

# Algebra und Diskrete Mathematik, PS3

Sommersemester 2017

27. März 2017

- 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  $k = 651$  bzw.  $2051$  und  $n = 3324$ .  
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  $x \in \mathbb{Z}_8$  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

$$(113 \cdot 62^2 - 21^3 \cdot 17^3 \cdot 5^6) \cdot 155$$

nach Division durch 9.

Berechnen Sie den Rest von  $5^{10000}$  nach Division mit Rest durch 11, den Rest von  $11^{1000}$  nach Division mit Rest durch 13 und den Rest von  $233^{100000}$  nach Division durch 9.

- 5) Aus: Pauer, F., Scheirer-Weindorfer, M., Simon, A.: Mathematik 3 HAK. öbv Wien 2013, 2. Auflage.

Die IBAN bei einer österreichischen Bank besteht immer aus genau 20 Stellen. Die ersten zwei Stellen sind mit den Buchstaben AT belegt, die nächsten zwei sind Prüfziffern, dann fünf Stellen für die Bankleitzahl und schließlich 11 Stellen für die Kontonummer. Wenn die Kontonummer weniger als 11 Ziffern hat, dann werden entsprechend viele Nullen vor die Kontonummer geschrieben. Das gleiche gilt für die Bankleitzahl.

Die Prüfziffern  $xy$  einer IBAN werden so berechnet: Man verschiebt die ersten vier Zeichen  $ATxy$  an das Ende der Zahl und ersetzt AT durch 1029 und  $xy$  durch 00. Wir nennen die so entstandene Zahl  $z$ . Die Zahl  $xy$  ist dann  $98 - (z \bmod 97)$ . Zahlen, die kleiner als 10 sind, werden dabei auch durch 2 Ziffern dargestellt, die erste ist 0.

*Aufgabe 901: Berechne die IBAN für die Kontonummer 555 555 555 bei der österreichischen Bank mit der Bankleitzahl 23456.*

- 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?*