Kryptografie http://de.wikibooks.org/wiki/Pseudoprimzahlen

Starke Pseudoprimzahlen zu

Basis	Starke Pseudoprimzahlen
2	
3	121,
4	341,
5	781, 1541,
6	217, 481,
7	325, 703,
8	65, 481, 3641,
9	121, 1729, 2821,
10	1729,
11	133, 793,
12	133, 145, 1729,
13	85,
14	841,
15	
16	1729, 4033,
17	145, 781, 2821,
18	49, 65,
19	49, 169,
20	
21	221,
22	
23	169, 553,

Fermatscher Satz

Wenn p Primzahl ist und a kein Vielfaches von p, dann gilt:

$$a^{p-1} \underset{p}{\equiv} 1$$

Definition:: Nicht-Primzahlen, für die es ein teilerfremdes a gibt, so dass obige Gleichung erfüllt ist, heißen **Fermatsche Pseudo-Primzahlen**.

Carmichael-Zahlen

```
-----------------------------------------------------------------
             561 =    3 *    11 *    17
           1.105 =    5 *    13 *    17
           1.729 =    7 *    13 *    19
           2.465 =    5 *    17 *    29
           2.821 =    7 *    13 *    31
           6.601 =    7 *    23 *    41
           8.911 =    7 *    19 *    67
          10.585 =    5 *    29 *    73
          15.841 =    7 *    31 *    73
          29.341 =   13 *    37 *    61
          41.041 =    7 *    11 *    13 *    41
          46.657 =   13 *    37 *    97
          52.633 =    7 *    73 *   103
          62.745 =    3 *     5 *    47 *    89
          63.973 =    7 *    13 *    19 *    37
          75.361 =   11 *    13 *    17 *    31
         101.101 =    7 *    11 *    13 *   101
         115.921 =   13 *    37 *   241
         126.217 =    7 *    13 *    19 *    73
         162.401 =   17 *    41 *   233
         172.081 =    7 *    13 *    31 *    61
         188.461 =    7 *    13 *    19 *   109
         252.601 =   41 *    61 *   101
         278.545 =    5 *    17 *    29 *   113
         294.409 =   37 *    73 *   109
         314.821 =   13 *    61 *   397
         334.153 =   19 *    43 *   409
         340.561 =   13 *    17 *    23 *    67
         399.001 =   31 *    61 *   211
         410.041 =   41 *    73 *   137
         449.065 =    5 *    19 *    29 *   163
```

Definition: Nicht-Primzahlen, für die es ein a gibt, so dass

$$a^{\frac{p-1}{2}} \underset{p}{\equiv} \pm 1$$

gilt, heißen **Eulersche Pseudoprimzahlen.**

Basis	Fermatsche Pseudoprimzahlen
2	341, 561, 645, 949, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, ...
3	91, 121, 286, 671, 703, 1105, 1541, 1729, 1891, 2465, 2665, 2701, 2821, 3281, 3367, 3751, ...
4	15, 85, 91, 341, 435, 451, 561, 645, 703, 1105, 1247, 1271, 1387, 1581, 1695, 1729, 1891, ...
5	124, 217, 561, 781, 1541, 1729, 1891, 2821, 4123, 5611, 5662, 5731, 7449, 7813, 8029, 5461, 6601
6	35, 185, 217, 301, 481, 1105, 1111, 1261, 1333, 1729, 2465, 2701, 2821, ...
7	25, 325, 561, 703, 817, 1105, 1825, 2101, 2353, 2465, 3277, 4525, 4825, 6697, ...
8 9	21, 45, 63, 65, 105, 117, 133, 153, 231, 273, 341, 481, 511, 561, 585, 645, 651, 861, 949, 1001, ...
9	28, 52, 91, 121, 205, 286, 364, 511, 532, 616, 671, 697, 703, 946, 949, 1036, 1105, 1288, 1387, ...
10	33, 91, 99, 259, 451, 481, 561, 657, 703, 909, 1233, 1729, 2409, 2821, 2981, 3333, 3367, ...

