

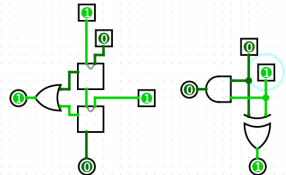
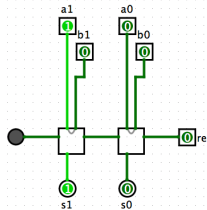
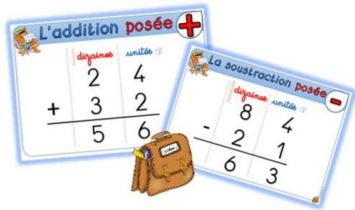
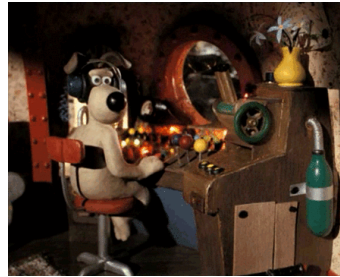
Concepts Informatiques I

2025–2026

Matthieu Picantin



- ♦ systèmes de numération & arithmétique associée
- ♦ représentation des nombres & arithmétique machine
- ♦ codes, codages, entropie, compression
- ♦ contrôle d'erreur (détection, correction)
- ♦ crypto (confidentialité, authenticité, intégrité)
- ♦ logique et calcul propositionnel
- ♦ circuits combinatoires



La "preuve" par 9 pour un calcul en base 10

- ♦ n'est pas une *preuve* de correction, mais un moyen simple de vérification (avec un certain indice de confiance): c'est un test, une épreuve
- ♦ utilise les propriétés de l'arithmétique modulaire
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo 9* (obtenus en faisant la somme de leurs chiffres, etc)

$$\sum_{k=0}^p a_k 10^k \equiv \sum_{k=0}^p a_k \pmod{9}$$



La "preuve" par 9 pour un calcul en base 10

- ♦ n'est pas une *preuve* de correction, mais un moyen simple de vérification (avec un certain indice de confiance): c'est un test, une épreuve
- ♦ utilise les propriétés de l'arithmétique modulaire
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo 9* (obtenus en faisant la somme de leurs chiffres, etc)

$$\sum_{k=0}^p a_k 10^k \equiv \sum_{k=0}^p a_k \pmod{9}$$

La "preuve" par $b - 1$ pour un calcul en base b

- ♦ n'est pas une *preuve* de correction, mais un moyen simple de vérification (avec un certain indice de confiance): c'est un test, une épreuve
- ♦ utilise les propriétés de l'arithmétique modulaire
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo $b - 1$* (obtenus en faisant la somme de leurs chiffres, etc)

$$\sum_{k=0}^p a_k b^k \equiv \sum_{k=0}^p a_k \pmod{b - 1}$$

La "preuve" par 11 pour un calcul en base 10

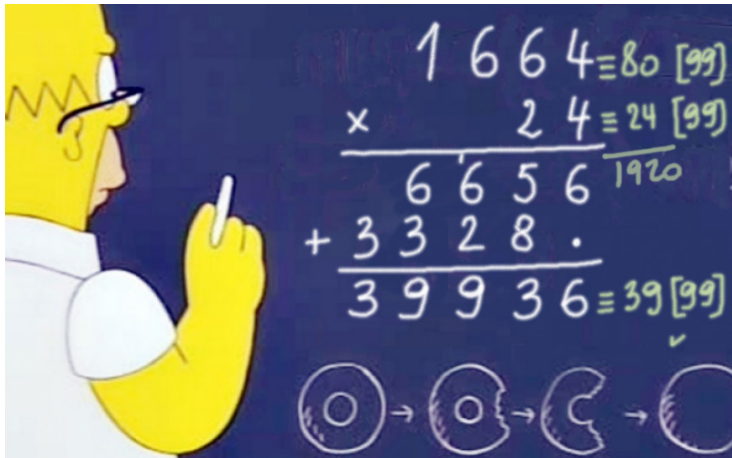
- ♦ est un moyen simple de vérification (avec certain indice de confiance)
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo 11* (obtenus en faisant la somme alternée de leurs chiffres, etc)

$$\sum_{k=0}^p a_k 10^k \equiv \sum_{k=0}^p (-1)^k a_k \pmod{11}$$

La "preuve" par 99 pour un calcul en base 10

- ♦ est un moyen simple de vérification (avec meilleur indice de confiance)
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo 99* (obtenus en faisant la somme des blocs de deux chiffres, etc)

$$\sum_{k=0}^p a_k 10^k \equiv \sum_{k=0}^{p/2} a_{2k+1} a_{2k} \pmod{99}$$



La "preuve" par $b + 1$ pour un calcul en base b

- ♦ est un moyen simple de vérification (avec certain indice de confiance)
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo* $b + 1$ (obtenus en faisant la somme alternée de leurs chiffres, etc)

$$\sum_{k=0}^p a_k b^k \equiv \sum_{k=0}^p (-1)^k a_k \pmod{b+1}$$

La "preuve" par $b^2 - 1$ pour un calcul en base b

- ♦ est un moyen simple de vérification (avec meilleur indice de confiance)
- ♦ consiste à "refaire" le calcul mais en considérant les nombres *modulo* $b^2 - 1$ (obtenus en faisant la somme des blocs de deux chiffres, etc)

$$\sum_{k=0}^p a_k b^k \equiv \sum_{k=0}^{p/2} a_{2k+1} a_{2k} \pmod{b^2 - 1}$$



... épreuves par \triangle , par $—$, par $\triangle\triangle$

Divisibilité par 2, 4, 5, 8, 10, 16, etc (en base 10)

- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 2 (*resp.* par 5) ssi a_0 l'est
- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 8 ssi $(a_2 a_1 a_0)_{10}$ l'est

Divisibilité par 3, 9, 11, etc (en base 10)

- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 3 (*resp.* par 9) ssi $a_p + \cdots + a_0$ l'est
- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_p + \cdots + a_2 - a_1 + a_0$ l'est

Divisibilité par 6, 12, 14, 15, 18, 20, etc (en base 10)

- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $(a_p \cdots a_0)_{10}$ est divisible par 2 **et** par 3

Divisibilité par 7, 13, 17, 19, etc (en base 10)

- ♦ $(a_p \cdots a_0)_{10}$ est divisible par 7 ssi $(a_p \cdots a_1)_{10} + 5a_0$ l'est

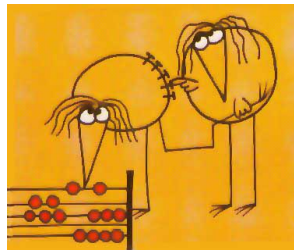
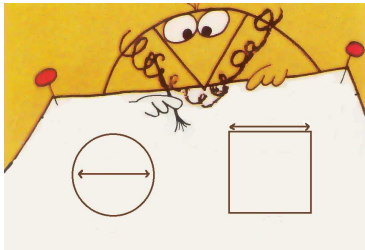
Et dans une base b quelconque?

Numération positionnelle en base $b > 1$

♦ exactement b chiffres, disons $\{0, 1, \dots, b-1\}$

♦ $(a_p \dots a_0, a_{-1} a_{-2} \dots a_{-q})_b$ représente le nombre réel $\sum_{k=-q}^p a_k b^k$, soit

$$a_p \times b^p + \dots + a_2 \times b^2 + a_1 \times b + a_0 + a_{-1} \times \frac{1}{b} + a_{-2} \times \frac{1}{b^2} + \dots + a_{-q} \times \frac{1}{b^q}$$



Comment convertir une écriture en base b $(a_p \cdots a_0, a_{-1} a_{-2} \cdots)_b$
 vers une écriture en base d ? $(c_q \cdots c_0, c_{-1} c_{-2} \cdots)_d$

Méthode (par divisions successives) pour la partie entière

♦ on convertit la partie entière $(a_p \cdots a_0)_b = (c_q \cdots c_0)_d$

Méthode par multiplications successives pour la partie fractionnaire

- ♦ on multiplie $(0, a_{-1} \cdots a_{-t})_b$ par d (calcul en base b toujours)
- ♦ on collecte la partie entière c_{-1} de ce produit
- ♦ on recommence avec sa partie fractionnaire
- ♦ on s'arrête quand $(0, c_{-1} \cdots c_{-r})_d$
 le produit est nul: on renvoie la **suite finie** des chiffres collectés
 ou déjà obtenu: on renvoie la **suite ultimement périodique**

$$(0, \underbrace{c_{-1} \cdots c_{-r}}_{\text{pré-période}} (\underbrace{c_{-r-1} \cdots c_{-r-s}}_{\text{période}})^\omega)_d$$

On adapte les autres méthodes: dépliage/repliage, recomp ou Horner.
 On peut aussi utiliser la périodicité...

Numération positionnelle en base $b > 1$

- ♦ exactement b chiffres, disons $\{0, 1, \dots, b-1\}$
- ♦ $(a_p \cdots a_0, a_{-1} a_{-2} \cdots a_{-q})_b$ représente le nombre réel $\sum_{k=-q}^p a_k b^k$
- ♦ $(a_p \cdots a_0, a_{-1} a_{-2} \cdots)_b$ représente le nombre réel $\sum_{k=-\infty}^p a_k b^k$

Non-unicité des représentations

- ♦ certains nombres admettent plusieurs représentations dans une même base

$$(1)_{10} = (0, 9999 \cdots)_{10}$$

$$(1)_{d+1} = (0, dddd \cdots)_{d+1}$$

Les nombres b -adiques pour une base $b > 1$

♦ exactement b chiffres, disons $\{0, 1, \dots, b-1\}$

♦ $(\dots a_2 a_1 a_0, a_{-1} a_{-2} \dots a_{-q})_b$ représente le nombre b -adique $\sum_{k=-q}^{+\infty} a_k b^k$

♦ tout nombre b -adique admet un opposé b -adique (ou *complément*)

$$(\dots 001)_{10} + (\dots 999)_{10} = 0$$

$$(\dots 001)_2 + (\dots 111)_2 = 0$$

$$(\dots 001)_{d+1} + (\dots dddd)_{d+1} = 0$$

