Le générateur de nombres aléatoires de la TI82-83

1. La commande NbAléat de la TI82-83

Dans le menu MATH, PRB, utilisez la commande NbAléat (ou rand si votre machine est en anglais), cette commande génère un nombre aléatoire compris entre 0 et 1.
Si le nombre affiché par votre calculatrice est 0.9435974025 c'est que c'est la première fois que vous utilisez cette commande depuis l'achat de votre calculatrice ou la date de la dernière réinitialisation de la mémoire de votre calculatrice, en effet votre calculatrice génère des nombres pseudo-aléatoires, c'est-à-dire qu'ils sont en fait produits par un programme implémenté dans votre calculatrice, ce programme est le même dans toutes les calculatrices TI82-83.
Il est possible de réinitialiser la commande NbAléat, pour cela saisissez à la calculatrice :

0→NbAléat

Si vous tapez ensuite NbAléat, le nombre affiché est 0.9435974025, le suivant 0.908318861, le suivant 0.1466878292 …
Comme vous pouvez le constater ces nombres sont connus, ils constituent donc une suite de nombres donc chaque élément dépend du précédent, on dit que ce sont des nombres pseudo-aléatoires. Il est extrêmement difficile de générer des nombres pseudo-aléatoires, lire en ligne sur Wikipédia.
Avec votre calculatrice, il est possible de contourner le problème de récurrence des nombres aléatoires obtenus avec ce programme :

```
PROGRAM:RANDOM
:While 1
:rand→R
:If getKey>0
:Disp R
:End
```

Appuyez sur n'importe quelle touche de la calculatrice excepté la touche ON pour obtenir un nouveau nombre. Quand vous appuyez sur ON puis Entrée, le programme s'interrompt et cesse de fonctionner.
Ce programme stocke dans R en continu les nombres de la suite de nombres aléatoires générés par la calculatrice, soit environ 49 nombres par seconde (si votre calculatrice n'est pas la même que la mienne, elle génère probablement les nombres aléatoires à une autre vitesse)[1], lorsque vous appuyez sur une touche de la calculatrice elle affiche le nombre stocké dans R à cet instant précis, vous pouvez vérifier que ce procédé ne génère pas des suites de nombres identiques. Cette méthode est celle utilisée dans les machines à sous des casinos, à ceci près que les nombres pseudo-aléatoires créés le sont au nombre d'environ 500 par seconde.
Parmi toutes les méthodes permettant de générer des nombres pseudo-aléatoires, nous allons nous intéresser à celle introduite en 1948 par Derrick Lehmer.

2. Générateur congruentiel linéaire

Un générateur congruentiel linéaire est un générateur de nombres pseudo-aléatoires dont l'algorithme, pour produire des nombres aléatoires, est basé sur des congruences et une fonction affine.
Les nombres pseudo aléatoires forment une suite dont chaque terme dépend du précédent, selon la formule suivante : $X_{n+1}=(a\,X_n+b)[m]$.

Où *a* est appelé le *multiplicateur*, *b* l'*incrément*, et *m* le *module*.

---

1 Exercice : Trouvez une approximation de cette vitesse en utilisant le programme ci-dessus conjointement avec un chronomètre (Comment ça « Je n'ai pas de chronomètre ! » ? Regarde dans ton téléphone portable ...). Comparez votre résultat avec celui de vos camarades.

Le terme initial, X_0 est appelé la graine (*seed* en anglais). C'est elle qui va permettre de générer une suite apparemment aléatoire. Pour chaque graine, on aura une nouvelle suite. Cependant, il est possible que certaines graines permettent d'obtenir une suite plus aléatoire que d'autres.

Du fait de l'opération de congruence, les termes de cette suite sont compris entre 0 et $m - 1$. De plus, comme chaque terme dépend entièrement du précédent, si un nombre apparaît une deuxième fois, toute la suite se reproduit à partir de ce nombre. Or le nombre de valeurs que le nombre peut prendre étant fini (égal à m), la suite est amenée à se répéter au bout d'un certain temps. On dit qu'elle est périodique.

Exercice

Dans une feuille de classeur d'un tableur programmez la feuille suivante :

	A	B	C	D
1	10	0,0321543408	a	m
2	263	0,845659164	25	311
3	57	0,1832797428	b	
4	194	0,6237942122	13	

Dans la colonne A se trouvent les X_n et dans la colonne B les $\frac{X_n}{m}$, nombres aléatoires compris entre 0 et 1.

