

CONTRIBUTEURS

ACT-1XXX Cours de première année

aut., cre. Alec James van Rassel

src. Ilie Radu Mitric

src. Hélène Cossette

src. Thomas Landry

Compléments de mathématiques

Algèbre linéaire

Soit :

$$\frac{A}{B} = Q \text{ remainder } R$$

où

A Nombre dividende.

B Nombre diviseur.

› Selon la deuxième équation ci-dessous, on l'appelle le *module*.

Q Quotient.

R Restant.

On peut donc aussi trouver que $A \bmod B = R$.

L'opérateur de congruence \equiv nous indique que 2 nombres ont le même restant.

Donc, $A \equiv B \pmod{C}$ implique que $A \bmod C = B \bmod C$.

› P. ex., $26 \bmod 5 = 1$ et $11 \bmod 5 = 1$ donc $26 \equiv 11 \pmod{5}$.

Intégrales utiles à connaître

Polynômes

$$\int \frac{1}{ax+b} dx = \frac{1}{a} \ln(ax+b) + C \quad \int x^{\frac{p}{q}} dx = \frac{q}{p+q} x^{\frac{p+q}{q}} + C$$

Fonctions exponentielles et logarithmiques

$$\int a^x dx = \frac{a^x}{\ln(a)} + C \quad \int \ln(x) dx = x \ln(x) - x + C$$

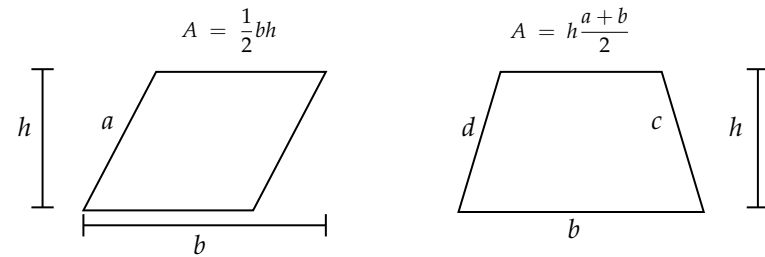
Dérivées utiles à connaître

$$\frac{\partial}{\partial x}(a^x) = a^x \ln(a)$$

$$\frac{\partial}{\partial x}(\sin(x)) = \cos(x)$$

$$\frac{\partial}{\partial x}(\cos(x)) = -\sin(x)$$

Aires de formes



Moyennes

La moyenne de n chiffres x_1, x_2, \dots, x_n .

Moyenne arithmétique

$$A(x) = \frac{1}{n} \sum_{i=1}^n x_i = \frac{x_1 + x_2 + \dots + x_n}{n}$$

Moyenne géométrique

$$G(x) = \left(\prod_{i=1}^n x_i \right)^{1/n} = (x_1 \times x_2 \times \dots \times x_n)^{1/n}$$

Note : $G(x) \leq A(x)$.

Sommations

$$\sum_{k=m}^n r^k = r^m \frac{1 - r^{n-m+1}}{1 - r}$$

$$\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2} \right)^2$$

$$\sum_{k=0}^{\infty} kv^k = \frac{v}{(1-v)^2}$$

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

Différenciation

Théorème des accroissements finis

Théorème de Rolle

Soit la fonction f qui répond aux critères suivants :

1. $f(x)$ est continue sur l'intervalle fermé $[a, b]$;
2. $f(x)$ est différentiable sur l'intervalle ouvert (a, b) ;
3. $f(a) = f(b)$.

Alors, il existe un nombre c tel que $a < c < b$ et $f'(c) = 0$; c'est-à-dire, $f(x)$ a un point critique dans (a, b) .

Soit la fonction f qui répond aux critères suivants :

1. $f(x)$ est continue sur l'intervalle fermé $[a, b]$;
2. $f(x)$ est différentiable sur l'intervalle ouvert (a, b) .

Alors, il existe un nombre c tel que $a < c < b$ et $f'(c) = \frac{f(b)-f(a)}{b-a}$.

Estimation Taylor

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!} (x - x_0)^n$$

$$\approx f(x_0) + f'(x_0)(x - x_0)$$

Théorème de Leibnitz

Soit :

- > une fonction $f(x, \alpha)$ continue sur $[a, b]$ et
- > des fonctions (dérivables) de α , $u(\alpha)$ et $v(\alpha)$, prenant valeur dans $[a, b]$.

