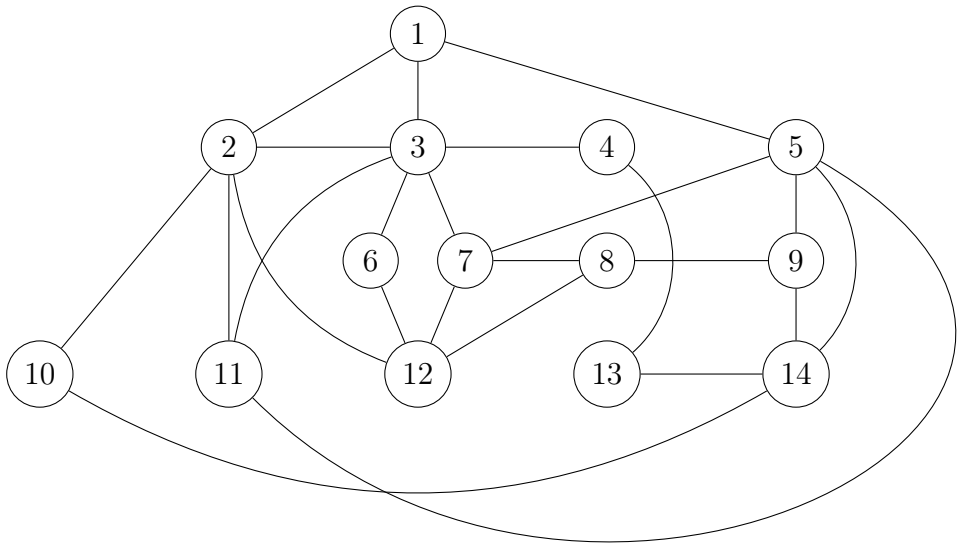
Übungsblatt 5

Punkte: 50

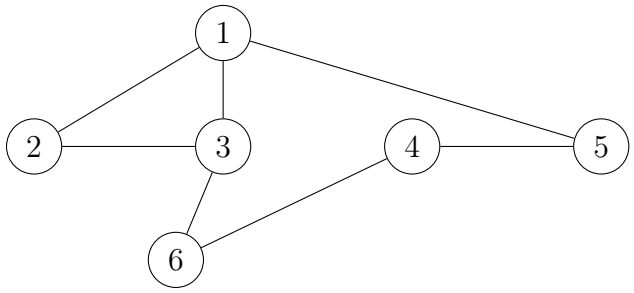
Hertrampf, Mattes
FMI/TI, FMI/ALG
Universität Stuttgart

Aufgabe 1: Graphen **[10]**

(a) Ist der folgende Graph planar? Begründen Sie Ihre Antwort mit
(i) Satz von Kuratowski
Wenn n die Anzahl der Knoten ist, dann hat der Graph höchstens $3n - 6$ Kanten.
Warum ist dies kein Widerspruch zur Eulerformel?



(b) Hat der folgende Graph einen Eulerkreis? Hat er einen Eulerpfad? Falls ein solcher Kreis oder Pfad existiert, geben Sie einen an.
Geben Sie einen Beweis für Ihre Antwort an!



Aufgabe 2: RSA-Verfahren **[15]**

Alice sendet Bob Neujahrsgrüße. Dieser möchte ihr gerne darauf antworten. Da er jedoch sehr gut in Algebra ist möchte er sich nur mit Menschen unterhalten, die seine Prüfung bestehen. Diese besteht darin, eine verschlüsselte Botschaft lesen zu können. Sein Lieblingsverfahren ist dabei das RSA Verfahren, seine Lieblingsprimzahlen sind 5 und 11. Da er am 9.9. Geburtstag hat, wird er immer die 9 wählen, falls dies möglich ist.

(a)Welches Schlüsselmaterial wird er Alice wohl schicken?

(b) Alice weiß, dass Bob ein kleines Wörterbuch mit Zahlencodes für jedes Wort besitzt. Sie hat eine Kopie eines Ausschnittes dieses Buches.

Welche verschlüsselte Nachrichten wird sie Bob senden, wenn sie jedes Wort einzeln verschlüsseln möchte?

(c) Als Bob Alice ebenfalls ein frohes neues Jahr wünscht, bekommt er die Nachricht $46, 18$ zurück. Was will Alice ihm nun noch mitteilen?

