

Les éléments primitifs de $\mathbb{Z}/11\mathbb{Z}$ sont donc : 2, 6, 7 et 8.
De la même façon on peut déterminer les éléments primitifs de $\mathbb{Z}/13\mathbb{Z}$.

$\text{VECTOR}(\text{VECTOR}(\text{MOD}(j^i, 13), i, 1, 12), j, 1, 12)$

1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	3	6	12	11	9	5	10	7	1
3	9	1	3	9	1	3	9	1	3	9	1
4	3	12	9	10	1	4	3	12	9	10	1
5	12	8	1	5	12	8	1	5	12	8	1
6	10	8	9	2	12	7	3	5	4	11	1
7	10	5	9	11	12	6	3	8	4	2	1
8	12	5	1	8	12	5	1	8	12	5	1
9	3	1	9	3	1	9	3	1	9	3	1
10	9	12	3	4	1	10	9	12	3	4	1
11	4	5	3	7	12	2	9	8	10	6	1
12	1	12	1	12	1	12	1	12	1	12	1

Il s'agit de : 2, 6, 7 et 11..

6 et 7 sont des éléments primitifs communs à $\mathbb{Z}/11\mathbb{Z}$ et à $\mathbb{Z}/13\mathbb{Z}$.

On considère alors le reste dans la division euclidienne par 10 de l'entier relatif égal à la différence du reste de 6^n dans la division par 11 et du reste de 7^n dans la division euclidienne par 13, n étant un entier naturel non nul donné.

Les restes possibles sont donc les entiers compris entre 0 et 9.

La suite de ces restes présente-t-elle une période ?

Pour cela on fera varier n de 1 à 70.

```

suite(mod(mod(6^n, 11) - mod(7^n, 13), 10), 1)
{9 3 2 0 9 3 2 1 4 7 4 2}
  
```

L'écriture est peu explicite. On peut l'écrire sous forme de matrice :

	F1	F2	F3	F4	F5	F6					
	Alg	Calc	Autre	ESPrgm	Nettoyage						
			9	3	2	0	9	3	2	1	4
			4	2	0	9	5	6	7	2	6
			8	9	5	8	3	5	3	5	1
			0	0	9	5	8	4	1	4	7
			5	1	1	6	2	1	6	3	5
			1	4	6	7	4	2	0	0	0
			9	3	2	0	9	3	2	1	4
	suite(suite(mod(mod(6^(i+10j)...										
	MAIN RAD AUTO FDISC 2/20										

La période est plus facile à trouver ici : la suite des nombres de la première ligne se retrouve à la dernière. la période est donc de 60.

On peut maintenant introduire des éléments supplémentaires que l'on notera s et t qui sont des entiers entre 1 et 10 pour s et entre 1 et 13 pour t .

On cherche alors la période de : $\text{mod}(\text{mod}(s \times 6^n, 11) - \text{mod}(t \times 7^n, 13), 10)$

On peut écrire cette liste de terme sous la forme d'une fonction à deux variables :

$$\text{ran}(s, t) = \text{mod}(\text{mod}(s \times 6^n, 11) - \text{mod}(t \times 7^n, 13), 10)$$

ou sous forme matricielle : $\text{ran}(s, t) = \text{mod}(\text{mod}(s \times 6^{i+10j}, 11) - \text{mod}(t \times 7^{i+10j}, 13), 10)$, avec i variant de 1 à 10 et j variant de 0 à 6.

Sur Derive :

```
ran(s, t) := VECTOR(VECTOR(MOD(MOD(s*6i + 10*j, 11) - MOD(t*7i + 10*j, 13), 10), i, 1,
10), j, 0, 6)
```

Sur la calculatrice l'instruction est identique si l'on remplace « vector » par « suite ».

