ELEMENTARE ZAHLENTHEORIE
2. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

(a) Finden Sie alle Primzahlen $p < 200$ mit Hilfe des Siebes des Eratosthenes. Eine Vorlage finden Sie auf der letzten Seite. Hinweis: $\sqrt{200} < 15$.

(b) Wir wollen ziegen, dass es unendlich viele Primzahlen der Form $6k - 1$ gibt.

  (i) Zeigen Sie zuerst, dass jede Primzahl $p \neq 2, 3$ der Form $6k \pm 1$ hat.

  (ii) Sei $\{p_1, \dots p_n\}$ eine Liste von Primzahlen der Form $6k - 1$ und setzen Sie $N \coloneqq 6(p_1 \cdots p_n) - 1$. Begründen Sie warum N eine Primzahlteiler q der Form $6k - 1$ hat (Hinweis: wenn nicht, dann habe alle der Form $6k + 1$), und dass $q \neq p_i$ für $1 \leq i \leq n$. Schließen Sie daraus, dass es unendlich viele solche Primzahlen geben muss.

(2+1+2 Punkte)

Aufgabe 2.

Für eine natürliche Zahl x und eine Primzahl p definieren wir

$$v_p(x) \coloneqq \max\{a \geq 0 \mid p^a \text{ teilt } x\}.$$

Es folgt nun zum Beispiel, dass $v_p(xy) = v_p(x) + v_p(y)$, und $d = \mathrm{ggT}(x, y)$ genau dann, wenn $v_p(d) = \min\{v_p(x), v_p(y)\}$ für alle p.

(a) Beweisen Sie mit Hilfe den Funktionen v_p, dass $\mathrm{ggT}(x, y, z) = \mathrm{ggT}(\mathrm{ggT}(x, y), z)$.

(b) Zeigen Sie mit Hilfe der Funktion v_2, dass $\sqrt{2} \notin \mathbb{Q}$.

(c) Benutzen Sie die Funktionen v_p um zu bestätigen, dass

$$\mathrm{kgV}(\mathrm{ggT}(x, y), z) = \mathrm{ggT}(\mathrm{kgV}(x, z), \mathrm{kgV}(y, z)).$$

Folgern Sie, dass $(I + J) \cap K = (I \cap K) + (J \cap K)$ für Ideale $I, J, K \trianglelefteq \mathbb{Z}$.

(1+2+3 Punkte)

Aufgabe 3.

(a) Sei k ein Körper. Wir wollen zeigen, dass der Polynomring $k[x]$ ein Hauptidealring ist. Für $0 \neq f \in k[x]$ definieren wir $\deg(f) = n$, falls $f = a_n x^n + \cdots + a_1 x + a_0$ mit $a_i \in k$ und $a_n \neq 0$. Wir setzen $\deg(0) \coloneqq -\infty$.

  (i) Zeigen Sie, dass $\deg(fg) = \deg(f) + \deg(g)$ und schließen Sie daraus, dass $k[x]$ nullteilerfrei ist.

  (ii) [Divisionsalgorithmus] Gegeben seien $f, g \in k[x]$ mit $f \neq 0$. Zeigen Sie, dass wir $g = qf + r$ mit $q, r \in k[x]$ und $\deg(r) < \deg(f)$ schreiben kann.

  (iii) [Hauptidealring] Sei $0 \neq I \trianglelefteq k[x]$ ein Ideal, und $0 \neq f \in I$ mit $\deg(f)$ minimal. Beweisen Sie, dass $I = (f)$ ein Hauptideal ist.

(1+2+2 Punkte)

Abgabe: Montag 29. April, bis 12 Uhr in die Postfächer der Tutoren im V3–126 (b)* Sei nun $R = \mathbb{Z}[i] \coloneqq \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$. Wir wollen zeigen, dass R ein Hauptidealring ist. Für $x = a + bi \in R$ definieren wir $\bar{x} \coloneqq a - bi$ und $N(x) \coloneqq x\bar{x} = a^2 + b^2$.

(i) Zeigen Sie, dass $N(xy) = N(x)N(y)$ und schließen Sie daraus, dass R nullteilerfrei ist.

(ii) [Division mit Rest] Gegeben seien $x, y \in R$ mit $x \neq 0$. Zeigen Sie, dass wir $y = qx + r$ mit $q, r \in R$ und $N(r) < \frac{1}{2}N(x)$ schreiben kann.

Hinweis: Setzen Sie $N \coloneqq N(x)$ und betrachten Sie $y\bar{x} = u + vi$. Zeigen Sie, dass es $m, n \in \mathbb{Z}$ mit $\frac{1}{2}N < u - Nm \leq \frac{1}{2}N$ und $\frac{1}{2}N < v - Nn \leq \frac{1}{2}N$. Definieren Sie nun $q \coloneqq m + ni$.

(iii) [Hauptidealring] Sei $0 \neq I \trianglelefteq R$ ein Ideal, und $0 \neq x \in I$ mit $N(x)$ minimal. Beweisen Sie, dass $I = (x)$ ein Hauptideal ist.

(nur zum Spaß)

Ein Ring in dem wir einen solchen Divisionalgorithmus durchführen kann, heißt ein euklidischer Ring. Also sind $\mathbb{Z}$, $k[x]$ für ein Körper k, und $\mathbb{Z}[i]$ euklidische Ringe. Es folgt wie hier und in der Vorlesung, dass jeder euklidischer Ring ein Hauptidealring ist. Es gibt aber Hauptidealringe, die nicht euklidisch sind, für die es also keinen solchen Divisionalgorithmus gibt.

Aufgabe 4.

Zu Erinnerung: Um die Lösungsmenge $L = \{(x, y) \mid ax + by = n\}$ zu finden machen wir Folgendes.

- Euklid : $d = \mathrm{ggT}(a, b) = as + bt$.
- d muss n teilen. Eine Lösung ist dann $(x_0, y_0) = (ns/d, nt/d)$.
- Andere Lösung (x, y). Dann gilt $a(x - x_0) = b(y_0 - y) \in (a\mathbb{Z}) \cap (b\mathbb{Z}) = \mathrm{kgV}(a, b)\mathbb{Z} = (ab/d)\mathbb{Z}$. Also $a(x - x_0) = b(y_0 - y) = abt/d$ für eine $t \in \mathbb{Z}$.
- $L = \{(x_0, y_0) + (bt/d, -at/d) \mid t \in \mathbb{Z}\}$.

Finden Sie die Lösungsmengen für die Gleichenungen und in beiden Fällen finden Sie die Lösung mit $|x|$ minimal.

(a) $62x + 105y = 651$.

(b) $12x - 501y = 33$.

(je 2 Punkte)

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200