Mathematische Methoden in der Kommunikationstheorie

(Sommersemester 2018)

Dr. Tobias Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Alexander Cant, M.Sc.
a.cant@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Technische Universität Braunschweig

Übungsblatt 5

(Abgabe: 08.05.2018 in der VL)

Aufgabe 1. (Diskreter Logarithmus)
Bestimmen Sie alle $x \in \{0, \dots 22\}$, welche die Kongruenz $x^x \equiv x \bmod 23$ erfüllen.

Aufgabe 2. (Sichere Primzahlen)
Eine Primzahl p heißt **sicher**, wenn $p = 2q + 1$ für eine andere Primzahl q gilt. Zeigen Sie:

a) Ist $p > 3$ eine Primzahl, so gilt entweder $p \equiv 1 \bmod 6$ oder $p \equiv 5 \bmod 6$.

b) Ist $p > 7$ eine sichere Primzahl, so gilt $p \equiv 5 \bmod 6, p \equiv 3 \bmod 4$ und $p \equiv 11 \bmod 12$.

c) Ist p eine sichere Primzahl, dann gibt es genau $\frac{p-3}{2}$ primitive Wurzeln modulo p.

d) Ist $p = 2q + 1$ eine sichere Primzahl, dann ist g genau dann eine primitive Wurzel modulo p, wenn $g \in \mathbb{Z}_p^* \setminus \{1, p-1\}$ und $g^q \bmod p \neq 1$.

Aufgabe 3. (Elgamal-Verschlüsselung)
Sie fangen die mit dem Elgamal-Verfahren verschlüsselte Nachricht $(7, 9)$ ab, die mit dem öffentlichen Schlüssel $(p, g, y) = (11, 2, 5)$ verschlüsselt wurde. Sie erkennen sofort, dass p viel zu klein gewählt wurde. Entschlüsseln Sie die Nachricht.

Aufgabe 4. (Elliptische Kurven und singuläre Punkte)
Sei E eine Kurve beschrieben durch die Gleichung

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{R}.$$

Setzen wir $f(x, y) = y^2 - x^3 - ax - b$, so können wir E auch beschreiben als die Menge der Punkte mit $f(x, y) = 0$. Wir nennen einen Punkt (u, v) auf E **singulär**, falls die beiden partiellen Ableitungen von f in (u, v) verschwinden, d.h. es gilt

$$\frac{\partial f}{\partial x}(u, v) = 0 \qquad \text{und} \qquad \frac{\partial f}{\partial y}(u, v) = 0.$$

Zeigen Sie:

a) E hat genau dann keine singulären Punkte, wenn $\Delta = 4a^3 + 27b^2 \neq 0$ gilt.

b) Gilt $\Delta = 0$ und $a = 0$, so hat E einen singulären Punkt in $(0, 0)$ und es gibt genau eine Tangente in diesem Punkt, welche durch die Gleichung $y = 0$ beschrieben wird. (Singularität vom Typ “cusp”).

c) Gilt $\Delta = 0$ und $a \neq 0$, so hat E einen singulären Punkt in $\left(-\frac{3b}{2a}, 0\right)$ und es gibt genau zwei Tangenten in diesem Punkt, welche durch die Gleichungen $y = \pm\sqrt{-\frac{9b}{2a}}\left(x + \frac{3b}{2a}\right)$ beschrieben werden. (Singularität vom Typ "node").

Hinweis: Erinnern Sie sich für b) & c) an den Begriff des **Tangentialkegels** aus der Analysis. Um eine Gleichung für den Tangentialkegel zu bestimmen, müssen wir eine mehrdimensionale (hier 2-dimensionale) Taylorentwicklung berechnen. Die Summe der Terme mit niedrigstem Totalgrad liefert dann eine Beschreibung des Tangentialkegels. Wir erinnern uns zusätzlich an die Form der 2-dimensionalen Taylorentwicklung von f im Punkt (x_0, y_0):

$$
\begin{aligned}
&Tf(x, y; x_0, y_0) \\
&= f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0) \\
&+ \frac{1}{2}\left[\frac{\partial^2 f}{\partial x^2}(x_0, y_0)(x - x_0)^2 + 2\frac{\partial^2 f}{\partial x \partial y}(x_0, y_0)(x - x_0)(y - y_0) + \frac{\partial^2 f}{\partial y^2}(x_0, y_0)(y - y_0)^2\right] \\
&+ \cdots
\end{aligned}
$$

In den folgenden Bildern sehen Sie links die Kurve $y^2 = x^3$ mit Singularität vom Typ "cusp" und rechts die Kurve $y^2 = x^3 - 3x + 2$ mit Singularität vom Typ "node" mit den jeweiligen Tangenten im singulären Punkt.