Tests probabilistes de primalité

- Test de Fermat.
- Test de Miller-Rabin.

Test de Fermat

Voici, pour $a = 2, 3, 5, 7, 11, 13$, la liste des puissances a^{n-1} (**mod** n) pour tous les entiers *n composites* impairs inférieurs à 2^{15} et tels que $2^{n-1} = 1$ (**mod** n), autrement dit les entiers pseudo-premiers pour la base 2.

	Factorisation	**2**	**3**	**5**	**7**	**11**	**13**
341	11 * 31	1	56	67	56	253	67
561	3 * 11 * 17	1	375	1	1	154	1
645	3 * 5 * 43	1	36	595	436	1	436
1105	5 * 13 * 17	1	1	885	1	1	936
1387	19 * 73	1	875	1122	1122	1141	1141
1729	7 * 13 * 19	1	1	1	742	1	533
1905	3 * 5 * 127	1	276	400	1561	226	1846
2047	23 * 89	1	1013	622	1013	1	1657
2465	5 * 17 * 29	1	1	1480	1	1	1
2701	37 * 73	1	1	2554	2554	2554	2554
2821	7 * 13 * 31	1	1	1	2016	1	2171
3277	29 * 113	1	1567	2727	1	1016	1016
4033	37 * 109	1	3442	3442	3442	2443	3442
4369	17 * 257	1	3333	2024	3469	4353	1735
4371	3 * 31 * 47	1	3291	2257	1834	2257	2257
4681	31 * 151	1	4589	3783	3783	1272	4589
5461	43 * 127	1	1377	1	1377	1162	1377
6601	7 * 23 * 41	1	1	1	3773	1	1
7957	73 * 109	1	1680	2116	2116	6058	2116
8321	53 * 157	1	5036	5036	1	5036	7209
8481	3 * 11 * 257	1	8031	1024	4819	6424	1783
8911	7 * 19 * 67	1	1	1	1274	1	1
10261	31 * 331	1	10200	7131	3752	7131	3721
10585	5 * 29 * 73	1	1	4235	1	1	1
11305	5 * 7 * 17 * 19	1	10641	8380	5796	10641	1
12801	3 * 17 * 251	1	3231	1	7141	7498	10813
13741	7 * 13 * 151	1	4096	13196	3381	8464	7267
13747	59 * 233	1	6668	6668	4426	6668	4426
13981	11 * 31 * 41	1	1024	1	1024	12463	1024
14491	43 * 337	1	7225	4129	11310	9547	1

15709	23 * 683	1	7177	9638	9132	2416	12214
15841	7 * 31 * 73	1	1	1	6790	1	1
16705	5 * 13 * 257	1	4096	14665	4096	1	14391
18705	3 * 5 * 29 * 43	1	15516	18010	436	1	436
18721	97 * 193	1	1	18334	1	18334	18334
19951	71 * 281	1	14840	6462	6462	14840	14840
23001	3 * 11 * 17 * 41	1	21198	13531	13531	11440	1
23377	97 * 241	1	98	7080	22018	1	16004
25761	3 * 31 * 277	1	17334	25600	19783	25600	22438
29341	13 * 37 * 61	1	1	1	1	1	18057
30121	7 * 13 * 331	1	25572	21295	1925	21295	9542
30889	17 * 23 * 79	1	1818	1818	1818	1818	1
31417	89 * 353	1	15843	15843	25811	1	15843
31609	73 * 433	1	14090	11024	1534	14090	14090
31621	103 * 307	1	1	12876	2473	12876	12876

Chaque case qui comporte la valeur 1 correspond à un entier *a* (dont la valeur figure en tête de colonne) *menteur* pour *n* (dont la valeur figure en début de ligne). Un menteur est inversible (**mod** *n*), et est donc nécessairement premier avec *n* ; les lignes comportant beaucoup de 1 correspondent, dans cette table, aux *nombres de Carmichael*, pour lesquels tout entier *a* premier avec *n* est menteur. Un nombre de Carmichael *n* est caractérisé par les propriétés suivantes :

- *n* est le produit d'au moins 3 nombres premiers distincts,
- pour chaque facteur premier *p*, *p* - 1 divise *n* - 1.

Par exemple 6601 = 7 * 23 * 41 et 6600 = 2^3 * 3 * 5^2 * 11 est divisible par 6, 22 et 40. Tout test de Fermat effectué en calculant a^{6600} avec *a* non divisible par 7, ni par 23, ni par 41 fera croire que 6601 est premier.

