Zahlentheorie III

Thomas Huber

Aktualisiert: 27. September 2017
vers. 1.6.8

Inhaltsverzeichnis

1 Spezielle Gleichungstypen **2**
1.1 Quadratische Gleichungen 2
1.2 Pythagoräische Tripel 4
1.3 Die Pell Gleichung 5
1.4 Konstruktion von Lösungen 9

2 Kongruenzen II **11**
2.1 Ordnungen 11
2.2 Primitive Wurzeln 14

3 Varia **18**
3.1 Die Gaussklammer 18

1 Spezielle Gleichungstypen

1.1 Quadratische Gleichungen

Sehr wichtig in der Zahlentheorie sind quadratische Gleichungen mit ganzen Koeffizienten. Sie treten viel öfter auf, als man vermuten würde, oft eben versteckt. Eine quadratische Gleichung in der Unbekannten x hat bekanntlich die Form

$$ax^2 + bx + c = 0,$$

wobei $a \neq 0, b, c$ reelle Konstanten sind. Sie besitzt zwei (komplexe) Lösungen x_1, x_2, die auch zusammenfallen können. Es gilt

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a},$$

wobei $D = b^2 - 4ac$ die *Diskriminante* der Gleichung ist. Diese Bezeichnung rechtfertigt sich dadurch, dass das Vorzeichen von D über die Lösungsmenge Auskunft gibt:

$D > 0$	$\Leftrightarrow$	Zwei verschiedene reele Lösungen.
$D = 0$	$\Leftrightarrow$	Eine doppelte reelle Lösung.
$D < 0$	$\Leftrightarrow$	Zwei konjugiert komplexe Lösungen.

Für uns von Bedeutung ist natürlich der Fall, wo die Koeffizienten ganze Zahlen sind. Unter welchen Voraussetzungen besitzt die Gleichung ganze Lösungen? Notwendig (aber nicht hinreichend) ist, dass D eine Quadratzahl ist. Dies kann man oft verwenden.

Beispiel 1. *Finde alle positiven ganzzahligen Lösungen der Gleichung*

$$xyz = x^2 + y + z.$$

Lösung. Obwohl die linke Seite Grad 3 hat, ist dies eine quadratische Gleichung in x. Die Diskriminante ist gleich

$$D = y^2z^2 - 4(y + z).$$

Für eine ganzzahlige Lösung muss D ein Quadrat sein. Nun ist aber immer $(yz)^2 > D$. Falls jetzt auch noch die Ungleichung $4(y + z) < 2yz - 1$ erfüllt ist, liegt D zwischen den aufeinanderfolgenden Quadraten $(yz - 1)^2$ und $(yz)^2$, kann also nicht selbst ein Quadrat sein. Es genügt daher, die Paare (y, z) zu betrachten, für die gilt $4(y + z) \geq 2yz - 1$. Diese Ungleichung ist äquivalent zu

$$(y - 2)(z - 2) \leq 4.$$

Also muss y oder z kleiner als 3 sein, oder (y, z) ist eines der Paare $(3,3), (3,4), (3,5), (3,6), (4,4)$ oder eine Vertauschung davon. Die Analyse der einzelnen Fälle sei nun dem Leser überlassen. Die Lösungen (x, y, z) mit $y \geq z$ sind:

$$(2,5,1), (3,5,1), (2,2,2), (1,3,2), (5,3,2).$$

□

Wenn man die Diskrimante betrachtet, und die Fälle finden möchte, in denen sie ein Quadrat ist, sollte man mit Abschätzungen arbeiten. Dies ist allgemein sehr effizient, wie das Beispiel zeigt. Algebraische Manipulationen und Modulobetrachtungen können zwar auch zum Ziel führen, meist jedoch nur über Umwege.

Wichtiger als die Diskriminante ist jedoch der Satz von Vieta. Zur Erinerung: sind $x_{1,2}$ die beiden Lösungen der Gleichung $x^2 + px + q = 0$, dann gilt

$$x_1 + x_2 = -p$$
$$x_1 \cdot x_2 = q$$

Insbesondere folgt daraus: sind p, q ganz und besitzt die Gleichung eine ganze Lösung, dann ist auch die zweite Lösung ganzzahlig. Dies ist von enormer Bedeutung, wie wir gleich sehen werden. Dies erlaubt einem nämlich, aus bereits bekannten Lösungen neue zu konstruieren. Einerseits kann man damit oft zeigen, dass Lösungen mit gewissen Eigenschaften existieren, andererseits hilft dies bei Argumentationen, wo Abschätzungen wichtig sind. Oft ist man nämlich gar nicht unbedingt an allen Lösungen einer Gleichung interessiert, sondern kann sich die Lösung gewissermassen auswählen. In diesem Fall ist es oft nützlich, sich eine *minimale* Lösung zu wählen und dann Vieta zu verwenden. Als Paradebeispiel schlechthin folgt nun eine wunderschöne Lösung einer wirklich schwierigen IMO Aufgabe.

Beispiel 2 (IMO 88)**.** *Seien a, b natürliche Zahlen, sodass $a^2 + b^2$ durch $ab + 1$ teilbar ist. Zeige, dass*

$$\frac{a^2 + b^2}{ab + 1}$$

eine Quadratzahl ist.

Lösung. Nehme an, es gilt

$$\frac{a^2 + b^2}{ab + 1} = q \tag{1}$$

mit einer natürlichen Zahl q, die keine Quadratzahl ist. Da (1) symmetrisch in a und b ist, können wir $a \geq b$ annehmen. Unter allen ganzzahligen Paaren (a, b) mit $a \geq b > 0$, für die (1) gilt, wählen wir jene mit *minimalem* a und unter allen solchen jenes mit *minimalem* b. Wir können nun (1) umformen zu einer quadratischen Gleichung in a:

$$a^2 - a \cdot qb + (b^2 - q) = 0.$$

Diese besitzt eine weitere Lösung a' und nach Vieta gilt

$$a + a' = qb$$
$$a \cdot a' = b^2 - q.$$

Aus der ersten Gleichung folgt, dass a' ebenfalls ganz ist. Nach Konstruktion erfüllt das Paar (a', b) ebenfalls (1), daher muss $a' \geq 0$ sein (sonst wäre entweder $a'b + 1 = 0$ oder $q < 0$). Aus der zweiten Gleichung folgt nun ausserdem $a' > 0$, denn sonst wäre $q = b^2$ eine Quadratzahl! Ebenfalls aus der zweiten Gleichung schliesst man weiter $aa' = b^2 - q < b^2 \leq a^2$, also ist $0 < a' < a$. Das bedeutet aber insgesamt, dass das Paar (a', b) oder das Paar (b, a') die minimale Wahl von (a, b) verletzt, Widerspruch. Folglich muss q ein Quadrat sein. □