Bitte stellen Sie Ihren Rechenweg ausführlich dar!

Hinweis: Das Folgende ist eine Kopie aus Bobs Wörterbuch:

Alles=2, *Dank* =8, *Gute=9*, *Jahr*=3, *neuen=4*, *Vielen*=6 ,*zum=5*,

Aufgabe 3: Eulersche ϕ-Funktion **[5]**

Geben Sie die Anzahl der Einheiten in den folgenden Restklassenringen an:

(a)$\mathbb{Z}/143\mathbb{Z}$
(b) $\mathbb{Z}/210\mathbb{Z}$
(c) $\mathbb{Z}/343\mathbb{Z}$
(d) $\mathbb{Z}/360\mathbb{Z}$

(A)[P] Bestimmten Sie alle natürlichen Zahlen $n \in 11\mathbb{Z}$ mit $\phi(n) = 60$

Aufgabe 4: RSA 2 **[5]**

In dieser Aufgabe werden wir Textnachrichten bzw. Wörter mithilfe des RSA-Verfahrens ver- und entschlüsseln. Dabei verwenden wir öffentliche Schlüssel (n, e) mit $n = 33$. Für die Elemente des Restklassenrings $\mathbb{Z}/33\mathbb{Z}$ führen wir eine abkürzende Schreibweise ein: Statt $r + 33\mathbb{Z}$ schreiben wir einfach $[r]$.

Als Alphabet für die Wörter wählen wir $\Sigma = \{␣^1, A, B, \ldots, Z, !, =, \}$. Ein Wort $w = a_1 \ldots a_n$ mit $a_1, \ldots, a_n \in \Sigma$ wird dann entsprechend folgender Tabelle buchstabenweise in eine Folge $([z_1], \ldots, [z_n])$ von Restklassen aus $\mathbb{Z}/33\mathbb{Z}$ codiert.

Klasse	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]
Zeichen	␣	A	B	C	D	E	F	G	H	I	J	K	L	M
Klasse	[14]	[15]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Zeichen	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	!

Beispiel: Das Wort „Skifahren“wird als Folge

$$([19], [11], [9], [6], [1], [8], [18], [5], [14])$$

[1]Dieses Zeichen stellt ein Leerzeichen dar.

codiert.

Eine Folge $([z_1], \ldots, [z_n]) \in (\mathbb{Z}/33\mathbb{Z})^n$ wird elementweise ver- bzw. entschlüsselt.

(a) [P] Verschlüsseln Sie mit dem öffentlichen Schlüssel $(n, e) = (33, 3)$ die Codierung des Worts „Skifahren “.
(b)[P] Ihnen fällt zufällig die Nachricht $([13], [26], [5], [26], [14], [3], [11])$ in die Hände. Sie wissen, dass diese mithilfe des RSA-Verfahrens mit dem öffentlichen Schlüssel $(n, e) = (33, 3)$ verschlüsselte wurde. Außerdem wissen Sie, dass es das Thema des Geheimprojektes Ihres Kontrahenten ist. Daher ist es für Sie von besonderem Interesse, die Nachricht zu entschlüsseln.
Bestimmen Sie den zugehörigen privaten Schlüssel (p, q, s). Geben Sie Ihren Rechenweg an oder beweisen Sie die Korrektheit Ihres Ergebnisses.

(c) Wie lautet die entschlüsselte und decodierte Nachricht?

Aufgabe 5: Fibonacci-Zahlen. **[15]**

Die Fibonacci-Zahlen sind folgendermaßen definiert:

$F_0 = 0$, $F_1 = 1$,$F_{n+2} = F_{n+1} + F_n$. Es ist außerdem $F_{-1} = 1$. Für $n \leq 0$ sei $F_n = F_{n-1} + F_{n-2}$.

Sei außerdem die Matrix M_z definiert als $M_z = \begin{pmatrix} F_{z-1} & F_z \\ F_z & F_{z+1} \end{pmatrix}$ und die Matrix M_1 als $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Zeigen Sie, dass $M_1^z = M_z \ \forall z \in \mathbb{Z}$. *Hinweis: Beginnen Sie mit einer Induktion über* $\mathbb{N}$.