablement que s'il n'y avait pas eu le système d'examens, j'aurais fait des mathématiques pas mal plus longtemps parce que fondamentalement ça m'amusait. J'aimais ce qu'on pouvait faire avec les maths. Pour moi la relation entre les mathématiques et les choses concrètes, c'est absolument fondamental, en terme de motivation.

Bulletin AMQ — Et ça remontre à loin ce goût des choses concrètes ?

Yves Langlois — Oui, d'ailleurs j'ai toujours construit des choses. Quand j'étais au secondaire, j'étais dans les scouts et je voulais être un inventeur. Durant ma carrière chez Bell, je me suis toujours arrangé pour construire des choses, des systèmes informatiques ou des processus.

Bulletin AMQ — Tu es bricoleur ?

Yves Langlois — Je suis bricoleur, oui, j'ai construit ma maison. Alors pour moi les mathématiques c'était comme un moyen de construire des choses. C'est pour ça, entre autres, que j'ai choisi les mathématiques appliquées. J'aimais beaucoup les choses concrètes et tout ce qui était spatial m'intéressait beaucoup : toute l'algèbre linéaire, les graphiques. J'aime les graphiques, j'aime les tendances, les analyses de tendances, les phénomènes d'inflexion, de concavité, pour moi ce sont des choses concrètes. Les méthodes numériques ou la simulation c'était concret, c'était presque physique pour moi. Alors que les statistiques, je trouvais ça beaucoup plus difficile.

Bulletin AMQ — Tu trouvais les statistiques abstraites ?

Yves Langlois — Oui, c'était très abstrait pour moi.

Bulletin AMQ — C'est curieux, les gens considèrent souvent que les statistiques c'est concret et c'est applicable.

Yves Langlois — C'est très appliqué, on applique beaucoup les statistiques, c'est une bonne source de travail.

Bulletin AMQ — Mais tu trouves ça abstrait.

Yves Langlois — Oui, moi je n'ai jamais vraiment compris ou senti les statistiques, je ne vibre pas avec les statistiques. Je comprends l'idée, mais je n'accroche pas. J'imagine qu'il y a différentes sensibilités chez les mathématiciens...

Bulletin AMQ — Il y a des mathématiciens où c'est l'arithmétique, les nombres, compter, des choses comme ça qui les inspirent et c'est ça qu'ils sentent. Mais toi j'ai l'impression que tu es un mathématicien du côté intuitif, spatial. C'est la géométrie ou les choses que tu peux dessiner qui te disent quelque chose.

Yves Langlois — Oui, oui.

Bulletin AMQ — Tu es un peu comme le grand Henri Poincaré qui était un intuitif et un géomètre, ce qui ne l'a pas empêché de faire des mathématiques tout à fait symboliques, c'est sûr. C'est une question de sensibilité fondamentale. Donc ton goût des mathématiques au fond est bien ancré dans ta psychologie fondamentale.

Yves Langlois — J'ai l'impression que oui, je raisonne comme ça et ça m'a servi beaucoup dans ma carrière. Il y en a même qui me disent : « Tu vois le monde comme des formules », mais moi je vois ça comme ça. J'essaie toujours d'interpréter ce que je vois ; c'est un réflexe, je ne peux pas m'empêcher de le faire. Je ne suis pas naïf quand même au point de dire qu'on peut tout calculer, mais il y a toujours des relations entre ce qui se passe et une certaine forme de mathématiques, que ce soit de l'analyse, de l'algèbre, etc. Il y a les phénomènes de convergence ou de divergence par exemple, ce sont des notions qu'on étudie dans les cours. J'ai toujours fait le parallèle entre ces notions et ce que je voyais autour de moi.

Bulletin AMQ — Dès tes études universitaires, quand tu étudiais par exemple l'analyse, tu parles de convergence. Qu'est-ce qui avait une résonance pour toi ?

Yves Langlois — L'idée d'infini est pour moi quelque chose de fantastique. Je « trippais » fort là-dessus. L'infini me fascine.

Bulletin AMQ — Tu es un grand mystique à ce que je vois...

Yves Langlois — Ah, peut-être.

Bulletin AMQ — Il y a peut-être seulement en mathématiques que l'on peut vraiment traiter rationnellement de l'infini. Les mathématiciens ont développé des outils pour maîtriser l'infini. Alors qu'ailleurs c'est la mystique, c'est la religion qui nous permet de traiter l'infini.

Yves Langlois — Moi, je pensais souvent aux mathématiques et les mathématiciens que j'admire le plus, ce sont ceux qui ont réussi à trouver des choses sur lesquelles ils n'avaient pas de base de référence physique. Quand on regarde les équations, je regarde ce que Newton a fait au début, ses équations de la mécanique. Il y a beaucoup d'abstraction là-dedans, mais la relation avec le monde physique est quand même là. Quand on commence à regarder les phénomènes d'astronomie, l'espace-temps de la théorie de la relativité, ces affaires-là, ça prend une intuition que je n'ai pas, ça me dépasse complètement. J'aurais aimé avoir le temps ou la capacité de travailler dans ces domaines, mais je ne l'avais pas.

Bulletin AMQ — Je t'ai apporté un numéro du Bulletin dans lequel on va publier ton entrevue et, justement, il y a là-dedans une conférence de clôture que Stéphane Durand a prononcée à l'un de nos congrès et qu'il a intitulée *L'imagination mathématique*. Ce que tu viens de dire me fait penser à cette très belle conférence où il dit que les mathématiques donnent un sixième sens. Il y a des choses qu'on ne peut pas percevoir avec nos sens ordinaires ; l'infiniment petit, l'infiniment grand, c'est en dehors de notre intuition ordinaire. Les mathématiques nous donnent alors une intuition seconde, une intuition supplémentaire.

Mais revenons à nos moutons : où as-tu fait tes études universitaires ?

Yves Langlois — À l'université de Sherbrooke. La raison pour laquelle je suis allé à Sherbrooke, c'était à cause du cours coopératif, parce que financièrement c'était plus facile. Puis j'aimais aussi l'idée qu'il y avait des stages qui donnaient un aspect concret à ce qu'on étudiait. Au début les stages étaient beaucoup reliés à l'informatique, mais je peux dire que j'ai été très chanceux parce que j'ai vraiment fait des stages en mathématiques. J'ai fait quatre stages : trois étaient vraiment en mathématiques et le dernier, aux Olympiques de 1976, était plus en informatique et en gestion de l'information, mais j'avais travaillé en simulation. Dans les trois premiers stages, j'ai travaillé sur un modèle pour contrôler le flux des eaux usées dans les intercepteurs qu'on était en train de construire pour l'usine d'épuration

de Montréal. Parce qu'en ce temps-là, on est au début des années 1970, les eaux usées se jetaient directement dans le fleuve et dans la rivière Des Prairies. Alors il y avait le projet de construire l'usine d'épuration qui collecterait toutes ces eaux et les amènerait pour les traiter. Il y avait des intercepteurs qui sont d'immenses tuyaux, intercepteur Nord, intercepteur Sud, qu'il fallait dimensionner en fonction du débit, de la vitesse de l'eau, etc. Et il y a évidemment des situations où on ne peut pas acheminer toute l'eau d'un coup, lorsqu'il y a une grosse pluie par exemple, donc il faut prévoir amener l'eau dans des bassins de rétention. Tout cela devant être contrôlé par ordinateur, il fallait un modèle de simulation. J'ai travaillé pendant trois stages là-dessus.

Bulletin AMQ — Trois stages pour la ville de Montréal ?

Yves Langlois — Oui, au Service d'assainissement des eaux.

Bulletin AMQ — Et là, tu faisais un travail vraiment mathématique ?

Yves Langlois — Ah oui, c'était très mathématique.

Bulletin AMQ — Dans quel sens ?

Yves Langlois — C'était de la simulation numérique, donc des équations hypercompliquées ; je ne me souviens plus. J'ai dû inverser des matrices 100 par 100 des milliers de fois et évidemment on n'avait rien de graphique. Mes sorties d'ordinateur étaient des imprimés d'à peu près quatre pouces d'épaisseur avec des nombres à 32 décimales en point flottant. Il fallait que je voie si les erreurs ou l'évolution que je voyais étaient des erreurs de troncature, ou provenaient des équations, ou si c'était vraiment le phénomène que j'essayais d'observer, mais il n'y avait rien de graphique.

Bulletin AMQ — À l'époque il n'y avait pas les moyens informatiques qu'on a maintenant ?

Yves Langlois — Ah non ! Juste pour te donner une perspective, il n'y avait pas d'ordinateur assez puissant à la ville de Montréal pour traiter mon modèle. On allait chez des consultants, ça s'appelait SDL, qui avaient un « main frame » fonctionnant en temps par-

tagé. Normalement, du temps partagé ça fonctionne comme ceci : tu remets ton programme à l'opérateur qui le met avec les autres programmes et gère la machine, mais alors, lorsqu'il chargeait mon programme, il prenait toute la mémoire RAM de la machine ; ça prenait cinq minutes pour le faire tourner et inverser mes matrices. Il n'y avait donc rien d'autre que mon programme qui pouvait tourner en même temps dans cet ordinateur-là. Ça coûtait 150 $ chaque fois que je faisais une passe, ce qui était à peu près 10 fois mon salaire ! Comme mon affaire marchait beaucoup par essais et erreurs, mon directeur de stage était découragé. Au bout d'une à deux semaines, il m'a dit : « Yves, arrête, je te laisse faire seulement deux passes par semaine ». Aujourd'hui on rit parce que, pour vous donner une idée de la capacité de la machine, je ne prenais que 900 K de mémoire RAM, mais c'était 90 % de toute la mémoire RAM disponible. Ça n'avait rien à voir avec la mémoire qu'on a aujourd'hui.

Bulletin AMQ — C'était les temps héroïques.

Yves Langlois — Oui, mais c'est là qu'on voit qu'on est capable de se débrouiller avec les moyens qu'on a. Ça va juste moins vite, mais on peut tout faire.

Bulletin AMQ — En tout cas, l'usine a été construite.

Yves Langlois — L'usine a été construite et elle fonctionne.

Bulletin AMQ — Donc, tu as fait trois stages à la même place, à la ville de Montréal, un dernier stage plutôt en informatique. Quel a été ton premier emploi, après le bac ?

Yves Langlois — Après mes études, après avoir pris quelques mois de vacances, je suis entré chez Bell Canada. C'était en 1977. Ce qui m'intéressait chez Bell, c'était les réseaux. Je ne m'attendais pas à faire de mathématiques, et d'ailleurs, c'est une chose que les stages m'avaient apprise : j'étais incapable d'oublier mes problèmes. Quand j'avais un problème mathématique dans la tête, il ne me sortait pas de là tant qu'il n'était pas réglé. Alors pendant mes stages, je ne dormais à peu près pas. J'ai alors réalisé, entre autres, que je n'étais probablement pas fait pour la recherche.

Bulletin AMQ — Parce que là tu aurais vécu avec tes problèmes 24 heures par jour.

Yves Langlois — Absolument, j'étais incapable de me déconnecter. Je suis encore comme ça, quand j'ai un problème, tant que j'ai pas trouvé la voie de la solution, il va prendre toute la place. Donc, j'ai réalisé que les mathématiques ou la recherche c'était pas vraiment une bonne chose pour moi.

Bulletin AMQ — Pour ta santé ?

Yves Langlois — Pour ma santé. Je suis donc entré chez Bell. C'est une compagnie où il y a beaucoup de technologies, beaucoup de problèmes complexes et où il y a du monde. Moi, j'aime travailler avec le monde.

Bulletin AMQ — Tu n'avais pas fait de stage chez Bell ?

Yves Langlois — Non.

Bulletin AMQ — Donc, il fallait une entrée un peu spéciale. Comment ça s'est passé ?

Yves Langlois — Ça c'est intéressant. Le domaine dans lequel j'ai commencé, l'approvisionnement du réseau, est un domaine associé à l'ingénierie et ce sont des ingénieurs qui sont dans ce département-là. À ce moment-là, Bell avait un programme accéléré de développement des cadres : ils allaient chercher des gradués universitaires et ils les mettaient dans un programme de développement accéléré pour en faire des cadres intermédiaires et des cadres supérieurs. Évidemment, tous les ans ils allaient sur les campus pour faire du recrutement, et traditionnellement ces gens-là allaient dans les facultés d'ingénierie. Mais, par chance, il y avait chez Bell un recruteur qui était mathématicien, c'était une exception à la règle. Il s'appelait Christian Gaudet. Quand il est venu faire des entrevues à Sherbrooke, il avait interviewé des ingénieurs évidemment, mais il avait aussi manifesté l'envie d'interviewer des mathématiciens. Il a demandé à M. Roberge, qui était en charge des stages, s'il n'y avait pas des mathématiciens qui seraient intéressés. Je me souviens, Roberge était entré dans un de nos cours et il avait dit « Il y a quelqu'un de Bell Canada qui voudrait faire passer des entrevues à des mathématiciens. Est-ce qu'il y en a qui sont intéressés ? ». Moi je m'étais montré intéressé parce que j'adorais passer des entrevues.

Bulletin AMQ — Ah oui !!!

Yves Langlois — J'adorais passer des entrevues.

Bulletin AMQ — Ça c'est surprenant ! Toi qui est affecté par le stress ?

Yves Langlois — Pour moi, ce n'était pas une source de stress, non, parce que j'aimais parler dans l'entrevue. J'étais curieux de savoir en quoi consistaient les problèmes que l'entreprise avait à régler, tellement que finalement c'est moi qui posais le plus de questions. Souvent j'étais sélectionné, alors pour moi c'était comme un jeu. C'est avec cette idée-là que je suis allé passer l'entrevue et ça a vraiment cliqué avec Christian. Sur le campus c'est toujours une présélection, ensuite, en concurrence avec trois ou quatre candidats, j'ai passé l'entrevue finale dans le milieu de l'entreprise, j'ai rencontré des dirigeants et puis j'ai été sélectionné. Je me souviens, il y avait un de mes concurrents, si je peux dire, qui allait passer l'entrevue en même temps que moi à Montréal. Il avait son habit, il était tout bien « checké », la belle valise, la cravate, je pense qu'il était en génie. Moi, j'avais les cheveux longs et j'étais en jeans. Je me souviens que la responsable du personnel m'avait dit : « Yves, nous chez Bell, on est des gens très ouverts, mais quand même tu devrais mettre toutes les chances de ton côté si la job t'intéresse. Tu devrais au moins attacher tes cheveux ». Elle m'avait gentiment dit d'améliorer mon apparence pour l'entrevue, puis je m'étais dit : « S'ils ne veulent pas m'avoir pour ce que j'ai dans la tête, tant pis pour eux autres ! ».

Bulletin AMQ — Tu étais un peu « baveux », si tu me permets de le dire...

Yves Langlois — J'étais baveux, puis je suis allé passer mon entrevue en jeans et c'est moi qu'ils ont sélectionné. Je suis chez Bell depuis ce temps-là, ça fait 27 ans.

Bulletin AMQ — Bien, bravo pour Bell qui a su distinguer la qualité qui se cachait sous des dehors peu conventionnels.

Yves Langlois — Je pense qu'il faut reconnaître que Bell est une compagnie très, très ouverte, où on encourage beaucoup les différences. C'est quelque chose qui est très valorisé chez Bell. On construit des équipes avec des gens de points de vue différents.

Bulletin AMQ — Au moment de ton engagement, quelle était ta fonction ?

