Kryptografie

Einige Fermatsche Pseudoprimzahlen bis 10000.

Sie erfüllen $a^{p-1} \underset{p}{\equiv} 1$ Dabei ist a teilerfremd zu p und p ist keine Primzahl. Bei den folgenden ist 1<a<11

{9,15,21,25,28,33,35,45,52,63,65,85,91,99,105,117,121,124,133,153,185,205,217,231,259,273,286,301,325,341,364,435,451,481,511,532,561,585,616,645,651,657,671,697,703,781,817,861,909,946,949,1001,1036,1105,1111,1233,1247,1261,1271,1281,1288,1333,1365,1387,1417,1541,1581,1649,1661,1695,1729,1785,1825,1891,1905,2047,2071,2101,2169,2353,2409,2465,2501,2665,2701,2806,2821,2926,2981,3052,3133,3145,3171,3201,3277,3281,3333,3367,3421,3565,3589,3605,3641,3683,3751,3913,4005,4033,4097,4123,4141,4187,4369,4371,4376,4495,4521,4525,4636,4641,4681,4795,4825,4859,4921,4961,5356,5461,5551,5565,5611,5662,5713,5731,5963,6305,6364,6533,6541,6601,6643,6697,6951,7081,7107,7161,7381,7449,7471,7777,7813,7913,7957,8029,8149,8321,8365,8401,8481,8695,8744,8866,8911,9061,9131,9211,9265,9331,9605,9709,9773,9881,9919,9945}

1	2	341	3	91	4	15	5	4
2	2	561	3	121	4	85	5	124
3	2	645	3	286	4	91	5	217
4	2	1105	3	671	4	341	5	561
5	2	1387	3	703	4	435	5	781
6	2	1729	3	949	4	451	5	1541
7	2	1905	3	1105	4	561	5	1729
8	2	2047	3	1541	4	645	5	1891
9	2	2465	3	1729	4	703	5	2821
10	2	2701	3	1891	4	1105	5	4123
11	2	2821	3	2465	4	1247	5	5461
12	2	3277	3	2665	4	1271	5	5611
13	2	4033	3	2701	4	1387	5	5662
14	2	4369	3	2821	4	1581	5	5731
15	2	4371	3	3281	4	1695	5	6601

Mit Angabe der Basis a

16	2	4681	3	3367	4	1729	5	7449
17	2	5461	3	3751	4	1891	5	7813
18	2	6601	3	4961	4	1905	5	8029
19	2	7957	3	5551	4	2047	5	8911
20	2	8321	3	6601	4	2071	5	9881
21	2	8481	3	7381	4	2465	5	
22	2	8911	3	8401	4	2701	5	
23	2		3	8911	4	2821	5	
24	2		3		4	3133	5	

4	3133
4	3277
4	3367
4	3683
4	4033
4	4369
4	4371
4	4681
4	4795
4	4859
4	5461
4	5551

4	6601
4	6643
4	7957
4	8321
4	8481
4	8695
4	8911
4	9061
4	9131
4	9211
4	9605
4	9919
4	

1	6	35	7	[illegible]	8	9	9	[illegible]	10	[illegible]
2	6	185	7	25	8	21	9	[illegible]	10	33
3	6	217	7	325	8	45	9	28	10	91
4	6	301	7	561	8	63	9	52	10	99
5	6	481	7	703	8	65	9	91	10	259
6	6	1105	7	817	8	105	9	121	10	451
7	6	1111	7	1105	8	117	9	205	10	481
8	6	1261	7	1825	8	133	9	286	10	561
9	6	1333	7	2101	8	153	9	364	10	657
10	6	1729	7	2353	8	231	9	511	10	703
11	6	2465	7	2465	8	273	9	532	10	909
12	6	2701	7	3277	8	341	9	616	10	1233
13	6	2821	7	4525	8	481	9	671	10	1729
14	6	3421	7	4825	8	511	9	697	10	2409
15	6	3565	7	6697	8	561	9	703	10	2821
16	6	3589	7	8321	8	585	9	946	10	2981
17	6	3913	7		8	645	9	949	10	3333
18	6	4123	7		8	651	9	1036	10	3367
19	6	4495	7		8	861	9	1105	10	4141
20	6	5713	7		8	949	9	1288	10	4187
21	6	6533	7		8	1001	9	1387	10	4521
22	6	6601	7		8	1105	9	1541	10	5461
23	6	8029	7		8	1281	9	1729	10	6533
24	6	8365	7		8	1365	9	1891	10	6541
25	6	8911	7		8	1387	9	2465	10	6601
26	6	9331	7		8	1417	9	2501	10	7107
27	6	9881	7		8	1541	9	2665	10	7471
28	6		7		8	1649	9	2701	10	7777
29	6		7		8	1661	9	2806	10	8149
30	6		7		8	1729	9	2821	10	8401

8	1785	9	2926	10	8911
8	1905	9	3052	10	
8	2047	9	3281	10	
8	2169	9	3367	10	
8	2465	9	3751	10	
8	2501	9	4376	10	
8	2701	9	4636	10	
8	2821	9	4961	10	
8	3145	9	5356	10	
8	3171	9	5551	10	
8	3201	9	6364	10	
8	3277	9	6601	10	
8	3605	9	6643	10	
8	3641	9	7081	10	
8	4005	9	7381	10	

8	4097	9	8401
8	4369	9	8695
8	4371	9	8744
8	4641	9	8866
8	4681	9	8911
8	4921	9	
8	5461	9	
8	5565	9	
8	5963	9	
8	6305	9	
8	6533	9	
8	6601	9	
8	6951	9	
8	7107	9	

8	7161
8	7957
8	8321
8	8481
8	8911
8	9265
8	9709
8	9773
8	9881
8	9945

Es gibt etwa etwa 10000/ln(10000)=1086 Primzahlen bis 10000.
hier sind 177 verschiedene Fermatsche Pseudoprimzahlen, allerdings nur mit Basen bis 11.