**Technische Universität München (I7)**
**Prof. J. Esparza / Dr. M. Luttenberger**

**Winter 2013/14**

# LÖSUNG

## Diskrete Strukturen – Wiederholungsklausur

*Beachten Sie:* Soweit nicht anders angegeben, ist stets eine Begründung bzw. der Rechenweg anzugeben!

### Aufgabe 1 — 4P

Sei $F = (((p \leftrightarrow r) \wedge (\neg q \rightarrow r)) \vee (q \wedge (\neg p \vee r)))$.

(a) Stellen Sie zu $F$ eine Wahrheitstafel auf. Füllen Sie diese vollständig entsprechend der Vorlesung aus.

(b) Bestimmen Sie aus der Wahrheitstafel eine zu $F$ semantisch äquivalente Formel in konjunktiver Normalform (KNF).

**Lösung:**

(a)

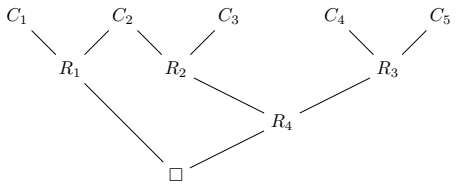
| $p$ | $q$ | $r$ | $(((\ p$ | $\leftrightarrow$ | $r\ )$ | $\wedge$ | $(\ \neg$ | $q$ | $\rightarrow$ | $r\ ))$ | $\vee$ | $(\ q$ | $\wedge$ | $(\ \neg$ | $p$ | $\vee$ | $r\ )))$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |

(b)

$$\begin{aligned} F &\equiv (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r) \\ &\equiv (p \vee q) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r) \end{aligned}$$

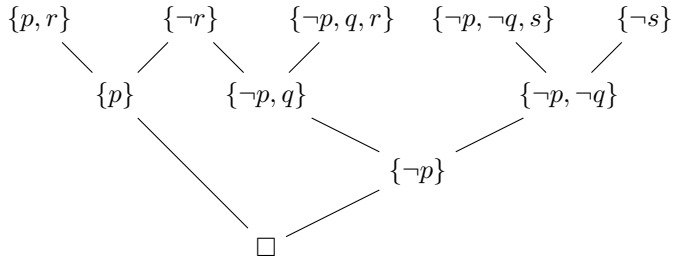
### Aufgabe 2 — 3P

Bestimmen Sie Klauseln $C_1, \ldots, C_5, R_1, \ldots, R_4$, so dass folgender Graph eine korrekte Resolution der leeren Klausel aus $F = \{C_1, \ldots, C_5\}$ darstellt:




**Ansage**: Alle Klauseln müssen (paarweise) verschieden sein ($|\{C_1, \ldots, C_5, R_1, \ldots, R_4\}| = 9$).

**Lösung:**



**Aufgabe 3** **4P**

Eine aussagenlogische Formel $F$ heißt *Horn-Formel*, falls $F$ in KNF ist und in jeder Klausel von $F$ höchstens ein positives Literal auftritt. (Beispiele: $p \wedge (\neg p \vee \neg q) \wedge (\neg q \vee r)$ ist eine Horn-Formel, $(p \vee q)$ ist keine Horn-Formel.)

Sei $F$ eine Horn-Formel. Zeigen Sie (ohne sich auf A4 zu beziehen):

(a) Falls $F$ keine Klausel enthält, welche genau aus einem positiven Literal besteht, dann ist $F$ erfüllbar.

(b) Falls $F$ eine Klausel $\{L\}$ enthält, welche genau aus einem positiven Literal $L$ besteht, dann ist $F$ genau dann erfüllbar, wenn $F[L := \text{true}]$ erfüllbar ist.

**Lösung:**

(a) Die minimale Belegung, die jeder in $F$ auftretenden Variablen den Wahrheitswert 0 zuweist, ist ein Modell: Auf Grund der KNF reicht es zu überprüfen, dass jede Klausel unter dieser Belegung erfüllt ist; eine Klausel ist genau dann erfüllt, wenn mindestens ein in ihr auftretendes Literal erfüllt ist; nach Annahme gibt es in jeder Klausel mindestens ein negatives Literal, das sich offensichtlich unter dieser Belegung zu dem Wahrheitswert 1 auswertet.