Alors,

$$\frac{\partial}{\partial \alpha} \int_{u(\alpha)}^{v(\alpha)} f(x, \alpha) dx = \int_{u(\alpha)}^{v(\alpha)} \frac{\partial}{\partial \alpha} f(x, \alpha) dx + f(v(\alpha), \alpha) \frac{\partial}{\partial \alpha} v(\alpha) - f(u(\alpha), \alpha) \frac{\partial}{\partial \alpha} u(\alpha)$$

Domaines

\mathbb{R} : Real numbers, $x \in (-\infty, \infty)$.

\mathbb{Z} : Integers; all integers positive & negative, $x \in \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

\mathbb{N} : Natural numbers; all positive integers numbers, $x \in \{1, 2, 3, \dots\}$.

\mathbb{Q} : Rational numbers; numbers written as fractions, for example 1.25%, -0.4775 , $3.\overline{153}$, $\frac{1}{2}$, $\frac{4}{7}$.

$\mathbb{R} \setminus \mathbb{Q}$: Irrational numbers; for example π , e , $\sqrt{3}$.

Intégrale de Riemann-Stieltjes

L'intégrale de Riemann-Stieltjes généralise l'intégrale de Riemann avec une fonction g comme mesure de distance entre les points x_{i-1} et x_i .

Soit les fonction $f, g : [a, b] \rightarrow \mathbb{R}$.

On maintient les définitions de l'intégrale de Riemann et substitue $(x_{i-1} - x_i)$ pour $(g(x_{i-1}) - g(x_i))$ pour obtenir l'intégrale de Riemann-Stieltjes :

$$\lim_{\|P\| \rightarrow 0} \sum_{i=1}^n f(t_i)(g(x_{i-1}) - g(x_i)) = \int_a^b f(x) dg(x).$$

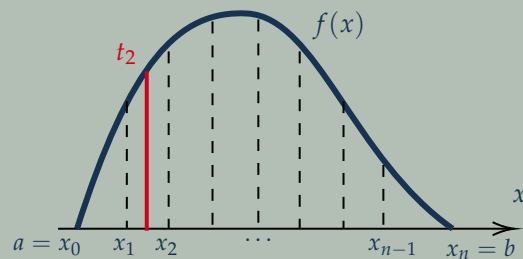
Intégrale de Riemann-Stieltjes

Intégrale de Riemann

Soit la fonction f continue sur l'intervalle $[a, b]$.

- > On divise l'ensemble $[a, b]$ en n sous-intervalles $c_i = [x_{i-1}, x_i]$.
- > Les n partitions P des sous-intervalles sont aux points $P = \{a = x_0 < x_1 < \dots < x_n = b\}$.
- > La norme des partitions est la longueur du plus long sous-intervalle $\|P\| = \max_{1 \leq i \leq n} \{x_i - x_{i-1}\}$.
- > On dénote le i^{e} point du sous-intervalle c_i par $t_i \in [x_{i-1}, x_i]$.

Visuellement :



On obtient donc l'intégrale de Riemann :

$$\lim_{\|P\| \rightarrow 0} \sum_{i=1}^n f(t_i)(x_i - x_{i-1}) = \int_a^b f(x) dx.$$

Fonction impaire

Une fonction est impaire (*odd*) lorsque $f(-x) = -f(x)$.

Par exemple, $\sin(-x) = -\sin(x)$.

Mathématiques financières

Intérêt simple

$$a(t) = 1 + it \qquad v(t) = \frac{1}{1 + it}$$

$$\text{Prix} = 100 \left(1 - \frac{it}{365} \right)^{-1}$$

facteurs d'actualisation et d'accumulation

$$a(t) = (1 + i)^t \qquad v(t) = (1 + i)^{-t}$$

$$= (1 - d)^{-t} \qquad = (1 - d)^t$$

$$= e^{\int_0^t \delta_s ds} \qquad = e^{-\int_0^t \delta_s ds}$$

Conversion de taux

$$d = \frac{i}{1 + i} \qquad i^R = \frac{i - r}{1 + r}$$

$$\text{Taux d'intérêt effectif annuel} \qquad i = \left(1 + \frac{i^{(m)}}{m} \right)^m - 1$$

$$\text{Taux d'intérêt nominal annuel} \qquad i^{(m)} = m \left((1 + i)^{1/m} - 1 \right)$$

$$\text{Taux d'escompte nominal annuel} \qquad d^{(m)} = m \left(1 - (1 - d)^{1/m} \right)$$