Test de Miller-Rabin

La table suivante indique le comportement du test de Miller-Rabin pour tous les menteurs (inférieurs ou égaux à 7) de la table précédente ; chaque case comporte la suite de carrés successifs :

$$p_0 = a^e, p_1 = a^{2e}, p_2 = a^{4e}, p_3 = a^{8e}, \ldots p_k = a^{n-1}$$

jusqu'à la valeur 1 ou -1. La première colonne (base 2), par exemple, se lit comme suit :

- *n* = 341, *n* - 1 = 4 * 85, 2^{85} = 32, 2^{170} = 1 (**mod** 341), donc 341 n'est pas premier.
- *n* = 2047, *n* - 1 = 2 * 1023, 2^{1023} = 1 (**mod** 2047), donc 2047 reste un candidat premier ; 2 est un menteur fort pour 2047.
- *n* = 3277, *n* - 1 = 4 * 819, 2^{819} = 128, 2^{1638} = -1 (**mod** 3277), donc 3277 reste un candidat premier ; 2 est un menteur fort pour 3277.

	Factorisation de n - 1	**2**	**3**	**5**	**7**
341	4 * 85	32, 1			

561	16 * 35	263, 166, 67, 1		23, 529, 463, 67, 1	241, 298, 166, 67, 1
645	4 * 161	257, 259, 1			
1105	16 * 69	967, 259, 781, 1	1093, 144, 846, 781, 1		827, 1039, 1041, 781, 1
1387	2 * 693	512, 1			
1729	64 * 27	645, 1065, 1	664, 1	1217, 1065, 1	
1905	16 * 119	128, 1144, 1			
2047	2 * 1023	1			
2465	32 * 77	1902, 1449, 1886, 1	2018, 144, 1016, 1886, 1		2437, 784, 871, 1886, 1
2701	4 * 675	2337, 147, 1	2071, 2554, 1		
2821	4 * 705	2605, 1520, 1	1301, 1	993, 1520, 1	
3277	4 * 819	128, -1			1016, 1
4033	64 * 63	3521, -1			
4369	16 * 273	2, 4, 16, 256, 1			
4371	2 * 2185	2915, 1			
4681	8 * 585	1			
5461	4 * 1365	128, 1		-1	
6601	8 * 825	2738, 4509, 1	3037, 1772, 4509, 1	3863, 4509, 1	
7957	4 * 1989	512, 7520, 1			
8321	128 * 65	8192, -1			2013, 8163, 1
8481	32 * 265	3596, 6172, 5413, 7195, 1			
8911	2 * 4455	6364, 1	-1	2813, 1	
10261	4 * 2565	1985, 1			
10585	8 * 1323	7958, 10294, 1	8422, -1		5453, 1944, 291, 1
11305	8 * 1413	10487, 2129, 10641, 1			
12801	512 * 25	3011, 3013, 2260, 1		11045, 11296, 12049, 2260, 1	
13741	4 * 3435	5286, 6343, 1			
13747	2 * 6873	9321, 1			
13981	4 * 3495	4806, 1024, 1		5116, 1024, 1	
14491	2 * 7245	10448, 1			
15709	4 * 3927	2048, 1			
15841	32 * 495	1	12802, 218, 1	3380, 3039, 218, 1	
16705	64 * 261	9027, 16444,			

		1301, 5396, 1			
18705	16 * 1169	2192, 16384, 1			
18721	32 * 585	512, 50, 2500, 15907, 18334, 1	962, 8115, 11468, -1		9852, 12240, 12158, 14669, 387, 1
19951	2 * 9975	6462, 1			
23001	8 * 2875	16532, 9142, 13531, 1			
23377	16 * 1461	16599, 5479, 3373, 15907, 1			
25761	32 * 805	3938, 25483, 1			
29341	4 * 7335	26424, -1	22569, 1	15127, 25011, 1	23496, 11101, 1
30121	8 * 3765	330, 18537, 1			
30889	8 * 3861	18171, 12720, 1818, 1			
31417	8 * 3927	8189, 15843, 10236, 1			
31609	8 * 3951	19200, 15842, 25113, 1			
31621	4 * 7905	31313, 1	-1		
	Factorisation de n - 1	**2**	**3**	**5**	**7**

On voit que seulement 7 sur 45 (resp. 4 sur 12, 1 sur 10 et 0 sur 8) entiers pseudo-premiers pour la base 2 (resp. les bases 3, 5 et 7) sont *fortement* pseudo-premiers. Aucun entier de la table n'est fortement pseudo-premier simultanément pour les bases 2 et 3.

En fait le plus petit entier fortement pseudo-premier simultanément pour les bases 2 et 3 est supérieur à 10^6. Voici la table de comparaison des tests de Fermat et de Miller-Rabin de ce point de vue ; la troisième ligne, par exemple, se lit comme suit :

- 1729 est le plus petit entier pseudo-premier simultanément pour 2, 3 et 5.
- 25326001 est le plus petit entier fortement pseudo-premier simultanément pour 2, 3 et 5.

	Fermat	**Miller-Rabin**
2	341	2047
2, 3	1105	1 373 653
2, 3, 5	1729	25 326 001
2, 3, 5, 7	29341	3 215 031 751
2, 3, 5, 7, 11	29341	2 152 302 898 747