

Algebra und Diskrete Mathematik, PS3

Sommersemester 2018

10. und 11. April 2018

- 1) Was ist eine *Primzahl*? Was besagt der Satz über die Zerlegung von positiven natürlichen Zahlen in *Primfaktoren*? Es seien u, v von Null verschiedene ganze Zahlen, deren größter gemeinsamer Teiler 1 ist.
Zeigen Sie: Die Bruchzahl $\frac{u}{v}$ kann genau dann exakt durch endlich viele Dezimalziffern dargestellt werden, wenn unter den Primfaktoren von v nur die Zahlen 2 und 5 auftreten. Formulieren und beweisen Sie eine analoge Aussage für Ziffern zur Basis $b \geq 2$.

- 2) Wie ist der Ring \mathbb{Z}_n (für $n \geq 2$) definiert? Welche Elemente von \mathbb{Z}_n sind invertierbar? Wie berechnet man das zu einem invertierbaren Element von \mathbb{Z}_n inverse Element?
Es seien $k = 789$ bzw. 3154 und $n = 3567$.
Überprüfen Sie, ob \bar{k} in \mathbb{Z}_n invertierbar ist. Wenn ja, berechnen Sie das zu \bar{k} inverse Element in \mathbb{Z}_n .
Berechnen Sie für alle Elemente $x \in \mathbb{Z}_5$ die dazu inversen Elemente x^{-1} und schreiben Sie x^{-1} als Potenz von x an.

- 3) Mit der „Neunerprobe“ hat man früher die Richtigkeit von Additionen (bis auf Vielfache von 9) überprüft, indem man die Reste nach Division durch 9 der Summe der Ziffern aller Summanden und der Ziffernsumme des Ergebnisses berechnet hat. Waren diese zwei Reste gleich, war die Rechnung bis auf Vielfache von 9 richtig.
Begründen Sie dieses Verfahren mithilfe des Ringes \mathbb{Z}_9 .
Wie kann es auf die Multiplikation übertragen werden?
Wodurch muß die „Neuner-Probe“ ersetzt werden, wenn man mit Zahlen rechnet, die durch Ziffern zur Basis $b \geq 2$ dargestellt werden?

- 4) Wie kann man Reste modulo n von Potenzen ganzer Zahlen mit wenig Rechenaufwand berechnen?

Berechnen Sie den Rest von

$$(117 \cdot 53^2 - 31^3 \cdot 15^3 \cdot 25^6) \cdot 155$$

nach Division durch 13.

Berechnen Sie den Rest von 7^{10123} nach Division durch 11, den Rest von 11^{1001} nach Division durch 8 und den Rest von 232^{100000} nach Division durch 13.

- 5) Versuchen Sie, mit Maple (oder analog mit einem anderen CAS) den Rest von $12^{1000000000}$ nach Division durch 43 auf zwei Arten zu berechnen: einmal mit

`irem(12^1000000000, 43);` oder $12^{1000000000} \bmod 43;$

und einmal mit

$$12 \&^{\wedge} 1000000000 \bmod 43;$$

Erläutern Sie den Unterschied.

- 6) Erläutern Sie das *RSA-Verfahren*.

Aus: Schneider, G. et al.: Mathematik III HAK. Trauner Verlag, Linz 2008. 2. Auflage 2007, Nachdruck 2008.

Aufgabe 4. 20: Der Börsen-Hai Mackie Messer übermittelt seinem Freund Brown den Geheimtext

11 21 02 39 39 25 15 14 13 25 .

Der öffentliche RSA Schlüssel ist $(55, 23)$. Knacken Sie den Kode, indem Sie den privaten Schlüssel $(55, d)$ ermitteln. Was will Mackie seinem Freund mitteilen?