Beispiel 3 (Taiwan 98)**.** *Existiert eine Lösung der Gleichung*

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65$$

in ganzen Zahlen x, y, z, u, v *grösser als* 1998*?*

Lösung. Die linke Seite der Gleichung hat Grad 2, die rechte im Wesentlichen Grad 5. Wenn nun alle fünf Variablen sehr gross sind, müsste doch eigentlich die rechte Seite der Gleichung viel grösser sein als die linke. Beachte jedoch: auf der linken Seite stehen reine Quadrate, rechts aber ein gemischter Term. Wenn nun zum Beispiel x viel grösser ist als y, z, u, v, dann können durchaus beide Seiten gleich gross sein. Es ist daher Vorsicht geboten! In der Tat lautet die Antwort ja.
Wir werden allgemeiner zeigen, dass Lösungen dieser Gleichung existieren, wobei die kleinste der fünf Variablen beliebig gross wird.
Angenommen, wir hätten irgendeine positive Lösung $(x_1, y_1, z_1, u_1, v_1)$ gefunden, wobei nicht alle fünf Zahlen gleich gross sind. Wegen der Symmetrie können wir dann $x_1 \leq \ldots \leq v_1$ annehmen, also gilt insbesondere $x_1 < v_1$. Wir fassen die Gleichung nun als quadratische in x auf, das heisst x_1 ist eine Lösung von

$$x^2 - (y_1 z_1 u_1 v_1)x + (y_1^2 + z_1^2 + u_1^2 + v_1^2 - 65) = 0$$

Nach Vieta ist die zweite Lösung $x_2 = y_1 z_1 u_1 v_1 - x_1$ auch ganz. Ebenfalls nach Vieta gilt $x_1 x_2 = y_1^2 + z_1^2 + u_1^2 + v_1^2 + 65 > v_1^2$, wegen $x_1 < v_1$ also $x_2 > v_1$. Wir erhalten somit eine neue Lösung $(y_1, z_1, u_1, v_1, x_2)$, in der nicht alle Zahlen gleich sind. Nach spätestens 4 solchen Operationen hat sich das kleinste Element vergrössert. Indem wir diese Operation genügend oft ausführen, können wir daher alle Zahlen beliebig gross machen, insbesondere grösser als 1998.
Was nun noch fehlt, ist irgendeine Lösung. Exzessives Suchen liefert zum Beispiel die Lösungen $(1, 2, 3, 4, 5)$ und $(1, 1, 3, 8, 10)$. □

1.2 Pythagoräische Tripel

Ein Tripel (x, y, z) positiver ganzer Zahlen, das Lösung der Gleichung

$$x^2 + y^2 = z^2$$

ist, heisst *Pythagoräisches Zahlentripel*. Haben x, y und z einen gemeinsamen Teiler q, dann ist offenbar auch $(\frac{x}{q}, \frac{y}{q}, \frac{z}{q})$ eine Lösung und daher können wir annehmen, dass dies nicht der Fall ist. Dann sind die drei Zahlen sogar paarweise teilerfremd, denn ein gemeinsamer Teiler von zweien teilt auch die dritte, wie man leicht sieht. Solche Pythagoräische Tripel heissen *primitiv*. In einem primitiven Tripel kann höchstens ein Zahl gerade sein. Andererseits können nicht alle ungerade sein, sonst wäre die linke Seite gerade, die rechte aber nicht.
Ausserdem kann z nicht gerade sein, sonst wäre die linke Seite $\equiv 2$, die rechte aber $\equiv 0 \pmod 4$. Der folgende Satz klärt die Struktur von primitiven Pythagoräischen Tripeln.

Satz 1.1. *Es ist äquivalent:*

(a) $x^2 + y^2 = z^2$, *mit teilerfremden natürlichen Zahlen* x, y, z *und* y *gerade.*

(b) Es gibt positive teilerfremde Zahlen m *und* n *mit* $m > n, m \not\equiv n \pmod 2$ *und*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Beweis. Nehme an, (x, y, z) sei wie in (a). Dann gilt $y^2 = (z - x)(z + x)$ und daher sind $y = 2v, z + x = 2u$ und $z - x = 2w$ gerade. Da x und z teilerfremd sind, gilt dies auch für u und w. Einsetzen zeigt daher, dass beide Quadratzahlen sind, $u = m^2$, $w = n^2$. Ausserdem sind u und w nicht beide ungerade, also gilt $m \not\equiv n \pmod 2$. Drücke x, y, z durch m und n aus, dann folgt (b). Umgekehrt erfüllt ein Tripel (x, y, z) wie in (b) natürlich auch (a). □

Es gibt also unendlich viele primitive Pythagoräische Tripel. Bekanntlich ist dies nicht mehr richtig, wenn der Exponent grösser als 2 ist. Der Vollständigkeit halber zitieren wir das Resultat, auch wenn der Beweis den Horizont dieses Skripts leicht übersteigt:

Satz 1.2 (Fermat's letzter Satz)**.** *Für* $n > 3$ *sind* $(1, 0, 1)$ *und* $(0, 1, 1)$ *die einzigen teilerfremden Lösungen in nichtnegativen ganzen Zahlen der Gleichung*

$$x^n + y^n = z^n.$$

Leicht zu sehen ist immerhin das Folgende: es genügt den Satz für n prim und $n = 4$ zu beweisen. Ersteres ist sehr schwierig und wurde 1995 von A. Wiles gemacht. Der Fall $n = 4$ ist aber elementar und euch als Übung überlassen (siehe Aufgaben).

1.3 Die Pell Gleichung

Bei der *Pell Gleichung* handelt es sich um eine quadratische Gleichung in zwei Variablen, die in vielen Problemen ganz natürlich auftaucht. In ihrer einfachsten Form lautet sie

$$x^2 - Dy^2 = 1 \tag{2}$$

wobei $D > 1$ eine natürliche Zahl ist, die durch kein Quadrat > 1 teilbar ist (man nennt D *quadratfrei*). Dies kann man übrigens immer annehmen, denn wenn D einen quadratischen Faktor hat, kann man diesen durch eine Umdefinition von y entfernen.
Um alle positiven, ganzen Lösungen dieser Gleichung zu finden, geht man in zwei Schritten vor:

- Finde die kleinste positive Lösung.
- Konstruiere daraus rekursiv alle anderen.

Zentral für das Folgende ist die Faktorisierung

$$x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y). \tag{3}$$

Wir assoziieren zu jeder positiven Lösung (x, y) die Zahl $a = x + \sqrt{D}y$. Beachte, dass sich (x, y) aus a rekonstruieren lässt, denn aus $x + \sqrt{D}y = u + \sqrt{D}v$ folgt $x = u$ und $y = z$, da D quadratfrei ist. Aus (3) folgt ausserdem: ist (x, y) eine Lösung von (2), dann gilt $x + \sqrt{D}y > 1$ und $0 < x - \sqrt{D}y < 1$.
Zuerst zur Minimalen Lösung. Eine positive Lösung (x_0, y_0) heisst *minimal*, falls $x_0 + \sqrt{D}y_0$ minimal ist unter allen positiven Lösungen. Sind (x_1, y_1) und (x_2, y_2) zwei positive Lösungen von (2), dann gilt $x_1 < x_2$ genau dann, wenn $y_1 < y_2$. Wenn es also überhaupt eine positive Lösung gibt, dann auch eine eindeutig bestimmte kleinste (x_0, y_0). Man kann beweisen, dass die Gleichung (2) *immer* eine positive Lösung besitzt, dies ist aber nicht einfach. Im konkreten Anwendungsfall findet man die minimale Lösung meist schnell durch probieren. Sie kann in manchen Fällen aber auch erschreckend gross sein. Es gibt ein allgemeines Verfahren, wie man (x_0, y_0) berechnen kann. Dazu muss man die minimalen Perioden in der Kettenbruchentwicklung von D bestimmen. Dies zu erklären, würde aber den Rahmen hier sprengen.

