# 33

# Circuits synchrones, nombres 2-adiques, et codages RSA

Jean Vuillemin
Digital PRL, Rueil Malmaison

[résumé par Paul Zimmermann]

L'exposé traite de l'arithmétique 2-adique et de ses propriétés, notamment vis-à-vis des circuits combinatoires. On montre l'équivalence entre un nombre 2-adique et un fil d'un circuit, entre une fonction sur les nombres 2-adiques et un circuit. On montre aussi que les différents types de circuits (combinatoire, synchrone) correspondent à des classes de fonctions (continues, strictes, en ligne). L'arithmétique $p$-adique a été utilisée pour un codage rapide d'informations par l'algorithme RSA.

## 1 Nombres $p$-adiques

Un rationnel 2-adique a une notation de la forme suivante

$$R = r_{-v} \dots r_0.r_1 \dots r_n \dots$$

qui représente le nombre $\sum_{k \geq -v} r_k 2^k$. Par exemple, $0.101(110)^*$ représente $2 + 8 + 16(3 + 3 \cdot 8 + 3 \cdot 8^2 + \cdots) \simeq 10 + 16 \cdot 3 \cdot 1/(1-8) = 10 - 48/7 = 22/7$. A l'opposé de l'arithmétique réelle, qui représente les nombres des poids forts vers les poids faibles, l'arithmétique 2-adique va des poids faibles vers les poids forts, et est donc en quelque sorte duale de l'arithmétique réelle.
Si $p$ est un entier premier, tout nombre rationnel a une représentation $p$-adique : $\mathbb{Q} \subset \mathbb{Q}_p$. La représentation $p$-adique des rationnels est ultimement périodique, et peut donc s'écrire de manière finie sous la forme $r_{-v} \dots r_0.r_1 \dots r_k (r_{k+1} \dots r_{k+l})^*$ où $r_{-v} \dots r_0.r_1 \dots r_k$ représente la partie positive $r_{-v}p^{-v} + \cdots + r_0 + r_1 p + \cdots + r_k p^k$ et $(r_{k+1} \dots r_{k+l})^*$ la partie négative $(r_{k+1}p^{k+1} + \cdots + r_{k+l}p^{k+l})/(1 - p^l)$.
Ainsi dans $\mathbb{Q}_2$, $-16$ s'écrit $0.000(1)^*$, $-6/7$ s'écrit $0.11(011)^*$, $-2/3$ s'écrit $0.1(01)^*$. La procédure Maple ci-dessous calcule une forme 2-adique d'un rationnel $q$ :

```
twoadic := proc(q) # returns a list [v,[r_{-v}, r_{-v+1}, ...]]
local a,b;
    if q<0 then # q = a - 2^b with 2^b>=|q|
            b:=ceil(log(-q)/log(2));
            a:=q+2^b;
            add(procname(a),[-b,[[1]]])
    elif type(q,nonnegint) then [0,convert(q,base,2)]
    elif denom(q) mod 2 = 0 then div2(procname(2*q))
    else # q = a/b with a and b odd : q = a/(1+2*c)
        odddiv(numer(q),(denom(q)-1)/2)
    fi;
end:
```

où `add` calcule la somme de deux représentations 2-adiques, et `odddiv(a,b)` calcule le quotient 2-adique de $a$ par $1+2b$.

```
> twoadic(1),twoadic(-1),twoadic(-6/7);

            [0, [1]],   [0, [[1]]],   [0, [0, 1, 1, 0, [1, 1, 0]]]
```

De la même façon, il est possible de retrouver le rationnel correspondant à un nombre 2-adique :

```
value := proc(x)
local v,l,s,t;
    v:=op(1,x); l:=op(2,x); s:=0; t:=2^(-v);
    while l<>[] and not type(l[1],list) do
        s := s + l[1]*t;
        l := subsop(1=NULL,l);
        t := 2*t;
    od;
    if l=[] then s
    else
        l := l[1];
        s + sum(l[i]*2^(i-1),i=1..nops(l))*t/(1-2^nops(l))
    fi
end:
```

```
> value(twoadic(355/113)), value(twoadic(-3/97));

                                   355
                                   ---, -3/97
                                   113
```

