Musterlösung zur Serie 3
Algebra und Zahlentheorie und ihre Didaktik

Dr. Daniel Skodlerack

15. Mai 2017

Aufgabe 1 (5+5 Punkte)**.** (Mersennesche Primzahlen) Gegeben sei eine natürliche Zahl n.

1. Beweisen Sie, dass n eine Primzahl sein muss, wenn $2^n - 1$ eine Primzahl ist.
2. Ist für jede Primzahl p die Zahl $2^p - 1$ eine Primzahl? Beweisen Sie ihre Antwort.

Eine Primzahl der Form $2^n - 1$ heißt Mersennesche Primzahl.

Lösung: Vorbemerkung: Für alle ganzen Zahlen a und b und alle natürlichen Zahlen n gilt:

$$a^n - b^n = (a-b)(\sum_{i=0}^{n-1} a^i b^{n-1-i}).$$

Beweis: (durch vollständige Induktion über n)
$n = 1$: Die Aussage folgt aus $a^0 b^0 = 1$.
$n > 1$: Aus der Induktionsvoraussetzung folgt:

$$a^{n-1} - b^{n-1} = (a-b)(\sum_{i=0}^{n-2} a^i b^{n-2-i}). \tag{1}$$

Des Weiteren gilt

$$a^n - b^n = a(a^{n-1} - b^{n-1}) + (a-b)b^{n-1} \tag{2}$$

Wir setzen die Gleichung (1) in Gleichung (2) ein. und erhalten

$$\begin{aligned} a^n - b^n &= a((a-b)(\sum_{i=0}^{n-2} a^i b^{n-2-i}) + (a-b)b^{n-1} \\ &= (a-b)((\sum_{i=0}^{n-2} a^{i+1} b^{n-2-i}) + b^{n-1}) \\ &= (a-b)((\sum_{i=1}^{n-1} a^i b^{n-1-i}) + b^{n-1}). \end{aligned}$$

Damit ist der Beweis der Induktionsbehauptung erbracht. Und damit ist die Vorbemerkung bewiesen. q.e.d.

1. Beweis: Angenommen n ist keine Primzahl, also $n = mt$ mit natürlichen Zahlen m und t größer 1. Dann gilt

   $$2^n - 1 = (2^t)^m - 1 = (2^t - 1)(\sum_{i=0}^{m-1} (2^t)^i),$$

   laut der Vorbermerkung. Die beiden Faktoren auf der rechten Seite sind beide größer 1. Damit erhalten wir einen Widerspruch dazu, dass $2^n - 1$ eine Primzahl sein soll. q.e.d.

2. Die Antwort auf die Frage ist Nein, da $2047 = 2^{11} - 1 = 23 * 89$ keine Primzahl ist, denn sie hat mehr als 2 Teiler in $\mathbb{N}$.

Aufgabe 2 (4+6+5* Punkte)**.** (ggT, kgV und Bézout)

1. Bestimmen Sie Bézout-Koeffizienten für $(2415, 3910, 4186)$, d.h. finden Sie ganze Zahlen a, b, c so dass $a2415 + b3910 + c4186 = \text{ggT}(2415, 3910, 4186)$ gilt. Hinweis: Führen Sie den erweiterten euklidischen Algorithmus zweimal durch.

2. Finden Sie den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache für die folgenden Paare: $(2541^{1001}, 1001^{2541}), (2^{16} - 1, 3^{16} - 2^{16})$ und $(7^{180} + 1, 7^{120} - 1)$.

3. Es seien zwei ganze Zahlen a und b Bézout-Koeffizienten für $2^{93} + 1352$ und $3^{27} + 11$. Gibt es eine ganzzahlige Lösung der Gleichung $aX + bY = 109$? Beweisen Sie ihre Antwort.

Lösung:

1. Eine Lösungstrategie ist die, den erweiterten euklidischen Algorithmus zuerst für $(2415, 3910)$ und dann für $(\text{ggT}(2415, 3910) = 115, 4186)$ durchzuführen und dann die erste Gleichung in die zweite einzusetzen. Man erhält dabei $13 * 2415 - 8 * 3910 = 115,\ 73 * 115 - 2 * 4186 = 23$ und dann die Bézout-Koeffizienten $(949, -584, -2)$.