Nun wenden wir uns der Konstruktion *aller* Lösungen zu.

Satz 1.3. *Nehme an,* (x_0, y_0) *sei die minimale positive Lösung von* (2). *Definiere rekursiv die Folgen*

$$\begin{aligned} x_{n+1} &= x_0 x_n + D y_0 y_n \\ y_{n+1} &= y_0 x_n + x_0 y_n. \end{aligned}$$

Die positiven Lösungen von (2) *sind dann genau die Paare* (x_n, y_n) *für* $n \geq 0$. *Insbesondere gibt es beliebig grosse Lösungen.*

Beweis. Mit vollständiger Induktion zeigt man leicht, dass x_n, y_n gerade so konstruiert sind, dass gilt

$$x_n + \sqrt{D}y_n = (x_0 + \sqrt{D}y_0)^{n+1}.$$

Aus (3) folgt, dass wenn $u + \sqrt{D}v$ und $w + \sqrt{D}z$ Lösungen sind, dann auch ihr Produkt und ihr Quotient. Mit obiger Formel folgt daraus, dass alle (x_n, y_n) Lösungen sind. Nehme

nun an, es existiert eine weitere Lösung $u + \sqrt{D}v$, die nicht von dieser Form ist. Dann gibt es ein n mit

$$(x_0 + \sqrt{D}y_0)^n < u + \sqrt{D}v < (x_0 + \sqrt{D}y_0)^{n+1}.$$

Multiplikation mit $(x_0 - Dy_0)^n$ liefert

$$1 < (u + \sqrt{D}v)(x_0 - \sqrt{D}y_0)^n < x_0 + \sqrt{D}y_0$$

Der mittlere Term ist grösser als 1 und daher eine positive Lösung von (2). Die rechte Ungleichung widerspricht aber der Minimalität von (x_0, y_0). □

Beispiel 4. *Zeige, dass es unendlich viele Dreiecke gibt, sodass die Seitenlängen drei aufeinanderfolgende ganze Zahlen sind und auch der Flächeninhalt ganz ist.*

Lösung. Seien $a = n-1, b = n$ und $c = n+1$ die Seitenlängen des Dreiecks. Nach Heron ist die Fläche gegeben durch

$$A = \frac{1}{4}\sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)} = \frac{n}{4}\sqrt{3(n^2-4)}$$

Damit A eine ganze Zahl ist, muss n gerade sein und der Ausdruck unter der Klammer eine Quadratzahl. Ersetze n durch $2x$ und $\frac{A}{n}$ durch m, dann wird die Gleichung zu $3x^2 - 3 = m^2$. Daraus folgt, dass m durch 3 teilbar ist, setze also $m = 3y$. Die Gleichung wird zu

$$x^2 - 3y^2 = 1.$$

Dies ist eine Pell Gleichung mit minimaler Lösung $(x_0, y_0) = (2, 1)$. Die anderen Lösungen sind gegeben durch die Rekursionen $x_{n+1} = 2x_n + 3y_n$ und $y_{n+1} = x_n + 2y_n$. Die ersten Lösungen lauten

$$(2,1), (7,4), (26,15), (97,56), (362,209), \ldots$$

Die gesuchten Dreiecke sind also genau die mit den Seitenlängen $2x_n - 1, 2x_n, 2x_n + 1$ und haben die Fläche $3x_n y_n$. Insbesondere gibt es unendlich viele davon. □

Die *verallgemeinerte Pell Gleichung* hat die Form

$$ax^2 - by^2 = c \tag{4}$$

mit ganzen Zahlen a, b, c, wobei a und b positiv und quadratfrei sind, und nicht beide gleich 1. Wenn a und b beide grösser als 1 sind, kann es mehrere kleinste Lösungen, sogenannte Fundamentallösungen, geben. Die ganze Geschichte wird dann sehr kompliziert. Wir beschränken uns daher auf den Fall, wo $a = 1$ oder $b = 1$ ist. Den Fall $a = c = 1$ haben wir oben ausführlich diskutiert. Wir geben nun eine Übersicht über die weiteren Resultate. Die Beweise sind nicht schwierig und dem Leser als Übung überlassen.

1. $b = c = 1$
   Die Gleichung hat dann die Form $ax^2 - y^2 = 1$ und lässt sich umschreiben zu $y^2 - ax^2 = -1$. Dieser Fall lässt sich daher auf den nächsten zurückführen.

2. $a = 1$
   Die Gleichung hat die Form
   $$x^2 - by^2 = c.$$
   Falls die Gleichung $x^2 - by^2 = c$ eine positive Lösung hat, gibt es unendlich viele solche. Sei (x_0, y_0) die kleinste und (x_1, y_1) die zweitkleinste Lösung. Definiere (p, q) durch
   $$\frac{x_1 + \sqrt{b}y_1}{x_0 + \sqrt{b}y_0} = p + \sqrt{b}q.$$
   p und q sind wohldefinierte positive rationale Zahlen (nach Konstruktion ist (p, q) eine rationale Lösung der Gleichung $x^2 - by^2 = 1$, die im Allgemeinen kleiner ist, als die minimale ganzzahlige positive Lösung).
   Die Gesamtheit der positiven Lösungen ist dann gegeben durch
   $$x_n + \sqrt{b}y_n = (p + \sqrt{b}q)^n(x_0 + \sqrt{b}y_0), n \geq 0.$$
   Mit anderen Worten, die Lösungen (x_n, y_n) erhält man über die Rekursionsgleichungen
   $$\begin{aligned} x_{n+1} &= px_n + bqy_n, \\ y_{n+1} &= qx_n + py_n. \end{aligned}$$
   Wenn $c \neq 1$, kann es auch sein, dass die Gleichung gar keine Lösungen besitzt, im Gegensatz zum Fall $c = 1$. Dies lässt sich oft mit Hilfe der Modulorechnung beweisen.

