Proseminar zu Algebra in den Anwendungen (SS 2015)

(12) Sei $GF(8)$ gegeben als der Körper aller quadratischen Polynome in α, wobei α eine Wurzel des primitiven Polynoms $x^3+x+1 \in \mathbb{Z}_2[x]$ ist. Stellen Sie die Additions und Multiplikationstabelle von $GF(8)$ auf.

(13) Berechnen Sie im Körper $GF(8)$ aus Beispiel 12 die folgenden Ausdrücke:

$$\begin{array}{ccc} \alpha^{17} & (\alpha^2+\alpha)^{33} & (\alpha^2+1)^{171} \\ \log_\alpha(\alpha^2+\alpha) & \log_{\alpha^2+\alpha}(\alpha) & \log_{\alpha^2+1}(\alpha^2) \end{array}$$

(14) Berechnen Sie im Körper $\mathbb{Z}_{17}$ die folgenden Ausdrücke:

$$\begin{array}{ccc} 5^{14} & 3^{12} & 4^{1985} \\ \log_5(12) & \log_3(15) & \log_4(1924) \end{array}$$

(15) Berechnen Sie im Körper $\mathbb{Z}_{63}$ die folgenden Ausdrücke:

$$\begin{array}{ccc} 2^{61} & 24^{21} & 14^{1985} \\ \sqrt[13]{45} & \sqrt[22]{46} & \sqrt[49]{5} \end{array}$$

(16) Bestimmen Sie $\varphi(47957)$, $\varphi(20899)$ und $\varphi(70811891)$.

(17) Eine zusammengesetzte natürliche Zahl N heißt Carmichael-Zahl, falls für alle zu n teilerfremden Zahlen a gilt, dass $a^{n-1} \equiv 1 \mod n$. Welche der folgenden Zahlen sind Carmichael-Zahlen: 99671, 24683, 208403, 62745 und 96331?

(18) Verwenden Sie die Primzahlen $p = 83$ und $q = 97$, um Ihren eigenen Namen, den Sie zuvor im ASCII Code codiert haben, mit Hilfe des RSA–Verfahrens zu verschlüsseln. Verschlüsseln Sie dazu jeden Buchstaben einzeln und wählen Sie dabei einen sinnvollen Exponenten e.

(19) Verwenden Sie den verschlüsselten Namen eines/r Kollegen/in und entschlüsseln Sie ihn. Geben Sie selbst ihren verschlüsselten Namen einem/r Kollegen/in.

(20) Finden Sie die kleinste ganze Zahl x, sodass $2x$ ein Quadrat einer ganzen Zahl, $3x$ eine dritte Potenz einer ganzen Zahl und $5x$ eine fünfte Potenz einer ganzen Zahl ist. Geben Sie auch die Primfaktorzerlegung von x an.

(21) Überlegen Sie, ob das RSA–Verfahren auch funktioniert, wenn eine der Zahlen p oder q nicht prim sondern eine Carmichael-Zahl ist.

(22) Führen Sie einen Fermatschen Primzahltest für die Zahlen aus Beispiel 17 durch, sodass die Wahrscheinlichkeit für eine Fehlklassifikation weniger als ein Promille ist.

(23) Führen Sie einen Miller-Rabin Primzahltest für die Zahlen aus Beispiel 17 durch für dieselbe Fehlerwahrscheinlichkeit.

(24) Finden Sie heraus, wie die Hashfunktion MD5 funktioniert und erklären Sie sie kurz.