**Proposition 1** *Les rationnels 2-adiques forment un corps* $\mathbb{Q}_2 = \{0,1,+,-,\times,/\}$ *admettant* $\mathbb{Q}$ *comme sous-corps. Les entiers 2-adiques forment un anneau* $\mathbb{Z}_2 = \{0,1,+,-,\times\}$ *admettant* $\mathbb{Z}$ *et* $\mathbb{Z}/(1+2\mathbb{Z})$ *comme sous-anneaux.*

## 2 Circuits

Il est montré dans cette partie un lien direct entre les nombres 2-adiques et les circuits logiques synchrones. Plus précisément, on verra qu'on peut associer à tout fil d'un circuit un nombre 2-adique, que pour tout rationnel 2-adique, on peut construire un circuit le "calculant", et qu'il existe un lien entre les fonctions calculables par des circuits synchrones et les fonctions continues.

**Définition 1** *(Circuit digital) La valeur de toute variable d'un circuit digital $C$ est un bit qui ne peut changer qu'à des temps entiers :*

$$\forall v \in \mathcal{V}(C), t \in \mathbb{R}, v^t = v^{\lfloor r \rfloor} \in \{0,1\}$$

*où $v^t$ représente la valeur du point $v$ du circuit à l'instant $t$.*

Ainsi, chaque point d'un circuit (ou fil, puisque la tension est la même en tout point d'un fil) est mis en correspondance avec un nombre 2-adique $v^0.v^1\dots v^n\dots$ De la même façon, les composants d'un circuit sont mis en correspondance avec des opérations sur les nombres 2-adiques :

**Définition 2** *(Multiplexeur et circuit combinatoire) Le multiplexeur noté ? est une fonction de* $\mathbb{Z}_2^3$ *dans* $\mathbb{Z}_2$*, définie par*

$$?(c\ t\ f) = m \qquad \textit{tel que} \qquad m = \begin{cases} t & \textit{si } c = 1 \\ f & \textit{si } c = 0. \end{cases}$$

*Un circuit combinatoire est un circuit comportant des entrées* $i_0, \ldots, i_n, \ldots$*, des sorties* $o_0, \ldots, o_n, \ldots$*, des multiplexeurs, et tel qu'il existe un ordre total sur les fils des multiplexeurs :*

$$\forall ?(c\ t\ f) \Rightarrow m, \quad c, t, f < m.$$

Par exemple, le circuit suivant est un circuit combinatoire effectuant l'addition de trois bits $a, b, c$ avec retenue. Il comprend cinq multiplexeurs, $(a + b + c) \bmod 2$ est mis dans $s$ et $(a + b + c)$ div 2 dans $r$ :

$$?(b\ 0\ 1) \Rightarrow \bar{b}, \quad ?(a\ \bar{b}\ b) \Rightarrow x, \quad ?(c\ 0\ 1) \Rightarrow \bar{c}, \quad ?(x\ c\ b) \Rightarrow r, \quad ?(x\ \bar{c}\ c) \Rightarrow s.$$

Il est intéressant de constater le lien entre les fonctions calculables par des circuits combinatoires et les fonctions continues :

**Théorème 1** *Les assertions suivantes sont équivalentes :*

1. $f(i_0, \ldots, i_n, \ldots) \Rightarrow (o_0, \ldots, o_n, \ldots)$ *est calculable par un circuit combinatoire.*
2. *La fonction* $f(\sum i_n 2^n) = \sum o_n 2^n$ *est continue sur* $\mathbb{Z}_2$ *avec la norme* $|r_v r_{v+1} \ldots|_2 = 2^{-v}$.
3. *Chaque sortie dépend d'un nombre fini d'entrées.*

Par exemple, le mélange de deux entrées $\pi$ et les projections $\pi_0$ et $\pi_1$ sont des circuits combinatoires, donc représentent des fonctions continues :

$$\begin{aligned} a \bmod 2 + 2\pi(b, a \text{ div } 2) &\Rightarrow \pi(a, b) \\ a \bmod 2 + 2\pi_0(a \text{ div } 4) &\Rightarrow \pi_0(a, b) \\ \pi_0(a \text{ div } 2) &\Rightarrow \pi_1(a, b) \end{aligned}$$

Au passage, on aura remarqué que ces trois fonctions mettent en évidence un isomorphisme entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.