Beispiel 5. *Zeige, dass die Gleichung $x^2 - 7y^2 = -1$ keine ganzzahlige Lösung besitzt.*

Lösung. Betrachte die Gleichung modulo 7. Dann muss gelten $x^2 \equiv 6 \pmod 7$. Dies ist nicht möglich. □

Beispiel 6 (Shortlist 95)**.** *Finde die kleinste natürliche Zahl n, sodass $19n+1$ und $95n+1$ beides Quadrate sind.*

Lösung. Setze $95n + 1 = x^2$ und $19n + 1 = y^2$. Dann muss gelten $x^2 - 5y^2 = -4$. Dies ist eine verallgemeinerte Pell Gleichung. Die beiden kleinsten Lösungen sind $(1, 1)$ und $(4, 2)$, daraus berechnet man leicht $(p, q) = (\frac{3}{2}, \frac{1}{2})$. Mit Hilfe der Rekursionsformeln
$$\begin{aligned} x_{n+1} &= \frac{3x_n}{2} + \frac{5y_n}{2} \\ y_{n+1} &= \frac{3y_n}{2} + \frac{x_n}{2} \end{aligned}$$
Findet man die ersten paar Werte von y_n :
$$1, 2, 5, 13, 34, 89, 233, 610, 1597, \ldots$$

Der Wert $y_0 = 1$ führt zu $n = 0$, ist also nicht zu beachten. Wegen $y^2 = 19n + 1$ suchen wir also die erste Zahl in dieser Lösungsfolge, deren Quadrat $\equiv 1 \pmod{19}$ ist. Eine kurze Rechnung zeigt, dass dies $y_8 = 1597$ ist. Die Antwort lautet daher:

$$n = \frac{1}{19}(y_8^2 - 1) = 134232.$$

□

1.4 Konstruktion von Lösungen

In diesem Abschnitt geht es darum, verschiedene Methoden zusammenzustellen, wie man Lösungen zu zahlentheoretischen Problemen konstruieren kann. Oft ist nämlich gar nicht verlangt, *alle* Lösungen einer Gleichung zu finden, sodern nur (unendlich) *viele*.
Es gibt viele verschiedene Techniken, die hier an Beispielen vorgestellt werden sollen.

Beispiel 7 (Kanada 91)**.** *Zeige, dass die Gleichung*

$$x^2 + y^5 = z^3$$

unendlich viele ganzzahlige Lösungen mit $xyz \neq 0$ besitzt.

Lösung. Die Lösung $(x, y, z) = (3, -1, 2)$ erfüllt $xyz \neq 0$. Die Gleichung ist nun in gewissem Sinne homogen, das heisst, jede Variable kommt mit nur einem Exponenten in der Gleichung vor und es gibt keinen konstanten Term. Ist daher (x, y, z) eine Lösung mit $xyz \neq 0$, dann auch $(a^{15}x, a^6y, a^{10}z)$ für alle $a \neq 0$. Insbesondere gibt es unendlich viele Lösungen. □

In diesem Beispiel konnten wir aus einer Lösung durch Skalieren unendlich viele konstruieren. Dies ist freilich nicht immer möglich. Das nächste Beispiel ist dafür einfach zu unhomogen:

Beispiel 8 (Italien 96)**.** *Zeige, dass die Gleichung*

$$a^2 + b^2 = c^2 + 3$$

unendlich viele ganzzahlige Lösungen besitzt.

Lösung. Ist a eine ungerade ganze Zahl, dann setze $b = \frac{a^2-5}{2}$ und $c = \frac{a^2-1}{2}$. Nun gilt

$$c^2 - b^2 = (c + b)(c - b) = a^2 - 3.$$

□

Hier konnten wir gleich eine ganze Lösungsfamilie explizit hinschreiben. Inspiriert sind die Ausdrücke für b und c natürlich durch die binomischen Formeln. Überhaupt ist quadratisches Ergänzen und herumspielen mit Quadraten, Kuben usw. ein vielversprechender Ansatz. Noch ein Beispiel:

Beispiel 9. *Zeige, dass für jede natürliche Zahl m eine natürliche Zahl n existiert, sodass $m+n+1$ eine Quadratzahl und $mn+1$ eine dritte Potenz ist.*

Lösung. Eine dritte Potenz der Form $mn+1$ ist zum Beispiel $m(m^2+3m+3)+1 = (m+1)^3$. Und tatsächlich gilt dann auch $m+\mathrm{n}+1 = m^2+4m+4 = (m+2)^2$. Wir können also einfach $n = m^2+3m+3$ setzen. □

Ein weiteres sehr wichtiges Verfahren ist jenes der rekursiven Konstruktion. Die Idee ist simpel. Hat man eine Lösung eines Problems, konstuiert man mit deren Hilfe eine weitere (grössere, bessere etc.).

Beispiel 10 (IMO 89)**.** *Zeige: für jede natürliche Zahl n gibt es n aufeinanderfolgende natürliche Zahlen, von denen keine eine Primzahlpotenz ist.*

Lösung. Wir verwenden Induktion nach n. Für $n = 1$ kann man 6 wählen. Sei $k > 1$ und seien

$$k-n, k-n+1, \ldots, k-1$$

n aufeinanderfolgende natürliche Zahlen, von denen keine eine Primpotenz ist. Dann sind

$$k\cdot k!+(k-n), k\cdot k!+(k-n+1), \ldots, k\cdot k!+(k-1), k\cdot k!+k$$

$n+1$ aufeinanderfolgende Zahlen, von denen keine eine Primpotenz ist. Denn $k\cdot k!+(k-i)$ ist durch $k-i$ teilbar für $i = 1, \ldots, n$. Nach Induktionsvoraussetzung ist aber k - i keine Primpotenz, also auch $k\cdot k!+(k-i)$ nicht. Ausserdem ist $k\cdot k!+k = k(k!+1)$ ein Produkt von zwei teilerfremden natürlichen Zahlen > 1, also auch keine Primpotenz. Dies vollendet den Induktionsschritt. □

Beispiel 11 (IMO 71)**.** *Zeige, dass es unendlich viele natürliche Zahlen der Form $2n-3$ gibt, die paarweise teilerfremd sind.*

Lösung. Es genügt folgendes zu zeigen: Sind $n_1, \ldots, n_k$ verschieden und $2^{n_1}-3, \ldots, 2^{n_k}-3$ paarweise teilerfremd, dann gibt es ein n_{k+1} , sodass $2^{n_{k+1}}-3$ teilerfremd zu den bereits konstruierten Zahlen.
Sei $\{p_1, \ldots, p_r\}$ die Menge der Primzahlen, die eine der Zahlen $2^{n_1}-3, \ldots, 2^{n_k}-3$ teilen. Setze $n_{k+1} = (p_1-1)(p_2-1)\ldots(p_r-1)+1$. Nun gilt für alle $i = 1, \ldots, r$

$$2^{n_{k+1}}-3 = 2\cdot 2^{(p_1-1)\ldots(p_r-1)}-3 \equiv 1 \pmod{p_i}$$

denn nach dem kleinen Satz von Fermat gilt $2^{p_i-1} \equiv 1 \pmod{p_i}$. Folglich ist $2^{n_{k+1}}-3$ nicht durch p_i teilbar, was nach Konstruktion der p_i bedeutet, dass diese Zahl teilerfremd ist zu $2n_1-3, \ldots, 2^{n_k}-3$. Dies beendet den Beweis. □

Man kann auch den Chinesischen Restsatz zur Konstruktion von Lösungen heranziehen (siehe Zahlentheorie II). Eine weitere Möglichkeit wurde im letzten Abschnitt vorgestellt: Pell'sche Gleichungen. Kann man die Existenz gewisser Lösungen auf eine Pell Gleichung

zurückführen, dann genügt es, eine einzige Lösung dieser Pell Gleichung zu finden. Daraus folgt automatisch, dass unendlich viele Lösungen existieren. Beachte dazu Beispiel 4 und 6. Man sollte auch an die Beziehung der beiden Lösungen einer quadratischen Gleichung denken. Damit kann man sich manchmal von einer Lösung zur nächsten schaukeln. Schliesslich noch eine letzte Bemerkung: In seltenen Fällen lässt sich durch einen Widerspruchsbeweis direkt zeigen, dass unendlich viele Dinge mit gewissen Eigenschaften existieren, wie zum Beispiel in Zahlentheorie I beim Satz über die Existenz unendlich vieler Primzahlen.