   Hier ist eine zweite Strategie: Durch Hinsehen kann man sich hier das Leben vereinfachen. Wir setzen $t := \text{ggT}(2415, 3910, 4186)$. Es gelten $4186 - 3910 = 276$, $9 * 276 = 2484$ und $2484 - 2415 = 69 = 3 * 23$. Wir haben also

   $$9 * 4186 - 9 * 3910 - 2415 = 69. \tag{3}$$

   Damit ist t ein Teiler von 69, und damit teilt t 23, da 3 kein Teiler von 3910 ist, denn 3 teilt nicht 10. Durch Nachrechnen erhält man $2415 = 23 * 105,\ 3910 = 23 * 170$ und $4186 = 23 * 182$. Also ist $t = 23$. 3910 ist nicht durch 3 teilbar, also gilt $\text{ggT}(69, 3910) = 23$. Wir bestimmen jetzt Bézout-Koeffizienten für $(69, 3910)$ und setzen dann Gleichung (3) ein.

   $$3910 = 56 * 69 + 46,\ 69 = 1 * 46 + 23.$$

   Also erhalten wir mit dem erweiterten euklidischen Algorithmus die Bézout-Koeffizienten: -1 und $1 - (-1) * 56 = 57$, also

   $$\begin{aligned} 23 &= (-1) * 3910 + 57 * 69 \\ &= (-1) * 3910 + 57 * (9 * 4186 - 9 * 3910 - 2415) \\ &= (-57) * 2415 + (-514) * 3910 + 513 * 4186. \end{aligned}$$

   Probe: $57 * 2415 = 120750 + 16905 = 137655$, $514 * 3910 = 10 * (514 * 391) = 10 * (154200 + 46260 + 514) = 10 * (200974) = 2009740$, $513 * 4186 = 2093000 + 41860 + 12558 = 2147418$. Weiter: $2147418 - 2009740 - 137655 = 0000023$. Also sind $-57, -514, 513$ Bézout-Koeffizienten für $(2415, 3910, 4186)$.

2. Vorbemerkung: Es seien n_1 und n_2 zwei natürliche Zahlen und t ihr größter gemeinsame Teiler. Es seien $m_i \in \mathbb{N}$, so dass $m_i t = n_i$, $i = 1, 2$. Dann gelten

   $$\text{kgV}(n_1, n_2) = m_1 n_2 = m_1 t m_2 = n_1 m_2 \text{ und } \text{ggT}(n_1, n_2)\text{kgV}(n_1, n_2) = n_1 n_2.$$

   Beweis: Es gilt $m_1 n_2 = m_1 t m_2 = n_1 m_2$. Wir setzen $k := \text{kgV}(n_1, n_2)$. Sowohl n_2 und n_1 teilen mn_2. Also gilt $k \leq mn_2$ nach Definition des kgVs. Andererseits ist n_2 ein Teiler von k, etwa $k = n_2 k'$. Es gilt $n_1 | k = n_2 k'$, also $m_1 | m_2 k'$. Da m_1 und m_2 teilerfremd sind, gilt $m_1 | k'$ (eine leichte Folgerung aus dem Lemma von Bézout). Also $m_1 n_2 | k$, und somit $m_1 n_2 \leq k$ nach Bemerkung 26, da $m_1 n_2$ und k positiv sind. Folglich gilt die behauptete Gleichung. q.e.d.

(a) Zu $(2541^{1001}, 1001^{2541})$: $\mathrm{ggT}(2541^{1001}, 1001^{2541}) = \mathrm{ggT}((3*7*11^2)^{1001}, (7*11*13)^{2541}) = 7^{1001} * (11^2)^{1001} = (7*121)^{1001} = 847^{1001}$. Hierbei wurde ein Satz aus der Übung zur Berechnung des ggTs mittels Primfaktorzerlegungen verwendet.
$\mathrm{kgV}((3*7*11^2)^{1001}, (7*11*13)^{2541}) = 3^{1001} * (7*11*13)^{2541} = 3^{1001} * 1001^{2541}$ nach der Vorbemerkung.

(b) Zu $(7^{180}+1, 7^{120}-1)$:

$$\begin{aligned}\mathrm{ggT}(7^{180}+1, 7^{120}-1) &= \mathrm{ggT}((7^{60})^3 - (-1)^3, (7^{60})^2 - (-1)^2) \\ &= ((7^{60}) - (-1))\mathrm{ggT}((7^{60})^2 + (-1)7^{60} + (-1)^2, 7^{60} + (-1)) \\ &= (7^{60}+1)\mathrm{ggT}((7^{60}-1)7^{60}+1, 7^{60}-1) \\ &= (7^{60}+1)\mathrm{ggT}(1, 7^{60}-1) \\ &= 7^{60}+1.\end{aligned}$$

$\mathrm{kgV}(7^{180}+1, 7^{120}-1) = (7^{180}+1)(7^{60}-1)$ nach der Vorbemerkung.