Definition: Fermatsche Pseudoprimzahlen, die auch Eulersche Pseudoprimzahlen sind, heißen **starke Pseudoprimzahlen**.

Eulersche Pseudoprimzahlen zu einer bestimmten Basis a

Basis	Eulersche Pseudoprimzahlen
2	341, 561, 1105, 1729, 1905, 2047, 2465,
3	121, 703, 1541, 1729, 2465,
4	341, 561, 645, 1105,
5	217, 781, 1541, 1729,
6	185, 217, 301, 481, 1111, 1261,
7	25, 325, 703, 781, 817, 1825, 2101, 2353, 2465,
8	21, 65, 105, 133, 273, 341, 481, 511, 561, 585, 1001, 1105, 1281,
9	91, 121, 671, 703, 949, 1105,
10	33, 91, 481, 657, 1233,
11	133, 305, 481, 645, 793, 1105, 1729, 2257, 2465,
12	65, 91, 133, 145, 247, 377, 385,
13	21, 85, 105, 561, 1099, 1785, 2465,
14	65, 781, 793, 841, 985,
15	341,
16	85, 91, 341, 435, 451, 561, 645, 703, 1105, 1247, 1271,
17	91, 145, 781, 1111, 1305, 1729, 2149,
18	25, 49, 65, 133, 343, 425, 1105, 1225,
19	45, 49, 169, 343, 561, 889, 905, 1105, 1661, 1849, 2353, 2465,

Satz: Alle Primzahlen >2 erfüllen die obige Eulersche Beziehung.
Definition; Bei **starken Primzahlen** ist auch (p-1)/2 eine Primzahl.

Definition: Nicht-Primzahlen, die <u>für alle</u> 0<a<p mit ggt(a,p)=1 die Gleichung $a^{p-1} \underset{p}{\equiv} 1$ erfüllen, heißen

Carmichael-Zahlen.

Wenn man nun alle Pseudoprimzahlen aus der Tabelle, unter der Weglassung der doppelten Pseudoprimzahlen auflistet, bekommt man folgende Folge:

```
 15,  21,  25,  28,  33,  35,  39,  45,  49,  51,  55,  57,  63,  65,  66,  69,  76,  77,  85,  87,  91,  93,  95,  99,
105, 111, 112, 115, 117, 119, 121, 124, 129, 133, 141, 145, 153, 169, 175, 177, 187, 190, 195, 205, 247, 259, 265, 301,
341, 415, 451, 623
```

Das sind 52 Zahlen. Zum Vergleich: Bis 10 existieren 4 Primzahlen, hier sind es 0 Pseudoprimzahlen; bis 100 sind es 25 Primzahlen, hier sind es 24 Pseudoprimzahlen; bis 1000 sind es 168 Primzahlen, hier sind es 52. Allerdings muß man zugestehen, das noch gar nicht alle Pseudoprimzahlen berücksichtigt werden konnten. Wie aber verhält sich die Verteilung der Pseudoprimzahlen nun wirklich? Gibt es innerhab bestimmter Grenzen mehr Pseudoprimzahlen als Primzahlen, oder verhält es sich umgekehrt?

Meint man dagegen die Menge aller fermatschen Pseudoprimzahlen, die zu irgendeiner Basis $a \geq 2$ pseudoprim ist, dann gibt es, in definierten Grenzen mehr Pseudoprimzahlen als Primzahlen:

```
 15   21   25   28   33   35   39   49   51   52   55   57   63   65   66   69   70   75
 76   77   85   87   91   93   95   99  105  111  112  115  117  119  121  123  124  125
129  130  133  135  141  143  145  147  148  153  154  155  159  161  165  169  171  172
175  176  177  183  185  186  187  189  190  195  196  201  203  205  207  208  209  213
215  217  219  221  225  231  232  235  237  238  244  245  246  247  249  253  255  259
261  265  267  268  273  275  276  279  280  285  286  287  289  291  292  295  297  299
301  303  304  305  309  310  315  316  319  321  322  323  325  327  329  333  335  339
341
```