Übungen zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig Blatt 9 vom 15. Dezember 2017

Aufgabe 1 (Fermat?!)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie Ihre Antwort (durch einen Beweis oder ein geeignetes Gegenbeispiel)!

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

Aufgabe 2 (Primpolynome)**.** Sei R ein faktorieller Ring. Zeigen Sie, dass der Polynomring $R[T]$ unendlich viele Primelemente enthält.
Hinweis. Was würde Euklid tun?!

Aufgabe 3 (RSA)**.**

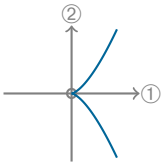
1. Bestimmen Sie einen passenden privaten Schlüssel zu dem öffentlichen Schlüssel $(6661, 8051)$.
2. Entschlüsseln Sie mit diesem privaten Schlüssel den folgenden mit dem öffentlichen Schlüssel $(6661, 8051)$ verschlüsselten Klassiker (Goethe!):

   937, 2978, 87, 4201, 4969, 1713, 4201, 7677, 2356, 6087, 2948, 3371, 449, 2978, 3207, 2789, 5702, 201, 1569, 7241, 4380, 4642, 4741, 6636, 1535, 7118, 7677, 2356, 4395, 900, 7902, 3371, 2978, 3207, 2789, 2974, 3371, 7058, 7061, 854, 3211, 4201, 4264, 7136, 672, 6350, 2789, 3574, 7757, 2788, 2177, 308, 4957, 3179, 1713, 1, 87, 2431, 6009, 3578, 1569, 7241, 7061, 6216, 3352, 7061, 854, 3369, 6292, 4264, 2788, 6093, 6040, 2978, 3207, 2789, 1743, 7252, 878, 1569, 7241, 1, 7058, 2773, 356, 4356, 4201, 2948, 4252, 959, 2595, 3207, 7180, 1569, 7241, 5938, 2170, 2356, 1518, 2773, 3371, 449, 1569, 7241, 4380, 7677, 2356, 1518, 2773, 977, 84, 2948, 6761, 2948, 1518, 2773, 6761, 2948, 6310, 4007, 5288, 84, 4715, 472, 84, 2948

   Hinweis. Das Leerzeichen wird durch 0 repräsentiert, die Buchstaben A, ..., Z des Alphabets durch $1, \dots, 26$. Die Zahlen x, y zu zwei aufeinanderfolgenden Buchstaben werden zu $[100 \cdot x + y] \in \mathbb{Z}/(8051)$ zusammengefasst. Dies wurde dann mit RSA verschlüsselt.

Aufgabe 4 (noch eine Kurve)**.** Sei K ein Körper. Sei $R := K[X, Y]/(Y^2 - X^3)$ der Ring zur Gleichung „$y^2 = x^3$“. Wir schreiben $x, y \in R$ für die von X bzw. Y repräsentierten Restklassen. Bearbeiten Sie zwei der folgenden vier Aufgaben:

1. Zeigen Sie, dass $Y^2 - X^3$ in $K[X, Y]$ prim ist und folgern Sie, dass R ein Integritätsring ist.
2. Zeigen Sie $x, y, x^3, y^2 \notin \{0\} \cup R^\times$.
   Hinweis. Wie kommen Sie via „$X \mapsto T^2$, $Y \mapsto T^3$“ von R nach $R[T]$?
3. Zeigen Sie, dass x und y in R irreduzibel sind, indem Sie passende Gleichungen in $K[X, Y]$ betrachten.
4. Folgern Sie, dass R *nicht* faktoriell ist und insbesondere $R \ncong K[X]$ gilt.



Bitte wenden

Bonusaufgabe (Kauderwelsch)**.** Entschlüsseln Sie folgenden deutschen Text:

> WMJXQNQRHQYDVYNZRPQR ZRC URAVBNQ. CUQ
> IFAZQBQYURRQR ZRC IFAZQBQY ... KVWNMYUIUQYQR
> RVNZQYBUFAQ HVABQR ZRC QYJUNNQBR CQYQR
> XYUJKVWNMYHQYBQPZRP, DMLQU IUQ IUFA CQY
> QURCQZNUPWQUN CUQIQY HQYBQPZRP LQDZIIN IURC; LQUJ
> KVWNMYUIUQYQR DQRCQR IUQ VZFA YQPQBR KZQY CUQ
> NQUBLVYWQUN CZYFA HDQU, CYQU, KZQRK ZRC HQAR
> HUQBPQYUFANQN VR. IUQ RZNHQR CUQIQ WQRRNRUIIQ VZFA
> KZQY VYPZJQRNVNUMRQR, HZJ LQUIXUQB UJ YVAJQR CQY
> LQVRNDMYNZRP VBBNVPIRVAQY KYVPQINQBBZRPQR.

Hinweis. Jedes Zeichen steht dabei immer für denselben Buchstaben. Satzzeichen bleiben unverschlüsselt. Welche Buchstaben sind im Deutschen am häufigsten?

Abgabe bis zum 22. Dezember 2017, 10:00 Uhr, in die Briefkästen