2 Kongruenzen II

2.1 Ordnungen

Sei n eine natürliche Zahl. Wir haben den Begriff der Ordnung einer Zahl modulo n bereits in Zahlentheorie II eingeführt. Hier nochmals die Definition: Ist a teilerfremd zu n, dann gibt es eine kleinste positive ganze Zahl d, sodass $a^d \equiv 1 \pmod{n}$ gilt. Dieses d heisst die Ordnung von a modulo n. Dass es überhaupt einen Exponenten $e > 0$ gibt mit $a^e \equiv 1 \pmod{n}$ folgt zum Beispiel aus dem Satz von Euler-Fermat, man kann nämlich $e = \varphi(n)$ wählen. Im Allgemeinen ist d aber viel kleiner als $\varphi(n)$ und schwierig zu berechnen. Wichtig ist die Ordnung vor allem wegen folgender Tatsache:

Lemma 2.1. *Sei a teilerfremd zu n und sei d die Ordnung von $a \pmod{n}$. Für eine ganze Zahl m gilt genau dann $a^m \equiv 1 \pmod{n}$, wenn m durch d teilbar ist.*

Beweis. Schreibe $m = kd + r$ mit ganzen Zahlen k, r und $0 \leq r < d$ (Division mit Rest). Nun gilt nach den Potenzgesetzen

$$a^m = a^{kd+r} = (a^d)^k \cdot a^r \equiv 1^k \cdot a^r = a^r \pmod{n},$$

also gilt $a^m \equiv 1$ genau dann, wenn auch $a^r \equiv 1$ ist. Nun ist aber $r < d$ und per Definition ist d ja die *kleinste* natürliche Zahl mit $a^d \equiv 1$. Daher gilt $a^r \equiv 1$ nur für $r = 0$, also genau dann wenn m durch d teilbar ist. □

Insbesondere ist also d immer ein Teiler von $\varphi(m)$. In manchen Situationen kann man nun zeigen, dass d auch ein Teiler einer anderen Zahl sein muss, die beinahe teilerfremd zu $\varphi(m)$ ist. Als Konsequenz ist dann d sehr klein, und genau das kann man oft brauchen. Als klassisches Beispiel besprechen wir den ersten Teil der Lösung einer alten IMO-Aufgabe.

Beispiel 12 (IMO 90)**.** *Finde alle natürlichen Zahlen n, sodass*

$$\frac{2^n + 1}{n^2}$$

eine ganze Zahl ist.

Lösung. Offenbar ist $n = 1$ eine Lösung. Wir nehmen nun $n > 1$ an und zeigen, dass der kleinste Primteiler von n gleich 3 sein muss. Offenbar ist n ungerade. Sei also p dieser kleinste Primteiler und sei d die Ordnung von 2 modulo p. Nach Voraussetzung ist jetzt p ein Teiler von $2^n + 1$, also gilt $2^n \equiv -1$ und quadrieren liefert $2^{2n} \equiv 1 \pmod{p}$. Mit Lemma 2.1 können wir diese Kongruenzen nun in Teilbarkeitsaussagen für d umschreiben:

$$2^n \not\equiv 1 \pmod{p} \Longrightarrow d \nmid n, \qquad 2^{2n} \equiv 1 \pmod{p} \Longrightarrow d \mid 2n.$$

Ausserdem gilt sowieso $d \mid \varphi(p) = p - 1$. In Kombination muss d also sogar $\mathrm{ggT}(2n, p-1)$ teilen! An dieser Stelle kommt nun ins Spiel, dass wir p als minimalen Primteiler von n gewählt haben. Dies impliziert nämlich, dass $p - 1$ nur Primteiler besitzt, die n nicht teilen. Also sind n und $p-1$ teilerfremd und somit gilt $\mathrm{ggT}(2n, p-1) = 2$. Das bedeutet $d = 1$ oder $d = 2$, der erste Fall kann aber nicht eintreten, denn sonst wäre d ein Teiler von n, was noch obigen Rechnungen nicht sein kann. Jetzt gilt also nach Definition der Ordnung $2^2 \equiv 1 \pmod{p}$ und das kann nur für $p = 3$ gelten. □

Der entscheidende Punkt in diese Argument war, dass d sowohl $2n$ als auch $p - 1$ teilen muss, und dass diese beiden Zahlen wirklich beinahe teilerfremd sind. Das Ganze hat deswegen funktioniert, weil p sowohl ein Teiler des Ausdrucks $2n + 1$ vorkommt, also auch im Exponenten von 2 auftaucht (als Teiler von n). Das ist genau die Situation, wo man zwei grundsätzlich verschiede Teilbarkeitsbedingungen für d kriegt. Die Idee, den kleinsten Primteiler einer Zahl mit solchen Methoden zu bestimmen, ist ganz wichtig und führt oft zum Ziel.

Die obige Lösung kann man wie folgt beenden: Zuerst zeigt man, dass n nicht durch 9 teilbar ist. Das ist der schwierigste Schritt. Danach hat man also $n = 3m$, wo m nicht durch 3 teilbar ist. Der letzte Schritt besteht dann darin zu zeigen, dass der kleinste Primteiler von m gleich 7 ist, was dann schnell auf einen Widerspruch führt. Dieser Schritt ist beinahe identisch zum obigen Argument und euch als Übung empfohlen.

Eine weitere wichtige Anwendung ist folgendes schönes Resultat, das doch recht überraschend ist:

Beispiel 13. *Sei p eine ungerade Primzahl und seien a, b zwei ganze Zahlen, die nicht durch p teilbar sind. Ist dann $a^{2^n} + b^{2^n}$ durch p teilbar, dann gilt $p \equiv 1 \pmod{2^{n+1}}$.*

Lösung. Sei b^{-1} ein multiplikatives Inverses von b modulo p, also eine ganze Zahl mit $b \cdot b^{-1} \equiv 1 \pmod{p}$. Zum Beispiel kann man $b^{-1} = b^{p-2}$ wählen nach dem kleinen Satz von Fermat (nach Voraussetzung ist ja b nicht durch p teilbar). Nun gilt

$$a^{2^n} + b^{2^n} \equiv 0 \Longleftrightarrow a^{2^n} \equiv -b^{2^n} \Longleftrightarrow (ab^{-1})^{2^n} \equiv -1 \pmod{p}.$$