Yves Langlois — J'ai été engagé pour faire du design de commutateurs téléphoniques, c'est un travail qui n'existe plus maintenant. En téléphonie, un commutateur, c'est finalement le système qui achemine les appels dans le réseau téléphonique. À partir du moment où on décroche le téléphone, il faut envoyer un signal de manœuvre, il faut reconnaître qui appelle, ensuite il faut intercepter la composition du client, l'analyser et voir où ça s'en va, ensuite il faut contacter le commutateur de la destination, que ce soit aux Etats-Unis, au Canada ou même à Montréal, enfin il faut faire sonner l'appareil chez le destinataire. Tout ça est géré par ce qu'on appelle un commutateur ou un réseau de commutateurs. Dans ce temps-là, tout était électromécanique, c'était des relais, c'était de l'algèbre booléenne. Les gens qui faisaient ça faisaient de l'algèbre booléenne sans le savoir. C'était typiquement des techniciens qui avaient énormément d'expérience. Toute l'intelligence d'acheminement – toi tu as le droit de faire ça, tu ne l'as pas, telle série de chiffres ça veut dire que c'est un interurbain, si les deux premiers chiffres du numéro de téléphone sont 32, ça veut dire que c'est Montréal-Nord, etc.– en somme tout le processus d'acheminement des appels était dans les relais. C'est pour cela que dans ce temps-là, dans une grande ville comme Montréal, tous les numéros qui commençaient par 5-2 c'était dans Lafontaine, c'était la centrale de Papineau, parce que c'était électromécanique. L'intelligence étant limitée, il fallait que ce soit procédural et séquentiel ; à mesure que tu composais un chiffre tu avançais dans la hiérarchie, alors qu'aujourd'hui avec les ordinateurs ça n'a plus tellement d'importance . Donc, mon travail c'était de concevoir d'un point de vue trafic les paramètres et les capacités de ces commutateurs-là.

Si on revient aux mathématiques, cela utilisait la théorie des files d'attente, donc des tables de Poisson, des choses comme ça., Évidemment, moi je comprenais ce que ça faisait, mais la plupart des gens qui l'utilisaient ne comprenaient pas ; comme c'était des tables, il y avait quand même des processus d'établis. J'ai fait ça pendant huit mois, ensuite je suis allé dans un autre département, toujours au trafic.

Bulletin AMQ — Là aussi il y a une logique ?

Yves Langlois — Oui, il y avait beaucoup de logique, beaucoup d'optimisation, mais moi ce que je trouvais, c'est que la mathématique était très cachée en dessous de tout ça. Sauf que quand on la comprenait, on pouvait peut-être faire des choses que la moyenne des gens

ne pouvait pas faire. Au niveau de l'optimisation, on pouvait aller plus loin. C'était des coûts phénoménaux, c'était des connections avec des fils, donc quand on changeait, quand on rebalançait les équipements, c'était des mois de travail avec des dizaines de techniciens dans un central. Ça pouvait coûter un million, on parle d'il y a 25 ans. Donc, c'était un travail très important, c'était toute la balance du trafic.

Ensuite, j'ai fait d'autres travaux, j'ai eu d'autres emplois autour du trafic, par exemple la gestion de ces équipements-là. Donc, beaucoup de collectes de données qui se faisaient, dans ce temps-là, avec des caméras et des fils. On avait des compteurs qui étaient tous alignés sur une baie de registres qui comptaient les appels avec une caméra. À toutes les demi-heures, il y avait une photo qui se prenait, le technicien envoyait le film au trafic, et nous on le développait. Après, on avait des adjoints qui additionnaient, faisaient les soustractions de registres pour compter le nombre d'appels par heure et mesurer la durée moyenne des appels. Avec nos tables de Poisson pour les files d'attente, on pouvait faire de la prévision et on pouvait déterminer que, par exemple, tel équipement dans telle centrale serait saturé en terme de capacité dans un an et demi, pendant la période la plus occupée. Parce qu'évidemment, dans le trafic il y a toute la question de coïncidence ou non-coïncidence des heures. Donc l'ingénierie est basée sur les pics. Un peu comme Hydro-Québec avec l'électricité, nous c'est au niveau de l'acheminement du trafic ; il y a des périodes de la journée qui sont plus occupées et il y a des périodes de l'année qui sont plus occupées. Il fallait vraiment suivre les périodes occupées et essayer de voir si ça bougeait et, de fait, ça bougeait d'une année à l'autre. Par exemple, à Montréal-Nord il y a beaucoup d'Italiens. Ce sont des gens qui ne font pas les mêmes choses que dans l'Ouest de l'île ; il y avait donc des heures occupées différentes. Dans les banlieues, c'était très différent, les heures occupées c'était le soir, donc il fallait faire l'ingénierie du réseau en fonction des heures de la journée. C'était très, très manuel, mais la base de tout cela était mathématique. C'était intéressant. Puis j'ai été promu assez rapidement et finalement je me suis retrouvé dans des postes de gestion. Le premier poste était un poste de gestion technique. J'avais des employés, mais c'était quand même assez technique. À mesure que j'ai avancé, ça été vraiment plus orienté vers la gestion, mais de la gestion dans un contexte technologique.

Bulletin AMQ — Je dois raconter ici que je t'ai vu récemment aux retrouvailles du Département de mathématiques de l'Université de Sherbrooke. Tu m'as parlé de ce que

tu faisais en disant : « J'ai passé ma vie à résoudre des problèmes chez Bell ». Pendant 27 ans, tu as résolu des problèmes ! C'est tout un programme et j'ai pensé tout de suite que je pourrais t'interroger là-dessus pour les lecteurs du Bulletin parce que tu as eu une carrière extraordinaire. Au fond, tu as été engagé pour résoudre des problèmes.

Yves Langlois — En un sens oui, mais je dois dire que j'ai été très chanceux parce que j'aimais tellement résoudre des problèmes que je me suis toujours trouvé dans des situations où j'étais le gars des tâches spéciales dans mon département à Bell Canada. Contrairement à beaucoup de mes collègues qui se retrouvaient dans des fonctions opérationnelles – par exemple, mes collègues ont typiquement 500 à 600 employés – j'ai toujours été affecté plutôt à des tâches spéciales où j'avais des équipes virtuelles, multidisciplinaires, pour régler des problèmes. Un problème ça peut être, par exemple, la consolidation de la surveillance ou de tout le processus de surveillance du réseau. J'ai fait un projet qui a duré deux ou trois ans où j'ai construit le centre de surveillance du réseau à Montréal.

Bulletin AMQ — Avec une petite équipe ?

Yves Langlois — Avec une équipe relativement petite, oui. Je dirais une vingtaine de personnes, mais si on inclut tous les gens qui ont travaillé indirectement, là c'est des centaines. Parce qu'évidemment il fallait construire le centre, et la construction ça prend du monde.

Bulletin AMQ — Mais pour la conception ?

Yves Langlois — Pour la conception, on parle d'une vingtaine de personnes. Il faut toujours structurer notre affaire, c'est un peu de la gestion de projet ; j'en ai fait beaucoup, mais il faut structurer notre affaire pour intervenir avec un nombre limité de personnes et il faut aussi avoir un processus qui fait que les choses se multiplient. Par exemple, dans un autre projet que j'ai réalisé, l'introduction de l'indicatif 450, il y a eu 1000 personnes qui ont travaillé là-dessus à Bell Canada. Tu ne peux pas travailler avec 1000 personnes, non, il faut différents niveaux d'équipes. L'équipe centrale, c'était cinq personnes. Après, il y avait une équipe étendue d'à peu près 35 personnes. Moi, je travaillais avec ces deux équipes-là. Mais chacun des 35 travaillait avec des centaines de personnes. Il fallait organiser ça. Chaque projet est différent, a une problématique différente, parfois c'est la complexité technique,

parfois c'est l'organisation ou autre chose. Mais moi, j'ai à peu près toujours fait ça, je me suis promené entre des postes opérationnels où j'avais vraiment une opération à gérer avec des employés. À un moment donné, j'identifiais un problème et je me disais : « Il faut qu'on règle ça ». Finalement mes patrons me disaient : « OK, tu vas le régler ». À coup de projets de deux ou trois ans, j'ai fini par faire ça toute ma carrière.

Bulletin AMQ — Donc sur 27 ans, 27 divisé par un peu plus que 2, tu as résolu une douzaine de problèmes ?

Yves Langlois — Une douzaine de problèmes.

Bulletin AMQ — De vrais problèmes ? De gros problèmes ?

Yves Langlois — Ils ne sont pas tous aussi gros, mais ce qui est une source de satisfaction pour moi aujourd'hui, c'est que quand je regarde en arrière, la plupart des choses que j'ai faites, même il y a très longtemps, existent encore aujourd'hui. Il y a des systèmes informatiques que j'ai implantés il y a presque 20 ans et qui existent encore aujourd'hui, sous une forme différente parce que la technologie a évolué. Par exemple, j'ai utilisé au tout début des PC et j'ai implanté un des premiers systèmes d'approvisionnement où on avait plusieurs applications qui parlaient à une même base de données. Aujourd'hui, c'est comme ça que tout est fait, mais dans le temps les ordinateurs étaient individuels.

Bulletin AMQ — Tu utilisais des bases de données relationnelles ?

Yves Langlois — Oui, plus ou moins relationnelles, ce n'était pas parfaitement relationnel, et les outils étaient dans le temps assez simplistes. On parle de D-Base III, IV, Clipper, des choses comme ça. L'avancée là-dedans, c'était que tout le monde pouvait se parler et partager la même information entre trois étages d'une même tour à bureau. Aujourd'hui, il n'y a personne qui pense que cela a déjà été un problème, mais dans le temps c'en était un. J'ai été dans l'évolution des premiers PC, je les faisais venir de Californie par train et c'était contre les politiques internes de l'Entreprise. Mes gars passaient des fils dans le plafond la nuit, on n'avait pas le droit de faire ça, pour connecter les ordinateurs ensemble et démontrer que ça pouvait se faire. Je me souviens qu'on avait fait une démonstration

à mon vice-président avec les gens de mon équipe où, au téléphone, on avait demandé à quelqu'un du 23e étage de changer quelque chose, une information, dans un fichier et il nous avait dit « OK, c'est changé » et là d'où on était, on est allé voir avec l'ordinateur et on voyait bien que c'était changé. Aujourd'hui, on rit de ça.

Bulletin AMQ — Le vice-président a été convaincu à ce moment-là ?

Yves Langlois — En fait, j'ai toujours été supporté dans mes projets. On poussait toujours un peu plus loin. Ce système-là existe encore aujourd'hui, ça fait quand même 20 ans, c'est intéressant.

Bulletin AMQ — Tu as été parmi les pionniers des méthodes nouvelles.

Yves Langlois — À l'université, même en mathématiques, on utilisait beaucoup les ordinateurs et je m'en étais servi aussi quand je travaillais au Service d'assainissement des eaux pour mon modèle de simulation. Quand je suis arrivé dans l'industrie, je regardais à quel point l'utilisation des ordinateurs était presque inexistante, c'était ridicule. Pourtant Bell Canada avait des ordinateurs centraux extrêmement puissants, mais c'était une chasse gardée, les groupes d'informatique ne voulaient pas de nous. Ils appelaient ça du « User Computing », ça n'était pas noble. Les centres de calculs étaient dédiés à la paye, à la facturation, aux actions, à ces choses-là, mais les gens qui travaillaient n'avaient pas le droit de faire de l'informatique. C'était extrêmement compliqué.

Bulletin AMQ — C'était vraiment une chasse gardée.

Yves Langlois — Ah oui, il fallait se battre.

Bulletin AMQ — Tu faisais venir des micro-ordinateurs de Californie et, au fond, il y avait un certain aspect subversif là-dedans.

Yves Langlois — Ah oui, absolument. J'aimais bien ça. J'aimais faire avancer les choses. Quand on sait ce que les maths et l'informatique peuvent faire et qu'on voit que les gens ne les utilisent pas, on se dit qu'il y a un potentiel terrible ; surtout dans une entreprise dont le but est d'optimiser les coûts, de faire les choses plus vite. Tu dis : « Hé ! Réveillez-

vous ! ». Puis l'industrie est souvent conservatrice, je trouve, et ce n'est pas particulier à Bell : les technologies ont mis du temps avant de « percoler » dans l'industrie. Peut-être moins aujourd'hui, parce que les communications sont plus rapides, mais je trouvais que l'entreprise était archaïque. Il y avait bien des affaires qui étaient archaïques, ça prenait du temps.

Bulletin AMQ — Mais tant que c'était un monopole, ce n'était pas trop grave ?

Yves Langlois — Je ne sais pas si c'était la raison. Il n'y avait peut-être pas assez de mathématiciens dans l'entreprise !

Bulletin AMQ — Un ingénieur a quand même des connaissances en mathématiques ?

Yves Langlois — Oui, mais c'est une approche différente. Les ingénieurs sont très pratiques, mais généralement beaucoup moins conceptuels.

Bulletin AMQ — Prétendrais-tu qu'il faut avoir un esprit moins pratique, moins immédiatement pratique, pour faire des choses qui comptent vraiment ?

Yves Langlois — C'est une bonne question. Je trouve qu'avec le temps, la plupart des gens oublient même ce qu'ils ont appris à l'école. J'ai des collègues, et je ne parle pas des ingénieurs en particulier, je trouve que les gens en général oublient des choses qui sont absolument fondamentales. Je ne peux pas penser qu'un mathématicien oublierait ces affaires-là. C'est sûr que moi, j'ai oublié 90 % des outils, mais je n'ai rien oublié des principes, absolument rien. Quand j'aborde un problème, j'essaie de le comprendre ! C'est bien stupide, peut-être que ça a l'air idiot, mais je trouve que la plupart des gens essaient d'aller à la solution trop vite avant d'avoir compris le problème. En mathématiques, tu ne peux pas faire ça : si tes hypothèses ne sont pas claires, si tu ne comprends pas d'où tu pars et d'où tu viens, tu ne peux pas avancer. En mathématiques, tu n'as pas le droit de prendre quoi que ce soit pour acquis, tu ne peux pas utiliser un théorème qui n'a pas été prouvé, sinon tout va tomber en morceaux. Ça marche comme ça dans la vraie vie aussi, même dans les contacts avec les autres personnes. Quand tu essaies de régler un problème, si tu ne l'as pas compris, ça ne sert à rien de chercher une solution. Je trouve qu'en général les gens

sont trop pressés, ils ne prennent pas assez le temps de *définir* les choses. Par exemple, il m'est arrivé souvent d'avoir des problèmes de processus qu'on essayait de régler en équipe, même des problèmes techniques. On discutait beaucoup et souvent les gens pensaient qu'ils étaient d'accord alors qu'ils ne l'étaient pas, ou au contraire pensaient qu'ils ne l'étaient pas sans se rendre compte qu'au fond ils l'étaient. C'était juste parce qu'ils ne s'entendaient pas sur ce dont ils parlaient, sur un mot.

Bulletin AMQ — Donc *définir* est primordial.

Yves Langlois — Oui. En fait, c'est l'approche de la mathématique. En tout cas, moi, ça m'a toujours servi et j'ai toujours senti que c'est quelque chose que j'avais, que les autres souvent n'exploitaient pas. C'est quelque chose que j'ai appris en étudiant les mathématiques. J'en avais une partie en moi, probablement parce que ça m'intéressait beaucoup personnellement, mais les cours m'ont permis d'intérioriser et de devenir conscient de l'approche mathématique. Je me souviens encore que dans certains de tes cours, ou les cours de certains autres profs, c'était un processus logique ; on commençait par poser la question : « Quel est le problème et qu'est-ce qui est donné, quelles sont les hypothèses que l'on va admettre ? C'est quoi les hypothèses. » Moi, je n'ai jamais oublié ça ! Face à un problème, j'applique la même démarche ; c'est une démarche qui est particulière aux mathématiques, ce n'est pas une approche d'ingénierie, pas du tout. Une approche d'ingénierie consiste généralement à utiliser des outils ou des principes connus, souvent avec des normes, puis de les appliquer en jouant avec les paramètres. L'approche des mathématiques, c'est de créer la formule. C'est complètement différent. C'est beaucoup plus fondamental.

Bulletin AMQ — Face à un problème nouveau, cette démarche, cet esprit est plus utile parce que finalement, il n'y a pas de formule au départ ?

Yves Langlois — Ça prend un mélange de toutes ces approches pour que les projets complexes fonctionnent, mais disons qu'en général, on ne prend pas le temps de se poser les questions fondamentales. C'est vrai dans tous les domaines. On veut passer à l'action. Pour moi, la date d'implantation dans un projet c'est important, mais à quoi ça sert si ce que l'on produit est de piètre qualité ? Dans l'industrie, ce qui est important c'est ce que tu vas livrer. Quand est-ce que tu vas livrer ? C'est sûr que c'est important, mais ce qui est encore

plus important, c'est qu'une fois que tu l'as livré, ça doit *survivre*. Pour que ça survive, il faut que tu l'aies mis sur des bases solides, donc tu ne prends pas la même approche pour régler les problèmes. Le développement durable, c'est pas juste pour les emballages...

