Proseminar zu Algebra in den Anwendungen (SS 2011)

(24) Im Körper $\mathbb{Z}_{17}$ berechnen Sie die folgenden Ausdrücke:

$$5^{14} \qquad 3^{12} \qquad 4^{1985}$$

$$\log_5(12) \qquad \log_3(15) \qquad \log_4(1924)$$

(25) Im Körper $GF(8)$ aus Beispiel 21 berechnen Sie die folgenden Ausdrücke:

$$\alpha^{17} \qquad (\alpha^2+\alpha)^{33} \qquad (\alpha^2+1)^{171}$$

$$\log_\alpha(\alpha^2+\alpha) \qquad \log_{\alpha^2+\alpha}(\alpha) \qquad \log_{\alpha^2+1}(\alpha^2)$$

(26) Bestimmen Sie $\varphi(47957)$ und $\varphi(20899)$

(27) Führen Sie einen Fermatschen Primzahltest für die Zahlen 99671, 24683, 208403, 62745 und 96331 durch, sodass die Wahrscheinlichkeit für eine Fehlklassifikation weniger als ein Promille ist.

(28) Führen Sie einen Miller-Rabin Primzahltest für die Zahlen aus Beispiel 27 durch für dieselbe Fehlerwahrscheinlichkeit.

(29) Welche Zahlen aus Beispiel 27 sind Carmichael–Zahlen?

(30) Verwenden Sie die Primzahlen $p = 83$ und $q = 97$, um Ihren eigenen Namen mit Hilfe des RSA–Verfahrens zu verschlüsseln. Wählen Sie dabei einen sinnvollen Exponenten e.

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

(32) 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. Gib auch die Primfaktorzerlegung von x an.

(33) Bestimmen Sie die Monoide zu den Halbautomaten IR–Flip-Flop, Trigger–Flip-Flop und Paritycheck.