(c) $(2^{16}-1, 3^{16}-2^{16})$: $\mathrm{ggT}(2^{16}-1, 3^{16}-2^{16}) = \mathrm{ggT}(2^{16}-1, 3^{16}-2^{16}+2^{16}-1) = \mathrm{ggT}(2^{16}-1, 3^{16}-1)$. Wir ermitteln für beide Zahlen die Primfaktorzerlegung:

$$2^{16}-1 = (2^8+1)(2^4+1)(2^2+1)(2^1+1)(2^1-1),$$

mittels mehrfacher Anwendung der Vorbemerkung aus Aufgabe 1.. (Hier war es nur die dritte binomische Formel.) Also erhalten wir für $2^{16}-1$ die Primfaktorzerlegung $257*17*5*3$. Nun für $3^{16}-1$:

$$\begin{aligned}3^{16}-1 &= (3^8+1)(3^4+1)(3^2+1)(3^1+1)(3^1-1) = 6562*82*10*4*2 \\ &= (17*2*193)*41*2*5*2^4 = 2^6*5*17*41*193.\end{aligned}$$

Damit erhlalten wir $\mathrm{ggT}(2^{16}-1, 3^{16}-1) = 5*17 = 85$. Also $\mathrm{ggT}(2^{16}-1, 3^{16}-2^{16}) = 85$.
Nach der Vorbemerkung gilt $\mathrm{kgV}(2^{16}-1, 3^{16}-2^{16}) = 257*3*(3^{16}-2^{16})$.

3. Behauptung: Sind a und b Bézout-Koeffizienten für zwei ganze Zahlen z_1, z_2, so dass $|z_1|+|z_2| > 0$, so sind a und b teilerfremd.

   Beweis: Wir haben $az_1 + bz_2 = t := \mathrm{ggT}(z_1, z_2)$, da a und b Bézout-Koeffizienten von z_1 und z_2 sind. Des Weiteren ist $\mathrm{ggT}(z_1, z_2)$ positiv, da nicht beide ganzen Zahlen z_1 und z_2 verschwinden. Aus $t > 0$ folgt aus der Gleichung auch $(a, b) \neq (0, 0)$. Des Weiteren folgt aus der Gleichung, dass $\mathrm{ggT}(a, b)t$ ein Teiler von t ist. Also ist $0 < \mathrm{ggT}(a, b)t \leq t$. Nun gilt aber auch $t \leq \mathrm{ggT}(a, b)t$ nach Bemerkung 26. Also gilt $t(\mathrm{ggT}(a, b) - 1) = 0$, und somit folgt aus der Nullteilerfreiheit, dass a und b teilerfremd sind. q.e.d.

   Nun können wir die Frage der Aufgabe beantworten: Ja, es gibt eine ganzzahlige Lösung von $aX + bY = 109$, nach dem Lemma von Bézout, da a und b teilerfremd sind. Genauer: Aus der Teilerfremdheit folgt die Existenz ganzer Zahlen c und d, so dass $ca + db$ gleich 1 ist. Also ist $(109c, 109d)$ eine Lösung der Gleichung $aX + bY = 109$.

Aufgabe 3 (5+5+5* Punkte)**.** Es seien eine natürliche Zahl n in der Dezimaldarstellung $n = \sum_{i=0}^{m} a_i 10^i$, $0 \leq a_i < 10$ und $a_m \neq 0$, und eine natürliche Zahl l gegeben. Wir setzen $a_i := 0$ für alle $i > m$. Wir bezeichnen

$$Q_l(n) := \sum_{j=0}^{q} \sum_{i=0}^{l-1} 10^i a_{jl+i}$$

als die *l-Blockquersumme* und

$$Q_{l,alt}(n) := \sum_{j=0}^{q} (-1)^j \sum_{i=0}^{l-1} 10^i a_{jl+i}$$

als die *alternierende l-Blockquersumme* von n, wobei q durch Division mit Rest, $m = ql + r$ mit $0 \leq r < l$, gegeben ist. Bitte wenden.