Bulletin AMQ — Est-ce que c'est arrivé qu'il y ait eu de mauvaises solutions à des problèmes, des solutions qui n'ont pas duré ? Après ce que tu viens de dire, une mauvaise solution, c'est une solution qui ne dure pas.

Yves Langlois — Ça arrive, ça arrive tellement souvent que je prétends, et je le dis à qui veut bien l'entendre, que plus de la moitié du travail qu'on a à faire c'est de réparer quelque chose que quelqu'un a brisé. Ce n'est pas compliqué. Je me suis arrêté souvent pour penser à ça, c'est vrai, surtout dans une grande entreprise ; dans une petite, c'est peut-être différent. Je ne peux pas dire que mon environnement est le même que celui de tout le monde, mais on passe beaucoup de temps à réparer. Même dans la société, c'est un peu pareil. Il y a des gens, on dirait que quand la rigueur est passée, ils étaient cachés derrière la porte. La rigueur n'est pas valorisée aujourd'hui, ce n'est pas assez valorisé.

Bulletin AMQ — Et tu trouves que la rigueur c'est important ?

Yves Langlois — C'est fondamental, mais il ne faut pas utiliser que la rigueur. La meilleure médecine du monde utilisée à outrance peut s'avérer toxique, mais la rigueur c'est fondamental, c'est absolument important, mais ce n'est pas la seule chose évidemment. Avec le temps, j'ai appris que tu ne pouvais pas tout gagner par la logique seulement, parce que l'être humain n'est fondamentalement pas logique. Il y a une partie logique, mais une grande partie est émotionnelle. Réaliser cela fait partie de la logique, ça fait partie de l'analyse du problème. Quand j'étais jeune, j'étais naïf comme on est quand on a 20 ans ; je me disais que la logique, même dans ma vie personnelle, la logique c'est la chose la plus importante, mais un moment donné ça ne marche pas. Ça ne marche pas avec tout le monde également. On apprend qu'il faut faire un mélange, il faut doser ça, mais à l'inverse, il n'y a rien qui peut fonctionner sans logique.

Bulletin AMQ — C'est un vieux problème de Blaise Pascal, philosophe, analyste, mathématicien et un des premiers à avoir écrit en français moderne autour des années 1650.

Yves Langlois — Plutôt qu'en latin ?

Bulletin AMQ — Plutôt qu'en vieux français. Quand on lit Montaigne, qui est venu un siècle avant Pascal, on ne comprend pas toujours malgré que ce soit écrit en français, mais quand on lit Pascal, on comprend sa langue, c'est la langue moderne. Pascal est l'un des créateurs de la langue moderne. Pascal parlait de l'esprit de géométrie et de l'esprit de finesse, deux affaires complètement différentes. Il dit que dans *l'esprit de géométrie* – c'est ton esprit logique – on agit selon un nombre très limité de principes, alors que dans *l'esprit de finesse*, il y a une multitude de principes, il y en a tellement qu'on ne peut pas les embrasser tous d'un seul coup avec l'esprit de géométrie. On est donc obligé de laisser tomber la logique pure, d'avoir une espèce de sensibilité spéciale, une intuition globale qui guide notre action. C'est intéressant de voir que tu retrouves cette idée. Il faut tenir compte de la complexité de certains problèmes. Mais les mathématiques peuvent aussi servir à maîtriser la complexité. C'est ce que tu as fait, au fond.

Yves Langlois — Indirectement peut-être, mais ce que j'ai utilisé le plus dans ma carrière, c'est l'approche mathématique pour régler des problèmes. J'ai senti que j'ai influencé beaucoup les gens autour de moi. Pas tout seul, mais souvent deux, trois personnes qui pensent de la même façon, mais d'une façon très différente d'un groupe, finissent par l'influencer. Par exemple, gérer avec des faits, ça semble assez simple, assez logique, mais il y a des années, malgré le fait qu'il y avait beaucoup d'informations disponibles, souvent les gens ne géraient pas en se basant sur des *faits* mais sur des *anecdotes*.

Bulletin AMQ — Quelle différence fais-tu entre *fait* et *anecdote*, qu'est-ce qu'un fait ?

Yves Langlois — Un fait, c'est quelque chose qu'on peut mesurer d'une certaine façon, quelque chose sur lequel plusieurs personnes, avec un point de vue différent, peuvent s'accorder pour dire que c'est un objet. On peut le regarder de plusieurs points de vue, mais il est là. Un fait, c'est aussi quelque chose de répétitif, par exemple si tel phénomène est arrivé la moitié du temps, on peut décrire cette situation comme un fait. Dans le passé, les gens géraient beaucoup avec des « vieilles histoires de ma grand-mère » et lorsqu'on a essayé de les vérifier, on a réalisé que ce n'était pas vrai, que c'était basé sur des anecdotes. Une anecdote, c'est souvent un événement assez exceptionnel pour qu'on s'en rappelle. Il

faut éviter le piège d'en faire une généralité. Mais cette approche a souvent servi à ceux qui voulaient maintenir un certain pouvoir. Les gens les plus expérimentés avaient droit de regard sur à peu près tout, prenaient des décisions pas nécessairement basées sur de l'information ou sur des bases solides. Moi, j'ai vu l'évolution des mentalités. Les ordinateurs et les bases de données nous ont amenés progressivement vers une façon plus rationnelle de gérer. J'ai travaillé dans un département pendant 7 ou 8 ans avec certains de mes collègues qui avaient une approche très semblable à la mienne et on a réussi à changer la façon de faire, la façon dont on gère l'entreprise. Là on parle de 3000 personnes qui dépensent un milliard par année ; ça compte. La rigueur devrait avoir sa juste place.

Bulletin AMQ — Donc une anecdote, c'est quelque chose d'unique au fond, ça arrive une fois comme ça ?

Yves Langlois — Ça arrive une fois et puis c'est interprété d'une certaine façon, ça peut être mis en dehors du contexte et c'est souvent perçu comme une habitude. Une anecdote, ça ne veut pas dire que ça va se répéter. Souvent le monde change et si on ne le mesure pas, si on ne mesure pas le changement, on vit encore avec les vieilles hypothèses. Si on ne se rend pas compte que le monde change, on fait de mauvais choix.

Bulletin AMQ — Un fait, c'est donc quelque chose qu'on peut, d'une certaine façon, mesurer, c'est un objet dont on peut faire le tour, qu'on peut regarder de différents points de vue. Ça me rappelle une phrase que je n'ai jamais oubliée de Poincaré : « La science se fait avec des faits, mais un ensemble de faits n'est pas plus de la science qu'un tas de pierres n'est une maison ».

Yves Langlois — C'est très vrai. Oui, parce qu'avec le même tas de pierres tu peux construire plusieurs sortes de maisons. Tu ne peux pas regarder chaque pierre et voir une maison, mais quand tu les as assemblées, tu as quelque chose qui était imprévisible avec les pierres seules. C'est la construction qui est la science.

Bulletin AMQ — J'aurais deux questions pour finir. Une question plus spécifique : dans ta formation secondaire, collégiale ou universitaire, est-ce qu'il y a des choses que tu aurais aimé faire, qui t'auraient été utiles par la suite, et que tu n'as pas faites ? Des cours, des notions

à propos desquelles, après coup, tu te dis par exemple « si j'avais fait ça au secondaire, ça m'aurait été utile » ?

Yves Langlois — En terme de contenu, je ne pourrais pas identifier quelque chose en particulier en disant : « Ça, ça m'a manqué, parce que si je l'avais eu, j'aurais eu un outil de plus pour travailler ». Par contre il y a la façon dont ça a été fait. Je pense que ça aurait pu m'accrocher et m'intéresser beaucoup plus. C'est toujours, encore une fois, le lien entre les mathématiques et l'application des mathématiques. Je me souviens qu'il y avait un cours d'histoire des mathématiques dans le programme. Je trouve qu'on aurait dû en faire plus et aussi d'une façon différente. Quand on regarde ce que Newton a fait, c'est absolument extraordinaire, et il me semble qu'il y aurait moyen de créer un intérêt bien plus grand pour la mathématique de Newton en présentant le contexte dans lequel il a travaillé et les outils qu'il avait pour cela. De quoi est-il parti ? Qu'est-ce que cela lui a permis de faire ? Je pense qu'on pourrait attirer beaucoup plus de gens vers les mathématiques comme cela. L'autre point, c'est que dans les cours eux-mêmes, quand on apprenait une technique, souvent on le faisait trop indépendamment de son applicabilité. Moi, j'aurais aimé plutôt qu'on parte d'un problème. J'aurais aimé qu'on arrive au début d'un cours puis qu'on dise : « Le but de ce cours-là, c'est d'apprendre à faire telle ou telle chose : quand tu auras fini, tu vas être capable de construire une maison, ou tu vas être capable de faire la plomberie dans une maison, ou tu vas comprendre l'électricité dans une maison ». C'est un exemple que je donne pour un cours de technique. En mathématiques, c'est sûr qu'à un moment donné, quand c'est pur, c'est quand même loin de l'applicabilité, mais il y a toujours des liens. Je trouve que dans le temps – les choses ont probablement changé – on ne faisait pas assez de liens avec les applications. Ça c'est une chose que je trouve qui m'a manqué. Et la bonne nouvelle, c'est qu'il y a quand même de l'intérêt pour les sciences dures. J'ai déjà lu que le livre de Stephen Hawking *Une brève histoire du temps* est un des livres scientifiques les plus vendus... C'est pas rien ça !

Mais ma plus grande frustration ne concerne pas la formation que j'ai reçue, mais plutôt ce que j'ai fait avec. Tu vois, j'aurais aimé avoir plus de talent et faire vraiment des maths. J'aurais aimé être aussi brillant que certains étudiants de ma classe. J'aurais vraiment « fait » des mathématiques. D'ailleurs pour faire un mathématicien, ça prend plus que trois ans d'université, ça prend une vie, et c'est pour ça d'ailleurs que je ne me considère pas

comme un mathématicien.

Bulletin AMQ — Tu ne devrais pas, tu es un mathématicien. Il y a beaucoup de mathématiciens et ces mathématiciens c'est comme les gens, ils vivent leur vie dans des contextes variés. Je considère que tu es un mathématicien.

Yves Langlois — Ce que je voulais dire, c'est qu'il est arrivé régulièrement dans mon travail des situations où j'aurais aimé savoir comment les mathématiques auraient pu m'aider à régler un problème. Il m'est arrivé quelquefois d'embaucher des mathématiciens pour régler des problèmes. Il y a des choses que j'aurais aimé connaître, comme par exemple toute la question d'intelligence artificielle. J'ai l'impression que, quand j'ai fini mon bac, je n'avais pas une vue globale de l'univers des mathématiques. J'avais fait de l'algèbre, j'avais fait de l'analyse, j'avais fait des méthodes numériques, j'avais fait des stats, mais je n'avais pas de globalité, je n'avais pas d'idée si ce que j'avais vu représentait 40 % du territoire, 4 % ou 90 % ? En terme de « stock » comme on dit en anglais.

Bulletin AMQ — Il n'y a aucun mathématicien actuellement qui domine toutes les mathématiques. Je pense quand même que dans les années 1970 il y avait dans les universités des programmes de mathématiques équilibrés où justement on essayait de montrer l'ampleur du sujet. À Sherbrooke en particulier, on avait un programme de maths appliquées, on faisait attention aux applications plus que dans d'autres programmes, d'autres universités par exemple. Moi, quand j'ai fait mon cours, c'était un cours de maths pures, et les applications il n'y en avait pas. Il y en avait quand même un peu, on a fait des équations aux dérivées partielles, des choses comme ça, mais vous avez été, je pense, assez bien servi de ce côté-là.

Yves Langlois — Ça c'est vrai, je dois l'avouer. J'ai des amis qui avaient fait des cours en mathématiques dans d'autres universités et ils n'avaient pas fait la moitié de ce que j'ai fait. Ils ont fait peut-être plus en profondeur certaines choses, mais c'était moins vaste que ce que nous on avait fait. Pour moi, c'était plus une question d'avoir une vue d'ensemble, peut-être que je l'avais sans avoir l'impression que je l'avais. C'est un « feeling » que j'ai eu. Par exemple, c'est comme quelqu'un qui aurait beaucoup voyagé, mais qui n'a jamais vu la mappemonde. Il ne peut pas savoir s'il a tout vu ; c'est un peu ça mon idée.

Bulletin AMQ — Au fond, c'est ce que donne une formation générale. Le but du cégep, c'est de donner une mappemonde pour l'ensemble des connaissances. Le but d'un bac en maths, c'est d'avoir une mappemonde pour les maths. On fait un zoom sur les maths et on veut une vue d'ensemble avant d'aller trop loin dans cette direction, mais on peut rater son affaire. Les programmes universitaires peuvent passer à côté, mais c'est leur but.

Yves Langlois — Mais à bien y penser, je pense que ça été réalisé, parce que si j'ai pu faire des choses que je détestais et des choses que j'aimais, ça veut dire qu'on a vu plein de choses !

Bulletin AMQ — J'ai déjà entendu un grand mathématicien, Jean-Pierre Kahane, dans un congrès sur l'enseignement des maths, dire que « au fond les programmes à l'université pour former des mathématiciens, ce n'est pas si important que ça. Les étudiants n'ont pas tellement besoin de programmes, mais ils ont besoin de professeurs. S'ils ont des professeurs, ils vont apprendre ce qu'il faut, mais s'ils ont un beau programme, mais pas de profs adéquats, ils n'apprendront pas ce qu'il faut ». J'ai trouvé ça un point de vue intéressant. Parce que à travers les cours, ce que vous avez vu au fond, ce sont des profs qui avaient une façon de voir et de faire les choses.

Yves Langlois — Absolument, oui, je suis d'accord avec ça. Les profs, c'est absolument essentiel. C'est au moins aussi important que la matière elle-même.

Bulletin AMQ — Aurais-tu un message à laisser à nos lecteurs ?

Yves Langlois — Un des messages que je leur laisserais, c'est que ce qu'ils font est absolument fondamental. Enseigner les maths, c'est la base, c'est une connaissance qui dure aussi longtemps que la personne vit, contrairement à plein d'autres choses qui ont une valeur dans le temps qui est très, très relative, qui ne dure pas longtemps. On peut apprendre un paquet de choses, mais avec la technologie qui évolue si vite aujourd'hui, la durée de vie des connaissances est de plus en plus courte. Ce qu'on apprend en mathématiques, ça dure pour toujours, c'est un outil irremplaçable, et d'après moi c'est aussi important que la philosophie. Malheureusement j'ai l'impression que ces deux matières si différentes en surface, mais si proches quant à leur rôle pour aider à former une personne, n'ont pas le

niveau d'appréciation qu'elles devraient avoir dans le public en général. Si l'on mettait plus l'accent sur la formation que sur l'acquisition de connaissances, ça pourrait changer la vie de bien du monde.

Bulletin AMQ — Et de bien des organisations ?

Yves Langlois — Et de bien des organisations, oui. Le truc serait de réussir à attirer en mathématiques des étudiants qui ne se destinent pas nécessairement vers l'enseignement ou la recherche. Je me souviens qu'au moment de faire mon choix pour entrer à l'université, je ne savais vraiment pas quoi choisir, et un professeur du collège m'avait conseillé d'aller en mathématiques dans ce cas en me disant que ça m'ouvrirait toutes les portes. Il avait raison et c'est probablement l'un des meilleurs conseils que j'aie reçus.

S'il y avait dans les entreprises et partout ailleurs plus de gens avec une formation en mathématiques, je pense que la société s'en porterait bien mieux.

