SMS1 für MC, FHS Hagenberg
7. Übungsblatt für den 24. November 2005

Satz zum Primzahltest von Miller und Rabin:
Sei $n > 2$, k ungerade und $s \geq 0$, sodass $n - 1 = 2^s \cdot k$. Sei $a \in \{1, \ldots, n-1\}$ sodass

$$a^k \not\equiv 1 \mod n$$

und

$$a^{2^r k} \not\equiv -1 \mod n$$

für alle $r \in \{0, 1, \ldots, s-1\}$. Dann heißt a ein *Zeuge gegen die Primalität* von n.

Es gilt: n ist genau dann eine Primzahl, wenn es keine Zeugen gegen die Primalität von n gibt.

1. Sind 2 und 3 Zeugen gegen die Primalität von 2047?
2. Erfüllt 1729 den Miller-Rabin Test für die Basis $a = 2$? Für $a = 3$?
3. Testen Sie mit dem Miller-Rabin Test, ob 2137 Primzahl ist.
4. Verwenden Sie den Miller-Rabin Test, um eine 2048-Bit Primzahl (d.h. eine Primzahl, die grösser als 2^{2048} ist) zu finden. Wie groß ist die Wahrscheinlichkeit, dass eine zusammengesetzte Zahl Ihren Primzahltest bestanden hat?