(b) Vorbemerkung: Da $F$ in KNF ist, ist auch $F[L := \text{true}]$ in KNF: $F[L := \text{true}]$ entsteht aus $F$, indem man aus $F$ jede Klausel, welche $L$ enthält, entfernt und aus allen anderen Klauseln das Literal $\overline{L}$ entfernt. Insbesondere gibt es für jede Klausel $C$ aus $F[L := \text{true}]$ eine Klausel $K$ aus $F$, so dass $C = K - \{L\}$ gilt.

Beweis der Behauptung:

Sei $\sigma$ eine $F$-erfüllende Belegung. Da $F$ in KNF, gilt $[K](\sigma) = 1$ für jede Klausel $K \in F$; wegen $\{L\} \in F$, muss somit auch $[\{L\}](\sigma) = [L](\sigma) = 1$ gelten. Sei $C$ eine beliebige Klausel aus $F[L := \text{true}]$. Dann gibt es eine Klausel $K$ aus $F$ mit $C = K - \{\overline{L}\}$. Wegen $[K](\sigma) = 1$ muss es ein Literal $L' \in K$ mit $[L'](\sigma) = 1$ geben. Wegen $[\overline{L}](\sigma) = 0$ muss $L' \neq \overline{L}$ und somit $L' \in C = K - \{\overline{L}\}$ gelten. Es folgt $[C](\sigma) = 1$.

Sei $\sigma$ eine $F[L := \text{true}]$-erfüllende Belegung, d.h. für jede Klausel $C \in F[L := \text{true}]$ gilt $[C](\sigma) = 1$. Da weder $L$ noch $\overline{L}$ in $F[L := \text{true}]$ auftreten, können wir ohne Einschränkung annehmen, dass $[L](\sigma) = 1$ gilt. Sei nun $K$ eine beliebige Klausel von $F$. Gilt $L \in K$, so folgt sofort $[K](\sigma) = 1$. Gilt $L \notin K$, so ist $C = K - \{\overline{L}\}$ eine Klausel aus $F[L := \text{true}]$. Aus $[C](\sigma) = 1$ und $C \subseteq K$ folgt sofort $[K](\sigma) = 1$.

**Aufgabe 4** **2P**

Sei $G := ((p \wedge q) \rightarrow \neg s) \wedge \neg t \wedge (r \rightarrow p) \wedge r \wedge q \wedge (u \rightarrow v) \wedge u \wedge (v \rightarrow \neg(s \wedge t))$.

(a) Überführen Sie $G$ entsprechend der Vorlesung durch Entfernen von Doppelnegationen und Verwendung von De Morgan und Distributivität in eine semantisch äquivalente Horn-Formel (siehe A3) . Verwenden Sie keine Wahrheitstabelle!

Mit Aufgabe 3 kann gezeigt werden, dass der folgende Algorithmus $\mathcal{A}$ die Erfüllbarkeit von Horn-Formeln korrekt entscheidet:

- Eingabe: Hornformel $F$ als Klauselmenge.
- **Falls** $F$ die leere Klausel enthält, gib „unerfüllbar" zurück; **sonst**:
  - **Falls** $F$ eine Klausel $\{L\}$ enthält, die genau aus einem positivem Literal $L$ besteht, berechne rekursiv $\mathcal{A}(F[L := \text{true}])$ und gib den erhaltenen Wert zurück; **sonst**: gib „erfüllbar" zurück.

(b) Wenden Sie den Algorithmus $\mathcal{A}$ auf die Horn-Formel, die Sie in (a) hergeleitet haben, an. Geben Sie die einzelnen Aufrufe von $\mathcal{A}$ einschließlich der übergebenen Klauselmengen und ausgewählten Literale an.

**Ansage:** Implikationen müssen/dürfen in (a) aufgelöst werden.

**Lösung:**

(a)

$$G = ((p \wedge q) \rightarrow \neg s) \wedge \neg t \wedge (r \rightarrow p) \wedge r \wedge q \wedge (u \rightarrow v) \wedge u \wedge (v \rightarrow \neg(s \wedge t))$$

Auflösen der Implikation:

$$G \equiv (\neg(p \wedge q) \vee \neg s) \wedge \neg t \wedge (\neg r \vee p) \wedge r \wedge q \wedge (\neg u \vee v) \wedge u \wedge (\neg v \vee \neg(s \wedge t))$$

Anwenden von deMorgan (und Assoziativität):

$$G \equiv (\neg p \vee \neg q \vee \neg s) \wedge \neg t \wedge (\neg r \vee p) \wedge r \wedge q \wedge (\neg u \vee v) \wedge u \wedge (\neg v \vee \neg s \vee \neg t)$$

