

Mathematik für Informatiker

Algebraische Strukturen

Übungsblatt 11

Abgabetermin Samstag, den 27.01.2024, 23:59 Uhr in OpenOlat.

1. Der öffentliche RSA-Schlüssel von Alice ist

$$\begin{aligned} n_A &= 186444745729857899758373984272541398503249351\dots \\ &\quad \dots 266417000699738642133172271283265124803102459 \\ e_A &= 2^{16} + 1 \end{aligned}$$

Bob hat eine verschlüsselte Nachricht

$$\begin{aligned} c &= 118065177034178781019606499196610289078537937\dots \\ &\quad \dots 154386810449387818970058015262198321770177073 \end{aligned}$$

an Alice geschickt. Was war der Inhalt der Nachricht?

Hinweise: Alice hat ungeschickterweise einen Primfaktor p von $n_A = p \cdot q$ so gewählt, dass $\varphi(p)$ nur Primpotenzfaktoren ≤ 200000 hat.

Verwenden Sie ein Verfahren, um $a^b \bmod n$ für $a, b, n \in \mathbb{N}$ effizient berechnen, in MAPLE etwa durch

$$\text{Power}(a,b) \bmod n$$

Testen Sie, ob auch Faktorisierungsroutinen in Computeralgebrasystemen zum Ziel führen, etwa die MAPLE-Funktion `ifactor`.

2. Seien $a, b, n \in \mathbb{N}$ und

$$b = b_0 2^0 + b_1 2^1 + b_2 2^2 + \dots$$

mit $b_i \in \{0, 1\}$ die Darstellung von b als Binärzahl.

- (a) Beschreiben Sie ein effizientes Verfahren zur Berechnung von

$$a^b \bmod n$$

durch sukzessives Quadrieren.

- (b) Implementieren Sie Ihr Verfahren (auch in Form von Pseudocode) und testen Sie Ihre Implementierung an Beispielen.

3. (a) Bestimmen Sie die Additionstabelle und Multiplikationstabelle des Körpers $\mathbb{Z}/5$.
 (b) Finden Sie über $\mathbb{Z}/5$ die Lösungsmenge des Gleichungssystems

$$\begin{aligned} x_1 + \bar{2}x_2 + \bar{3}x_3 &= 0 \\ \bar{2}x_1 + \bar{3}x_2 + \bar{4}x_3 &= 0 \\ \bar{3}x_1 + \bar{4}x_2 + \bar{0}x_3 &= 0 \end{aligned}$$

4. Finden Sie das eindeutige Polynom $f \in \mathbb{R}[x]$ von Grad $\deg f \leq 3$ mit

$$f(-2) = 0 \quad f(0) = 1 \quad f(1) = 0 \quad f(4) = 0$$

und zeichnen Sie den Funktionsgraphen.

Hinweis: Verwenden Sie den Ansatz

$$f = x_1 t^3 + x_2 t^2 + x_3 t + x_4 \in \mathbb{R}[t]$$

und ersetzen Sie die obigen Bedingungen an f durch

$$f(-2) = 0 \quad f(0) = x_5 \quad f(1) = 0 \quad f(4) = 0.$$

5. (4 Zusatzpunkte) Der Fermatsche Primzahltest: $n \in \mathbb{N}$ heißt Fermatsche Pseudoprimzahl zur Basis a , wenn n nicht prim ist, aber dennoch wie für Primzahlen

$$a^{n-1} \equiv 1 \pmod{n}$$

gilt. Bestimmen Sie mit Computerhilfe jeweils alle Pseudoprimzahlen $n \leq 1000$ zur Basis a mit $a = 2, 5, 7$. Wieviele Zahlen $n \leq 1000$ würden Sie anhand aller durchgeführten Tests fälschlicherweise für prim halten?

Hinweis: Sie können z.B. die MAPLE-Funktionen `nextprime` und `mod` verwenden.