Bulletin AMQ — Comme tu le sais peut-être, on fait le contraire dans beaucoup de programmes de cégeps, en particulier dans les programmes techniques et en sciences humaines ; depuis une quinzaine d'années, on évacue tout simplement les cours de mathématiques, prétextant, dans les programmes techniques par exemple, que les profs de techniques sont mieux placés pour faire les mathématiques nécessaires à leur technique. On évacue tout cet aspect dont tu parles, la rigueur, la façon de voir, etc. On évacue ça pour regarder juste le niveau horizontal. On a besoin de telle technique pour faire telle chose, on va leur montrer ça, et si on pense que quelque chose n'a pas une utilité immédiate, on ne le fait pas. C'est malheureusement le mouvement actuel et toi, comme tu as toujours fait dans ta vie, tu vas contre le courant.

Yves Langlois — Absolument, c'est l'obsolescence. Ce que les étudiants apprennent ne vaut plus rien s'ils n'ont pas appris à construire quelque chose ; ils auront juste appris à appliquer des formules.

Bulletin AMQ — Tu considères qu'il faudrait qu'il y ait plus de monde qui apprenne à construire des choses.

Yves Langlois — Oui.

Bulletin AMQ — Et que c'est possible qu'une majorité de gens atteigne ce niveau-là.

Yves Langlois — Absolument.

Bulletin AMQ — Parce que d'autres disent : « Ça c'est vrai, c'est bon pour l'élite, pour un petit nombre ». Ils ne sont pas contre, mais seulement pour un petit nombre parce qu'ils disent : « Bon, des dirigeants on en a besoin, mais moins que des gens qui appliquent des formules ».

Yves Langlois — Le monde n'est pas aussi binaire que ça. Il n'y a pas que les dirigeants et les autres. Il y a des tonnes de gens avec des responsabilités diverses qui sont organisés dans un réseau d'interrelations très complexe. Même le simple employé qui travaille dans son coin et qui applique une formule peut apporter beaucoup plus à son entreprise s'il la comprend et s'il peut exercer son jugement. On a dépassé depuis longtemps l'ère du Taylorisme. Aujourd'hui les entreprises ont besoin que tous les employés se servent de leur initiative. Tu serais surpris de voir combien de haut dirigeants appliquent des formules toutes faites et combien de « simples » employés se cassent la tête pour améliorer les processus et convaincre leurs dirigeants que certaines décisions qu'ils prennent n'ont pas de sens.

Ç'est certain que tout le monde ne construit pas des choses également complexes, mais tout le monde a quelque chose à construire.

De toute façon, si on le prend au sens littéral du terme, dans une entreprise comme Bell, il y a beaucoup de dirigeants. Et les problèmes sont complexes. Il y a la technologie, la gestion de la qualité, la productivité, la gestion du capital et des dépenses, le financement, les ressources humaines, les communications, les systèmes d'information... À un moment donné, il faut organiser tout ça, dans un contexte où tout change à une vitesse grand V.

Il n'y a aucun programme qui donne à quelqu'un les connaissances pour faire face à tout ça. J'ai travaillé la majeure partie de ma carrière dans un environnement d'ingénierie et pourtant je n'ai pas fait de cours en génie ; c'est une connaissance qui ne m'a jamais manquée. Pourquoi ? Parce que quand on s'attaque à un problème, il faut de toute façon regarder ce qu'est le problème : c'est quoi les paramètres, c'est quoi le langage. L'ingénierie, c'est un langage, mais il y a d'autres langages. Les ressources humaines, c'est un autre

langage, et c'est un autre type de problème.

Et si on revient à la question qui concerne les dirigeants et à ce que j'observe dans mon environnement de gestion, on peut dire qu'on oublie assez rapidement les connaissances qu'on acquiert et que, de toute façon, le monde change tellement vite que leur vie utile raccourcit de plus en plus rapidement. C'est le cas de la plupart de mes collègues de génie qui exercent des postes de direction dans un environnement technologique : ce qu'ils ont appris ne sert à peu près plus à rien, parce que ça a tellement changé. Ce qui leur est le plus utile, c'est la méthodologie qu'ils ont assimilée lorsqu'ils ont vu dans l'ensemble de leurs cours comment un ingénieur pense devant un problème.

D'une façon générale, je pense qu'une formation mathématique donne une façon rationnelle de voir les choses qui dure toute la vie, alors que les connaissances techniques ont une durée de vie beaucoup plus limitée.

Bulletin AMQ — Sur ce message positif, je te remercie beaucoup de cette intéressante entrevue.

Yves Langlois — Ça m'a fait un grand plaisir.

Un exemple de problématique rencontrée chez Bell au cours de ma carrière

Yves Langlois

Le contexte global

Il y a environ trois ans, mon unité d'affaires était aux prises avec un problème de plus en plus critique. Dans les mois qui ont suivi l'explosion de la bulle technologique, la majorité des entreprises qui ont survécu se sont retrouvées dans une situation où il était de plus en plus difficile d'obtenir du capital sur le marché financier.

Les entreprises avaient investi énormément et les investisseurs étaient de plus en plus hésitants. Les analystes financiers et toute l'industrie avaient réalisé l'importance de balancer les investissements de capital avec le niveau de revenu. Ça semble naturel et surtout

évident, mais il faut se rappeler que, durant cette période, beaucoup de gens investissaient dans des entreprises qui n'avaient pas nécessairement une santé financière solide. Cette attitude créait un mouvement de hausse artificielle de la valeur des actions, ce qui attirait encore plus d'investisseurs... Un cercle infernal !

Les analystes financiers, qui ont beaucoup d'influence sur la communauté des investisseurs (trop, de l'avis de beaucoup), utilisent aussi des formules pour évaluer la santé d'une entreprise et conseiller les investisseurs. Ça prend souvent la forme de ratios et les ratios « importants » changent au cours des cycles économiques et des modes. Au sortir de l'explosion de la bulle, le ratio des ratios était « l'intensité du capital », exprimé en capital dépensé divisé par les revenus bruts de l'entreprise.

Toutes les entreprises étaient donc scrutées à la loupe et la mienne n'y faisait pas exception. Pour mon entreprise cependant, ce ratio est le résultat de sommes énormes : bon an mal an, le budget annuel de mon service était de l'ordre de plusieurs centaines de millions de dollars.

Et l'arithmétique est très simple : si tes revenus sont plus faibles qu'anticipés, tu dois réduire tes investissements dans la même proportion si tu ne veux pas te retrouver avec un problème grave. Lorsque le président s'engage à rencontrer un objectif auprès du conseil d'administration et de la communauté des investisseurs, il faut que ça arrive...

Lorsque la concurrence s'intensifie, ça exerce une pression à la baisse sur les revenus, soit à cause d'une perte de part de marché, soit à cause de marges de profit moins grandes engendrées par la réduction des tarifs.

D'autre part, à cause de l'évolution rapide de la technologie, il *faut* investir des sommes énormes pour offrir les nouveaux services sur un territoire très vaste.

En fin de compte, tout ceci exerce des pressions sur le budget de capital pour soutenir la croissance normale du réseau, ce qui constitue environ la moitié du budget de mon service.

Le contexte local

Le financement du budget de capital de mon service pour la croissance est effectué par un groupe corporatif qui utilise un modèle tenant compte de prévisions économiques, d'historiques de consommation de capital, d'historiques de coûts des équipements approvisionnés, ainsi que de la consommation moyenne de chacun des services vendus en termes

d'équipements de réseau. Le groupe de gestion du capital fait tourner le modèle à chaque année et alloue le budget de capital pour l'année par secteur géographique.

Le modèle utilisé par la corporation n'est pas différent de tous les modèles, en ce sens qu'il comporte des faiblesses qui ont parfois des effets dramatiques selon le contexte. Pour les régions dont les caractéristiques s'éloignent de la moyenne, les résultats peuvent être carrément inacceptables.

Il s'ensuit alors une série de négociations où chacun y va de ses arguments, ce qui crée une compétition parfois malsaine puisque l'enveloppe totale n'augmentera pas, avec comme conséquence qu'une région va augmenter son budget au détriment des autres. Avec le temps s'installent un climat de méfiance ainsi qu'un manque de transparence qui font qu'il est parfois difficile de s'y retrouver et d'assurer que les investissements sont alloués aux bons endroits.

Avec la pression de plus en plus importante sur l'enveloppe globale de capital, cette situation était devenue intenable. Au cours d'une réunion du Service d'approvisionnement du réseau, mes collègues m'ont demandé si je pouvais tenter d'améliorer ce processus afin de le rendre plus rigoureux.

Les éléments de base de la problématique

Afin d'augmenter les chances de succès de cette initiative, il fallait tenir compte des considérations suivantes :

- Quelles que soient les améliorations que nous apporterions au modèle corporatif, il ne serait jamais parfait et, par conséquent, il y aurait toujours des situations où le résultat devrait être ajusté ;
- La dynamique de compétition entre les entités géographiques ne pourrait être changée puisque nous allions développer un modèle qui réallouerait les sommes proposées sans toutefois augmenter l'enveloppe globale. Par contre, si nous réussissions notre pari, l'atmosphère ainsi que la dynamique dans laquelle cette compétition s'exercerait feraient en sorte que l'exercice pourrait être positif ;
- Une grande partie du succès devrait reposer sur la confiance. Cette dernière dépendait de plusieurs facteurs, dont le sentiment d'appartenance aux décisions ainsi que la compréhension du fonctionnement du modèle que nous allions proposer.

L'approche prise pour développer le modèle

En tenant compte de tout ce qui précède, j'ai privilégié l'approche suivante :

- J'ai formé une équipe virtuelle avec des candidats choisis pour leur niveau d'expertise, d'expérience ainsi que de crédibilité. Chaque entité géographique avait un membre dans l'équipe ;
- Nous avons mis des règles en place au départ. Entre autres, leur mandat n'était pas de veiller aux intérêts de leur entité, mais plutôt de contribuer au développement d'un modèle et d'un processus d'allocation avec lequel ils devaient éventuellement être à l'aise quelle que soit la position qu'ils pourraient avoir dans l'équipe. Le problème était celui du département et non celui d'un ensemble d'entités ;
- Nous nous sommes entendus sur l'indicateur qui devait être optimisé par le modèle, c'est-à-dire le taux de « services différés ». (Il s'agit de calculer le ratio de commandes de service pour lequel nous ne pouvons pas rencontrer la date d'approvisionnement standardisée parce qu'il n'y a pas d'équipement disponible et donc que le processus d'approvisionnement n'a pas fonctionné correctement) ;
- Ce sont eux qui ont défini les paramètres du modèle. Je me suis contenté de les diriger dans leur cheminement logique, et je me suis assuré que les besoins d'affaires étaient discutés en premier lieu, et la mathématique ensuite. On a donc traduit leurs idées, on a validé leurs perceptions à l'aide des outils mathématiques plutôt que de développer un modèle qu'on aurait essayé de leur vendre ensuite ;
- Nous avons d'abord examiné le fonctionnement du modèle corporatif existant pour en dégager les forces ainsi que les faiblesses. Comme notre modèle ne serait pas utilisé à la place du modèle corporatif mais en aval, il était inutile de reproduire dans notre modèle des éléments déjà considérés en amont ;
- Nous avons introduit la notion de *risque*, que nous avons traduit par un facteur selon lequel une entité recevrait plus de fonds qu'une autre si son niveau de risque calculé s'avérait plus élevé que les autres. Cette notion visait à compenser le phénomène qui fait que les entités à forte croissance obtiennent des fonds qui permettent non seulement de supporter le gain, mais également de réagir plus facilement aux fluctuations sans l'apport de fonds supplémentaires ;
- Nous avons ensuite identifié une série de facteurs *mesurables* qui de l'avis des membres

de l'équipe pouvaient avoir une influence sur le niveau de risque et d'investissements requis. Il ne s'agissait pas ici de juger de la valeur de tel ou tel facteur, mais plutôt d'inclure dans la liste tous les facteurs jugés pertinents par au moins un des membres sans nécessairement qu'il y ait consensus ;

– Nous avons ensuite effectué des tests de corrélation entre ces facteurs et l'indicateur de services différés, ainsi que celui du risque. Nous avons représenté ces résultats graphiquement en « cachant » les noms des régions au départ. Cet exercice a permis d'éliminer certains facteurs ou de relativiser leur poids sur l'ensemble ;
– Nous avons ensuite construit un modèle (relativement) simple qui réallouait le capital par entité en fonction du risque relatif de chacune d'elle, celui-ci étant calculé en utilisant un mécanisme de pondération pour chacun des facteurs ;
– Nous avons ajouté des paramètres d'ajustement de l'importance du risque pour le taux de ré-allocation, ainsi que pour la pondération de chacun des facteurs sur l'ensemble ;
– Nous avons développé un modèle « multiplicatif » et un modèle « additif » pour voir lequel des deux se comportait le mieux. Ensuite nous avons joué avec les facteurs de pondération jusqu'à ce qu'un consensus émerge.

L'application du modèle

Deux mois après la formation de l'équipe, nous avons utilisé le modèle pour la première fois, avec l'engagement formel que l'équipe viendrait à la rescousse d'une entité si jamais l'allocation fournie s'avérait insuffisante.

Nous avions entre autres mis en place un mécanisme de suivi trimestriel du risque qui nous permettait d'ajuster le tir en cours d'année.

Au cours des deux dernières années, nous avons bien sûr ajusté, ajouté ou retiré certains paramètres. C'est toujours la même équipe qui gère l'allocation de capital à l'intérieur du service et cela se passe très bien.

Les effets positifs de cette initiative se sont fait sentir au-delà de la gestion interne puisque l'augmentation de notre niveau de crédibilité a eu comme conséquence qu'il est dorénavant plus facile d'augmenter l'enveloppe globale en utilisant des arguments plus convaincants auprès des groupes de finance.

Une autre conséquence positive est qu'étant donné que nous avons dorénavant des

mécanismes de suivi du risque, une meilleure crédibilité, ainsi qu'une meilleure « atmosphère », les gens sont plus portés à prendre des risques, parce qu'ils savent qu'on ne les laissera pas tomber si ça chauffe. Le résultat net, c'est que nous avons réussi des réductions budgétaires de l'ordre de dizaines de millions par année. Pas mal non plus...

Yves Langlois, août 2005.

Mathématiques et civilisation

André Ross
Cégep de Lévis-Lauzon

Cartographie terrestre et céleste

Nous avons tous déjà regardé un globe terrestre, des cartes de différents pays, admiré des photos prises par satellite, vu des images prises à l'aide d'un télescope ou par des sondes spatiales. Toutes ces images et photos nous ont permis de développer graduellement une représentation mentale de notre univers.

Quelle serait notre représentation de l'univers si nous n'avions pas observé toutes ces images ?

Le monde habitable tel que le concevait Hécatée de Milet, qui vécut vers ∼515, ressemblait à la carte suivante. On considère habituellement que ce système de représentation du monde habitable à trois continents entourés d'eau a été transmis des Grecs aux Romains puis à la Chrétienté médiévale.

Le modèle de cette carte représentant dans un cercle trois continents entourés d'eau a été utilisé jusqu'au Moyen Âge. Dans la Chrétienté médiévale, cette pratique était liée à l'histoire de Noé dont les trois fils auraient peuplé chacun un continent.

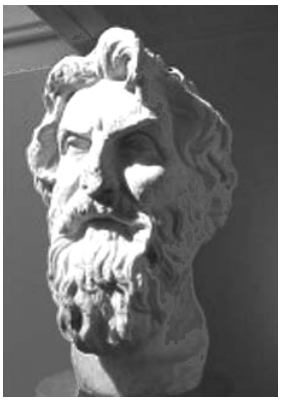
Au XVI^{e} et au XVII^{e} siècles, la traduction des ouvrages de Ptolémée et les grandes explorations contribueront à l'apparition de nouvelles cartes tracées grâce au système de longitude et de latitude. En les comparant aux *mappae mundi* circulaires du Moyen Âge, on supposera alors que les lettrés de cette époque considéraient que la Terre était un disque rond posé sur l'Océan. Ce mythe de la *Terre plate* n'est cependant pas appuyé par les textes accompagnant les *mappae mundi*. Au contraire, les textes plaident en faveur d'une terre sphérique.