On obtient par exemple :

ran(1, 1)

9	3	2	0	9	3	2	1	4	7
4	2	0	9	5	6	7	2	6	8
8	9	5	8	3	5	3	5	1	9
0	0	9	5	8	4	1	4	7	2
5	1	1	6	2	1	6	3	5	1
1	4	6	7	4	2	0	0	0	0
9	3	2	0	9	3	2	1	4	7

ran(3, 7)

7	4	1	4	6	8	9	3	2	1
6	2	0	0	9	3	0	5	3	5
3	7	9	8	8	9	3	0	4	7
4	1	6	3	7	7	2	6	7	2
5	3	7	7	4	2	1	4	6	8
8	8	8	9	5	6	8	9	5	6
7	4	1	4	6	8	9	3	2	1

ran(6, 4)

1	6	2	0	0	9	3	0	5	3
5	3	7	9	8	8	9	3	0	4
7	4	1	6	3	7	7	2	6	7
2	5	3	7	7	4	2	1	4	6
8	8	8	8	9	5	6	8	9	5
6	7	4	1	4	6	8	9	3	2
1	6	2	0	0	9	3	0	5	3

ran(10, 11)

3	2	1	4	7	4	2	0	9	5
6	7	2	6	8	8	9	5	8	3
5	3	5	1	9	0	0	9	5	8
4	1	4	7	2	5	1	1	6	2
1	6	3	5	1	1	4	6	7	4
2	0	0	0	0	9	3	2	0	9
3	2	1	4	7	4	2	0	9	5

Dans chaque cas la période est de 60 qui est égal à $\frac{(11-1)(13-1)}{2}$.

Si l'on remplace modulo 10 par modulo 16 par exemple, cela ne change rien

```

ranb(s, t) := VECTOR(VECTOR(MOD(MOD(s-6i + 10·j, 11) - MOD(t-7i + 10·j, 13), 16), i, 1,
10), j, 0, 6)

```

```

ranb(7, 8)

```

5	8	4	1	10	13	8	11	7	1
6	2	1	6	3	11	7	1	10	12
13	4	2	0	0	0	0	15	9	2
0	15	9	2	1	10	13	4	2	0
15	5	12	13	8	12	14	14	15	5
8	3	11	3	11	7	5	0	0	15
5	8	4	1	10	13	8	11	7	1

Recommençons avec deux autres nombres premiers, par exemple 17 et 23 :
les éléments primitifs de $\mathbb{Z}/17\mathbb{Z}$ sont :

```

VECTOR(VECTOR(MOD(ji, 17), i, 1, 16), j, 1, 16)

```

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

Les éléments primitifs sont : 3, 5, 6, 7, 10, 11, 12, 14.

On reprend le même calcul avec $\mathbb{Z}/23\mathbb{Z}$:

```

VECTOR(VECTOR(MOD(ji, 23), i, 1, 22), j, 1, 22)

```

On trouve que les éléments primitifs sont : 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

On construit comme précédemment la fonction :

```

ran(s, t) := VECTOR(VECTOR(MOD(MOD(s-14i + 10·j, 17) - MOD(t-21i + 10·j, 23), 10), i, 1,
10), j, 0, 19)

```

Selon le résultat précédent nous nous attendons à une période de :

$$\frac{(23-1)(17-1)}{2} = \frac{22 \times 16}{2} = 176$$

On peut essayer avec $s = 7$ et $t = 8$.

On trouve :

ran(7, 8)

6	3	0	3	6	7	7	9	3	1
7	5	7	6	9	4	6	0	3	4
7	5	1	1	9	2	2	5	0	3
8	3	8	6	1	8	6	0	1	8
2	3	3	3	4	5	4	4	3	6

4	5	5	9	3	4	0	7	2	8
4	2	7	5	4	4	8	7	1	0
8	4	3	4	1	7	6	8	5	9
3	9	8	4	4	1	9	2	7	6
7	8	1	8	8	6	2	8	0	0
2	5	8	7	7	3	0	9	2	6
2	8	8	9	5	0	5	2	7	6
9	9	8	3	1	1	2	5	1	0
6	8	9	4	3	7	4	9	1	0
0	0	4	1	9	4	5	3	9	1
6	8	5	7	5	2	6	1	9	1
2	1	4	2	1	7	4	2	4	2
5	9	9	2	0	9	6	3	0	3
6	7	7	9	3	1	7	5	7	6
9	4	6	0	3	4	7	5	1	1

Le 177^{ème} terme.

Les nombres premiers choisis par Texas sont $p = 2^{31} - 85$ et $p' = 2^{31} - 249$ avec comme éléments primitifs : $a = 40014$ et $a' = 40692$.

La période est : $\frac{(2^{31} - 85 - 1) \times (2^{31} - 249 - 1)}{2} = 2305842648436451838$

Les valeurs de s et de t sont variables : il s'agit en fait des termes successifs de deux suites géométriques modulo p ou p' , de raisons respectives a et a' et dont le premier terme est défini par l'initialisation.