Dans l'aide du tableur recherchez la fonction MOD() et lisez ce qui en est dit, cela vous permettra de programmer plus simplement la feuille de calcul ci-dessus.

Utilisez la feuille de calcul pour répondre aux questions suivantes :

a) On considère la suite de Lehmer définie par $U_{n+1}=(25U_n+16)[256]$. Que se passe-t-il pour $U_0=10$? $U_0=11$? $U_0=12$?

b) On considère la suite de Lehmer définie par $U_{n+1}=(31415821U_n+1)[10^8]$ et $U_0=1$. Regarder le dernier chiffre des premiers termes. Expliquer.

3. Le générateur de nombres aléatoires de la TI82-83

Le générateur de nombres aléatoires de la TI82-83 a été inventé par Pierre L'Écuyer en 1988 en croisant deux suites de Lehmer judicieusement choisies.

$p=2^{31}-85$, $q=2^{31}-249$, $a=40014$, $b=40692$, soient les suites de Lehmer (s_n) et (t_n) définies par $s_{n+1}=as_n[p]$ et $t_{n+1}=bt_n[q]$, (w_n) la suite d'entiers définie par $w_n=s_n-t_n[p-1]$ et enfin $(aléa_n)$ la suite définie par $aléa_n=\frac{w_n}{p-1}$.

$(aléa_n)$ est une suite de nombres au hasard de l'intervalle $]0\ ;1[$, de période $T=\frac{(p-1)(q-1)}{2}\approx 2.205\times 10^{18}$.

En posant $s_0=12345$ et $t_0=67890$, ces nombres sont ceux générés par votre calculatrice.

Exercice

Créez la feuille de calcul qui va vous permettre de générer ces nombres aléatoires :

	A	B	C	D	E	F	G
1	s_n	t_n	s_n – t_n	s_0	t_0	p - 1	aléa_n
2	12345	67890	2026359911	12345	67890	2147483562	0,9435974025
3	493972830	615096481	1950599823	p	q		0,9083188610
4	390105768	586989507	315009702	2147483563	2147483399		0,1466878292
5	1781664868	1466655166	1105313978	a	b		0,5147019505
6	1526187241	420873263	871469535	40014	40692		0,4058096418
7	866180343	2142194370	1575849876				0,7338123112

Programmation de ce générateur dans votre calculatrice :

1. Il n'existe pas dans votre calculatrice de commande permettant de calculer le reste dans la division euclidienne de *a* par *b*, trouvez une formule qui vous permet de faire cela et que vous utiliserez ensuite dans votre programme.
2. Programmez ce générateur de nombres aléatoires dans cotre calculatrice.

Prolongement sur Algobox

Programmation de ce générateur sur Algobox :

1. Dans Algobox, la commande permettant de calculer le reste dans la division euclidienne de *a* par *b* est *a*%*b*, elle ne fonctionne pas si *a*<0, or dans le calcul des W_n, il arrive que $S_n - T_n$ soit un nombre négatif, donc lorsque l'on calcule $w_n = s_n - t_n[p-1]$, le programme dysfonctionne, trouvez une parade à cela.
2. Programmez ce générateur de nombres aléatoires dans Algobox pour les dix premiers nombres de la suite $(aléa_n)$. Que constatez-vous ? Il existe une parade à ce problème d'affichage des nombres mais là n'est pas le propos de cette activité.
3. Utilisez votre programme en ligne sur le site http://proglab.fr/ pour obtenir l'affichage attendu.

Bibliographie

- Générateur de nombres pseudo-aléatoires, http://fr.wikipedia.org/wiki/Générateur_de_nombres_pseudo-aléatoires
- Derrick Lehmer sur Wikipédia, http://fr.wikipedia.org/wiki/Derrick_Lehmer
- Pierre Lécuyer, http://www.iro.umontreal.ca/~lecuyer/
- cacm88.pdf P. L'Ecuyer, ``Efficient and Portable Combined Random Number Generators", Communications of the ACM, 31 (1988), 742--749 and 774.
- Bulletin vert, n°491, de l'APMEP, Thierry Lambre, Qu'est-ce qu'un générateur de nombres au hasard ?.