Les premières cartes géographiques ont cependant été construites à l'aide des informations obtenues par les marchands, les voyageurs, les ambassadeurs et les soldats ayant participé à des expéditions guerrières. Tout naturellement les concepteurs de ces cartes se sont placés au centre du monde habitable et les cartes sont plus détaillées autour de la Méditerranée.

Nous allons rappeler les principales découvertes du monde grec qui ont permis l'évolution de la représentation de l'univers et du monde habitable. Cela nous permettra de comprendre en quoi les cartes médiévales représentaient un recul par rapport à l'héritage du monde grec.

Aristarque de Samos

Aristarque est né à Samos vers ∼310 et est décédé vers ∼230.



Le seul ouvrage d'Aristarque qui a été conservé est un petit traité intitulé *Sur les dimensions et distances du Soleil et de la Lune*. Il y décrit comment il a cherché à déterminer ces

distances et dimensions et les résultats qu'il a obtenus. Il fut le premier à proposer un système héliocentrique, c'est-à-dire un système centré sur le Soleil. Ce système eut un certain succès mais fut rejeté principalement pour deux raisons.

La première de ces raisons est l'absence de parallaxe visible. On croyait que les étoiles fixes étaient beaucoup plus proches et que les constellations apparaîtraient déformées si la Terre se déplaçait autour du Soleil. On peut faire l'expérience de ce que signifie l'absence de parallaxe de la façon suivante :

- tendre le bras, index levé, et, en regardant en direction de l'index, fermer alternativement l'oeil droit et l'oeil gauche. Observer comment la position apparente de l'index semble varier par rapport aux objets à l'extrémité de la pièce.
- demander à une autre personne d'aller à l'extrémité de la pièce et de tendre son index. Fermer alternativement l'oeil droit et l'oeil gauche. Observer comment la position apparente de l'index ne semble pas varier par rapport aux objets à l'extrémité de la pièce (lorsqu'on est seul dans la pièce, on peut faire la même chose en considérant un objet plus rapproché).

En fermant alternativement un oeil, c'est comme si on changeait de point d'observation. La position du doigt semble changer par rapport aux détails sur le mur. Cependant, si le doigt est très éloigné de l'observateur, cette impression disparaît. Cette simple expérience illustre que : si la Terre est en mouvement, il faut que la sphère des étoiles soit très éloignée pour que ce déplacement ne se traduise pas par une déformation des constellations. On a longtemps considéré que la sphère des étoiles fixes était contiguë à celle de Saturne, la plus éloignée des planètes connues à l'époque. On ne pouvait se résoudre à ce que la sphère des étoiles fixes soit très éloignée, car il aurait alors fallu envisager qu'il y avait un grand espace vide entre la sphère de Saturne et la sphère des étoiles fixes. L'existence du vide était incompatible avec la conception de l'univers d'Aristote. Celui-ci avait développé plusieurs raisonnements par l'absurde pour démontrer l'impossibilité du vide.[1]

La deuxième raison est que l'élément « terre », le plus lourd des quatre (terre, eau, air et feu), devait être au centre de l'univers. Cela permettait d'expliquer la gravité. Les corps lourds (appelés graves, comme les notes de musique) cherchaient à rejoindre leur place naturelle au centre de l'univers et cela expliquait la chute des corps.

[1] Raisonner par l'absurde ? Quelle idée !, André Ross, Bulletin de l'AMQ, volume 45, no 1, mars 2005.

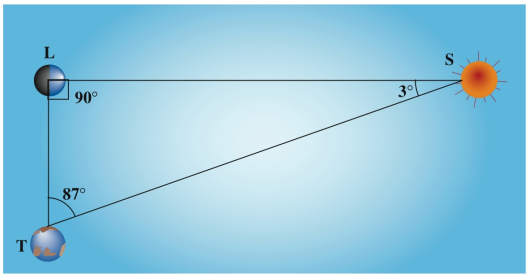
POSTULATS D'ARISTARQUE

Aristarque est né douze ans après la mort d'Aristote et dans son ouvrage il a procédé selon le modèle de construction de la connaissance élaboré par Aristote[2] en établissant des postulats à partir de l'observation et en utilisant le raisonnement par déduction pour « *reproduire dans le langage et dans la pensée la complexité d'ensemble de l'organisation des choses* ». Dans son étude des distances célestes, Aristarque pose d'abord les six postulats suivants :

1. La Lune reçoit sa lumière du Soleil.
2. La Lune se déplace comme si elle était sur la surface d'une sphère dont la Terre est le centre.
3. Lorsque la moitié de la Lune est éclairée, le grand cercle qui sépare la partie sombre de la partie éclairée est dans la direction de notre oeil[3].
4. Lorsque la moitié de la Lune est éclairée, l'angle formé par les directions de la Lune et du Soleil est de 87° [4].
5. La largeur de l'ombre de la Terre à la distance où la Lune la traverse lors d'une éclipse est de deux fois la largeur de la Lune.
6. La portion du ciel que la Lune couvre en n'importe quel moment est le quinzième d'un signe du zodiaque (cette mesure est erronée).

Voici son raisonnement pour déterminer les distances relatives Terre-Lune et Terre-Soleil.

La Terre, la Lune et le Soleil forment un triangle dans l'espace. Lorsque la moitié du disque lunaire est éclairée, l'angle au sommet occupé par la Lune doit être de 90°.



[2]Logique aristotélicienne, du concept au raisonnement, André Ross, Bulletin de l'AMQ, volume 44, no 3, octobre 2004.

[3]La frontière entre la zone éclairée et la zone d'ombre est alors une droite.

[4]La valeur réelle est de 89° 52′.

Selon son quatrième postulat, l'angle en T mesure 87° (en notation moderne). L'angle en S est donc de 3°.

Il lui faut alors évaluer le rapport des côtés dans un triangle rectangle ayant de tels angles. En notation moderne, il doit évaluer le sinus d'un angle de 3°, soit le rapport du côté opposé à cet angle et de l'hypoténuse. Il estime que :

$$\frac{1}{20} < \sin 3^\circ < \frac{1}{18} \quad [5]$$

Le côté opposé à l'angle de 3° est la distance Terre-Lune (TL) et l'hypoténuse est la distance Terre-Soleil (TS). Il obtient donc :

$$\frac{1}{20} < \frac{TL}{TS} < \frac{1}{18}$$

En considérant la première inégalité, il détermine :

$$\frac{1}{20} < \frac{TL}{TS}, \text{ d'où } TS < 20\ TL$$

La deuxième inégalité donne :

$$\frac{TL}{TS} < \frac{1}{18}, \text{ d'où } 18\ TL < TS$$

Il conclut que la distance Terre-Soleil est entre 18 et 20 fois la distance Terre-Lune. Pour la première fois dans l'histoire, Aristarque a déterminé par une approche rationnelle une estimation du rapport des distances Terre-Lune et Terre-Soleil. Cependant, ses instruments de mesure n'avaient pas la précision nécessaire pour bien évaluer l'angle LTS. En prenant la valeur de 89° 52′ pour l'angle en T, on trouve que la distance Terre-Soleil est environ 400 fois la distance Terre-Lune.

Ce qui est remarquable, c'est la méthode, la démarche plus que le résultat. C'est le développement de la méthode qui fait la gloire du scientifique, le résultat peut toujours être amélioré avec le développement d'instruments de mesure plus précis. C'est dans l'élaboration de la démarche qu'il faut faire preuve d'imagination et de créativité.

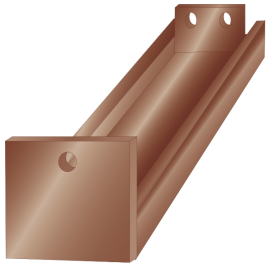
DISTANCES CÉLESTES

Dans la construction de la connaissance, il faut observer, prendre des mesures sans savoir nécessairement à l'avance lesquelles seront utiles, mettre en relation divers phénomènes,

[5] $1/20 = 0,05 < \sin 3^\circ = 0,052335956 < 1/18 = 0,05555\ldots$

faire des hypothèses et tirer les conclusions de celles-ci. C'est ce que fait Aristarque pour comparer le rayon de la Terre et la distance Terre-Lune.

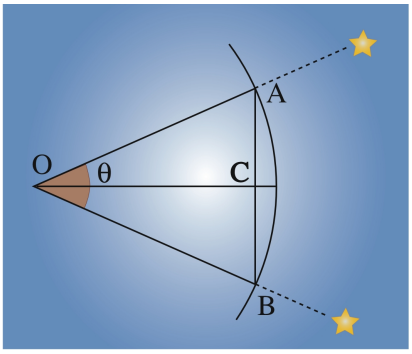
Pour prendre des mesures, il faut un instrument. L'illustration suivante présente l'un de ces instruments.



Cet instrument est muni d'une plaque fixe, percée d'un trou, et d'une plaque coulissante, percée de deux trous, que l'on peut déplacer dans une rainure.

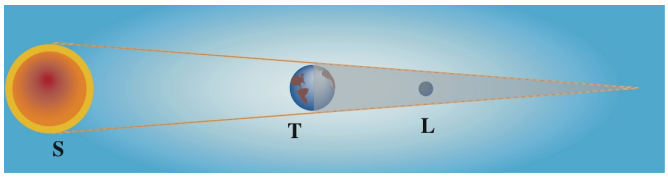
L'instrument permet de viser, par exemple, les deux bords d'une planète. La distance entre la plaque fixe et la plaque mobile est la mesure cherchée. On détermine ainsi la grandeur angulaire de la planète.

On peut également déterminer la distance angulaire entre deux étoiles, celles-ci étant supposées fixées sur la sphère extérieure aux confins de l'univers.



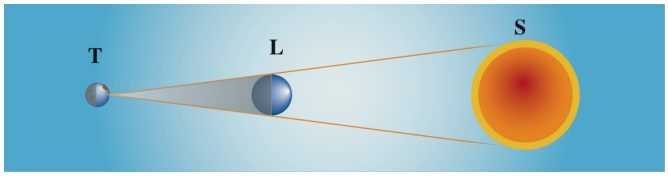
Puisque la distance entre les deux orifices de la plaque mobile est connue, on a alors la base et la hauteur d'un triangle isocèle et on peut caractériser l'angle au sommet par le rapport des côtés.

Durant une éclipse de Lune, Aristarque mesure le temps écoulé entre le moment où la Lune pénètre dans le cône d'ombre de la Terre et le moment où elle disparaît complètement. Il constate que ce temps est le même que celui durant lequel la Lune est complètement cachée.

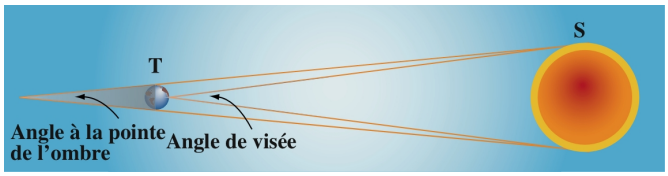


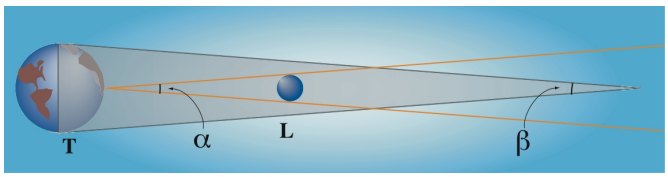
Il en conclut que la largeur de l'ombre de la Terre, à l'endroit où elle est traversée par la Lune lors d'une éclipse, est le double du diamètre de la Lune.

Durant une éclipse de Soleil, la Lune et le Soleil ont le même angle de visée.



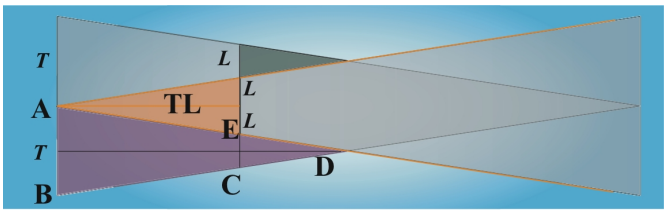
De plus, Aristarque considère que le Soleil est beaucoup plus gros que la Terre et fait l'hypothèse que l'angle à la pointe de l'ombre de la Terre doit être à peu près égal à l'angle de visée du Soleil.





Puisqu'au moment de l'éclipse de Soleil la grandeur angulaire de la Lune est la même que celle du Soleil. Aristarque faisait donc l'hypothèse que l'angle β à la pointe de l'ombre est égale à la grandeur angulaire α de la Lune. Il y a alors un seul endroit où la Lune peut couvrir la moitié de la largeur de l'ombre.

Dans la figure précédente, le rayon de la Terre semble une quantité non négligeable car la figure n'est pas à l'échelle. En négligeant cette grandeur, on peut considérer que le sommet de l'angle α est au centre de la Terre et obtenir une configuration comme suit.



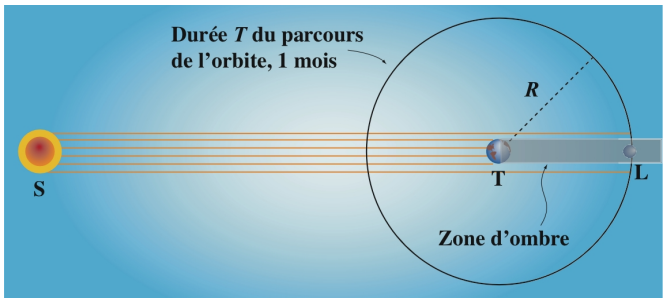
Puisque les angles α et β sont égaux, les triangles isocèles sont tous semblables et on peut facilement montrer, par le rapport de la base et de la hauteur des triangles CED et ABD que $T = 3L$, où T et L sont respectivement le rayon de la Terre et le rayon de la Lune. Aristarque en conclut que la Lune est trois fois plus petite que la Terre.

Sans l'hypothèse à l'effet que l'angle β à la pointe de l'ombre est égale à la grandeur angulaire α de la Lune, Aristarque ne serait pas parvenu à cette évaluation.

DISTANCE TERRE-LUNE

Considérant que la Lune décrit un grand cercle autour de la Terre, Aristarque va en calculer la distance. Soit R le rayon de ce cercle et T le temps mis par la lune pour faire un tour, environ un mois. On a donc $T = 672$ heures. Pendant ce temps la lune couvre une distance de $D = 2\pi R$.

Une éclipse de lune se produit si la Lune, du côté opposé au Soleil, traverse l'ombre de la terre (c'est donc au moment d'une pleine Lune).



Si r est le rayon de la Terre, en considérant que les rayons du Soleil sont parallèles, la largeur de l'ombre est à peu près le diamètre de la Terre $d = 2r$. Dans les éclipses les plus longues, qui se produisent quand la Lune passe par le centre de l'ombre de la Terre, le temps t nécessaire pour que le centre de la lune croise le centre de l'ombre est environ 3 heures.

Si la Lune se déplace autour de la terre à vitesse constante, on a :

$$\frac{D}{d} = \frac{2\pi R}{2r} = \frac{T}{t}$$

En simplifiant, Aristarque obtient :

$$\frac{R}{r} \approx 60 \quad [6]$$

Cela donne la distance Terre-Lune utilisée de nos jours, soit une distance de 60 rayons terrestres.

Il y a plusieurs approximations dans ce calcul, la durée réelle du « mois lunaire » est de 29,53 jours, mais la période orbitale sidérale de la Lune est plus courte de 2.21 jours, cela est dû au fait que le Soleil s'est déplacé durant ce mois lunaire. En raffinant la valeur de π et en corrigeant les approximations faites par Aristarque, on parvient quand même à environ 60 rayons terrestres (60 RT).

Aristarque avait obtenu précédemment que la distance Terre-Soleil (TS) est entre 18 et 20 fois la distance Terre-Lune (TL),

$$18\ TL < TS < 20\ TL$$

Il pouvait donc conclure que :

$$1080\ RT < TS < 1200\ RT$$

Les mesures et calculs d'Aristarque sont imprécis, mais sa principale conclusion est que le Soleil est beaucoup plus grand que la Terre. Il semblait donc raisonnable qu'il soit au centre de l'univers, plutôt que la Terre. Cette conclusion n'a été acceptée ni par Hipparque, ni par Ptolémée. Pour la raison suivante :

Si la Terre tournait autour du Soleil, on serait des deux côtés opposés du Soleil tous les 6 mois. Si la distance était aussi grande qu'Aristarque le prétend, on devrait percevoir du changement dans les positions relatives des étoiles.