Pour bien en comprendre le fonctionnement, donnons un exemple.

Supposons que l'on se donne deux nombres s_1 et s_2 comme termes initiaux des deux suites récurrentes que nous allons construire.

On a $u_0 = s_1$ et $v_0 = s_2$.

On aura alors $u_1 = \text{mod}(u_0 \times a, p)$ et $v_1 = \text{mod}(v_0 \times a', p')$.

Le premier nombre aléatoire calculé par la machine est alors : $\frac{\text{mod}(u_1 - v_1, p - 1)}{p - 1}$.

Sur la TI-89 ou sur la TI-92, on peut modifier les valeurs de ces termes initiaux. Ils sont rangés dans les variables système **seed1** et **seed2**.

40014 → a1	40014
40692 → a2	40692
$2^{31} - 85$ → p1	2147483563
$2^{31} - 249$ → p2	2147483399
23 → seed1	23
79 → seed2	79

On calcule les deux premiers termes des deux suites autres que les termes initiaux :

$\text{mod}(\text{seed1} \cdot a1, p1) \rightarrow s1$	920322.
$\text{mod}(\text{seed2} \cdot a2, p2) \rightarrow s2$	3214668.
$\frac{\text{mod}(s1 - s2, p1 - 1)}{p1 - 1}$.998931611845
nbrAléat()	.998931611844
seed1	920322.
seed2	3214668.

On remarque que la calculatrice modifie les deux variables systèmes avec les contenus des premiers termes des suites.

Regardons un coup plus loin.

$\text{mod}(s1 \cdot a1, p1) \rightarrow s1$	318543937.
$\text{mod}(s2 \cdot a2, p2) \rightarrow s2$	1962266316.
$\frac{\text{mod}(s1 - s2, p1 - 1)}{p1 - 1}$.234582090366
nbrAléat()	.234582090365
seed1	318543937.
seed2	1962266316.

On remarquera toutefois la légère différence dans les valeurs approchées (on peut penser que Texas ayant le même générateur sur les TI-83 et les TI-89 a choisi une précision de calcul correspondant à celle de la TI-83).

L'instruction IniNbrAl permet l'initialisation du générateur, c'est-à-dire des deux termes initiaux. Cette instruction n'a qu'un argument qui est un entier (on peut prendre un décimal comme argument, mais la calculatrice le remplace par sa partie entière).

Pour 0 et 1, on a :

IniNbrAl 0	Fait
seed1	12345.
seed2	67890.
IniNbrAl 1	Fait
seed1	40014.
seed2	1.

Pour 2 et 10 par exemple :

```

■ IniNbrAl 2 Fait
■ seed1 80028.
■ seed2 2.
■ IniNbrAl 10 Fait
■ seed1 400140.
■ seed2 10.

```

Pour 59623 par exemple :

```

■ IniNbrAl 59623 Fait
■ seed1 238271159.
■ seed2 59623.
■ 59623·40014 2385754722
■ Mod(2385754722, p1) 238271159

```

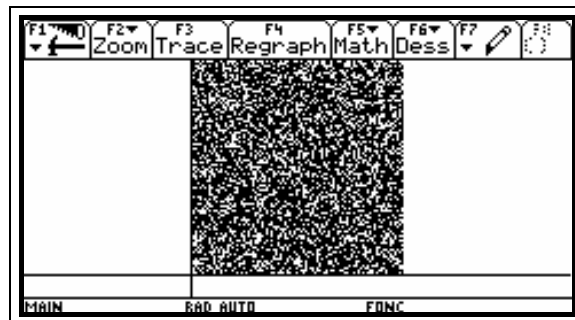
Reste à prouver que cela donne bien une distribution uniforme. Mathématiquement c'est une autre histoire. On peut toutefois se donner une idée graphique de ce qui se passe. On commence par un petit programme permettant le tracé de points dont les deux coordonnées sont des nombres aléatoires compris entre 0 et 1 :

```

: nbral(n)
: Prgm
: Local i, a, b
: For i, 1, n
:   nbrAléat()→a
:   nbrAléat()→b
:   PtAff a, b
: EndFor
: EndPrgm

```

Ce qui donne pour n=10000



Et sur la TI-83 :

```

PROGRAM: NBRAL
: For(I, 1, 1000)
:   NbrAléat→A
:   NbrAléat→B
:   Pt-Aff(A, B)
: End

```

Et la représentation graphique :

