Diskrete Mathematik

10. Übungsblatt

Präsenzübungen

Aufgabe P10.1 (Graph-Automorphismen)

Zeigen Sie, dass für jeden Graph G die Menge $\mathrm{Aut}(G)$ eine Untergruppe von $\mathrm{Sym}(G)$ ist.

Aufgabe P10.2 (RSA und Faktorisierung)

Malory ist in der Lage, aus einem öffentlichen Schlüssel (n, e) den privaten Schlüssel d zu gewinnen. In dieser Aufgabe wollen wir uns ansehen, wie sie ihr Wissen nutzen kann, um n zu faktorisieren. Sei $n = p \cdot q$. Wir schreiben außerdem $e \cdot d - 1 = 2^s \cdot k$ mit k ungerade.

a) Sei $a \in \{0, \ldots, n-1\}$. Zeigen Sie: wenn $a + \mathbb{Z}/p\mathbb{Z}$ und $a + \mathbb{Z}/q\mathbb{Z}$ unterschiedliche (multiplikative) Ordnung haben, dann gibt es eine Potenz a^e von a mit $\gcd(a^e - 1, n) \neq 1, n$. Damit ist $\gcd(a^e - 1, n)$ ein echter Teiler von n, den zu finden Malorys Ziel ist.

b) Zeigen Sie, dass für jedes $a \perp n$ die Ordnung von $a^k + \mathbb{Z}/n\mathbb{Z}$ ein Teiler von 2^s ist. Man kann zeigen, dass für wenigstens die Hälfte der $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ die Ordnung von $a^k + \mathbb{Z}/pZ$ und $a^k + \mathbb{Z}/q\mathbb{Z}$ verschieden ist.

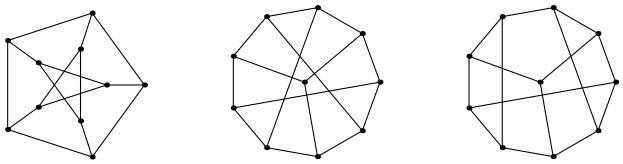
c) Leiten Sie ein Verfahren ab, mit dem Malory n faktorisieren kann. Nach v Versuchen hat sie Erfolg mit einer Wahrscheinlichkeit $1 - 2^{-v}$.

Hausübungen

Aufgabe H10.1 (Graphen vergleichen)

a) Von den unten dargestellten Graphen sind zwei isomorph zueinander. Geben Sie einen Isomorphismus an (z.B. indem Sie die Ecken beschriften).

b) Zeigen Sie, dass der dritte Graph nicht isomorph zu den anderen beiden ist.



Hinweis: Für (b) können Sie zum Beispiel einen Untergraph finden, den ein Graph enthält, der andere aber nicht.

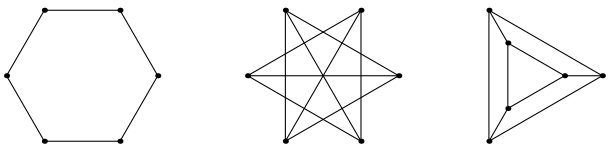
(3+3 Punkte)

Aufgabe H10.2 (Graph-Automorphismen)

Wir bezeichnen die unten angegebenen Graphen mit C_6, $\bar{C}_6$ und CC_6.

a) Zeigen Sie, dass $\mathrm{Aut}(C_6) = \mathrm{Aut}(\bar{C}_6)$. Welches allgemeine Phänomen steckt dahinter?

b) Zeigen Sie, dass $\mathrm{Aut}(C_6)$ nicht isomorph zu $\mathrm{Aut}(CC_6)$ ist.



Hinweis: Vergleichen Sie für (b) die Elementordnungen.

(3+3 Punkte)

Aufgabe H10.3 (Schnelle Exponentiation)

Verwenden Sie schnelle Exponentiation um $41^{181} \mod 4096$ zu berechnen.

(2 Punkte)

Abgabe bis 22.1.2016.