Nous connaissons maintenant la réponse : les étoiles sont si éloignées de nous que même nos meilleurs télescopes peuvent à peine observer le décalage des plus proches d'entre elles. Il a fallu presque 18 siècles avant que les idées d'Aristarque ne soient rétablies par Copernic. Celui-ci devra d'ailleurs repousser la sphère des étoiles fixes à une très grande distance pour expliquer cette absence.

[6] Aristarque a fait cette estimation vers ∼270, Archimède avait alors 17 ans et n'avait pas encore estimer la valeur de π. Aristarque a utilisé une valeur trop grande pour π.

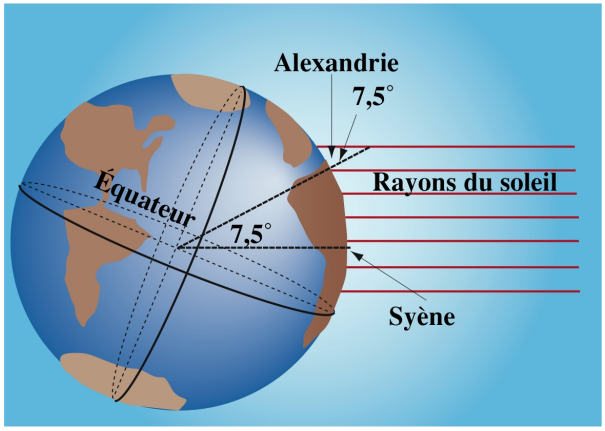
Ératosthène de Cyrène

Aristarque a calculé des distances relatives en exprimant le rayon de la Lune, la distance Terre-Lune et la distance Terre-Soleil en fonction du rayon de la Terre. Pour traduire ces distances en unité usuelle, il fallait déterminer la mesure du rayon de la Terre dans cette unité de mesure. Cette mesure sera obtenue grâce aux travaux d'Ératosthène et d'Archimède.

Ératosthène est né en ∼276 à Cyrène (Shahhat, Libye) et est décédé à Alexandrie en ∼194. Après avoir étudié à Alexandrie et à Athènes, il s'installe à Alexandrie où il devient directeur de la bibliothèque. Il fait des recherches en géométrie et en théorie des nombres. Il est surtout connu par la mesure de la circonférence terrestre et le *crible d'Ératosthène* qui consiste à éliminer de la liste des nombres tous les multiples des nombres premiers en succession pour ne retenir que les nombres premiers. Le crible, sous une forme modifiée, est encore un instrument important de nos jours en théorie de nombres. Il fut également géographe.

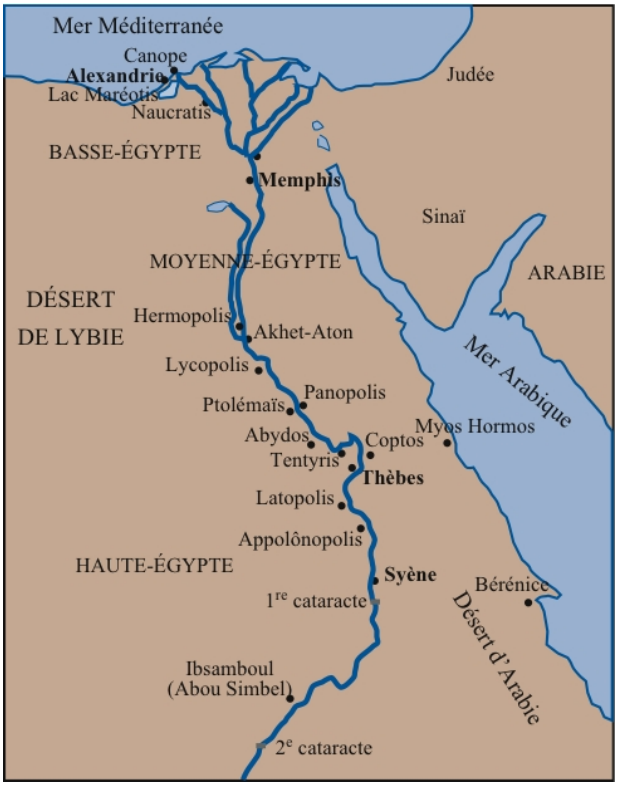
circonférence terrestre par ératosthène

Disposant de tous les faits observés dans l'empire, Ératosthène a été en mesure de calculer la circonférence terrestre. Il obtint environ 40 000 km (voir texte sur Ératosthène). Ératosthène était bibliothécaire d'Alexandrie et il disposait de tous les renseignements sur les événements curieux observés dans l'empire d'Alexandre. C'est ainsi qu'il apprit qu'au solstice d'été, le Soleil se réfléchissait à midi dans l'eau d'un puits profond de Syène (aujourd'hui Assouan) non loin de la première cataracte du Nil. À ce moment, le Soleil était donc à la verticale du puits. Le même jour à midi, dans la ville d'Alexandrie, l'ombre d'un pilier permettait de déterminer que le Soleil était à 7,5 degrés de la verticale.



Il ne restait qu'à déterminer la distance d'Alexandrie à Syène. C'est en marchant qu'il faut le faire et en suivant le Nil. Il faut bien sûr marcher d'un pas constant et apporter les corrections pour les méandres du fleuve.

C'est donc une expédition de plusieurs jours comme on peut le constater sur la carte ci-dessous.



En unité de mesure moderne, il a obtenu une distance de 830 km. En utilisant ces

informations et le fait que la mesure de l'angle au centre est égale à la mesure de l'arc intercepté, il a fait le calcul suivant :

$$C = \frac{360^\circ}{7,5^\circ} \times 830 \text{ km} \approx 40\,000 \text{ km}$$

Connaissant la circonférence terrestre et la valeur de π, il était alors possible de calculer le rayon de la Terre. L'Homme a commencé à déterminer les dimensions de son univers.

CALCUL DE π PAR ARCHIMÈDE

Le calcul d'une valeur approchée du rapport de la circonférence sur le diamètre d'un cercle par Archimède[7] ($\sim$287-$\sim$212) a permis de calculer le rayon de la Terre à partir des résultats d'Ératosthène.

Archimède a calculé que :

$$223/71 < \pi < 22/7$$

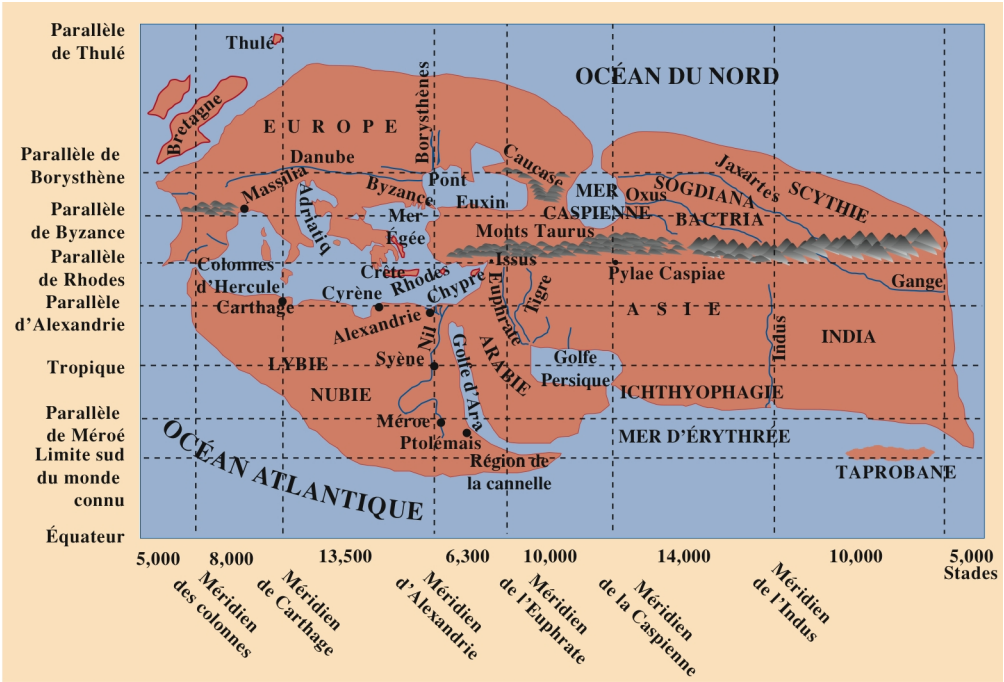
Ce qui permet de déterminer que le rayon de la Terre est d'environ 6 400 km. En utilisant cette valeur avec les calculs d'Aristarque, on obtient 1 600 km pour le rayon de la Lune et 384 000 km pour la distance Terre-Lune.

MONDE HABITABLE SELON ÉRATOSTHÈNE

Ératosthène a également introduit l'usage des parallèles et méridiens dans les cartes géographiques. Peut-être a-t-il été inspiré par le plan d'urbanisme d'Alexandrie. Là, une ville fut développée à partir d'un plan constitué de rues rectilignes se coupant à angle droit. Elle a un quartier égyptien, un quartier grec et un quartier juif. Nous sommes habitués à ce type de plan d'urbanisme et nous savons que cela permet de s'orienter facilement et de tracer simplement la carte d'une ville.

[7] De la comparaison d'aires au calcul de π, André Ross, Bulletin de l'AMQ, volume 44, no 1, mars 2004.


PLAN D'ALEXANDRIE
MÉDITERRANÉE
Phare
Palais royal
Casernes
Grand
Port
Quartier
Théâtre
Juif
Forum
Ile de Pharos
Quartier royal
Musée
Gymnase
Canal vers le Nil
Quartier égyptien
Temple de Sérapis
Lac
Maréotis
Stade


Parallèle de Thulé
Parallèle de Borysthène
Parallèle de Byzance
Parallèle de Rhodes
Parallèle d'Alexandrie
Tropique
Parallèle de Méroé
Limite sud du monde connu
Équateur
Thulé
OCÉAN DU NORD
Bretagne
EUROPE
Danube
Borysthènes
Massilia
Adriatique
Byzance
Pont Euxin
Caucase
MER CASPIENNE
Oxus
SOGDIANA
Jaxartes
SCYTHIE
BACTRIA
Mer Égée
Monts Taurus
Colonnes d'Hercule
Crète
Rhodes
Issus
Pylae Caspiae
Gange
Carthage
Cyrène
Chypre
Euphrate
Tigre
A S I E
Alexandrie
Nil
Golfe d'Arabie
Indus
INDIA
LYBIE
Syène
Golfe Persique
NUBIE
ICHTHYOPHAGIE
Méroé
Ptolemais
MER D'ÉRYTHRÉE
Région de la cannelle
TAPROBANE
OCÉAN ATLANTIQUE
5,000
8,000
13,500
6,300
10,000
14,000
10,000
5,000 Stades
Méridien des colonnes
Méridien de Carthage
Méridien d'Alexandrie
Méridien de l'Euphrate
Méridien de la Caspienne
Méridien de l'Indus

Hipparcos de Nicée

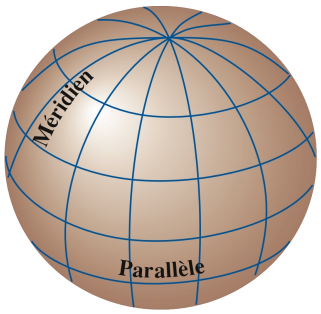
Considéré comme le plus grand astronome de toute l'antiquité classique, Hipparque de Nicée fit des observations d'une bonne précision entre ∼161 et ∼127 depuis Rhodes et Alexandrie.

Il mit en évidence un grand nombre de phénomènes insoupçonnés auparavant, détermina une valeur de 365 j 5h 55 min 12 s pour la durée de l'année tropique, valeur bien plus précise que tout ce qui avait été proposé avant lui, cependant encore trop surestimée par rapport à la vraie valeur égale à 365 j 5h 48 min 46 s.

Hipparque a transformé l'astronomie grecque d'une science descriptive à une science prédictive. Il a lui aussi estimé les distances Terre-Lune et Terre-Soleil, ainsi que les tailles réelles de ces astres, obtenant une valeur tout à fait correcte pour la distance Terre-Lune et la taille de la Lune et une valeur dix fois trop petite pour la distance Terre-Soleil. Il trouva tout de même que le Soleil devait être dix fois plus gros que la Terre.

Il a dressé un catalogue de 800 étoiles, notant leur position avec précision et en évaluant leur grandeur apparente. Il fut le premier à reconnaître la précession des équinoxes, c'est-à-dire le déplacement lent du point vernal (équinoxe de printemps) sur le zodiaque.

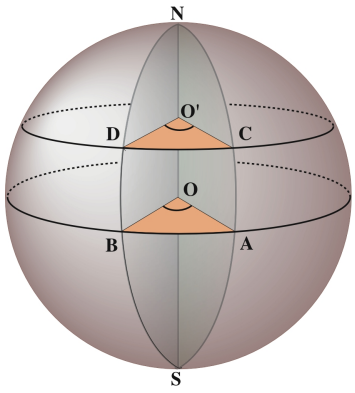
Hipparque a développé l'idée d'Ératosthène d'utiliser des méridiens et des parallèles. Il a étendu cette idée à toute la sphère terrestre.



Cette extension l'a amené à poser les fondements de la trigonométrie sphérique, soit l'étude des triangles sur la surface d'une sphère, pour pouvoir déterminer la distance entre deux points qui ne sont pas sur le même méridien ni sur le même parallèle.

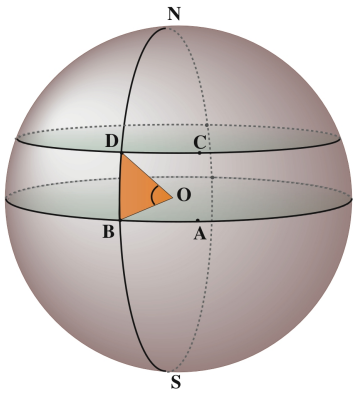
LONGITUDE ET LATITUDE

La longitude du point B, à l'équateur, est donnée par la mesure de l'angle AOB, où O est le centre de la sphère. Le point D sur le même méridien a la même longitude, les angles AOB et $CO'D$ étant égaux, où O' est le centre du cercle parallèle à l'équateur.



La différence de longitude est l'angle au centre entre deux grands cercles passant par les pôles.

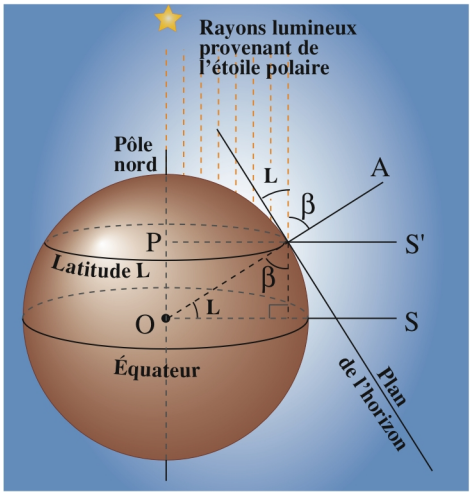
La latitude du point D est donnée par la mesure de l'angle au centre BOD. La latitude est la même pour tous les points sur un cercle parallèle à l'équateur.



La différence de latitude est l'angle au centre entre deux cercles parallèles à l'équateur.

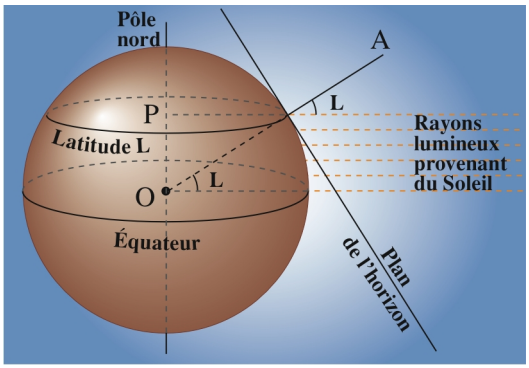
Pour donner la position d'un point sur la sphère, il suffit alors de donner sa longitude et sa latitude.

