Klausur Wahrscheinlichkeitsrechnung und Kryptographie

Zugelassen sind alle Hilfsmittel (außer Kommunikationsmitteln)

Sie können maximal 60 Punkte erreichen, aber 5 davon sind "Zusatzpunkte". Sie erhalten also für 55 Punkte eine "1", und ab 28 Punkten (> 50% von 55) haben Sie bestanden.

1) Beim Schachspiel kann ein Turm nur vertikal oder horizontal ziehen bzw. schlagen.

   Wir betrachten nun ein "verallgemeinertes Schachbrett" mit $n \times n$ Feldern.

   Wie viele Möglichkeiten gibt es, n ununterscheidbare Türme so auf diesem Brett zu verteilen, dass keiner einen anderen bedroht?

   In jeder (horizontalen) Reihe und jeder (vertikalen) Linie darf also nur höchstens ein Turm stehen. (4 P)

2) Wie viele verschiedene fünfstellige Zahlen kann man durch Nebeneinanderlegen von 5 von 6 Kärtchen bilden, auf denen die Ziffern 1, 1, 2, 2, 2, 3 stehen? (7 P)

3) In einer Urne liegen 3 blaue, 2 rote und 5 grüne Bälle.

   Sie greifen blind hinein und holen nacheinander 2 Bälle heraus, und zwar

   a) ohne Zurücklegen, (3 P)

   b) mit Zurücklegen. (3 P)

   Wie groß ist jeweils die Wahrscheinlichkeit, zwei gleichfarbige Bälle zu erhalten?

4) Sie werfen zwei Würfel. Wie groß ist die Wahrscheinlichkeit, dass

   a) mindestens einer der Würfel eine 6 zeigt, (2 P)

   b) die Summe der beiden Augenzahlen gleich 7 ist, (2 P)

   c) das Produkt der beiden Augenzahlen ein Vielfaches von 10 ist? (3 P)

5) Anne und Britta spielen ein Tennismatch über 4 Sätze. Anne ist die bessere Spielerin: Sie gewinnt einen Satz mit einer Wahrscheinlichkeit von 2/3.

   Wie groß ist die Wahrscheinlichkeit, dass

   a) Anne alle 4 Sätze gewinnt, (2 P)

   b) Anne 2 Sätze gewinnt und zwei verliert, (3 P)

   c) Anne mindestens 2 Sätze gewinnt? (3 P)

Klausur Wahrscheinlichkeitsrechnung und Kryptographie

6) Die kontinuierliche Zufallsvariable X besitze die Dichtefunktion

$$f(x) = \begin{cases} C\left(1 - x^2\right) & \text{für } -1 \le x \le 1 \\ 0 & \text{sonst} \end{cases}$$

a) Welchen Wert muss C haben?
Skizzieren Sie den Verlauf von f(x). (2 P)

b) Wie groß ist die Standardabweichung von X? (3 P)

c) Berechnen Sie die Wahrscheinlichkeit, dass |X| < ½ gilt. (3 P)

7) Beweisen Sie ohne viel Rechnerei, dass gilt:

$$387262113029 \cdot 849531714455 \equiv 20 \pmod{25}$$ (5 P)

8) Eine monoalphabetische, monographische Chiffrierung eines deutschen Textes, der nur aus den Großbuchstaben **V** = { A, B, … , Z } besteht (Satzzeichen und Wortzwischenräume wurden weggelassen), funktioniere wie folgt:

Den Buchstaben $\in$ **V** seien wie üblich die Zahlen { 0, 1, … , 25 } zugeordnet, damit man mit ihnen „rechnen“ kann. Die Verschlüsselung eines Klartextbuchstaben $x \rightarrow f(x)$ erfolgt über die Formel

$$\mathbf{f(x) = (ax + b) \bmod 26}$$

mit ganzen Zahlen a, b $\in$ { 0, 1, … 25 }.

Eine Häufigkeitsanalyse ergibt: Der häufigste Buchstabe des Geheimtextes ist das Y (entsprechend dem E des Klartextes), der zweithäufigste das K (entsprechend dem N des Klartextes).

Welche Werte haben a und b? (7 P)

9) In einem Public-Key-System nach dem **RSA-Verfahren** fangen Sie als böser Lauscher den Geheimtext c = 60 ab, der an einen Empfänger gerichtet ist, dessen öffentlicher Schlüssel aus e = 43 und m = 77 (das ist der Modul) besteht.

Wie lautet die Klarnachricht z, die sich hinter dem Geheimtext c verbirgt? (8 P)