Principes de fonctionnement des machines binaires

2020-2021

Matthieu Picantin



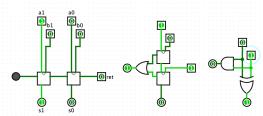


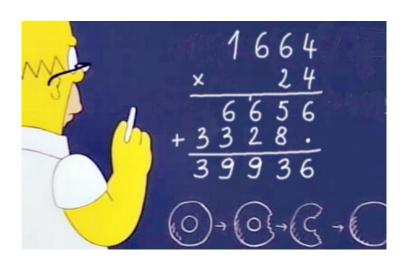


- numération et arithmétique
- numération et arithmétique en machine
- numérisation et codage (texte, images)
- compression, cryptographie, contrôle derreur
- logique et calcul propositionnel
- circuits numériques









picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020 4 / 14

Addition posée

- on s'appuie sur la table d'addition en base b
- on dispose les nombres en colonnes: chiffres des unités, chiffres des b-aines, chiffres des b²-aines, etc
- on effectue la somme des chiffres de la colonne la plus à droite: on pose son chiffre des unités on reporte la retenue sur la ou les colonnes à gauche
- on recommence sur la colonne immédiatement à gauche, etc

Multiplication posée

- on s'appuie sur les tables d'addition et de multiplication en base b
- on dispose les deux nombres (a_p···a₀)_b et (c_q···c₀)_b en colonnes: chiffres des unités, chiffres des b-aines, chiffres des b²-aines, etc
- on effectue le produit de $(a_p \cdots a_0)_b$ par le nombre $c_k b^k$ pour $0 \le k \le c$
- on conclut avec l'addition posée de ces q + 1 produits intermédiaires

picantin@irif.fr PF1 Amphi#02 07□09/09/2020 5 / 14

Addition posée

- on s'appuie sur la table d'addition en base b
- on dispose les nombres en colonnes: chiffres des unités, chiffres des b-aines, chiffres des b²-aines, etc
- on effectue la somme des chiffres de la colonne la plus à droite: on pose son chiffre des unités on reporte la retenue sur la ou les colonnes à gauche
- on recommence sur la colonne immédiatement à gauche, etc

Multiplication posée

- on s'appuie sur les tables d'addition et de multiplication en base b
- on dispose les deux nombres (a_p···a₀)_b et (c_q···c₀)_b en colonnes: chiffres des unités, chiffres des b-aines, chiffres des b²-aines, etc
- on effectue le produit de $(a_p \cdots a_0)_b$ par le nombre $c_k b^k$ pour $0 \le k \le q$
- on conclut avec l'addition posée de ces q + 1 produits intermédiaires

picantin@irif.fr PF1 Amphi#02 07□09/09/2020 5 / 14

La "preuve" par 9

- n'est pas une preuve de correction, mais un moyen simple de vérification (avec un certain indice de confiance)
- 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)

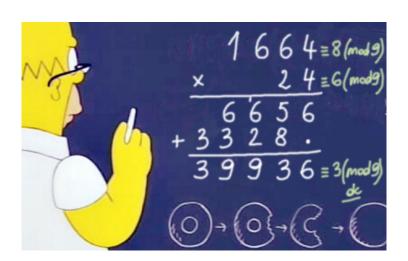
$$\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k \; (\text{mod } 9)$$

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)
- 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)

$$\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k \; (\text{mod } 9)$$

picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020 6 / 14



picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020

7/14

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)

$$\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p/2} a_{2k+1} a_{2k} \; (\text{mod 99})$$

picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020 8 / 14

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)

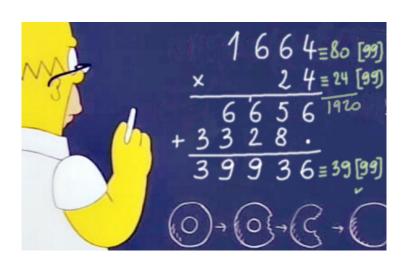
$$\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} (-1)^k a_k \pmod{11}$$

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)

$$\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p/2} a_{2k+1} a_{2k} \; (\text{mod 99})$$

picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020 8 / 14



picantin@irif.fr PF1 Amphi#02 07\u00ed09/09/2020 9 / 14

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)
- 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)

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

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)

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

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 b² (obtenus en faisant la somme des blocs de deux chiffres, etc)

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

picantin@irif.fr PF1 Amphi#02 07□09/09/2020 11 / 14

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)

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

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 b² − 1 (obtenus en faisant la somme des blocs de deux chiffres, etc)

