Universität Bielefeld **Wintersemester 2013/14**
C. Huck

Präsenzübungen zur Vorlesung

Diskrete Mathematik

Blatt 14

Aufgabe 1
Bestimmen Sie $\varphi(20)$ und die Einheitengruppe $\mathbb{Z}_{20}^{\times}$ von $\mathbb{Z}_{20}$. Bestimmen Sie das multiplikatiive Inverse von 9 modulo 20.

Aufgabe 2
Sei $a \in \mathbb{Z}$ und p prim mit $p \not| a$. Zeigen Sie, dass für $m \in \mathbb{N}$ mit $m \equiv 1 \pmod{p-1}$ gilt:

$$a^m \equiv a \pmod{p}$$

Hinweis. Verwenden Sie den Satz von Fermat.

Aufgabe 3
Verschlüsseln Sie die Nachricht "AB" mit dem RSA-System unter Verwendung des öffentlichen Schlüssels $n = 115$, $k = 3$. Berechnen Sie dann den geheimen Schlüssel m und entschlüsseln Sie die verschlüsselte Nachricht. Erläutern Sie abschließend, warum das RSA-System als sicher angesehen wird und an welcher Stelle der Satz von Fermat eingeht.

Aufgabe 4
Beschriften Sie die Vertices v des Ordnungsgraphen G des Posets $(\mathcal{P}(\{1,2,3,4\}), \subset)$ mit den Werten $\mu(\varnothing, v)$ der zugehörigen Möbiusfunktion. Ist G ein Baum? Ist G bipartit? Bestimmen Sie einen Spannbaum von G. Gibt es in G Zykel ungerader Länge? Gibt es in G einen eulerschen Weg? Gibt es in G einen hamiltonschen Zyklus?

Aufgabe 5
Wenden Sie die Möbiusinversion auf die Funktion g, gegeben durch $g(n) = \sum_{d|n} d\varphi(d)$ an.

Aufgabe 6
Beschreiben Sie einen Algorithmus zur Färbung eines Graphen G mit möglichst wenigen Farben. Auf keinen Fall darf Ihr Verfahren mehr als $\Delta(G) + 1$ Farben benötigen (wir hatten ja $\chi(G) \leq \Delta(G) + 1$).

Aufgabe 7
Bestimmen Sie die chromatische Zahl des vollständigen Graphen K_n.