(b)
- Start:

$$\{ \quad \{\neg p, \neg q, \neg s\}, \quad \{\neg t\}, \quad \{\neg r, p\}, \quad \{r\}, \quad \{q\}, \quad \{\neg u, v\}, \quad \{u\}, \quad \{\neg v, \neg s, \neg t\} \quad \}$$

- Setze $q := 1$:
$$\{ \quad \{\neg p, \neg s\}, \quad \{\neg t\}, \quad \{\neg r, p\}, \quad \{r\}, \quad \{\neg u, v\}, \quad \{u\}, \quad \{\neg v, \neg s, \neg t\} \quad \}$$
- Setze $r := 1$:
$$\{ \quad \{\neg p, \neg s\}, \quad \{\neg t\}, \quad \{p\}, \quad \{\neg u, v\}, \quad \{u\}, \quad \{\neg v, \neg s, \neg t\} \quad \}$$
- Setze $p := 1$:
$$\{ \quad \{\neg s\}, \quad \{\neg t\}, \quad \{\neg u, v\}, \quad \{u\}, \quad \{\neg v, \neg s, \neg t\} \quad \}$$
- Setze $u := 1$:
$$\{ \quad \{\neg s\}, \quad \{\neg t\}, \quad \{v\}, \quad \{\neg v, \neg s, \neg t\} \quad \}$$
- Setze $v := 1$:
$$\{ \quad \{\neg s\}, \quad \{\neg t\}, \quad \{\neg s, \neg t\} \quad \}$$
- Gib „erfüllbar" aus.

**Aufgabe 5** **4P**

(a) Wie viele symmetrische Relationen $R \subseteq [10] \times [10]$ gibt es?

(b) Wie viele asymmetrische Relationen $R \subseteq [10] \times [10]$ gibt es?

Begründen Sie Ihre Antwort. Die genauen Zahlenwerte müssen nicht angegeben werden. Es reicht in allen Fällen, die gesuchten Werte mit Hilfe bekannter Zählkoeffizienten z.B. als Summen darzustellen. Die Ausdrücke sollten jedoch möglichst einfach sein, unnötig komplizierte Ausdrücke werden ggf. nicht gewertet.

**Lösung:**

(a) Für jedes Paar $(x, x)$ hat man die freie Wahl, ob man es in $R$ aufnimmt; ansonsten kann man noch wählen, welche ungeordneten Paare $\{x, y\}$ $(x \neq y)$ man aufnimmt: $2^{10} \cdot 2^{9 \cdot 10/2} = 2^{55}$.

(b) Eine asymmetrische Relation ist stets irreflexiv; somit muss man nur für jedes ungeordnete Paar $\{x, y\}$ $(x \neq y)$ entscheiden, ob man keines der beiden oder genau eines der beiden geordneten Paare aufnimmt: $3^{9 \cdot 10/2}$.

**Aufgabe 6** **7P**

Der ASCII-Code enthält exkl. dem Leerzeichen 94 druckbare Zeichen, darunter die 10 Ziffern $\mathcal{Z} = \{0 \ldots 9\}$, die 52 Buchstaben $\mathcal{B} = \{a, \ldots, z, A, \ldots, Z\}$ und die verbleibenden 32 druckbaren Sonderzeichen $\mathcal{S} = \{+, !, \ldots, \sim\}$. Sei $\Sigma = \mathcal{Z} \cup \mathcal{B} \cup \mathcal{S}$.

(a) Wie viele Wörter $\omega = \alpha\beta \in \Sigma^9$ der Länge 9 mit $\alpha \in \mathcal{B}^*$ und $\beta \in \mathcal{Z}^*$ gibt es?

(b) Wie viele Wörter $\omega \in \Sigma^8$ der Länge 8 gibt es, die nicht von der Form $\alpha 1234 \beta$ mit $\alpha, \beta \in \Sigma^*$ sind?

(c) Wie viele Wörter $\omega \in \Sigma^7$ der Länge 7 gibt es, die mindestens ein Zeichen aus jeder der drei Mengen $\mathcal{Z}, \mathcal{B}, \mathcal{S}$ enthalten?

