Mathematische Grundlagen der Kryptografie

5. Übungsblatt, SS 2006 — 13.06.2006

43. Der Sieb des Erathostenes um alle Primzahlen $\leq n$ zu finden funktioniert so: zunächst schreibt man alle Zahlen von 2 bis n in eine Liste. Dann entfernt man alle Vielfachen von 2, wählt die nächste verbleibende Zahl aus der Liste (nämlich 3) und entfernt dessen Vielfachen, usw. bis man die ganze Liste abgearbeitet hat. Das Ergebnis sind alle Primzahlen $\leq n$. Berechnen Sie alle Primzahlen ≤ 40.

44. Finden Sie alle Basen für die 21 eine Pseudoprimzahl ist.

*45. Beweisen Sie die folgende Aussage: Für jede Basis $a \in \mathbb{Z}$ existieren unendlich viele a-Pseudoprimzahlen.

Hinweis: Man zeige dass für jede ungerade Primzahl p die $a(a^2-1)$ nicht teilt, die Zahl

$$\frac{a^p-1}{a-1} \cdot \frac{a^p+1}{a+1}$$

eine a-Pseudoprimzahl ist.

*46. Zeige, dass p^2 (mit $p \in \mathbb{P}$) eine Pseudoprimzahl zur Basis a ist, genau dann wenn $a^{p-1} \equiv 1 \bmod p^2$.

*47. Zeigen Sie, dass eine Carmichael-Zahl n von der Form $n = p_1 \cdots p_r$ sein muss, wobei p_i jeweils verschiedene Primzahlen sind und $r \geq 3$ sein muss.

48. Bestimmen Sie eine Carmichael-Zahl, die das Produkt von 4 Primzahlen ist.

49. Zeigen Sie mithilfe des Fermat-Testes das $2047 = 2^{11} - 1$ zusammengesetzt ist.

50. Implementieren Sie den Miller-Rabin-Test in `Mathematica` und vergleichen Sie die Laufzeit mit der der `PrimeQ`-Funktion von `Mathematica`.
Bestimmen Sie mit Ihrer Implementierung die kleinste 512-Bit Primzahl.

51. Eine Fermat-Zahl ist eine Zahl der Form $F_n = 2^{2^n} + 1$. $F_0, \ldots, F_4$ sind Primzahlen und es wurde (vor langer Zeit) vermutet, dass alle F_n prim sind. Heutzutage geht man davon aus, dass alle F_n für $n \geq 5$ zusammengesetzt sind.
Benutzen Sie den Miller-Rabin-Test um zu beweisen, dass F_5 zusammengesetzt ist.

52. Implementieren Sie den deterministischen Primzahltest von Agrawal-Kayal-Saxena in `Mathematica`. Siehe dazu "PRIMES is in P" auf:

    http://www.cse.iitk.ac.in/users/manindra

53. Rechnen Sie Aufgabe 48 indem Sie den Primzahltest von Agrawal-Kayal-Saxena verwenden.