Rentes constantes

$$\ddot{a}_{\overline{n}|}^{(m)} = \frac{1 - v^n}{(i^{(m)}|d^{(m)})}$$

$$\ddot{a}_{\infty} = \frac{1}{(i|d)}$$

$$\ddot{s}_{\overline{n}|}^{(m)} = \frac{(1 + i)^n - 1}{(i^{(m)}|d^{(m)})}$$

Rentes continues

$$(\bar{I}\bar{s})_{\overline{n}|i} = \frac{\bar{s}_{\overline{n}|i} - n}{\delta} \qquad (\bar{D}\bar{s})_{\overline{n}|i} = \frac{nv^n - \bar{s}_{\overline{n}|i}}{\delta}$$

$$(\bar{I}\bar{a})_{\overline{n}|i} = \frac{\bar{a}_{\overline{n}|i} - nv^n}{\delta} \qquad (\bar{D}\bar{a})_{\overline{n}|i} = \frac{n - \bar{a}_{\overline{n}|i}}{\delta}$$

Rentes (dé)croissantes annuellement

$$(I^{(m)}\ddot{a})_{\overline{n}|}^{(m)} = \frac{\ddot{a}_{\overline{n}|}^{(m)} - nv^n}{(i|d^{(m)})} \qquad (D^{(m)}\ddot{a})_{\overline{n}|}^{(m)} = \frac{n - a_{\overline{n}|}^{(m)}}{(i|d^{(m)})}$$

$$(I^{(m)}\ddot{s})_{\overline{n}|}^{(m)} = \frac{\ddot{s}_{\overline{n}|}^{(m)} - n}{(i|d^{(m)})} \qquad (D^{(m)}\ddot{s})_{\overline{n}|}^{(m)} = \frac{n(1 + i)^n - s_{\overline{n}|}^{(m)}}{(i|d^{(m)})}$$

Rentes croissantes continûment

$$(I\ddot{a})_{\infty} = \frac{1}{d(i|d)}$$

Païement en continu, valeurs accumulée et actualisée

$$(\bar{I}\bar{s})_{\overline{n}|\delta_s, h(t)} = \int_0^n h(t) e^{\int_t^n \delta_s ds} dt$$

$$(\bar{I}\bar{a})_{\overline{n}|\delta_s, h(t)} = \int_0^n h(t) e^{-\int_0^t \delta_s ds} dt$$

Rentes avec croissance géométrique

$$\ddot{a}_{\overline{n}|r} = \frac{1 - \left[\frac{1+r}{1+i} \right]^n}{i - r} (1 + i) \qquad \ddot{s}_{\overline{n}|r} = \frac{(1 + i)^n - (1 + r)^n}{i - r} (1 + i)$$

T-Bills

$$\text{Prix} = 100 \left(1 - \frac{dt}{360} \right)^t$$

Obligations

Notation

- P Le **prix** de l'obligation;
- F La **valeur nominale** de l'obligation.
- › « *face amount* » ou « *par value* »;
 - › La valeur nominale est l'unité dans laquelle l'obligation est émise.
- C La valeur de remboursement de l'obligation;
- › « *redemption value* »;
 - › Par défaut, $F = C$.
- r Le taux de coupon par période de paiement;
- › « *coupon rate* »;
 - › Le montant de chaque coupon est Fr ;
 - › Le taux est habituellement donné sous base **annuelle** mais la majorité des obligations ont des coupons payables semi annuellement.
- g Le taux de coupon "spéciale" utilisé dans les formules mathématiques;
- › Taux tel que $Cg = Fr$.
- n Number of remaining coupon **payments**.
- i Le taux d'intérêt effectif par période de paiement;
- › C'est le « *yield-to-maturity* » pour une obligation se transigeant au prix P .
Donc, contrairement au taux r qui est une composante fixe de l'obligation, i va varier selon le prix P ;
 - › C'est donc le taux i tel que $P = PV(\text{bond payments})$.