## 2.1 Circuits synchrones

**Définition 3** *(Registre et circuit synchrone) Le registre à décalage, noté* $2\times$*, est une fonction de* $\mathbb{Z}_2$ *dans* $\mathbb{Z}_2$*, définie par*

$$2 \times i \Rightarrow r \qquad \textit{tel que} \qquad r^0 = 0, r^{t+1} = i^t.$$

*Un circuit synchrone est un circuit combinatoire comportant en plus des registres, et ayant un nombre fini d'entrées et de sorties.*

L'ajout des registres permet, même avec des entrées constantes, de faire varier les sorties au cours du temps. Ainsi, à chaque fil $v$ est associé le nombre 2-adique $B = v^0.v^1 \ldots v^n \ldots$ Le registre transforme $B$ en $2B$, l'inverseur transforme $B$ en $-1 - B$. Ainsi, on peut construire un circuit "calculant" -16, -6/7, -2/3 ou 22/7!

**Théorème 2** *Les assertions suivantes sont équivalentes :*

1. *$f(i) \Rightarrow o$ est calculable par un circuit synchrone.*
2. *$f(\sum i^t 2^t) = \sum o^t 2^t$ est à la fois en ligne ($\forall B, n, f(B) = f(B \bmod 2^n) \bmod 2^n$) et stricte ($\forall B, f(2B) = 2f(B)$).*

Le fait d'être en ligne signifie que les $n$ premiers bits de la sortie ne dépendent que des $n$ premiers bits de l'entrée. Le fait d'être stricte signifie que l'on peut faire du *retiming*, c'est-à-dire que l'on peut faire commuter des registres avec le circuit.
Les circuits courants comme $\cap, \cup, +, -, \pi$ sont stricts. Le ou exclusif, la multiplication, les fonctions $1/(1+2b)$ et $\sqrt{1+8b}$ sont en ligne, mais pas la division par 2 (le $n$-ème bit de la sortie dépend du $(n+1)$-ème de l'entrée), ni $\pi_0$ et $\pi_1$ (le $n$-ème bit de la sortie dépend des bits $2n-1$ et $2n$ de l'entrée).
On peut ainsi fabriquer un circuit synchrone "universel" qui comporte une entrée $B$, des registres à décalage qui calculent $2B$, $4B$, $8B$, $\ldots$, des multiplexeurs $F_0$, $F_1$, $F_2$, $\ldots$, commandés par une ligne de registres à décalage tels qu'à l'instant $n$, la sortie de $F_n$ soit la sortie du circuit. Il suffit donc de mettre en entrée de $F_n$ un circuit combinatoire idoine ayant $B$, $2B$, $4B$, $\ldots 2^n B$ comme entrées.
Alors que les circuits d'addition et de soustraction sont de taille finie, les circuits de multiplication et de racine carrée sont de taille *infinie*.

Enfin, un circuit en ligne de produit modulaire $A \times B \bmod C$ a été réalisé sur une carte PAM, pour des entiers 4-adiques de 256 bits. Ce circuit est à la base d'un système de codage RSA à 200KB par seconde.

## Références

[1] Y. Amice. *Les nombres p-adiques.* Presses Universitaires de France, 1975.

[2] R. E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, 35(8):677–691, 1986.

[3] K. Hensel. *Zahlentheorie.* Göshen, Berlin-Leiptzig, 1913.

[4] N. Koblitz. *p-adic Numbers, p-adic Analysis and Zeta Functions.* Springer-Verlag, 1977.

[5] C. Leiserson and J. Saxe. Retiming synchronous circuitry. *Algorithmica*, 6(1):5–35, 1991.

[6] C. Mead. *Analog VLSI and Neural Systems.* Addison-Wesley, 1989.

[7] J. Vuillemin. On Circuits and Numbers. Preprint.