Évidemment, il n'est pas possible de se rendre au centre de la Terre pour y mesurer des angles. Cependant la géométrie nous permet de pallier à cet inconvénient. Dans l'hémisphère nord, on peut calculer la latitude à l'aide de l'étoile polaire.



En mesurant l'angle d'élévation de l'étoile polaire par rapport à l'horizon dans la direction nord, on obtient directement la latitude du point.

On peut également mesurer la latitude en mesurant la distance zénithale du Soleil à midi aux équinoxes. Le Soleil est alors à la verticale de l'équateur.



L'angle entre le zénith et la direction du Soleil à midi aux équinoxes est égal à l'angle au centre, soit la latitude, puisque ce sont des angles correspondants.

CALCUL DE LA LONGITUDE

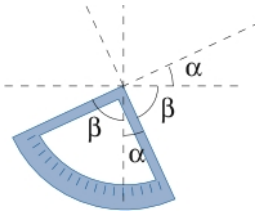
Pour calculer la longitude en un point, il faut, à midi, déterminer la différence d'heures entre ce point et le méridien de référence. Il y a 24 méridiens et une différence d'une heure avec le méridien de référence signifie une différence de longitude de 15°.

Le méridien de référence, qui fut d'abord celui de Paris, est maintenant situé à Greenwich en Angleterre.

LES INSTRUMENTS

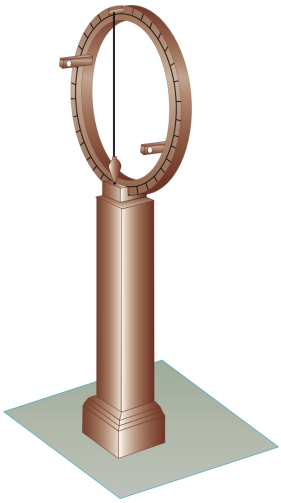
On peut facilement mesurer l'angle que fait une direction avec la verticale à l'aide d'un quadrant gradué et d'un fil à plomb.

L'angle avec l'horizontale est alors l'angle complémentaire à celui avec la verticale.



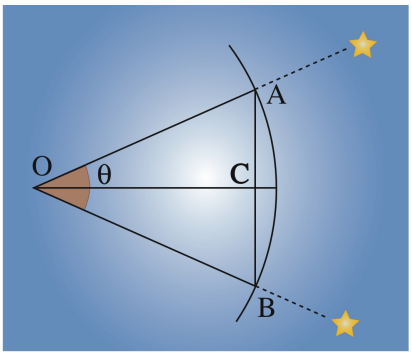
Pour assurer une bonne précision, il faut utiliser un instrument stable. Le fil à plomb de l'instrument suivant permet de s'assurer qu'il est bien aligné dans la direction zénithale. Il est muni de deux anneaux dont l'un est fixe et l'autre est mobile.

La partie mobile de cet instrument comporte deux viseurs. La lecture de l'angle de visée se fait sur l'anneau gradué. C'est le type d'appareil qui a été utilisé par Ptolémée pour mesurer l'obliquité de l'écliptique.



GÉOMÉTRIE DES CORDES

Hipparque a développé une géométrie des cordes qui est l'ancêtre de la trigonométrie moderne.



La géométrie des cordes consiste à déterminer dans un cercle de rayon OC donné la longueur de la corde AB sous-tendue par un angle au centre θ. Selon Théon d'Alexandrie (vers 365), Hipparque aurait rédigé un traité en 12 livres sur le calcul des cordes dans un cercle.

Ptolémée

Claude Ptolémée (85-165) est un astronome, mathématicien et géographe grec membre de l'Université d'Alexandrie. Il y fit ses observations de 127 à 141 et publia un ouvrage qui est un exposé complet du système géocentrique.

La carte ci-dessous a été réalisée en utilisant les méridiens et les parallèles pour situer les lieux. Ce planisphère, qui serait dû à Ptolémée, marque le début de la science des cartes.

On est frappé par l'évolution lorsqu'on compare cette carte à celle reconstruite à partir des données d'Hécatée de Milet.

Conclusion

Les astronomes d'Alexandrie ont posé les fondements de la cartographie terrestre et céleste. Ils ont développé des méthodes pour construire des cartes géographiques et pour déterminer les positions des étoiles. Ils ont cherché à déterminer les rayons et les distances de la Terre, de la Lune et du Soleil. La tâche n'était pas facile, mais en persévérant ils sont parvenus à obtenir certaines estimations correctes, d'autres moins. Ils ont également voulu développer une astronomie prédictive, ce qui les amenés à raffiner les modèles décrivant les orbes des planètes.

Cependant, pour répondre adéquatement aux exigences de la navigation, la science des cartes va devoir évoluer. En plus de la longitude et de la latitude, des notions mathématiques liées au développement de la perspective et de la géométrie projective seront utilisées.

Bibliographie

Astronomy Before the Telescope, Édité par Christopher Walker, The trustees of the British Museum St. Martins Press, New-York.

Ferguson, Kitty, Measuring the universe, New-York, Walker and company, 1999, 342 p.

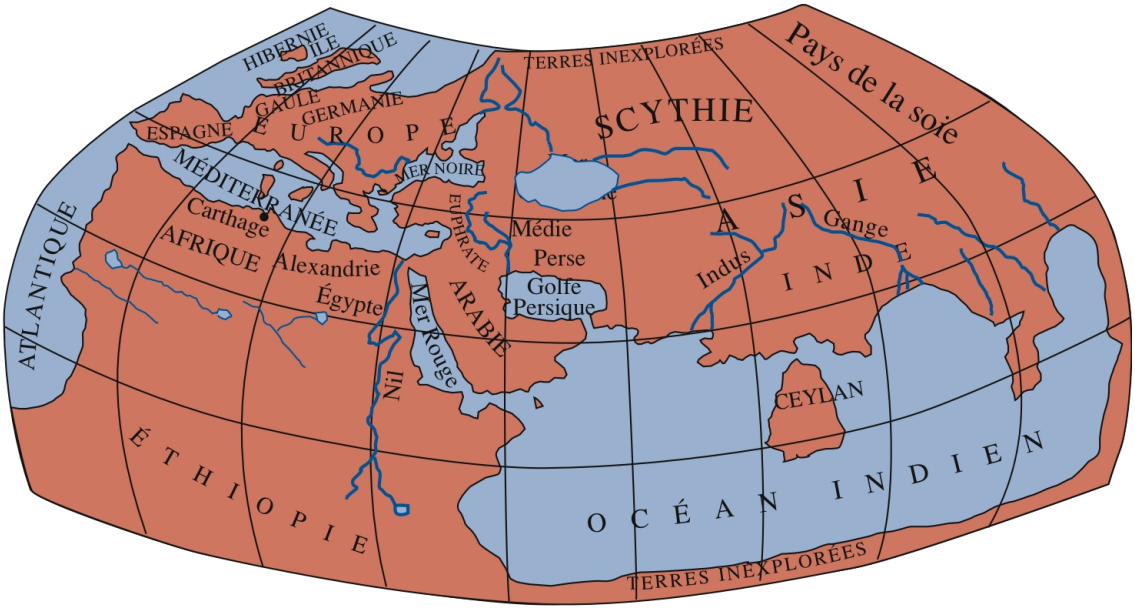
Kline, Morris, *Mathematics, A Cultural Approach*, Reading, Mass. : Addison-Wesley, 1962, 70 p.

Kline, Morris, *Mathematics in Western Culture*, New York, Oxford University Press, 1974, 484 p.

Ptolemy's Almagest, translated and annoted by G.J. Toomer, Princeton, Princeton University Press, 1998, 693 p.

Maor, Eli, Trigonometric Delights, Princeton, Princeton University Press, 1998, 236 p.

http ://www-groups.dcs.st-and.ac.uk/~history/



Planisphère de Ptolémée

Lu pour vous

Robert Bilinski
Collège Montmorency

Sous la présente rubrique, vous trouverez une grande variété de livres. Trois d'entre eux sont des livres de vulgarisation : le premier se spécialise sur les jeux, le deuxième sur le baseball et le dernier est un recueil traitant de différents sujets. Il y a ensuite deux livres savants : le premier est une « bible » sur les nombres de Fibonacci, le second traite du bioterrorisme. On trouvera également un livre sur l'utilisation de la calculatrice graphique TI-92 s'adressant aux professeurs. Vous commencerez la chronique en découvrant un recueil de nouvelles mathématiques fort intéressantes. Pour couronner le tout, Hélène Kayler nous fait part d'une de ses récentes lectures : il s'agit d'un livre d'histoire portant sur les femmes en sciences. Merci beaucoup Hélène !

Benoît Rittaud, *L'assassin des échecs et autres fictions mathématiques,*

***Le Pommier,* 2004, 228 p., ISBN 2-74650176-7, environ 34 $.**

Ce livre est en théorie un recueil contenant 12 nouvelles dont un poème. En fait c'est bien plus et la table des matières ne dit pas tout. En effet, chaque nouvelle est suivie d'un « Prolongement ». Ces sections, invisibles à la table des matières, sont constituées d'explications mathématiques de ce que l'on retrouve dans les nouvelles qui les précèdent et permettent une lecture bien plus intéressante des nouvelles. La vulgarisation est bien faite et un effort a visiblement été fait pour que celle-ci soit accessible à tous les lecteurs (beaucoup de texte, aucune équation et plusieurs illustrations). Ces prolongements sont des

atouts majeurs de ce livre, mais la plus belle surprise pour moi a été de loin la grande qualité littéraire des nouvelles.

En effet, l'auteur a déjà écrit plusieurs articles et livres de vulgarisation. Réussir dans ce style n'est pas nécessairement un gage de qualité littéraire. Cependant, les histoires sont bien écrites, originales et agréables à lire. Dans ce livre, on retrouve d'ailleurs plusieurs styles : nouvelles à contrainte, lettres, poèmes et nouvelles « normales ». Le contenant moule à merveille le contenu. Une recherche et une réflexion ont clairement été faites avant l'écriture sur le Quoi, le Comment et le Pourquoi des histoires.

La première nouvelle, intitulée « Début de Journée », est celle que j'appelle nouvelle à contrainte. Un homme se réveille et va au travail. Rien de plus banal. Par contre, il y a visiblement eu une contrainte : « mettre en relief » les mathématiques rencontrées sur son trajet. La vraie histoire se situe plutôt à ce niveau ! Le travail de l'auteur est clair : il fallait intégrer ce contenu de manière agréable dans l'histoire. C'est chose faite. Mais, on comprend vite pourquoi le texte ne fait que cinq pages. Chapeau !

C'est la seule histoire dont le contenu mathématique n'est pas limité à un seul thème. Les autres histoires illustrent clairement un thème comme le montre la liste suivante :

« L'homme qui entendait les confidences du ciel » parle de l'estimation de la hauteur d'une pyramide par Thalès. Le thème est le fameux théorème de Thalès.

« En roues libres » raconte l'histoire de l'héritage d'un vieux « patenteux ». Elle a pour thème les courbes mathématiques et les instruments que l'on peut construire pour les exploiter.

« La prison verte » illustre un cambriolage et la fuite des criminels. Elle a pour thème la topologie appliquée aux labyrinthes et les techniques de résolution de ces derniers.

« L'assassin des échecs » met en scène un meurtre. La combinatoire est vitale à l'intrigue.

« Le mur du 100 mètres » est une lettre d'un futur président du comité olympique. On y parle des nombres, de suites et de convergence.

Les six autres histoires traitent de cryptographie, de théorie des jeux, de logique, de comptabilité légiste (statistique), de probabilités et de l'irrationalité des nombres. Les personnages sont bien pensés et crédibles. Les histoires sont bien adaptées à leur thème, et contiennent leur dose de suspens et d'émoi. Il n'y a pas de redondances, les thèmes sont variés ainsi que les histoires. Bravo à l'auteur. J'attends déjà le prochain recueil avec impatience.

R. Eastaway et J. Wyndham, *Pourquoi les autobus arrivent-ils toujours par trios ?,*

***Flammarion,* 2001, 221 p., ISBN 2-08-068100-1.**

Le livre contient 19 chapitres portant sur des sujets forts variés. Les auteurs traitent à leur manière quelques portions des mathématiques que l'on retrouve souvent dans les livres de vulgarisation. On retrouve, entre autres, les classiques que sont les nombres de Fibonacci, le nombre π, la cryptographie, les loteries et les sept ponts de Königsberg. Le livre contient aussi quelques sujets un peu moins courants, comme les sondages. Les auteurs font un bon travail de vulgarisation et ils réussissent à écrire un livre qui se distingue des autres livres que l'on trouve sur le marché, notamment à l'aide de quelques sujets originaux que les auteurs abordent aussi avec succès. On note en particulier le marketing, les partages de gâteaux, les tours de mathémagie, le pavage du plan, la température de l'eau de douche et les chaînes de Markov.

D'un point de vue mathématique, tous les sujets traités le sont avec précision et concision (au niveau des idées fondamentales car il s'agit d'un texte de vulgarisation, non de mathématique). En ce qui concerne le style, je ne sais pas si c'est moi, le traducteur ou les auteurs, mais il me semble que la manière d'écrire les textes est plus enjouée dans les chapitres « originaux » que dans les chapitres « classiques ». Il n'y a pas de plan directeur pour tous les chapitres : dans certains, une seule idée va être illustrée à l'aide d'un exemple. Dans d'autres, une idée sera illustrée par une suite d'anecdotes qui s'enfilent à la manière de perles sur un collier. Il m'est arrivé plus d'une fois d'être surpris de l'effet de petits résultats bien placés dans le corps du texte.

Je recommande fortement ce livre, non pas pour le style d'écriture, mais plutôt pour le fond. Les auteurs ont visiblement une grande culture mathématique et ont une passion pour le monde mathématique. Ils explorent avec allégresse ses diverses contrées, et les vulgarisent avec grand talent. Ce livre complète bien les autres livres du même style que j'ai recommandés récemment. Bonne lecture !

Thomas Koshy, *Fibonacci and Lucas numbers with applications*, Pure and Applied Mathematics,

***Wiley Interscience,* 2001, 652 p., ISBN 0-471-39969-8, environ 150 $.**

J'ai souvent entendu parler de ce livre. Je m'implique dans la revue de la société mathématique du Canada intitulée Crux Mathematicorum. On y retrouve beaucoup de problèmes, concours, olympiades et exercices mathématiques de tous les niveaux. Ainsi, les nombres de Fibonacci s'y retrouvent souvent de part leur simplicité apparente, leur omniprésence « dans la nature » et leur réelle profondeur mathématique. Le livre apparaissait souvent dans les références et, à la longue, mon intérêt a été piqué.

Ce livre est une oeuvre d'un passionné qui a passé au peigne fin une quantité impressionnante de documents de référence afin de colliger son livre (14 pages contenant 37 références chaque, pour plus de 500 références environ). Le livre est séparé en 47 chapitres d'une quinzaine de pages chacun et contenant suffisamment de matière pour arriver à obtenir des chapitres intéressants.

Il est à noter que je n'ai pas aimé le premier chapitre, le trouvant soit trop « ésotérique » et « nonmathématique », soit rempli de coïncidences numériques ou plutôt numérologiques. Tout au long de ce chapitre, je me demandais comment on avait pu écrire un tel livre dans une collection de mathématiques si reconnue. Cette curiosité m'a poussé à lire le second chapitre. Par chance ! Quelle bourde j'aurais fait de me laisser prendre à mes premières impressions ! Ce livre est plein de perles, riche en mathématiques variées et précises (séries, géométrie, fonctions génératrices, suites, nombres complexes, fonctions...) et « facile » à lire. J'avais bien d'autres choses à faire, mais je n'arrivais pas à le déposer. Le livre est plein d'exercices. Je les ai observés avec intérêt. D'ailleurs, les exercices sont référencés aussi pour attribuer à César ce qui lui revient. Belle touche.