Formule pour prix

$$\begin{aligned} P &= Fra_{\overline{n}|} + Cv^n \equiv Cga_{\overline{n}|} + Cv^n \\ &= C + (Fr - Ci)a_{\overline{n}|} \equiv C + (Cg - Ci)a_{\overline{n}|} \end{aligned}$$

Condition	Équivalent	Obligation transigée	anglais
$P > C$	$Fr > Ci$	avec prime	with premium
$P = C$	$Fr = Ci$	avec parité	at par
$P < C$	$Fr < Ci$	avec escompte	with discount

Amortissement d'obligations

Book value

$$BV_t = (Fr - C)_{n-t}a_j + C$$

Immunsation

$P(i)$ Valeur actualisée des flux monétaires au taux effectif i .

$$P(i) = \sum_{t=0}^n (A_t v^t)$$

Note La duration de *Macaulay* est surnommée « *duration* » par défaut alors que la convexité *modifiée* est surnommée « *convexité* » par défaut.

Approximation de Macaulay Basée sur la duration de Macaulay.

$$P(i) \approx P(i_0) \left(\frac{1+i_0}{1+i} \right)^{D_{\text{mac}}(i_0)}$$

Duration

$$D_{\text{mac}}(i) = \frac{-P'(\delta)}{P(\delta)} = \frac{\sum_{t=0}^n (t)(A_t v^t)}{P(i)}$$

$$D_{\text{mod}}(i) = \frac{-P'(i)}{P(i)} = \frac{\sum_{t=0}^n (t)(A_t v^{t+1})}{P(i)}$$

$$D_{\text{mod}}(i) = v D_{\text{mac}}(i)$$

Portfeuille de n obligations ayant chacune un prix de P_k :

$$D_{\text{mac}}(\text{ptf.}) = \frac{\sum_{k=1}^n D_{\text{mac}}(k\text{-ème obligation}) P_k}{\sum_{k=1}^n P_k}$$

Convexité

$$C_{\text{mod}}(i) = \frac{P''(i)}{P(i)} = \frac{\sum_{t=1}^n t(t+1)v^{t+2}A_t}{P(i)}$$

$$C_{\text{mac}}(i) = \frac{P''(\delta)}{P(\delta)} = \frac{\sum_{t=1}^n t^2 v^t A_t}{P(i)}$$

$$C_{\text{mod}}(i) = (C_{\text{mac}}(i) + D_{\text{mac}}(i))v^2$$

Approximations

Approximation linéaire Basée sur la duration modifiée.

$$P(i) \approx P(i_0)[1 - (i - i_0)D_{\text{mod}}(i_0)]$$

Obligation zéro-coupon de n années

Mesure	Égale
C_{mac}	n^2
D_{mac}	n
C_{mod}	$\frac{n(n+1)}{(1+i)^2}$
D_{mod}	$\frac{n}{1+i}$

Taux au comptant et taux à terme

Notation

r_t Taux de rendement annuel effectif d'un investissement sur t années.

- **Taux au comptant** ou « *spot rate* ».
- Parfois appelé le taux zéro-coupon car $r_t = P_t^{-1/t} - 1$ où P_t est le prix d'une obligation zéro-coupon.
- C'est en fait une moyenne des taux sur la période.

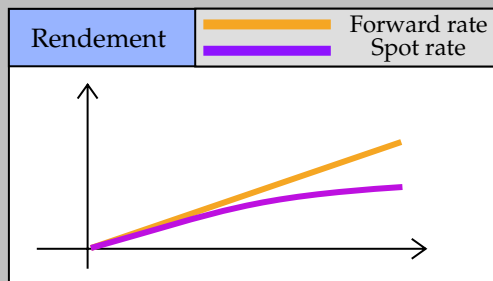
$$(1 + r_n)^n = \prod_{i=1}^n (1 + f_{t_i})$$

$f_{[t_1, t_2]}$ Taux d'intérêt annuel effectif en vigueur de t_1 à t_2 .

- **Taux à terme** ou « *forward rate* ».
- Habituellement, la période est d'un an ou d'un trimestre, mais en théorie il peut être appliqué sur n'importe quelle longueur de période.
- Le taux à terme est une anticipation pour une période future en date d'aujourd'hui.
- $(1 + f_{[t_1, t_2]})(1 + f_{[t_2, t_3]}) = (1 + f_{[t_1, t_3]})$
- Corrolaire :

$$f_{[t_1, t_2]} = \left[\frac{(1 + r_{t_2})^{t_2}}{(1 + r_{t_1})^{t_1}} \right]^{1/(t_2 - t_1)} - 1$$

Pour bien saisir la distinction entre les deux :



- Déterminer le taux de rendement i (« *Yield-to-Maturity* », « *IRR* ») qui, en actualisant les CF_t , reproduit le prix P .

$$4. P = \sum_t \frac{CF_t}{(1+r_t)^t} = \sum_t \frac{CF_t}{(1+i)^t}$$

Application aux obligations

- Identifier les flux monétaires de l'obligation CF_t .
- Actualiser chaque CF_t selon son taux à terme r_t pour déterminer le prix P .

