7.Übungsblatt zur Algebra

Anne Henke, Sam Thelin, WS 2018

1. (Zum Votieren.) Bob und die krankhaft geheimnisvolle Alice haben heute Abend etwas vor. Eve, die eine unverbesserliche Tratschtante ist, will unbedingt wissen, was die beiden planen. Zu ihrem Glück ist Bob ein großer Trottel und hat in der Mensaschlange zwei zerknitterte Zettel verloren. Eve freut sich zuerst ganz arg, ist jedoch schnell sehr enttäucht: Von dem einen Zettel ist ein Teil schon abgerissen worden, und was übrig bleibt lautet:

$$5, b = 4, y = 05102304101200.$$

Der andere Zettel ist wohl unbeschädigt, aber auch auf diesem steht nur komischer Mathe-Kram:

$$p = 1080419, e = 720279, y = 87838.$$

Eve studiert Germanistik im dritten Jahr und kann damit nichts anfangen. Doch, dann erinnert sie sich an Marvin, den sie auf einer abgründig schlechten WG-Party kennengelernt hat. Er konnte zwar ums Verrecken nicht küssen, schien jedoch ein recht schlauer Typ zu sein und hat irgendetwas von Algebra und Kryptografie gelabert. Glücklicherweise war sie zu faul, seine Nummer zu löschen. Marvin geht sofort ans Telefon, und er weiß Bescheid. Sie auch? Marvin hat Zugang zu einem Taschenrechner und https://jumk.de/formeln/division-mit-rest.shtml, aber das verrät er Eve nicht, der schlaue Fuchs.

2. (Schriftlich, 9 Punkte.) Bestimmen Sie die Lösungen der folgenden Kongruenzensysteme, oder beweisen Sie, dass es keine Lösung gibt.

   (a) $x \equiv 3 \mod 7, \quad x \equiv 4 \mod 11$;

   (b) $x \equiv 13 \mod 15, \quad x \equiv 24 \mod 35$;

   (c) $5x \equiv 2 \mod 8, \quad 2x \equiv 1 \mod 11$;

   (d) $x \equiv 3 \mod 8, \quad x \equiv 17 \mod 26$.

   Begründen Sie jeweils Ihre Antwort. (*Hinweis*: Es gilt $5 \in \mathbb{Z}_8^\times$.)

3. (Zum Votieren.) Julian, Inga und Frederik wollen zusammen in den Urlaub fahren. Unglücklicherweise kann Julian nur jede 11. Woche, Inga nur jede 16. Woche, und Frederik nur jede 17. Woche frei nehmen. Julians nächster Urlaub ist in drei, Ingas in vier und Frederiks in sieben Wochen. Wann können die drei jungen Freunde das nächste Mal gemeinsam Urlaub machen? Sollten Sie dazu nach Ibiza oder nach Sylt fahren? Begründen Sie Ihre Antwort.

4. (Schriftlich, 12 Punkte.) In dieser Aufgabe bestimmen wir alle Unterringe von $\mathbb{Q}$ mit Eins. Für jede Menge Π von Primzahlen definieren wir

$$S_\Pi = \{n \in \mathbb{N} : n \text{ ist ein Produkt aus Zahlen von } \Pi\} \cup \{1\}$$

und

$$\mathbb{Z}_\Pi = \{\frac{m}{n} \in \mathbb{Q} : m \in \mathbb{Z} \text{ und } n \in S_\Pi\}.$$

   (a) Zeigen Sie, dass $\mathbb{Z}_\Pi$ für jedes Π ein Unterring von $\mathbb{Q}$ mit Eins ist.

   (b) Bestimmen Sie $\mathbb{Z}_\Pi$ falls $\Pi = \varnothing$ und falls Π die Menge aller Primzahlen ist.

   Sei R ein Unterring von $\mathbb{Q}$ mit Eins.

   (c) Sei $\frac{m}{n} \in R$ mit $\mathrm{ggT}(m, n) = 1$ und sei p ein Primteiler von n. Zeigen Sie, dass $\frac{1}{p} \in R$. (*Hinweis:* Laut Bezout's Lemma gibt es ganze Zahlen a und b mit $am + bn = 1$).

   (d) Folgern Sie, dass $\mathbb{Z}_{\{p\}} \subseteq R$.

   (e) Zeigen Sie, dass es eine eindeutige Menge Π gibt, so dass $R = \mathbb{Z}_\Pi$ ist.

5. (Zum Votieren.) Wir betrachten $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ als Gruppe bezüglich Multiplikation und definieren die folgenden zwei Untermengen von $\mathbb{C}^\times$:

$$\begin{aligned} E_n(\mathbb{C}) &:= \{z \in \mathbb{C} \colon z^n = 1\} = \{\zeta^k \colon 1 \le k \le n\}, \text{ wobei } \zeta = e^{2\pi i/n}, \text{ und} \\ E'_n(\mathbb{C}) &:= \{z \in E_n(\mathbb{C}) \colon \operatorname{ord}(z) = n\}. \end{aligned}$$

(a) Zeigen Sie, dass $E_n(\mathbb{C})$ eine Untergruppe von $\mathbb{C}^\times$ ist mit $E_n(\mathbb{C}) \simeq \mathbb{Z}_n$, und dass $|E'_n(\mathbb{C})| = \varphi(n)$ ist.

Wir definieren

$$\phi_n = \prod_{z \in E'_n(\mathbb{C})} (X - z).$$

(b) Berechnen Sie die Polynome ϕ_1, ϕ_2 und ϕ_3.

(c) Erklären Sie, warum $E_n(\mathbb{C}) = \bigcup\!\!\cdot_{d|n} E'_d(\mathbb{C})$ ist. Folgern Sie, dass $X^n - 1 = \prod_{d|n} \phi_d$ ist.

(d) Berechnen Sie das Polynom ϕ_9.

Begründen Sie jeweils Ihre Antwort.

6. (Zum Selbststudium.) Sei R ein kommutativer Ring mit Eins und sei I ein Ideal in R. Die Menge

$$\sqrt{I} := \{a \in R \colon a^n \in I \text{ für ein } n \in \mathbb{N}\} \subseteq R$$

heißt Radikal von I.

(a) Zeigen Sie, dass $\sqrt{I}$ ein Ideal von R ist.

(b) Zeigen Sie: Ist $a \in \sqrt{\{0\}}$, so ist $1 + a$ eine Einheit in R.

(c) Berechnen Sie das Ideal $\sqrt{180\mathbb{Z}}$ in $\mathbb{Z}$. Begründen Sie Ihre Antwort.