Algebra: Übungen

Prof. Dr. C. Löh/F. Hofmann Blatt 9 vom 12. Dezember 2025

Hinweis. Die Fingerübungen werden nicht abgegeben und nicht korrigiert. Sie werden teilweise in den Übungsgruppen besprochen und können zum „Aufwärmen“ beim täglichen Üben verwendet werden.

Fingerübung A (Wiederholung: Primfaktorzerlegungen)**.** Wiederholen Sie die *Eindeutigkeit von Primfaktorzerlegungen* und geben Sie einen Beweis.

Fingerübung B (letzte Ziffern)**.** Bestimmen Sie die letzte Ziffer von

1. 43^{42} im Zehnersystem;
2. 43^{42} im Zwölfersystem.

Fingerübung C (Baby-RSA)**.** Bestimmen Sie sinnvolle private und öffentliche Schlüssel für das RSA-Verfahren, wenn man mit den Primzahlen 11 und 17 beginnt.

Fingerübung D (Primbewertungen)**.** Berechnen Sie jeweils die folgenden Bewertungen zu den angegebenen Primelementen in den angegebenen Ringen:

1. $\nu_3(\frac{42}{99})$ in $Q(\mathbb{Z})$ für $3 \in \mathbb{Z}$
2. $\nu_3(\frac{99}{42})$ in $Q(\mathbb{Z})$ für $3 \in \mathbb{Z}$
3. $\nu_3(3 \cdot T^3 + \frac{1}{3} \cdot T^2 - 7 \cdot T + 99)$ in $Q(\mathbb{Z})[T]$ für $3 \in \mathbb{Z}$
4. $\nu_T(3 \cdot T^3 + \frac{1}{3} \cdot T^2 - 7 \cdot T + 99)$ in $\mathbb{Q}[T]$ für $T \in \mathbb{Q}[T]$

Hinweis. Die Wiederholungsaufgaben sind freiwillig, können aber gut zur Wiederholung und als Bonuspunkte genutzt werden.

Bonusaufgabe (Wiederholung) (Restklassenringe; 2 (=0+1+1) Punkte)**.** Begründen Sie jeweils Ihre Antwort!

0. Wiederholen Sie die Konstruktion von *Restklassenringen*.
1. Bestimmen Sie alle Ideale des Rings $\mathbb{Z}/(42)$.
2. Bestimmen Sie alle Ideale des Rings $\mathbb{Z}/(3) \times \mathbb{Z}/(14)$.

Hinweis. Achten Sie beim Aufschreiben auf präzise und verständliche Formulierungen. Der Leser soll lesen, nicht dechiffrieren.

Aufgabe 1 ((vor)letzte Ziffern; 4 (=1+3) Punkte)**.** Bestimmen Sie ...

1. die letzte Ziffer der Dezimaldarstellung von $(87^{88})^{99}$.
2. die letzten beiden Ziffern der Dezimaldarstellung von $(13^{1313})^{131313}$.

Hinweis. Die Lösungen müssen so dargestellt sein, dass sie ohne technische Hilfsmittel nachvollziehbar sind.

Bitte wenden

Aufgabe 2 (ganz kleiner Fermat; 4 (=2+2) Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort!

1. Ist $m \in \mathbb{N}_{>0}$ und $x \in \mathbb{Z}$, so gilt $x^m \equiv x \mod m$.
2. Ist $p \in \mathbb{N}$ prim und $x \in \mathbb{Z}$, so gilt $x^{p+1} \equiv x^2 \mod p$.

Aufgabe 3 (RSA; 4 (=2+2) Punkte)**.** Wir betrachten das RSA-Verfahren.

1. Bestimmen Sie einen passenden privaten Schlüssel zu dem öffentlichen Schlüssel $(4891, 8633)$. Erklären Sie Ihr Vorgehen.
2. Entschlüsseln Sie mit diesem privaten Schlüssel den folgenden mit dem öffentlichen Schlüssel $(4891, 8633)$ verschlüsselten Klassiker (Goethe!). Erklären Sie, wie Sie bei der Entschlüsselung vorgegangen sind und welche Hilfsmittel Sie wie eingesetzt haben.

   1405, 8498, 5261, 6651, 7932, 6255, 6651, 815, 6745, 7124, 4394, 334, 3844, 8498, 5038, 3826, 3757, 2624, 8357, 6188, 7195, 5587, 8059, 5057, 858, 1220, 815, 6745, 1413, 1764, 4046, 334, 8498, 5038, 3826, 7031, 334, 7091, 2876, 5386, 656, 6651, 1076, 4201, 5718, 1912, 3826, 759, 538, 6741, 7251, 5447, 8222, 5454, 6255, 1, 5261, 770, 1836, 3848, 8357, 6188, 2876, 5129, 4874, 2876, 5386, 7836, 4228, 1076, 6741, 846, 5647, 8498, 5038, 3826, 926, 6315, 492, 8357, 6188, 1, 7091, 6680, 4257, 198, 6651, 4394, 307, 7243, 7512, 5038, 6080, 8357, 6188, 4682, 6632, 6745, 6770, 6680, 334, 3844, 8357, 6188, 7195, 815, 6745, 6770, 6680, 1169, 6071, 4394, 2775, 4394, 6770, 6680, 2775, 4394, 7573, 8494, 4689, 6071, 1814, 4034, 6071, 4394

   Hinweis. Das Leerzeichen wird durch 0 repräsentiert, die Buchstaben A, ..., Z des Alphabets durch $1, \ldots, 26$. Die Zahlen x, y zu zwei aufeinanderfolgenden Buchstaben werden zu $[100 \cdot x + y] \in \mathbb{Z}/(8633)$ zusammengefasst. Dies wurde dann mit RSA verschlüsselt.

Aufgabe 4 (Primpolynome; 4 Punkte)**.** Sei R ein faktorieller Ring. Zeigen Sie, dass der Polynomring $R[T]$ unendlich viele Primelemente enthält.
Hinweis. Was würde Euklid tun?

Bonusaufgabe (Kauderwelsch; 4 Punkte)**.** Entschlüsseln Sie folgenden deutschen Text. Erklären Sie Ihr Vorgehen. Skizzieren Sie insbesondere, in welcher Reihenfolge Sie welche Dinge entschlüsseln/erkennen konnten.

> YUJECWCOFCNGHNWAOLCO AOV DOIHBWC. VDC XKIACBCNDOOCO AOV XKIACBCN ... RHYWUNDXDCNCO OHWACNBDKIC FHIBCO AOV CNJDWWCBO VCNCO ENDJRHYWUNFCNBCLAOL, GUTCD XDC XDKI VCN CDOVCAWDLYCDW VDCXCN FCNBCLAOL TCGAXXW XDOV; TCDJ RHYWUNDXDCNCO GCOVCO XDC HAKI NCLCBO RACN VDC WCDBTHNYCDW VANKI FGCD, VNCD, RACOR AOV FCIO FDCBLCNDKIWCW HO. XDC OAWFCO VDCXC YCOOWODXXC HAKI RACN HNLAJCOWHWDUOCO, FAJ TCDXEDCB DJ NHIJCO VCN TCHOWGUNWAOL HBBWHLXOHICN RNHLCXWCBBAOLCO.

Hinweis. Jedes Zeichen steht dabei immer für denselben Buchstaben. Satzzeichen bleiben unverschlüsselt. Welche Buchstaben sind im Deutschen am häufigsten? Zusatzfrage: Woher stammt dieser Text?

Abgabe bis 19. Dezember 2025, 8:25, via Briefkasten/GRIPS