Analyse probabiliste des risques actuariels

Analyse combinatoire

Analyse combinatoire La théorie mathématique du comptage.

Principe de base de comptage

Deux expériences sont effectuées.

La première a m événements possibles, et la deuxième a n événements possibles.

Ensemble, il y a $m \times n$ événements possible pour les deux expériences.

On peut visualiser ceci avec un tableau :

(1,1)	(1,2)	...	(1,n)
(2,1)	(2,2)	...	(2,n)
⋮	⋮	⋱	⋮
(m,1)	(m,2)	...	(m,n)

➤ Par exemple, la première cellule à l'événement 1 pour l'expérience 1 et l'événement 2 pour l'expérience 2.

Théorèmes probabilistes

Théorème du binôme

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}, \forall n \in \mathbb{N}$$

Théorème multinomial

$$(x_1 + \dots + x_r)^n = \sum_{\substack{(n_1, \dots, n_r): \\ n_1 + \dots + n_r = n}} \binom{n}{n_1, \dots, n_r} x_1^{n_1} \dots x_r^{n_r}$$

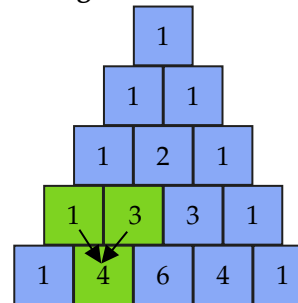
Relations factoriels

$$\binom{n}{k} = \binom{n}{n-k}$$

Règle de Pascal

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Triangle de Pascal



- Triangle des coefficients binomiaux
- Chaque nombre est la somme des 2 nombres directement au-dessus.

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Moments

Moment d'ordre n (autour de l'origine).

$$E[X^n] = \sum_i x_i^n \Pr(X = x_i)$$

Moment *centré* d'ordre n .

$$E[(X - E[X])^n] = \sum_i (x_i - E[X])^n \Pr(X = x_i)$$

Moment *réduit* d'ordre n .

$$E\left[\left(\frac{X}{\sqrt{V(X)}}\right)^n\right] = \sum_i \left(\frac{x_i}{\sqrt{V(X)}}\right)^n \Pr(X = x_i)$$

Moment *centré-réduit* d'ordre n .

$$E\left[\left(\frac{X - E[X]}{\sqrt{V(X)}}\right)^n\right] = \sum_i \left(\frac{x_i - E[X]}{\sqrt{V(X)}}\right)^n \Pr(X = x_i)$$

Coefficient d'asymétrie (*Skewness*)

$$\gamma_X = E\left[\left(\frac{X - E[X]}{\sqrt{V(X)}}\right)^3\right]$$

Coefficient d'aplatissement (*Kurtosis*)

$$\kappa_X = E\left[\left(\frac{X - E[X]}{\sqrt{V(X)}}\right)^4\right]$$

Fonction stop-loss

$$\pi_X(d) = E[\max(X - d; 0)]$$

Fonction d'excès-moyen

$$\pi_X(d) = E[X - d | X > d]$$

Note : Il est intéressant de savoir que les moments impairs d'une loi normal avec

moyenne nulle sont nuls. Ceci est la normal avec une moyenne nulle est parfaitement symétrique tel que $f(-x) = -f(x)$; pour plus de détails, voir [ce vidéo YouTube](#).

