Vorbereitungsblatt zur Prüfung in Angewandter Diskreter Mathematik

D. Ufer

Im Folgenden ein Paar Übungsaufgaben zur Vorbereitung auf die Prüfung. Das Blatt soll mittels Stift und Papier aber ohne sonstige Hilfsmittel zu lösen sein. Es ist nicht wichtig alle Rechnungen bis ins Einzelne durchzuführen, sondern die Vorgehensweise zu erklären.
Das Blatt erhebt nicht den Anspruch den gesamten Prüfungsstoff zu decken oder eine Musterprüfung zu liefern. Das Niveau der Aufgaben ist aber wahrscheinlich ähnlich zur Prüfung.

Aufgabe 1: Primzahlen

(a) Definieren und erklären Sie folgende Begriffe:
Teiler, Primzahl, Primfaktorzerlegung, größter gemeinsamer Teiler

(b) Berechnen Sie die Primfaktorzerlegung von:
$a = 121$, $b = 341$, $c = 2761$

(c) Bestimmen Sie anhand der Primfaktorzerlegung den $d = \mathrm{ggT}(a, b)$.

(d) Finden sie $x, y \in \mathbb{Z}$, so dass $d = xa + yb$. Sind die ganzen Zahlen x, y eindeutig?

Aufgabe 2: Kongruenzen

(a) Definieren und erklären Sie folgende Begriffe und Notationen:
$a \equiv b \mod m$, wobei $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, *Kongruenzklasse, vollständiges Restsystem*

(b) Bestimmen Sie die Lösungsmenge folgender Kongruenzen:

(i) $8a + 7 \equiv 8 \mod 26$

(ii) $8a + 6 \equiv 8 \mod 26$

Aufgabe 3: Der kleine Satz von Fermat

(a) Definieren und erklären Sie folgende Begriffe:
Inverses, reduziertes Restsystem, Eulersche φ-Funktion

(b) Bestimmen Sie das Inverse von 5 modulo 26 mittels erweiterten euklidischen Algorithmus.

(c) Berechnen Sie:

(i) $10^{144} \mod 21$.

(ii) $\varphi(341)$

(iii) $5^{-1} mod 306$

Aufgabe 4: Schnelle Exponentiation Erklären Sie 18^{107}, 13^{107}, 18^{107} jeweils modulo 2761 berechnet.

Aufgabe 5: Chinesischer Restsatz Berechnen Sie die Lösungsmenge folgender Systeme von Kongruenzen:

(a) $n \equiv 1 \mod 2$, $n \equiv 3 \mod 4$, $n \equiv 6 \mod 7$

(b) $n \equiv 2 \mod 3$, $n \equiv 3 \mod 6$, $n \equiv 7 \mod 9$

(c) Durch Weglassen einer einzigen Kongruenz lassen sich in dem System mit leerer Lösungsmenge doch wieder Lösungen finden.

Aufgabe 6: Kryptographie In (c)-(g) sind keine vollständigen Rechnungen gefragt, sondern nur, wie man dies durchführt.

(a) Definieren und erklären Sie folgende Begriffe:
symmetrisches/asymmetrisches Schlüsselverfahren, affine Chiffre, RSA

(b) Welcher Zusammenhang besteht zwischen der eulerschen φ-Funktion $\varphi(n)$ und der Primfaktorzerlegung von n? Was bedeutet das für die Sicherheit des RSA-Verfahrens?

(c) Verschlüsseln Sie folgende Nachricht mit der affinen Chiffre von Signatur $(3, 18)$: "GUT"

(d) Wie muss eine sinnvolle Signatur aussehen? Begründen Sie.

(e) Entschlüsseln Sie folgende Nachricht, die mit der affinen Chiffre von Signatur $(5, 8)$ kodiert wurde: "LWJ"

(f) Verschlüsseln Sie folgende Nachricht mit dem RSA-Verfahren und dem Schlüssel $(107, 2761)$: "ANANAS"

(g) Entschlüsseln Sie folgende Nachricht, die mit dem RSA-Verfahren und dem Schlssel $(1667, 2761)$ "AZRHB!", wobei "!" das Zeichen mit der Nummer 86 sei.

Aufgabe 7: Primzahltests

(a) Definieren und erklären Sie folgende Begriffe:
Pseudoprimzahl, Charmichael-Zahl, starke Pseudoprimzahl

(b) Zeigen Sie oder widerlegen Sie:

(i) Die Zahl 5083 ist eine Charmichael-Zahl.

(i) Die Zahl 341 ist eine starke Pseudoprimzahl zur Basis 2.

Aufgabe 8: Polynomring

(a) Erklären Sie anhand eines Beispiels, was ein Körper ist.

(b) In welchen Dingen ist der Polynomring $K[X]$ eines Körpers K ähnlich wie der Ring $\mathbb{Z}$ der ganzen Zahlen?

(c) Sind folgende Polynome irreduzibel ber $\mathbb{F}_3$, gibt es Nullstellen, welche Vielfachheit haben diese?

(i) $X^3 + X^2 + 1$

(ii) $X^3 + X$

(iii) $X^4 - 2$

(d) Faktorisieren Sie $X^4 + 1$ in $\mathbb{F}_3$ und $\mathbb{F}_5$.

Aufgabe 9: Endliche Körper

(a) Konstruieren Sie einen Körper $\mathbb{F}_9$ mit 9 Elementen (resp. $\mathbb{F}_{27}$ Krper mit 27 Elementen).

(c) Zeigen Sie: 2 ist ein Quadrat in $\mathbb{F}_9$. Was ist die Wurzel α von 2 in $\mathbb{F}_9$?

(d) Berechnen Sie das Inverse von α.

Aufgabe 10: Geben Sie für einen der folgenden Aussagen und Sätze einen Beweis oder eine Beweisskizze:

(a) Es gibt unendlich viele Primzahlen.

(b) Sei $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$. Sei $g = \mathrm{ggT}(c, m)$. Falls $ac \equiv bc \mod m$ gilt, dann ist $a \equiv b \mod m/g$.

(c) Satz von Euler

(d) Sei $a \in \mathbb{Z}/m\mathbb{Z}^*$, $m \in \mathbb{N}$. Dann teilt die Ordnung von a die Anzahl der invertierbaren Elemente $\varphi(m)$ von $\mathbb{Z}/m\mathbb{Z}$.

(e) Chinesischer Restsatz