1. Zeigen Sie, dass n genau dann durch 3 teilbar ist, wenn ihre Quersumme $Q_1(n)$ durch 3 teilbar ist.
2. Für welche Primzahlen p lässt sich die Teilbarkeit von n durch p mittels der alternierenden 3-Blockquersumme $Q_{3,alt}(n)$ bestimmen? Beweisen Sie Ihre Antwort.
3.* Gibt es eine Blockquersumme, alternierend oder nicht, mit der man die Teilbarkeit durch 37 bestimmen kann? Beweisen Sie Ihre Antwort.

Lösung: Wir setzen $Q_{l,1} := Q_l$ und $Q_{l,-1} := Q_{l,alt}$. Es sei ϵ gleich 1 oder -1. Dann gilt

$$n = \sum_{j=0}^{q} (10^l)^j \sum_{i=0}^{l-1} 10^i a_{jl+i} = \sum_{j=0}^{q} ((10^l)^j - \epsilon^j) \sum_{i=0}^{l-1} 10^i a_{jl+i} + Q_{l,\epsilon}(n). \tag{4}$$

Für eine ganze Zahl t sind wir an der folgenden Aussage $A(t, l, \epsilon)$ interessiert:

$$\forall m \in \mathbb{N} : \ (t|m \Leftrightarrow t|Q_{l,\epsilon}(m)).$$

Nach der Vorbemerkung aus Aufgabe 1 teilt $10^l - \epsilon$ jede der Zahlen $(10^l)^j - \epsilon^j$, $j \in \mathbb{N}_0$.
(*) Also ist aufgrund der Gleichung (4) für jeden Teiler t von $10^l - \epsilon$ die Aussage $A(t, l, \epsilon)$ wahr.
Wir betrachten nun die einzelnen Teilaufgaben:

1. Beweis: Wir haben hier den Fall $l = 1, \epsilon = 1$. Die Primzahl 3 teilt $9 = 10 - 1$. Also gilt $A(3, 1, 1)$ nach Aussage (*). q.e.d.
2. Behauptung: Es handelt sich um die Primzahlen $7, 11$ und 13.

   Beweis: Wir setzen $M := \{7, 11, 13\}$. Der Beweis besteht aus zwei Teilen:

   Teil 1: Für $p \in M$ gilt $A(p, 3, -1)$.

   Teil 2: Für jede Primzahl $p \notin M$ gilt $A(p, 3, -1)$ nicht.

   Zu Teil 1: Es gilt $10^3 - (-1)^3 = 1001 = 7 * 11 * 13$. Also folgt Teil 1 aus Aussage (*).

   Zu Teil 2: Es gilt $Q_{3,alt}(1001) = 0$, und Null ist durch alle Primzahlen teilbar. Also muss jede Primzahl p, die $A(p, 3, -1)$ erfüllt, auch ein Teiler von 1001 sein. Also erfüllen die Primzahlen ausserhalb von M die Aussage $A(p, 3, -1)$ nicht. q.e.d.
3. Antwort: Ja, zum Beispiel die 3-Blockquersumme.

   Beweis: Wir betrachten $l = 3$ und $\epsilon = 1$. Es gilt $10^3 - 1 = 999 = 37 * 27$. Damit folgt aus Aussage (*) die Aussage $A(37, 3, 1)$. q.e.d.

Aufgabe 4 (10 Punkte)**.** Zeigen Sie, dass für jede natürliche Zahl n zwei Primzahlen p_1 und p_2 existieren, so dass $p_2 - p_1$ größer als n ist und keine Primzahl p mit $p_1 < p < p_2$ existiert.

Für die Aufgabe brauchen wir die folgende Bezeichnung. Für eine natürliche Zahl n bezeichnen wir das Produkt $n! := 1 \cdot \ldots \cdot n$ als die Fakultät von n.

Lösung: Beweis: Wir wählen $m > n$. Die natürlichen Zahlen

$$2 + m!, 3 + m!, \ldots, m + m!$$

sind keine Primzahlen, da für jedes $i \in \mathbb{N}^{\leq m} \setminus \{1\}$ die Zahl $i + m!$ durch i teilbar ist, und

$$1 < i \leq m < m! + i$$

gilt. Da es nach dem Satz von Euklid unendlich viele Primzahlen gibt, folgt aus dem Wohlordnungssatz die Existenz einer kleinsten Primzahl p_2 größer als $m + m!$. Da $2 + m!$ größer als 2 ist, gibt es nach Satz 14 eine größte Primzahl p_1 in $\mathbb{N}^{\leq 1+m!}$. Dann gibt es nach Wahl von p_1 und p_2 keine Primzahl p mit $p_1 < p < p_2$, und die Differenz $p_2 - p_1$ ist größer gleich $m + 1 + m! - (1 + m!)$, also größer gleich m und somit größer als n. q.e.d.