En plus, le livre est bien structuré et bien pensé. L'auteur a fait attention au rythme. On y retrouve quelques chapitres appliqués au début qui, sans qu'on s'en rende compte, deviennent théoriques et, naturellement, on se retrouve en présence d'algèbre avancée. Quand on s'en rend compte, on est habitué et le rythme est soutenu. Lorsque l'on se fatigue de voir des « x, F_n et Σ », on retombe au bon moment dans la géométrie et les applications :

les traditionnelles applications en biologie et en art, mais aussi les moins conventionnelles en génie électrique, chimie, neurophysiologie et combinatoire.

Bon, que dire de plus ? Ce livre est un « must » pour les fanas de Fibonacci, mais il peut aussi attirer les mathématiciens amateurs et professionnels. Par contre, le contenu est très poussé après le sixième chapitre et donc je ne recommande pas ce livre aux étudiants pré-universitaires. Par contre, leurs professeurs pourront peut-être s'en inspirer. J'ai réussi à le lire comme un livre et non comme un manuel scolaire, ce n'est pas peu dire de l'auteur. Bonne lecture !

Jörg Bewersdorff, *Luck, logic and white lies : The mathematics of games,*
***A. K. Peters,* 2005, 486 p., ISBN 1-56881-210-8, environ 66 $.**

Avec un nom comme celui-là, je ne pouvais pas m'empêcher de me le procurer. La couverture est belle : bleue, avec un jeu d'échecs, des dés et un jeu de Backgammon stylisé réalisé en 3D par ordinateur. Comme le titre l'indique, ce livre expose les enjeux mathématiques des jeux en utilisant les trois approches prônées par les mathématiciens pour étudier les jeux : la probabilité et les statistiques, la combinatoire et la théorie des jeux. Ce livre est gros, même très gros, mais il est rempli d'innombrables petits chapitres d'environ cinq pages chacun à 20 pages pour les plus longs. Bon, je me rétracte, ils ne sont pas innombrables, il y en a 45...

Ce livre est bon. Et même, j'oserais dire qu'il est incontournable pour ceux qui jouent, qui aiment jouer ou qui commencent à étudier les jeux. Un professionnel le trouvera peut-être trop de base, mais pour un coup d'œil général sur le domaine, je ne pense pas qu'on puisse mieux trouver. Il est vraiment complet au point de vue des techniques utilisées et des jeux étudiés. On y retrouve bien des jeux en allant du tic-tac-toe au go, en passant par le poker, le backgammon, les échelles et serpents, le monopoly et les jeux théoriques en théorie des nombres et en politique. De la même manière, on aborde bien des techniques comme les simulations, les graphes, la théorie des jeux, les probabilités, la statistique, le simplexe et la combinatoire. Pour rajouter une autre qualité à ce livre, l'auteur démontre

une culture approfondie. Au fil de l'étude mathématique, on découvre l'historique des jeux et de leur résolution. Bien que je ne sois pas un spécialiste de l'histoire des mathématiques, il me semble que l'auteur rend à César ce qu'il lui doit.

Un défaut est que les références sont majoritairement en allemand. On en retrouve quelques-unes ici et là en anglais et même en français, mais je ne crois pas que ce ne soit assez pour que nos lecteurs puissent approfondir le sujet en les utilisant. Le traducteur aurait peut-être dû ajouter quelques titres aux bibliographies. J'ai lu le livre d'un trait pour pouvoir en faire une recension complète et cela m'a pris deux semaines en été. Je ne sais pas si cela peut être considéré comme un point négatif, mais attendez-vous à une lecture de longue haleine. Par contre, vu la structure en petits chapitres du livre, il pourrait se lire de manière discontinue. Ce livre a été conçu pour être lu dans l'ordre, et je conseille vivement que les lecteurs fassent la même chose. Les chapitres coulent l'un dans l'autre si naturellement que l'on ne peut s'empêcher de penser à tout le travail mis à l'écrire. Les idées, les techniques et la complexité des jeux évoluent au gré des chapitres.

Ce livre est pédagogique et a un penchant constructiviste. Chaque chapitre porte sur un jeu qui est étudié en particulier. Puis les conclusions sont élargies quand c'est possible à d'autres jeux ou situations. Le livre contient peu de formules (deux pour tout le livre), mais on rentre tellement en détail dans la mécanique des techniques utilisées que ce livre s'adresse définitivement à un lectorat mathématiquement avancé :

- Un bachelier dans un domaine scientifique (génie, mathématique, physique, informatique, économétrie, ...) devrait le lire.
- Un cégépien allant dans un de ces domaines aussi devrait le lire pour se donner une idée de ce qui l'attend ou qui veut se servir de ses (ces) mathématiques pour gagner dans les jeux.
- Un professeur qui veut avoir un outil de plus pour répondre à la question « À quoi ça peut me servir ? »
- Un amateur de jeux qui veut aller au-delà de l'excitation et qui veut comprendre son jeu.
- Un mathématicien qui veut un livre de référence sur le sujet pour se remémorer les grandes lignes des résultats.

Bonne lecture !

Jean-Jacques Dahan, *Introduction à la géométrie avec la TI-92, Ellipses,* 1998, 237 p., ISBN 2-7298-9877-8.

Pour profiter à fond de ce livre, il faut une calculatrice avec un logiciel de géométrie intégré. Compte tenu que le logiciel sur la TI-92 est Cabri, ce livre peut tout aussi bien servir aux gens avec des micro-ordinateurs. Il faut noter par contre que cela demandera plus de travail de la part de l'usager puisqu'on y retrouve maintes références à des boutons de la calculatrice que l'on ne retrouve pas sur son ordinateur. Un usager expérimenté de Cabri pourra par contre s'adapter rapidement.

La première chose qui frappe quand on lit ce livre est le grand soin pédagogique apporté à l'écriture par l'auteur. On retrouve des illustrations abondantes de toutes les étapes des constructions. Les chapitres sont tous faits en trois temps : s'initier aux options nécessaires (souvent par le jeu) dans la section « Pour s'initier en s'amusant », approfondir les options en dessinant un motif plus compliqué (lettre, bicyclette...) dans la section « Pour s'entraîner en s'amusant », répondre à une question de géométrie « typique » dans la section « Problème ». Parsemées dans les chapitres, il y a des sous-sections « Pour voir si vous avez compris » qui contiennent quelques configurations à refaire avec sa calculatrice. Ce sont des exercices sans solution, mais la réponse est la configuration elle-même : on l'a faite ou on ne l'a pas faite.

Dans les chapitres plus avancés, on fait de l'animation de base, voire en 3D. L'auteur utilise assez rapidement les options « trace » et « animation » pour donner de l'effet aux figures. On retrouve une grande variété de constructions qui demandent chacune une utilisation des mathématiques assez poussée. Les constructions sont sous la forme de recettes « prêtes à manger » et les mathématiques sous-jacentes ne sont pas expliquées. Le soin revient donc au professeur qui utiliserait ces activités en classe de compléter par une discussion sur les outils mathématiques nécessaires aux constructions (pourquoi un cercle ici ?...).

Loin d'être « simple », ce livre reste tout de même très abordable pour des jeunes de niveau secondaire. Le travail fournit par l'auteur à la rédaction de ce livre est grand

et il reste maintenant au professeur de profiter pleinement des situations pédagogiques et ludiques soulevées par l'auteur. J'ai eu la chance de le voir à l'œuvre lors d'un congrès de mathématiques. En commençant avec ce livre, on s'initie aux options de Cabri et on pourra s'en servir plus aisément dans des contextes plus difficiles, comme dans sa conférence (champs de vecteurs...). En lisant ce livre, j'ai appris un peu plus sur Cabri, mais j'entrevois plus de possibilités. Si je n'arrive pas à vous en convaincre, alors il faut lire la préface de Jean-Marie Laborde, le créateur de Cabri qui qualifie ce livre de « Vrai régal ! ». Bonne lecture !

H. Banks et C. Castillo-Chavez, *ed., Bioterrorism,* Frontiers of Applied Mathematics,
***SIAM,* 2005, 240 p., ISBN 0-89871-549-0, environ 96 $.**

Avouez que le titre de ce livre est d'actualité ! La curiosité a été plus forte que moi et je voulais savoir ce qu'il en était. Ce recueil d'articles savants est le fruit de travaux effectués en 2002 pendant des congrès et ateliers de DIMACS. Le contenu n'est pas entièrement nouveau puisque des modèles épidémiologiques existent depuis longtemps, comme le montrent les travaux de Kermack et Mckendrick en 1927 par exemple. Par contre, les modèles classiques ne tiennent pas compte d'une propriété évidente de l'épidémiologie par terrorisme : la volonté humaine d'essayer de faire le plus de morts. Cette caractéristique, on en convient, est fort différente de la propagation « naturelle » de maladies.

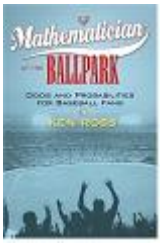
Ainsi, dans le premier chapitre, on évoque dans un tour d'horizon différentes branches des mathématiques et leurs outils les plus utiles à ce genre d'études, soit les mathématiques discrètes et l'informatique théorique. Naturellement, on évoque aussi les grandes difficultés que l'on a à appliquer ces techniques. En particulier, on apprend sur les méthodes de surveillance, l'analyse de données en direct, l'analyse factorielle, la visualisation de grandes quantités de données, le nettoyage de données, la compréhension du langage naturel, la cryptographie, la théorie des graphes (réseaux sociaux, modélisations géographiques, réseaux de transports...), la prise de décision, la théorie des jeux, la théorie de l'ordre et les tests de groupes combinatoires. Ce chapitre constitue en fait une revue de certaines méthodes,

comme en témoignent les 250 références que l'on retrouve à la fin.

Par contre, ce chapitre n'est pas un résumé du livre, puisque les autres chapitres font appel à de nombreuses techniques qui ne s'y retrouvent pas : les graphes aléatoires, équations différentielles et opérateurs, les statistiques, processus stochastiques et les chaînes de Markov, etc. En fait, les chapitres de ce livre se succèdent, mais ne se ressemblent pas dans leur contenu mathématique. La beauté de ce livre est justement le tour d'horizon qu'il permet de faire. On retrouve des analyses locales sur un cercle de connaissances, mais aussi une macro-analyse qui tient compte de la géographie des villes. On apprend aussi sur les subtilités des maladies auxquelles on aura à faire face selon toute vraisemblance : anthracite, influenza, variole... et le fanatisme des terroristes (voir chapitre 7). On apprend sur les différentes manières de générer des graphes et les propriétés que l'on obtient ainsi que les correspondances dans la réalité. En parlant de réalité, je trouve fort intéressant l'aspect « graphique » de ce livre. En effet, chaque chapitre (sauf le 1er et le 5^{e}) est plein de visualisions intéressantes. Je ne sais pas, par contre, si on doit se réconforter ou être désespéré de justement voir la variété des sujets traités : ne démontrent-ils pas notre vulnérabilité ?

En somme, ce livre intéressera les étudiants gradués en biomathématique, en bioinformatique et ceux en modélisation de tout genre. Par contre, les professeurs de cégep, toujours pressés de trouver des « applications » des mathématiques, pourront y trouver leur compte. Mais ils devront aussi faire attention de ne pas effrayer leurs étudiants par le contenu théorique « plein de formules » de ce livre. L'effet des formules est par contre amenuisé par la grande variété des graphiques qui demandent malheureusement eux aussi de l'effort. Même s'il est en anglais, ce livre est écrit d'une manière accessible : langage simple et clair... J'en sors une fois de plus impressionné par l'universalité et la beauté des mathématiques. Bonne lecture !

K. Ross, *A Mathematician at the Ballpark,*
***π Press,* 2004, 190 p., ISBN 0-13-147990-3, environ 20 $.**



Ce livre est curieux. L'auteur, un mathématicien, essaie de faire comprendre les probabilités et les statistiques en parlant de baseball et de ce que les fans de ce jeu considèrent

des statistiques. Clairement, M. Ross s'y connaît en probabilités et il semble avoir fait le tour de la littérature concernant le calcul du rendement d'un joueur de baseball. Ne nous étonnons pas ! C'est après tout le sport national au sud du 45$^{\text{e}}$ parallèle. Par contre, ce livre contient assez de mathématiques pour nous être intéressant.

En fait, l'auteur s'attarde dans le premier chapitre à la question de la mesure du rendement d'un batteur. Loin d'être évidente, cette question remet beaucoup de choses sur le tapis : doit-on utiliser la norme établie (le % de coups sûrs) ou bien doit-on utiliser d'autres mesures plus « justes ». L'auteur pose sans y répondre la question de l'erreur dans l'utilisation de l'expression « moyenne au bâton » alors que celle-ci est clairement fausse. Un autre aspect intéressant est l'utilisation dans le milieux des sports des paris du type « a contre b » à la place des probabilités $P(\text{pour}) = \frac{a}{a+b}$. En fait, l'exploration de ce tic sert de tremplin pour explorer le concept de jeu équitable. Par la suite, on explore les sujets classiques d'un cours d'introduction aux probabilités (stratégie de pariage, espérance, indépendance, binomiale...) et aux statistiques (distributions théorique et empirique, corrélation et valeur$-p$).

Tout en étant mathématiquement correct, l'auteur semble avoir trouvé le moyen de demeurer accessible. Mais la question reste : accessible à qui ? Aux mathématiciens ou aux amateurs de baseball ? Souvent dans le livre, l'auteur sortira de l'univers du baseball pour illustrer les concepts au besoin avec des jeux de chance ou le fameux paradoxe des tests médicaux. Ces parties sont naturellement moins vulgarisées, mathématiquement correctes, mais elles souffrent aussi d'un manque « d'élégance » relativement aux autres parties du livre.

Un coup d'oeil dans les annexes de ce livre est obligatoire ! On y apprend beaucoup de choses sur le culte de la statistique de la balle. On apprend même qu'une société forte de 6 600 membres, la S.A.B.R., s'y adonne continuellement et publie même deux journaux « savants » sur le sujet. Même si on a perdu nos Expos, ce livre devrait faire plaisir aux amateurs de sport parmi nous. Bonne lecture !

Voici une recension invitée ! Je remercie Hélène Kayler, qui me simplifie la vie une fois de plus. Elle m'apporte aussi la possibilité de couvrir des livres dont je ne connais pas l'existence et qui augmente la variété des livres recensés. Merci !

Jean-Pierre Poirier, *Histoire des femmes de Sciences en France - Du Moyen Âge à la Révolution*, Éditions Pygmalion / Gérard Watelet, 411 pages.

Cette « galerie de portraits tirés de l'oubli ... recense beaucoup de collaboratrices, d'inspiratrices ou de vulgarisatrices, (et) ne contient pas à proprement parler d'initiatrices ou d'inventrices. Toutes ces femmes ont pourtant ouvert la voie ... . » (précise la Ministre qui en a rédigé la préface). Ces 56 portraits sont regroupés selon le domaine de la science concerné, et huit sont des « mathématiciennes ». Bien sûr, il y a de grosses restrictions : la période (avant la Révolution française) et le lieu (en France) ; ainsi ni Marie Curie, ni Emmy Noether n'y figurent. Parmi les chapitres qui m'ont particulièrement intéressée : celui sur Mme du Châtelet et la révolution newtonienne qui a opposé les partisans de Descartes et ceux de Newton.

Ce livre, qui est fort intéressant en soi, pourra alimenter des discussions sur la place des femmes en sciences, question qui est toujours d'actualité.

À venir :

En français :	Jeux Mathématiques et vice versa, L'empire des nombres, Le calcul et l'imprévu, Visualiser la quatrième dimension, Mathématiques, Promenades Mathématiques, ...
En anglais :	Dissections : plane and fancy, The pea and the sun, Statistics and public policy, The Mathematical traveler, Euclid I the rainforest, Misbehaviour of Markets ...

Robert Bilinski
Collège Montmorency
rbilinski@gmail.com

Vous venez de lire un ouvrage qui vous a passionné ? Ou qui vous a choqué ? Nous attendons vos commentaires : un bref texte que vous postez à Robert Bilinski, Dép. de Maths, 475, boul. de L'avenir, Laval (Québec), H7N 5H9. Vous pouvez aussi utiliser le courrier électronique (rbilinski@cmontmorency.qc.ca).