Begründen Sie Ihre Antwort. Die genauen Zahlenwerte müssen nicht angegeben werden. Es reicht in allen Fällen, die gesuchten Werte mit Hilfe bekannter Zählkoeffizienten z.B. als Summen darzustellen. Die Ausdrücke sollten jedoch möglichst einfach sein, unnötig komplizierte Ausdrücke werden ggf. nicht gewertet.

**Lösung:**

(a) Fallunterscheidung nach $l = |\alpha|$.
$$\sum_{l=0}^{9} 52^l \cdot 10^{9-l}$$

(b) Man kann die Position $l \in [5]$ wählen, an der 1234 beginnt, und die 4 weiteren Zeichen $\alpha\beta \in \Sigma^4$, dabei zählt man allerdings das Wort 12341234 doppelt.

Es gibt also $5 \cdot 94^4 - 1$ viele Wörter der Länge 8, die 1234 als zusammenhängendes Teilwort enthalten.

Somit gibt es $94^8 - 5 \cdot 94^4 + 1$ viele Wörter der Länge 8, die 1234 nicht als zusammenhängendes Teilwort enthalten.

(c) Sei $[B > 0]$ (bzw. $[Z > 0]$ bzw. $[S > 0]$) die Menge aller Wörter aus $\Sigma^7$, die mindestens einen Buchstaben (bzw. eine Ziffer bzw. ein Sonderzeichen) enthalten.

Dann ist $|[B > 0] \cap [Z > 0] \cap [S > 0]|$ gesucht bzw. $|\Sigma|^7 - \left|\overline{[B > 0]} \cup \overline{[Z > 0]} \cup \overline{[S > 0]}\right|$. (Im Weiteren $[B > 0, S > 0] := [B > 0] \cap [S > 0]$ und $[B = 0] := \overline{[B > 0]}$ usw.)

Mittels Siebformel:

$$\begin{aligned}|[B = 0] \cup [Z = 0] \cup [S = 0]| = {} & |[B = 0]| + |[Z = 0]| + |[S = 0]| \\ & - |[B = 0, Z = 0]| - |[B = 0, S = 0]| - |[Z = 0, S = 0]| \\ & + |[B = 0, S = 0, Z = 0]|\end{aligned}$$

$|[B = 0]| = \left|(\mathcal{Z} \cup \mathcal{S})^7\right| = 42^7$.

$|[Z = 0]| = \left|(\mathcal{B} \cup \mathcal{S})^7\right| = 84^7$.

$|[S = 0]| = \left|(\mathcal{B} \cup \mathcal{Z})^7\right| = 62^7$.

$|[B = 0, Z = 0]| = \left|\mathcal{S}^7\right| = 32^7$.

$|[B = 0, S = 0]| = \left|\mathcal{Z}^7\right| = 10^7$.

$|[Z = 0, S = 0]| = \left|\mathcal{B}^7\right| = 52^7$.

$|[B = 0, Z = 0, S = 0]| = \left|\emptyset^7\right| = 0$.

Insgesamt:

$$|B \cap Z \cap S| = 94^7 - \left(42^7 + 84^7 + 62^7 - (32^7 + 10^7 + 52^7)\right)$$

**Aufgabe 7** **6P**

Sei $G = (V, E)$ ein endlicher, einfacher Graph. Wir nehmen an, dass die Knoten $V = \{v_1, v_2, \ldots, v_n\}$ nach aufsteigendem Knotengrad aufgezählt werden, d.h. $\deg(v_i) \leq \deg(v_j)$ für $1 \leq i < j \leq n$. Dann ist die Gradfolge von $G$ gerade die Sequenz $(\deg(v_1), \deg(v_2), \ldots, \deg(v_n))$. Begründen Sie jeweils kurz, ob

(a) jeder einfache Graph mit Gradfolge $(1, 3, 3, 4, 4, 5)$ zusammenhängend ist?

(b) es einen einfachen kreisfreien Graphen mit Gradfolge $(2, 2, 2, 3, 3)$ gibt.

(c) jeder einfache kreisfreie Graph mit Gradfolge $(1, 1, 2, 2, 2)$ ein Baum ist?

(d) jeder einfache Graph mit Gradfolge $(4, 4, 4, 4, 4, 4, 4, 4, 4, 4)$ eine Euler-Tour enthält.

(e) es einen einfachen Graphen mit Gradfolge $(1, 2, 3, 3, 4, 5)$ gibt, der einen Hamilton-Kreis enthält.

(f) es einen einfachen Graphen mit Gradfolge $(2, 4, 4, 4, 4, 4)$ gibt, der einen Hamilton-Kreis enthält.