Am Ende gibt es noch als Ergänzung zur Vorlesung den verallgemeinerten Bézout, der aus Zeitgründen in meiner Montagsübung fehlte. Bitte wenden.

Satz E.1. (Verallgemeinerter Bézout) Es seien $z_1, \ldots, z_n$ ganze Zahlen und t ihr größter gemeinsame Teiler. Dann existieren ganze Zahlen $a_1, \ldots, a_n$, so dass die folgende Gleichung gilt:

$$a_1 z_1 + a_2 z_2 + \ldots + a_n z_n = t.$$

Dazu benötigen wir einen Hilfssatz.

Lemma E.2. Es seien $z_1, \ldots, z_n$ ganze Zahlen, und es sei $t \in \mathbb{N}_0$ ein gemeinsamer Teiler von $z_1, \ldots, z_n$. Dann sind äquivalent:

1. t ist der größte gemeinsame Teiler von $z_1, \ldots, z_n$.
2. Jeder gemeinsame Teiler von $z_1, \ldots, z_n$ teilt t.

Beweis: $1 \Rightarrow 2$: Falls alle z_i null sind, so ist $t = 0$ und somit t durch alle ganzen Zahlen teilbar. Es sei nun mindestens ein z_i ungleich Null. Damit ist t größer als Null. Es sei s ein gemeinsamer Teiler von $z_1, \ldots, z_n$. Ohne Einschränkung betrachten wir $s > 0$, da wir ansonsten zu $|s|$ übergehen könnten. Wir setzen $r := \mathrm{ggT}(t, s)$, und es seien t' und s' natürliche Zahlen, so dass $rt' = t$ und $rs' = s$. Fixiere ein $i \in \mathbb{N}^{\leq n}$. Wir wählen den Komplemantärteiler t_i' von z_i zu t, also $z_i = t_i' t$. Es gilt $s | z_i = t_i' r t'$, also $s' | t_i' t'$. Also gilt $s' | t_i'$, da s' und t' teilerfremd sind. Damit folgt, dass $s't$ ein Teiler von z_i ist. Da i beliebig gewählt wurde, folgt, dass $s't$ ein gemeinsamer Teiler der z_i ist. Damit muss $s' = 1$ gelten, da ansonsten $s't$ größer als t wäre. Also $s | t$.

$2 \Rightarrow 1$: Wenn alle z_i null sind, dann folgt aus 2, dass t durch Null teilbar ist, und damit muss t Null sein, und stimmt mit $\mathrm{ggT}(0, \ldots, 0)$ überein. Es sei nun mindenstens ein z_i ungleich Null. Aus 2 folgt, dass $\mathrm{ggT}(z_1, \ldots, z_n)$ die natürliche Zahl t teilt. Also folgt aus Bemerkung 26 $\mathrm{ggT}(z_1, \ldots, z_n) \leq t$. Andererseits ist t ein gemeinsamer Teiler von $z_1, \ldots, z_n$, und damit nach Definition des ggTs kleiner gleich $\mathrm{ggT}(z_1, \ldots, z_n)$. Also ist t gleich dem größten gemeinsamen Teiler von $z_1, \ldots, z_n$. q.e.d.

Beweis: [vom Satz vom Verallgemeinerten Bézout] Der Beweis benutzt eine vollständige Induktion über n. Für $n = 1$ ist nichts zu zeigen, und der Fall $n = 2$ folgt aus dem Lemma von Bézout aus der Vorlesung. Es sei $n > 2$. Aus dem Hilfssatz folgt $\mathrm{ggT}(z_1, \ldots, z_n) = \mathrm{ggT}(\mathrm{ggT}(z_1, \ldots, z_{n-1}), z_n)$, denn die rechte Seiten ist in $\mathbb{N}_0$ und ein gemeinamer Teiler von $z_1, \ldots, z_n$, und sie erfüllt Bedingung 2 von Lemma E.2, wie man nach zweimaliger Anwendung von Lemma E.2 erkennt. Wir wenden das Lemma von Bézout auf $(\mathrm{ggT}(z_1, \ldots, z_{n-1}), z_n)$ an und erhalten ganze Zahlen a, b, so dass

$$a\mathrm{ggT}(z_1, \ldots, z_{n-1}) + b z_n = t,$$

und wir setzen die Gleichung aus der Induktionsvoraussetzung in die obige Gleichung ein und erhalten die Induktionsbehauptung. q.e.d.