Raccourci bernoulli

Soit

$$X = \begin{cases} a & p \\ b & 1 - p \end{cases}$$

Alors

$$\text{Var}(X) = (b - a)^2 p(1 - p)$$

Conditionnels

$$E[X] = E_Y[E[X|Y]] \quad V(X) = E_Y[V(X|Y)] + V_Y(E[X|Y])$$

$$\text{Cov}(X, Y) = E[XY] - E[X]E[Y]$$

1. $\text{Cov}(X, Y) = \text{Cov}(Y, X)$
2. $\text{Cov}(X, X) = V(X)$
3. $\text{Cov}(X, Y) \perp 0$
4. $\text{Cov}(c, X) = 0$
5. $\text{Cov}(cX, Y) = c\text{Cov}(X, Y)$
6. $\text{Cov}(\sum_{i=1}^n \alpha_i X_i, \sum_{j=1}^m \beta_j Y_j) = \sum_{i=1}^n \sum_{j=1}^m \alpha_i \beta_j \text{Cov}(X_i, Y_j)$

$$V(\sum_{i=1}^n \alpha_i X_i) = \sum_{i=1}^n \sum_{j=1}^m \alpha_i^2 V(X_i) + 2 \sum_{i < j} \alpha_i \alpha_j \text{Cov}(X_i, X_j)$$

$$\rho_P(X, Y) = \frac{\text{Cov}(X, Y)}{\sigma_X \sigma_Y}$$

Convolution

Convolution de deux variables aléatoires

Soit deux v.a. continues indépendantes X et Y .

Le produit de convolution de X et Y est :

$$f_X * f_Y(s) = f_{X+Y}(s) = \int_{-\infty}^{\infty} f_X(s - y) f_Y(y) dy$$

$$F_{X+Y}(s) = \int_{-\infty}^{\infty} F_X(s - y) f_Y(y) dy$$

Soit deux v.a. discrètes indépendantes X et Y .

Le produit de convolution de X et Y est :

$$\Pr(X + Y = s) = \sum_{y=0}^s \Pr(X = s - y) \Pr(Y = y)$$

Variable aléatoire

Soit X une variable aléatoire.

Soit la fonction

de densité	$f_X(x) = \Pr(X = x)$	Density Function
de masse de probabilité	$f_X(x) \neq \Pr(X = x)$	Probability Mass Function (PMF)
de répartition	$F_X(x) = \Pr(X \leq x)$	Cumulative Density Function (CDF)
de survie	$S_X(x) = \Pr(X > x)$	Survival Function (CDF)

$F_X(x)$

Lois multivariées

Loi multinomiale

$$\Pr(X_1 = x_1, \dots, X_r = x_r) = \binom{n}{x_1, \dots, x_r} p_1^{x_1} \dots p_r^{x_r}$$

Loi normale multivariée

$$f_{\mathbf{X}}(\mathbf{x}) = \frac{1}{(2\pi)^{\frac{n}{2}} \sqrt{\det(\Sigma)}} e^{-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu})^\top \Sigma^{-1}(\mathbf{x} - \boldsymbol{\mu})}$$

Théorèmes limites

Inégalité de Markov

Soit la variable aléatoire (non-négative) X .

Alors $\forall a > 0$ on a :

$$\Pr(X \geq a) \leq \frac{E[X]}{a}$$

Inégalité de Tchebychev

Soit la variable aléatoire X avec $\mu, \sigma^2 < \infty$.

Alors $\forall k > 0$ on a :

$$\Pr(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2} \quad \text{ou} \quad \Pr(|X - \mu| \geq k^*) \leq \frac{\sigma^2}{(k^*)^2}$$

Loi (faible) des grands nombres (WLLN)

Soit la suite de variables aléatoires (iid) X_1, \dots, X_n tel que $\forall i = 1, \dots, n$
 $E[X_i] = \mu$ et $\text{Var}[X_i] = \sigma^2 > 0$.

Alors $\forall \epsilon > 0$ où $\bar{X}_n = \frac{X_1 + \dots + X_n}{n}$:

$$\lim_{n \rightarrow \infty} \Pr(|\bar{X}_n - \mu| \geq \epsilon) \rightarrow 0 \quad \Leftrightarrow \quad \bar{X}_n \xrightarrow[n \rightarrow \infty]{\mathbb{P}} \mu$$

où \mathbb{P} représente la convergence en probabilité.

Théorème central limite (CLT)

Soit la suite de variables aléatoires (iid) X_1, \dots, X_n tel que $\forall i = 1, \dots, n$
 $E[X_i] = \mu$ et $\text{Var}[X_i] = \sigma^2 > 0$.

