Albert–Ludwigs–Universität Freiburg
Institut für Mathematik
Abteilung für Reine Mathematik
PD Dr. K. Halupczok
Dipl.–Math. S. Feiler

Übungen zur Vorlesung

Elementare Zahlentheorie

Sommersemester 2009

5. Übungsblatt

18. Mai 2009

Abgabe der Lösungen bis zum **25. Mai 2009 um 14.$\underline{15}$ Uhr**

Aufgabe 17 (g–adische Darstellung reeller Zahlen) 5 Punkte

Seien $g \in \mathbb{N} \setminus \{1\}$ und $t \in \mathbb{R}$ mit $t \geq 1$.

Zeigen Sie, dass es eine eindeutige Folge $a : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{N}_0 \\ j & \mapsto & a_j \end{array} \right\}$ gibt, so dass $a_j \leq g-1$ für alle $j \in \mathbb{Z}$ und $t = \sum\limits_{j \in \mathbb{Z}} a_j \cdot g^j$ sind, sowie $a_n \neq 0$ nur für endlich viele $n \in \mathbb{N}_0$ und $a_{-n} \neq g-1$ für unendlich viele $n \in \mathbb{N}_0$ gelten.

(Tipp: Definiert man $\beta_1 := t - \lfloor t \rfloor$ und $\beta_{n+1} := g\beta_n - \lfloor g\beta_n \rfloor$ für alle $n \in \mathbb{N}$, so gilt $a_{-n} = \lfloor g\beta_n \rfloor$ für alle $n \in \mathbb{N}$.)

Aufgabe 18 (RSA–Verfahren)

Seien $\mathcal{K} := \{ n \in \mathbb{N}_0 \, ; n < 31 \}$ und $\mathcal{V} := \{ n \in \mathbb{N}_0 \, ; n < 32 \}$.

Nach der folgenden Tabelle sollen nun die Buchstaben des Alphabets, das Leerzeichen und der Punkt den Zahlen aus $\mathcal{V}$ zugeordnet werden.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü	ß	␣	.

Seien $N := 32399$ und $t := 1463$.

a) Verschlüsseln Sie den Klartext „SEI␣EPSILON␣“ wie im Skript im Beispiel zum RSA–Verfahren beschrieben!

b) Geben Sie die Primfaktorzerlegung von N an und finden Sie ein $s \in \mathbb{N}$ mit

$$st \equiv 1 \bmod \varphi(N) .$$

c) Entschlüsseln Sie den wie im Skript im Beispiel zum RSA–Verfahren beschrieben verschlüsselten Text „GF.SPCAAXÖOM“!

(Bemerkung: Sie dürfen einen PC zur Hilfe nehmen, um die Ver– $(v(k) \equiv k^t \bmod N)$ und Entschlüsselung $(k \equiv (v(k))^s \bmod N)$ durchzuführen.
Beachten Sie auch die Tabelle im Anhang an das Übungsblatt.)

bitte wenden

Aufgabe 19 (Teilbarkeit durch 7) 3 Punkte

a) Zeigen Sie, dass eine Zahl $n \in \mathbb{N}$, deren letzte Stelle im Dezimalsystem gerade r sei, genau dann durch 7 teilbar ist, wenn $\left\lfloor \frac{n}{10} \right\rfloor - 2r$ durch 7 teilbar ist!

b) Eine im Dezimalsystem gegebene Zahl $n \in \mathbb{N}$ werde an ihrer vorletzten Stelle getrennt. Es entstehen eine Zahl $a \in \mathbb{N}$, die zwei Stellen weniger als n hat und eine zweistellige Zahl $b \in \mathbb{N}$, die aus den letzten beiden Ziffern von n besteht.

Zeigen Sie $\quad 7|n \quad \Longleftrightarrow \quad 7|\,(2a+b) \quad$!

c) Stellen Sie für alle $n \in \mathbb{N}$ eine Teilbarkeitsregel durch alle $m \in \mathbb{N}$ mit $|10^n - m| = 1$ für im Dezimalsystem gegebene Zahlen auf!

Leiten Sie daraus eine Teilbarkeitsregel durch 7 für im Dezimalsystem gegebene Zahlen her!

Aufgabe 20 (Schnelles Potenzieren)

a) Geben Sie den kleinsten nichtnegativen Rest von 2^{917} modulo 111 an!

b) Der HALLEYsche Komet war am 16.11.1835, am 20.04.1910 und am 09.02.1986 zuletzt am Himmel zu sehen. Sein nächstes Auftauchen wird für den 28.07.2061 vorausgesagt.

Mark TWAIN wurde am 30.11.1835 zwei Wochen nach dem Auftauchen des Kometen geboren und wird zitiert mit: *I came in with* HALLEY*'s comet in 1835. It's coming again next year, and I expect to go out with it. It will be the greatest disappointment of my life if I don't go out with* HALLEY*'s Comet. The Almighty has said no doubt: "Now here are these two unaccountable freaks; they came in together, they must go out together."* (1909) Mark TWAIN starb am 21.04.1910.

Zeigen Sie, dass $1835^{1910} + 1986^{2061}$ durch 7 teilbar ist!

c) Zeigen Sie $1312|\,(3^{1024} - 1) \quad$!

Geben Sie sämtliche Rechenschritte an und verwenden Sie keine elektronischen Hilfsmittel!

$x \cdot 31^0$															
0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7
8	8	9	9	10	10	11	11	12	12	13	13	14	14	15	15
16	16	17	17	18	18	19	19	20	20	21	21	22	22	23	23
24	24	25	25	26	26	27	27	28	28	29	29	30	30		

$x \cdot 31^1$															
0	0	1	31	2	62	3	93	4	124	5	155	6	186	7	217
8	248	9	279	10	310	11	341	12	372	13	403	14	434	15	465
16	496	17	527	18	558	19	589	20	620	21	651	22	682	23	713
24	744	25	775	26	806	27	837	28	868	29	899	30	930		

$x \cdot 31^2$															
0	0	1	961	2	1922	3	2883	4	3844	5	4805	6	5766	7	6727
8	7688	9	8649	10	9610	11	10571	12	11532	13	12493	14	13454	15	14415
16	15376	17	16337	18	17298	19	18259	20	19220	21	20181	22	21142	23	22103
24	23064	25	24025	26	24986	27	25947	28	26908	29	27869	30	28830		

$x \cdot 32^0$															
0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7
8	8	9	9	10	10	11	11	12	12	13	13	14	14	15	15
16	16	17	17	18	18	19	19	20	20	21	21	22	22	23	23
24	24	25	25	26	26	27	27	28	28	29	29	30	30	31	31

$x \cdot 32^1$															
0	0	1	32	2	64	3	96	4	128	5	160	6	192	7	224
8	256	9	288	10	320	11	352	12	384	13	416	14	448	15	480
16	512	17	544	18	576	19	608	20	640	21	672	22	704	23	736
24	768	25	800	26	832	27	864	28	896	29	928	30	960	31	992

$x \cdot 32^2$															
0	0	1	1024	2	2048	3	3072	4	4096	5	5120	6	6144	7	7168
8	8192	9	9216	10	10240	11	11264	12	12288	13	13312	14	14336	15	15360
16	16384	17	17408	18	18432	19	19456	20	20480	21	21504	22	22528	23	23552
24	24576	25	25600	26	26624	27	27648	28	28672	29	29696	30	30720	31	31744

Es sind $16^2 = 256$, $17^2 = 289$ und $23^2 = 529$.