

ÜBUNGSAUFGABEN ZUR ALGEBRA (BACHELOR)

Blatt 6

Abgabe am 28. November 2016 bis 10:15 Uhr

21. Als RSA-verschlüsselte Nachricht wird Ihnen die Zahl

6277666

übermittelt. Ihr öffentlicher Schlüssel besteht aus dem Produkt $N = 13942867$ der beiden Primzahlen 4591 und 3037, sowie der Zahl $e = 3389653$. Ihr privater Schlüssel ist $\varphi(N)$. Entschlüsseln Sie die Nachricht.

In der entschlüsselten Zahl stehen je zwei Ziffern für einen Buchstaben mit der Korrespondenz $A \mapsto 01, B \mapsto 02, \dots, Z \mapsto 26$. Wie lautet das gesuchte Wort? (Sie dürfen natürlich mit Computer oder Taschenrechner arbeiten, die Rechenschritte müssen aber nachvollziehbar sein.)

22. Betrachten Sie das Ideal $I = \langle x^2 + 1 \rangle$ im Polynomring $\mathbb{R}[x]$.
- (a) Beweisen Sie, dass jedes Element im Faktoring $\mathbb{R}[x]/I$ die Form $a + bx + I$ hat, für $a, b \in \mathbb{R}$.
- (b) Verwenden Sie den Isomorphiesatz, um $\mathbb{R}[x]/I \cong \mathbb{C}$ zu zeigen.
23. Es sei K ein Körper und seien $f, g \in K[x]$ teilerfremde Polynome mit $f, g \notin K$. Zeigen Sie, dass dann

$$f - g \cdot y \in K(y)[x]$$

irreduzibel im Polynomring $K(y)[x]$ ist.

24. Zeigen Sie, dass das Ideal $\langle x^2 + 1 \rangle$ im Ring $\mathbb{Z}[x]$ ein Primideal ist, jedoch kein maximales Ideal.