Sei d die Ordnung von ab^{-1} modulo p. Dann folgt aus der Kongruenz oben ähnlich wie im letzten Beispiel, dass d kein Teiler von 2^n aber ein Teiler von 2^{n+1} ist (für ersteres braucht man, dass $p \neq 2$ ist, denn sonst gilt $-1 \equiv 1$). Das kann aber nur für $d = 2^{n+1}$ der Fall sein. Ausserdem teilt d wie immer $\varphi(p) = p - 1$, also gilt $p \equiv 1 \pmod{2^{n+1}}$ wie gewünscht. □

Die Aussage sieht doch recht technisch aus, wir schlachten sie daher noch ein bisschen aus. Es folgt nämlich zum Beispiel:

- Sind a und b teilerfremd, dann ist jeder ungerade Primteiler von $a^{2^n}+b^{2^n}$ kongruent zu $1 \pmod{2^{n+1}}$! Das gilt insbesondere im wichtigen Spezialfall $b = 1$.
- Noch spezieller ist der Fall $a = 2, b = 1$. Man erhält die sogenannten Fermat Zahlen $F_n = 2^{2^n} + 1$, von denen Fermat fälschlicherweise vermutete, dass sie alle prim sind. Zum Beispiel besitzt F_5 den Primteiler 641. Trotzdem sind die Primteiler von F_n recht gross, denn sie sind alle $\equiv 1 \pmod{2^{n+1}}$, also sicher nicht kleiner als $2^{n+1}+1$. Dies ist der Grund, wieso die Fermat Zahlen sehr schwierig zu faktorisieren sind.
- Ist $p \equiv 3 \pmod 4$ ein Primteiler von $a^2 + b^2$, dann teilt p sogar a und b.
- Wir haben früher schon gesehen, dass die Pell-Gleichung $x^2 - Dy^2 = -1$ nicht immer eine Lösung besitzt. Wir können jetzt eine starke Bedingung an D ableiten, die erfüllt sein muss, wenn die Gleichung Lösungen besitzt. Umformen liefert nämlich $Dy^2 = x^2 + 1$, daher teilt jeder Primteiler von D die rechte Seite. Also ist jeder ungerade Primteiler von D (und auch von y) $\equiv 1 \pmod 4$.

In allen bisherigen Beispielen konnten wir durch betrachten von Ordnungen Aussagen über die Primteiler verschiedener Zahlen machen. Das ist ganz allgemein das Ziel der Sache. Keine andere Methode, die wir kennengelernt haben, liefert ähnlich starke Aussagen. Daher sind Ordnungen auch ein unverzichtbares technischen Hilfsmittel bei der Lösung von zahlentheoretischen Problemen.

Als letztes Beispiel noch ein bekanntes und nützliches Resultat über die Primteiler von geometrischen Folgen. Wir erinnern daran, dass für $a \neq 1$ und jede natürliche Zahl n die Formel $a^{n-1} + a^{n-2} + \ldots + a + 1 = \frac{a^n-1}{a-1}$ gilt.

Beispiel 14. *Sei p eine Primzahl und $a \neq 1$ eine ganze Zahl. Ist q ein Primteiler von*

$$\frac{a^p - 1}{a - 1}$$

dann gilt $q = p$ oder $q \equiv 1 \pmod p$. Dann kann der Fall $p = q$ nur dann auftreten, wenn $p \mid a - 1$.

Lösung. Sei q ein solcher Primteiler und sei d die Ordnung von a modulo q. Dann gilt $q \mid a^p - 1$, also $a^p \equiv 1 \pmod q$. Daraus folgt $d \mid p$ und da p prim ist also $d = 1$ oder $d = p$. Wir analysieren zuerst den ersten Fall $d = 1$. Dann ist q auch ein Teiler des Nenners $a - 1$, wir berechnen daher den ggT von Zähler und Nenner:

$$\begin{aligned}(a^p - 1, a - 1) &= (a^{p-1} + a^{p-2} + ... + a + 1, a - 1) = (2a^{p-2} + a^{p-3} + ... + a + 1, a - 1)\\ &= (3a^{p-3} + a^{p-4} + ... + a + 1, a - 1) = ... = (pa, a - 1) = (p, a - 1),\end{aligned}$$

denn $a - 1$ ist teilerfremd zu a. Also muss q ein Teiler von p, also gleich p sein. Dies gilt genau dann, wenn $p \mid a - 1$. Im Fall $d = p$ folgt $p = d \mid \varphi(q) = q - 1$, also $q \equiv 1 \pmod p$. □

2.2 Primitive Wurzeln

Sei n eine natürliche Zahl und a teilerfremd zu n. Wir haben gesehen, dass die Ordnung von a modulo n immer ein Teiler von $\varphi(n)$ ist. Wir nennen a eine primitive Wurzel modulo n, falls a die maximal mögliche Ordnung $\varphi(n)$ besitzt. Zum Beispiel rechnet man leicht nach, dass 9 eine primitive Wurzel modulo 17 ist, dass 11 eine primitive Wurzel modulo 18 und dass 2 eine primitive Wurzel modulo 19 ist. Im Gegensatz dazu existiert keine primitive Wurzel modulo 20, denn trotz $\varphi(20) = 8$ gilt stets $a^4 \equiv 1$ wenn a teilerfremd zu 20 ist.

Existiert eine primitive Wurzel a modulo n, dann sind die Potenzen $1, a, a^2, \dots a^{\varphi(n)-1}$ paarweise nicht kongruent $\bmod(n)$ und durchlaufen daher die zu n teilerfremden Restklassen genau einmal. Somit lässt sich das Rechnen mit dieses Restklassen auf das Rechnen mit Potenzen von a zurückführen, was natürlich wesentlich einfacher ist.

Entscheidend für diesen Abschnitt ist nun das folgende Resultat, das wir mit unseren Mitteln leider nicht beweisen können:

Satz 2.2. *Jede Primzahl besitzt eine primitive Wurzel.*

Bevor wir uns der allgemeinen Situation zuwenden, zuerst ein Beispiel für die Nützlichkeit von primitiven Wurzeln.

Beispiel 15 (SMO 03)**.** *Finde die grösste natürliche Zahl n, die für alle ganzen Zahlen a ein Teiler von $a^{25} - a$ ist.*

Lösung. Zuerst zeigen wir, dass n quadratfrei ist. Für jeden Primteiler p von n muss nämlich n nach Voraussetzung ein Teiler von $p^{25} - p = p(p^{24} - 1)$ sein. Dann ist n aber sicher nicht durch p^2 teilbar.
Sei nun p ein Primteiler von n. Sei a eine ganze Zahl, die nicht durch p teilbar ist, und sei d die Ordnung von a modulo p. Wegen $a^{24} \equiv 1 \pmod{p}$ gilt $d \mid 24$ und allgemein haben wir $d \mid \varphi(p) = p - 1$. Wenn d sehr klein ist, gibt dies kaum Informationen über p. Interessant wird die Sache erst, wenn wir d im Verhältnis zu $p - 1$ sehr gross wählen können. Aber genau dies ist der Fall, wenn wir für a eine primitive Wurzel modulo p wählen, dann gilt ja sogar $d = p - 1$ und wir erhalten $p - 1 \mid 24$. Die einzigen Möglichkeiten sind demnach $p = 2, 3, 5, 7, 13$.
Umgekehrt folgt aus dem kleinen Satz von Fermat sofort, dass diese Primzahlen stets Teiler von $a^{25} - a$ sind, wir erhalten also die Lösung $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$. □

Wir stellen nun das Hauptresultat dieses Abschnittes vor, dessen Beweis wir für den interessierten Leser ans Ende des Abschnittes verschieben.

