Algebra und Diskrete Mathematik, PS3

Sommersemester 2019

1., 2. und 3. April 2019

1) Wie kann man Reste modulo n von Potenzen ganzer Zahlen mit wenig Rechenaufwand berechnen?
Berechnen Sie den Rest von

$$(207 \cdot 45^2 - 22^5 \cdot 23^3 \cdot 67^6) \cdot 199$$

nach Division mit Rest durch 17.
Berechnen Sie den Rest von 6^{12345} nach Division mit Rest durch 11, den Rest von 8^{789} nach Division mit Rest durch 14 und den Rest von 357^{100000} nach Divison durch 17.

2) 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.

3) 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?*

4) Was ist eine *Polynomfunktion*? Was heißt *eine Polynomfunktion in einem Element des Definitionsbereichs auswerten*? Werten Sie die Polynomfunktion

$$f : \mathbb{R} \longrightarrow \mathbb{R},\ z \longmapsto 3 - 5z + 4z^4 - z^4 + 11z^5$$

in $\frac{2}{3}$ aus.
Werten Sie die Polynomfunktion

$$g : \mathbb{Z}_7 \longrightarrow \mathbb{Z}_7,\ z \longmapsto \bar{3} + \bar{4}z + z^6 + z^{2019}$$

in $\bar{4}$ aus. Wieviele Multiplikationen sind dazu jeweils mindestens nötig?

5) Wann sind zwei Funktionen *gleich*? Überprüfen Sie, ob $f = g$, $f = h$ und $h = g$ ist.

$$f : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3,\ z \longmapsto \bar{1} + z + \bar{2}z^2 - z^4$$
$$g : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3,\ t \longmapsto \bar{1} + t^2 + t^3$$
$$h : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3,\ x \longmapsto \bar{2}(x - \bar{1}) + (x - \bar{1})^2 + (x - \bar{1})^3$$

Zeigen Sie, dass zwei Polynomfunktionen von $\mathbb{Z}_3$ nach $\mathbb{Z}_3$ mit den Koeffizienten a_0, a_1, a_2 und b_0, b_1, b_2 genau dann gleich sind, wenn $(a_0, a_1, a_2) = (b_0, b_1, b_2)$ ist. Wieviele solche Polynomfunktionen gibt es? Wieviele Funktionen von $\mathbb{Z}_3$ nach $\mathbb{Z}_3$ gibt es? Zeigen Sie, dass jede Funktion von $\mathbb{Z}_3$ nach $\mathbb{Z}_3$ eine Polynomfunktion ist.

6) Was ist ein *Modul* über einem Ring R, was ist eine *Basis* eines Moduls und was ist ein *freier Modul*?

Es sei M der von $(3, 0), (1, 2)$ und $(0, 3)$ erzeugte Untermodul von $\mathbb{Z}^2$. Überprüfen Sie, ob $((3, 0), (0, 3))$ eine $\mathbb{Z}$-Basis von M ist. Zeigen Sie, dass M ein freier $\mathbb{Z}$-Modul ist und geben Sie eine Basis davon an. Überprüfen Sie, ob $(8, -2) \in M$ und ob $(-8, -7) \in M$ ist.

Betrachten Sie $\mathbb{Z}_4 \times \mathbb{Z}_4$ einmal als Modul über $\mathbb{Z}$ und einmal als Modul über $\mathbb{Z}_4$. Bestimmen Sie für beide Fälle vier Untermoduln. Ist einer dieser zwei Moduln frei? Geben Sie in diesem Fall drei Basen an.