**Lösung:**

(a) Ja. Es gibt 6 Knoten, wobei ein Knoten $v$ zu den restlichen 5 benachbart ist. Somit gibt es von jedem Knoten $u$ zu jedemn Knoten $w$ einen Pfad über $v$.

(b) Nein. In jedem kreisfreien Graphen ist jede Zusammenhangskomponente ein Baum, somit ist jeder kreisfreie Graph ein Wald. Es müsste somit mindestes ein Blatt, d.h. Knoten vom Grad 1 geben.

(c) Ja. Nach Übungen ist jeder einfache kreisfreie Graph mit $|E| = |V| - 1$ ein Baum. Letzteres gilt wegen $2\,|E| = \sum_{i=1}^{5} d_i = 8 = 2(5 - 1) = 2(|V| - 1)$.

(d) Nein. Man betrachte z.B. den Graphen, der aus zwei Zusammenhangskomponenten besteht, die beide jeweils isomorph zum $K_5$ sind. Da dieser nicht zusammenhängend ist, kann es keine Euler-Tour geben.

(e) Nein. Es gibt einen Knoten $u$ vom Grad 1. Der einzige Nachbar von $u$ muss somit zweimal besucht werden. Ein Kreis besucht (nach Vorlesung) aber einen Knoten höchstens einmal.

(f) Ja. Man nehme z.B. den $K_5$ und unterteile eine beliebige Kante durch Hinzufügen eines weiteren Knoten.

**Aufgabe 8** **4P**

Die Funktion $S(\cdot)$ ordnet jedem binären Wurzelbaum $T = (V, E, v)$ mit Wurzel $v$ eine Zahl $S(T) \in \mathbb{N}_0$ wie folgt zu, wobei $\Gamma(v)$ die Nachbarschaft von $v$ bezeichnet:

- Gilt $\Gamma(v) = \emptyset$, so sei $S(T) := 0$.
- Gilt $\Gamma(v) = \{v_1, v_2\}$, so seien $T_1, T_2$ die Wurzelbäume mit Wurzeln $v_1, v_2$, in die $T$ durch Entfernen von $v$ zerfällt. Gilt $S(T_1) = S(T_2)$, so sei $S(T) := S(T_1) + 1$; ansonsten gelte $S(T) := \max\{S(T_1), S(T_2)\}$.

Zeigen Sie: Jeder binäre Wurzelbaum $T$ hat mindestens $2^{S(T)}$ Blätter.

**Lösung:** Sei $L(T)$ die Anzahl der Blätter von $T$.

Induktion nach Anzahl $n$ der Knoten von $T$.

$n = 1$: Dann besteht $T$ nur aus der Wurzel $v$ und besitzt somit genau ein Blatt. Nach Definition gilt auch $S(T) = 0$. Insofern gilt auch die zu zeigende Behauptung $L(T) = 1 \geq 2^0 = 2^{S(T)}$.

$n \to n + 1$: $T$ besitzt mindestens zwei Knoten. Zerfällt $T$ durch Entfernen der Wurzel $v$ in zwei Teilbäume $T_1, T_2$ mit $S(T_1) = S(T_2)$, so gilt $S(T) = S(T_1) + 1$ nach Definition von $S(\cdot)$. Weiter ist in diesem Fall jedes Blatt von $T$ auch ein Blatt von genau einem der beiden Teilbäume, d.h. es gilt $L(T) = L(T_1) + L(T_2)$. Da $T_1$ und $T_2$ jeweils mindestens einen Knoten weniger als $T$ besitzen, gilt induktiv $L(T_i) \geq 2^{S(T_i)}$ $(i = 1, 2)$. Insgesamt somit:

$$L(T) = L(T_1) + L(T_2) \geq 2^{S(T_1)} + 2^{S(T_2)} = 2^{S(T_1)} + 2^{S(T_1)} = 2^{S(T_1)+1} = 2^{S(T)}.$$

Ansonsten gilt $S(T) = \max\{S(T_1), S(T_2)\}$. Weiter gilt stets $L(T) \geq \max\{L(T_1), L(T_2)\}$. Induktiv gilt wieder $L(T_i) \geq 2^{S(T_i)}$ $(i = 1, 2)$. Es folgt:

$$L(T) \geq \max\{L(T_1), L(T_2)\} \geq \max\{2^{S(T_1)}, 2^{S(T_2)}\} = 2^{\max\{S(T_1), S(T_2)\}} = 2^{S(T)}.$$

**Aufgabe 9** **6P**

Die naive Verwendung des RSA-Verfahrens als Verschlüsselungssystem lautet wie folgt:

- Sei $N = pq$ das Produkt zweier verschiedener Primzahlen $p$ und $q$, und sei $c \in \mathbb{Z}^*_{\varphi(N)}$. (Hier gilt $\varphi(N) = (p-1)(q-1)$.)
- Dann wird ein „Zeichen" $x \in \mathbb{Z}_N$ zu $(x^c \bmod N)$ verschlüsselt.

