

Aufgabenblatt 5
(NUR FÜR ULI-STUDENTEN)

(URL: <http://www3.hpi.uni-potsdam.de/index.php?id=411>)

Abgabe: Mo, 23.05.2005, bis 12 Uhr MEZ (per E-Mail an
mathias.kutzner@hpi.uni-potsdam.de)

Thema: Wahrscheinlichkeitstheorie, Zahlentheorie, Algebraische Strukturen

Erreichbare Punkte: 22

Aufgabe 1:

6 Punkte

Geburtstagsparadoxon:

Wie viele Personen müssen in einem Raum sein, damit die Wahrscheinlichkeit, dass mindestens zwei Personen am gleichen Tag Geburtstag haben, größer als $\frac{1}{2}$ ist?

Dokumentieren Sie Ihren Lösungsweg nachvollziehbar. (Zur Vereinfachung müssen Schaltjahre nicht beachtet werden und es kann eine Gleichverteilung der Geburtstage angenommen werden.)

Was hat das Geburtstagsparadoxon mit Kryptografie zu tun?

Tipps:

$$\forall x \geq 0: (1-x) \leq e^{-x}$$

Definieren und benutzen Sie die folgenden Wahrscheinlichkeiten:

- $P(n,k)$ ist die Wahrscheinlichkeit, dass mindestens ein Wert doppelt in k Elementen vorkommt, wobei jedes Element gleichermaßen n verschiedene Werte zwischen 1 und n annehmen kann.
 - $Q(n,k)$ ist die Wahrscheinlichkeit, dass in k Elementen kein Wert mehrmals vorkommt, wobei jedes Element gleichermaßen n verschiedene Werte zwischen 1 und n annehmen kann.
-

Aufgabe 2:

6 Punkte

$[a]$ ist invertierbar $\Leftrightarrow \text{ggT}(a,n) = 1$.

Bestimmen Sie alle invertierbaren Kongruenzklassen modulo 14 und berechnen Sie alle Inverse. Geben Sie ihren Lösungsweg an.

Aufgabe 3:

6 Punkte

Bestimmen Sie die Ordnung aller Elemente in Z_{15}^* . Stellen Sie dar, wie Sie die Lösung ermittelt haben.

Aufgabe 4:

4 Punkte

Berechnen Sie von Z_{17}^* die Untergruppe mit der kleinstmöglichen Anzahl an Elementen, unter der Voraussetzung, dass $[2]_{17}$ ein Element dieser Untergruppe und die Operation die Multiplikation ist. Geben Sie Ihren Rechenweg an.
