SMS1 für MC, FHS Hagenberg
6. Übungsblatt für den 11. November 2004

1. Schreiben Sie eine Mathematica-Funktion `BBSGenerator`, die eine Pseudozufallsbitfolge nach dem Verfahren von Blum, Blum, und Shub generiert.

   Eingabeparameter sollen s (seed) und l (Länge der Zufallsbitfolge) sein. Die Primzahlen p, q (mit je mindestens 6 Stellen) sollen im Programm fix sein.

   Bestehende Mathematica-Funktionen, die eventuell nützlich sein können: `GCD`, `Mod`, `Prime`.

2. Internet-Recherche: Welche statistischen Tests muß ein Pseudozufallszahlengenerator für kryptographische Anwendungen nach dem amerikanische Standard FIPS 140-1 erfüllen.

3. Wählen Sie einen der statistischen Tests aus Bsp. 2 und überprüfen Sie, ob Ihr Zufallszahlengenerator aus Bsp. 1 ihn erfüllt.

   Bestehende Mathematica-Funktionen für Listen, die eventuell nützlich sein können: `Count`, `Partition`, `Split`.

4. Faktorisieren Sie 29341 mit dem quadratischen Sieb.

5. Faktorisieren Sie 41041 mit dem quadratischen Sieb.

6. Internet-Recherche (RSA challenge numbers): Stellen Sie fest, bis zu welcher Größe RSA-Moduln zur Zeit faktorisiert werden können. Wie hoch ist der Rechenaufwand dafür? Ab welcher Größe gelten Moduln noch als sicher?