Im Folgenden gelte $p = 7$ und $q = 11$.

(a) Bestimmen Sie das kleinste $k \in \mathbb{N}_0$, so dass $(2^k + 1) \in \mathbb{Z}^*_{\varphi(N)}$ gilt.

(b) Sei $c = 13$. Wir identifizieren die Großbuchstaben $A, B, \ldots, Z$ mit den Zahlen $1, 2, \ldots, 26$ entsprechend ihrer Reihenfolge im Alphabet. Verschlüsseln Sie folgende Nachricht, indem Sie die naive RSA-Verschlüsselung der Reihe nach auf jeden Buchstaben anwenden.

ESEL

*Hinweis*: Es gilt $E \mapsto 5$, $L \mapsto 12$ und $S \mapsto 19$. Nutzen Sie geeignet aus, dass $x^{13} \equiv_N ((x^3 \bmod N)^2 \bmod N)^2 \cdot x$ gilt.

(c) Entschlüsseln Sie folgenden Text (bestehend aus 5 Zeichen, zur besseren Lesbarkeit durch Kommata getrennt), der analog zu (b) unter Verwendung von $c = 13$ verschlüsselt wurde:

12, 26, 61, 26, 46

Geben Sie auch den zu $c = 13$ gehörenden Entschlüsselungsexponenten an.

*Hinweis*: $46^{12} \equiv_{77} 15$.

**Lösung:**

(a) $\varphi(77) = (7-1)(11-1) = 60 = 2^2 \cdot 3 \cdot 5$. $2^k + 1 \rightsquigarrow 2, 3, 5, 9, 17, \ldots$. Also $k = 4$

(b)

$$E \mapsto 5^{13} = ((5^3)^2)^2 \cdot 5 \equiv_{77} (48^2)^2 \cdot 5 \equiv_{77} (-6)^2 \cdot 5 \equiv_{77} 36 \cdot 5 \equiv_{77} 26 \qquad L \mapsto 12^{13} \equiv_{77} 12 \qquad S \mapsto 19^{13} \equiv_{77} 61$$

Somit: 26 61 26 12

(c) Mit (b) entschlüsselt man sofort die ersten vier Zeichen zu $LESE$.

Zum Entschlüsseln des letzten Buchstabens berechnet man das multiplikative Inverse von 13 modulo 60 mittels dem erweiterten euklidischen Algorithmus:

- $(a_1, b_1) = (13, 60)$, $k_1 = \lfloor 60/13 \rfloor = 4$

- $(a_2, b_2) = (8, 13)$, $k_2 = \lfloor 13/8 \rfloor = 1$
- $(a_3, b_3) = (5, 8)$, $k_3 = \lfloor 8/5 \rfloor = 1$
- $(a_4, b_4) = (3, 5)$, $k_4 = \lfloor 5/3 \rfloor = 1$
- $(a_5, b_5) = (2, 3)$, $k_5 = \lfloor 3/2 \rfloor 1$
- $(a_6, b_6) = (1, 2) \rightsquigarrow \mathrm{ggT}(a_6, b_6) = 1 \cdot a_6 + 0 \cdot b_6 \rightsquigarrow (x_6, y_6) = (1, 0)$

$$\begin{pmatrix} -k_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_3 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_4 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_5 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_6 \\ y_6 \end{pmatrix} = \begin{pmatrix} -23 \\ 5 \end{pmatrix}$$

Damit erhält man $\mathrm{ggT}(13, 60) = -23 \cdot 13 + 5 \cdot 60 = 1$, also $13^{-1} \equiv_{60} -23 \equiv_{60} 37$.

Entschlüsseln: $46^{37} = (46^{12})^3 \cdot 46 \equiv_{77} 15^3 \cdot 46 \equiv_{77} 18 \mapsto R$.