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

07 109/09/2020 picantin@irif.fr Amphi#02 11 / 14

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

Amphi#02 07 🗆 09/09/2020 picantin@irif.fr

12 / 14

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

Amphi#02 picantin@irif.fr 07 09/09/2020 12 / 14

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

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

- $(a_p \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 6 ssi $a_0 + \cdots + a_0$ est divisible par 3 et a_0 par 2
- (a_p ··· a₀)₁₀ est divisible par 9 ssi a_n + ··· + a_n l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_0 a_1 + a_0$ l'est

- $(a_p \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 6 ssi $a_0 + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_0 a_1 + a_0$ l'est

- $(a_p \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $a_p + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_p + \cdots + a_n$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_2 a_1 + a_0$ l'est

- $(a_p \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $a_p + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_p + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_2 a_1 + a_0$ l'est

- $(a_p \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $a_p + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_p + \cdots + a_0$ l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_2 a_1 + a_0$ l'est

- $(a_0 \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $a_p + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_p + \cdots + a_0$ l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_2 a_1 + a_0$ l'est

Divisibilité par 7, en base 10

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

- $(a_0 \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- (a_p ··· a₀)₁₀ est divisible par 5 ssi a₀ 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $a_p + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_p + \cdots + a_0$ l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_2 a_1 + a_0$ l'est

Divisibilité par 7, en base 10

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

- $(a_0 \cdots a_0)_{10}$ est divisible par 2 ssi a_0 l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 4 ssi $(a_1 a_0)_{10}$ l'est
- $(a_0 \cdots a_0)_{10}$ est divisible par 5 ssi a_0 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, 6, 9 ou 11, en base 10

- $(a_0 \cdots a_0)_{10}$ est divisible par 3 ssi $a_0 + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 6 ssi $a_p + \cdots + a_0$ est divisible par 3 et a_0 par 2
- $(a_p \cdots a_0)_{10}$ est divisible par 9 ssi $a_p + \cdots + a_0$ l'est
- $(a_p \cdots a_0)_{10}$ est divisible par 11 ssi $(-1)^p a_0 + \cdots + a_2 a_1 + a_0$ l'est

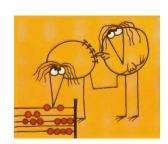
Divisibilité par 7, en base 10

• $(a_p \cdots a_0)_{10}$ 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

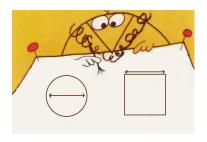
- exactement *b* chiffres, disons $\{0, 1, \dots, b-1\}$
- $(a_p \cdots a_0, a_{-1}a_{-2} \cdots a_{-q})_b$ représente le nombre réel $\sum_{k=-a}^{P} a_k b^k$, soi

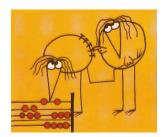


Numération positionnelle en base b > 1

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

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



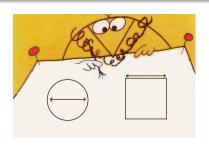


picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020 13 / 14

Numération positionnelle en base b > 1

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

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





picantin@irif.fr PF1 Amphi#02 07⊔09/09/2020 13 / 14

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

Comment convertir une écriture en base b $(a_{p} \cdots a_{0}, a_{-1} a_{-2} \cdots)_{b}$ $(c_a \cdots c_0, c_{-1}c_{-2}\cdots)_d$ vers une écriture en base d?

Méthode (par divisions successives) pour la partie entière

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

14 / 14 picantin@irif.fr Amphi#02 07 09/09/2020

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
 le produit est nul: on renvoie la suite finie des chiffres collectés
 ou déjà obtenu: on renvoie la suite ultimement périodique

picantin@irif.fr PF1 Amphi#02 07□09/09/2020 14 / 14

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····c_{-r})_d
 le produit est nul: on renvoie la suite finie des chiffres collectés
 ou déjà obtenu: on renvoie la suite ultimement périodique

picantin@irif.fr PF1 Amphi#02 07□09/09/2020 14 / 14

Comment convertir une écriture en base b $(a_{p} \cdots a_{0}, a_{-1} a_{-2} \cdots)_{b}$ vers une écriture en base d?

$$(C_0 \cdots C_0, C_{-1}C_{-2} \cdots)_d$$

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

$$(0,\underbrace{C_{-1}\cdots C_{-r}}_{\text{principle}}(\underbrace{C_{-r-1}\cdots C_{-r-s}}_{\text{principle}})^{\omega})_d$$

07 109/09/2020 picantin@irif.fr Amphi#02 14 / 14