Satz 2.3.

(a) Es existiert genau in den folgenden Fällen eine primitive Wurzel modulo n:

(i) $n = 2, 4$

(ii) $n = p^k$ *für eine Primzahl* $p \geq 3$

(iii) $n = 2p^k$ *für eine Primzahl* $p \geq 3$.

(b) Ist p prim und a eine primitive Wurzel modulo p, dann sind unter den Zahlen $a, a+p, \ldots, a+(p-1)p$ alle ausser genau einer primitive Wurzeln modulo p^2 .

(c) Ist $p \geq 3$ prim und ist a eine primitive Wurzel modulo p^2 , dann ist a auch eine primitive Wurzel modulo p^k für alle natürlichen Zahlen k.

(d) Für $k \geq 3$ hat 5 die Ordnung 2^{k-2} modulo 2^k und es gibt kein Element grösserer Ordnung. Jede ungerade Restklasse $\pmod{2^k}$ *lässt sich eindeutig in der Form $\pm 5^m$ mit $0 \leq m < 2^{k-1}$ schreiben.*

Am meisten mag vielleicht (c) erstaunen: Beispielsweise folgt daraus, dass 2 eine primitive Wurzel modulo allen 3er-Potenzen ist, denn 2 ist eine solche modulo 9. Diese Tatsache erlaubt es uns jetzt, die Lösung von Beispiel 12 sehr einfach zu vervollständigen

Lösung. Wir haben bereits gezeigt, dass $n = 1, 3$ Lösungen sind, und dass jede Lösung $n > 3$ durch 9 teilbar sein muss. Wir schreiben daher $n = 3^k m$ mit $k \geq 1$ und $3 \nmid m$. Nach Voraussetzung gilt $2^n \equiv -1 \pmod{3^{2k}}$ und da 2 eine primitive Wurzel modulo 3^{2k} ist, folgt für den Exponenten $n \equiv 3^{2k-1} \pmod{2 \cdot 3^{2k-1}}$. Das bedeutet aber, dass n durch 3^{2k-1} teilbar sein muss. Nach Definition von k ist somit $2k - 1 \leq k$, also $k = 1$. Dies zeigt, dass keine Lösungen $n > 3$ existieren. □

Der Rest dieses Abschnittes ist dem Beweis von Satz 2.3 gewidmet.
Die folgenden drei technischen Lemmata sind der Schlüssel zu allem. Wir bezeichnen die Ordnung von a modulo n abkürzend mit $\mathrm{ord}_n(a)$.

Lemma 2.4.

(a) Ist n eine natürliche Zahl und ist a teilerfremd zu n, dann gilt

$$\mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{\mathrm{ggT}(\mathrm{ord}_n(a), k))}.$$

(b) Sind $n_1, \ldots, n_k$ paarweise teilerfremde natürliche Zahlen und ist a teilerfremd zu $n_1 \ldots n_k$, dann gilt

$$\mathrm{ord}_{n_1 \cdots n_k}(a) = kgV(\mathrm{ord}_{n_1}(a), \ldots, \mathrm{ord}_{n_k}(a)).$$

(c) Ist $n_1 \mid n_2$ und a teilerfremd zu n_2 , dann gilt

$$\mathrm{ord}_{n_1}(a) \mid \mathrm{ord}_{n_2}(a) \quad \textit{und} \quad \frac{\mathrm{ord}_{n_2}(a)}{\mathrm{ord}_{n_1}(a)} \,\Big|\, \frac{\varphi(n_2)}{\varphi(n_1)}$$

Beweis.

(a) Es gilt $(a^k)^m \equiv 1$ genau dann, wenn $\mathrm{ord}_n(a) \mid km$. Die kleinste natürliche Zahl m mit dieser Eigenschaft ist aber $m = \frac{\mathrm{ord}_n(a)}{ggT(\mathrm{ord}_n(a),k)}$.

(b) Es gilt $a^m \equiv 1 \pmod{n_1 \dots n_k}$ genau dann, wenn $a^m \equiv 1 \pmod{n_i}$ gilt für $1 \leq i \leq k$. Letzteres ist genau dann der Fall, wenn m durch $\mathrm{ord}_{n_1}(a), \dots, \mathrm{ord}_{n_k}(a)$ teilbar ist und die kleinste natürliche Zahl mit dieser Eigenschaft ist $m = kgV(\mathrm{ord}_{n_1}(a), \dots, \mathrm{ord}_{n_k}(a))$.

(c) Ist $a^m \equiv 1 \pmod{n_2}$, dann natürlich auch $a^m \equiv 1 \pmod{n_1}$, dies zeigt $\mathrm{ord}_{n_1}(a) \mid \mathrm{ord}_{n_2}(a)$. Für den zweiten Teil können wir uns induktiv auf den Fall beschränken, wo $\frac{n_2}{n_1} = p$ eine Primzahl ist. Gilt $a^m \equiv 1 \pmod{n_1}$, dann ist $a = 1 + bn_1$ mit einer ganzen Zahl b. Wir betrachten nun zwei Fälle:

(i) Wenn n_1 durch p teilbar ist, dann gilt $\frac{\varphi(n_2)}{\varphi(n_1)} = p$. Nun ist

$$a^{mp} = (1 + bn_1)^p = 1 + bpn_1 + \sum_{i=2}^{p} \binom{p}{i} b^i n_1^i \equiv 1 \pmod{n_2},$$

denn alle Summanden ausser dem ersten sind durch n_2 teilbar (beachte: $n_2 \mid n_1^2$). Dies zeigt $\mathrm{ord}_{n_2}(a) \mid p\,\mathrm{ord}_{n_1}(a)$.

(ii) Wenn n_1 nicht durch p teilbar ist, dann gilt $\frac{\varphi(n_2}{\varphi(n_1)} = p - 1$. Da a nach Voraussetzung nicht durch p teilbar ist, gilt sicher $a^{p-1} \equiv 1 \pmod{p}$ und somit ist $a^{m(p-1)} \equiv 1 \pmod{n_2}$, also wieder $\mathrm{ord}_{n_2}(a) \mid (p-1)\,\mathrm{ord}_{n_1}(a)$.