Alors pour $S_n = \sum_{i=1}^n X_i$:

$$\lim_{n \rightarrow \infty} \Pr\left(\frac{S_n - E[S_n]}{\sqrt{\text{Var}(S_n)}} \leq z\right) = \Phi(z) \quad \Leftrightarrow \quad \frac{S_n - E[S_n]}{\sqrt{\text{Var}(S_n)}} \xrightarrow{\mathcal{L}} \mathcal{N}(0, 1)$$

où \mathcal{L} représente la convergence en distribution ("law").

Méthodes numériques

Génération de nombres aléatoires uniformes

Congruence

Les nombres a et b sont dits *équivalents*, ou **congruents modulo m** si leur différence est divisible par m .

$$a \equiv b \pmod{m} \Leftrightarrow \frac{b-a}{m} = k, k \in \mathbb{Z}$$

P. ex. :

> $5 \equiv 14 \pmod{3}$ car $\frac{14-5}{3} = 3$ —14 et 5 sont distants de 9, un multiple de 3.

> $-1 \equiv 5 \pmod{2}$ car $\frac{5-(-1)}{2} = 3$ —5 et -1 sont distants de 6, un multiple de 3.

Générateurs congruentiels linéaires

Tout nombre dans la suite générée détermine le nombre suivant avec la relation $x_i = (ax_{i-1} + c) \pmod{m}$ où $0 \leq x_i < m$ et :

a Multiplicateur.

c L'incrément.

> Si $c = 0$, le générateur est *multiplicatif*.

> Sinon, il est *mixe*.

m Le module.

x_0 L'amorce (« seed »).

> Pour générer des nombres entre 0 et 1, on définit $u_i = \frac{x_i}{m}$

Arithmétique des ordinateurs

Unité	Capacité	Symbole
Bit	1 b	b
Octet (« byte »)	8 b	o
Kiloctet	1 024 o	ko
Megaoctet	1 048 576 o	mo
Gigaoctet	1 073 741 824 o	go

Base de numération b

Une "base" de numération correspond au nombre de chiffres utilisé pour représenter des nombres.

> Nous utilisons la base 10 comportant 10 chiffres (0, 1, ..., 9).

> La base 2 correspond au binaire avec 0 et 1 comme chiffres.

> Au delà de 10, on utilise des lettres pour représenter des chiffres.

> P. ex., la base 12 a les chiffres 0, 1, 2, ..., 9, A, B, C.

Représentation d'un nombre sous une base quelconque

Notation

x Nombre composé de m chiffres (ou symboles).

b Base de numération.

Sous cette notation, on écrit $x = x_{m-1}x_{m-2} \dots x_1x_0$ où $x_i \in [0, b-1]$.

On peut réécrire ce chiffre comme $x = \sum_{i=0}^{m-1} x_i b^i$.

Par exemple, le nombre 12 sous la base 10 est $12 = 1 \times 10^1 + 2 \times 10^0$.

Quotient d'une division

Partie entière de la division de deux entiers a et d : $q = \left\lfloor \frac{a}{d} \right\rfloor$.

P. ex. : $\left\lfloor \frac{13}{3} \right\rfloor = 4$.

☰ Restant d'une division

L'écart entre le nombre et le prochain multiple de la division :

$$r = a - d \times \left\lfloor \frac{a}{d} \right\rfloor = a \bmod d.$$

P. ex. : $13 - 3 \times \left\lfloor \frac{13}{3} \right\rfloor = 13 - 3 \times 4 = 1.$

› Il s'ensuit que $r \in \{0, 1, d - 1\}.$

📄 Convertir un nombre de la base 10 à une base b

Pour convertir un nombre a vers la base b , on trouve récursivement le restant $r = a \bmod b$ avec le quotient de la division précédente jusqu'à ce que le quotient soit nul.

P. ex., pour convertir le nombre 12 à la base 2 :

› $a \bmod b = 12 \bmod 2 = 0 = x_0$, le quotient est $\left\lfloor \frac{12}{2} \right\rfloor = 6$ et le restant de la division 0.

› $q \bmod b = 6 \bmod 2 = 0 = x_1$, le quotient est $\left\lfloor \frac{6}{2} \right\rfloor = 3$ et le restant de la division 0.

› $3 \bmod 2 = 1 = x_2$, le quotient est $\left\lfloor \frac{3}{2} \right\rfloor = 1$ et le restant de la division 1.

› $1 \bmod 2 = 1 = x_3$, le quotient est $\left\lfloor \frac{1}{2} \right\rfloor = 0$ et le restant de la division 1.

› Donc, $12 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$