□

Lemma 2.5. *Sei p eine Primzahl, $1 \leq b \leq p-1$ eine natürliche Zahl und sei a eine primitive Wurzel modulo p. Dann ist a oder $a + bp$ eine primitive Wurzel modulo p^2.*

Beweis. Nach Voraussetzung und Lemma 2.4 (c) haben a und $a + bp$ die Ordnung $p - 1$ oder $p(p-1) modulo p^2$. Wir nehmen nun an, beide Zahlen hätten die Ordnung $p - 1$. Dann gilt aber $\pmod{p}$

$$1 \equiv (a + bp)^{p-1} = a^{p-1} + (p-1) \cdot a^{p-2}bp + \sum_{i=2}^{p-1} \binom{p-1}{i} a^{p-1-i} b^i p^i$$

$$a^{p-1} - a^{p-2}bp \equiv 1 - a^{p-2}bp,$$

also müsste $a^{p-2}b$ durch p teilbar sein, Widerspruch. □

Lemma 2.6. *Sei p eine Primzahl und k eine natürliche Zahl mit $k \geq 2$ falls $p \geq 3$ bzw. $k \geq 3$ falls $p = 2$. Sei a teilerfremd zu p, dann gilt*

$$\left.\begin{aligned} \mathrm{ord}_{p^{k-1}}(a) &= (p-1)p^{m-1} \\ \mathrm{ord}_{p^k}(a) &= (p-1)p^m \end{aligned}\right\} \Longrightarrow \mathrm{ord}_{p^{k+1}}(a) = (p-1)p^{m+1}$$

Beweis. Nach Voraussetzung gilt $a^{(p-1)p^{m-1}} \equiv 1 \pmod{p^{k-1}}$ und $a^{(p-1)p^{m-1}} \not\equiv 1 \pmod{p^k}$. Daraus folgt

$$a^{(p-1)p^{m-1}} = 1 + bp^{k-1} \quad mit p \nmid b.$$

Nach Voraussetzung und Lemma 2.4 (c) ist $\mathrm{ord}_{p^{k+1}}(a)$ entweder gleich $(p-1)p^m$ oder gleich $(p-1)p^{m+1}$. Wir nehmen ersteres an und führen dies zu einem Widerspruch. Dann wäre nämlich

$$\begin{aligned} 1 \equiv (a^{(p-1)p^{m-1}})^p &= (1 + bp^{k-1})^p \\ &= 1 + p \cdot bp^{k-1} + \sum_{i=2}^{p} \binom{p}{i} b^i p^{i(k-1)} \pmod{p^{k+1}} \\ &\equiv 1 + bp^k. \end{aligned}$$

Dabei gilt die letzte Kongruenz, weil alle Terme in der Summe durch p^{k+1} teilbar sind: Für $i \geq 3$ folgt dies aus $i(k-1) \geq k+1$ wegen $k \geq 2$ und für $i = 2$ folgt dies aus $k \geq 3$ falls $p = 2$ und aus $p \mid \binom{p}{2}$ falls $p \geq 3$. Obige Kongruenz zeigt aber, dass b durch p teilbar sein muss, ein Widerspruch. □

Wir kommen nun zum Beweis von Satz 2.3:

(c) Ist $k \geq 2$ und ist a eine primitive Wurzel modulo p^k , dann gilt $\mathrm{ord}_{p^{k-1}}(a) = (p-1)p^{k-2}$ und $\mathrm{ord}_{p^k}(a) = (p-1)p^{k-1}$. Also sind die Voraussetzungen von Lemma 2.6 für $m = k-1$ erfüllt und die Aussage desselben ist gerade, dass a auch eine primitive Wurzel modulo p^{k+1} ist. Die Behauptung folgt jetzt induktiv.

(a) Wir zeigen zunächst, dass in den Fällen (i) bis (iii) primitive Wurzeln existieren. Für (i) ist das klar. Für (ii) garantiert Satz 2.2 die Existenz einer solchen für p, Lemma 2.5 für p^2 und (c) für alle höheren Potenzen. Für (iii) beachte man $\varphi(2p^k) = \varphi(p^k)$. Somit ist jede ungerade primitive Wurzel modulo p^k auch eine solche modulo $2p^k$ (d.h. man wählt einfach eine primitive Wurzel modulo p^k und addiert gegebenenfalls p^k dazu).
Ist umgekehrt n nicht vom Typ (i)-(iii), dann ist n entweder eine 2er-Potenz ≥ 8 oder ein Produkt zweier teilerfremder Zahlen $n_1, n_2 \geq 3$. Im ersten Fall kann n keine primitive Wurzel besitzen, weil schon 8 keine hat. Im zweiten Fall sind $\varphi(n_1)$ und $\varphi(n_2)$ beide gerade und mit Lemma 2.4 (b) folgt für jede zu n teilerfremde Zahl a

$$\mathrm{ord}_n(a) = kgV(\mathrm{ord}_{n_1}(a), \mathrm{ord}_{n_2}(a)) \leq kgV(\varphi(n_1), \varphi(n_2)) < \varphi(n_1)\varphi(n_2) = \varphi(n).$$

Also ist a keine primitive Wurzel modulo n.

(d) Es gilt $\mathrm{ord}_8(5) = 2$ und $\mathrm{ord}_1 6(5) = 4$. Ähnlich wie im Beweis von (c) folgt daraus mit Lemma 2.6 induktiv $\mathrm{ord}_{2^k}(5) = 2^{k-2}$ für alle $k \geq 3$. Dies ist nach (a) ausserdem die grösstmögliche Ordnung. Wir zeigen als nächstes, dass $-1 \not\equiv 5^m \pmod{2k}$ gilt für alle m und alle $k \geq 2$. Sonst wäre nämlich sogar $1 \equiv 5^m \equiv 1 \pmod 4$, ein Widerspruch. Somit sind die 2^{k-1} Restklassen $\pm 5^m$ mit $0 \leq m < 2^{k-2}$ paarweise

verschieden und müssen somit alle ungeraden Restklassen $\pmod{2^k}$ genau einmal durchlaufen.

(b) Aus Lemma 2.5 folgt sofort, dass *mindestens* $p-1$ der Zahlen $a, a+p, \ldots, a+(p-1)p$ primitive Wurzel modulo p^2 ist. Insgesamt gibt es aber $\varphi(\varphi(p)) = \varphi(p-1)$ primitive Wurzeln modulo p und $\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$ solche modulo p^2 , also *genau* $p-1$ mal so viele. Wären also für ein a wie oben alle p Zahlen primitive Wurzeln modulo p^2, dann gäbe es insgesamt zu viele davon, ein Widerspruch.

3 Varia

3.1 Die Gaussklammer

Für eine reelle Zahl x bezeichnet $\lfloor x \rfloor$ die grösste ganze Zahl $\leq x$. Zum Beispiel gilt $\lfloor 5 \rfloor = 5$, $\lfloor -2.6 \rfloor = -3$ und $\lfloor \pi \rfloor = 3$. Man nennt $\lfloor \cdot \rfloor$ auch *Gaussklammer*. Die ganze Zahl $\lfloor x \rfloor$ ist eindeutig bestimmt durch die Ungleichungen

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Man kann diese auch umschreiben zu

$$x - 1 < \lfloor x \rfloor \leq x.$$

Für eine reelle Zahl x bezeichnet $\{x\} = x - \lfloor x \rfloor$ den *gebrochenen Teil* von x. Zum Beispiel gilt $\{-3.1\} = 0.9$, $\{\pi\} = 0.1415\ldots$, insbesondere ist stets $\{x\} \geq 0$ mit Gleichheit genau dann, wenn x ganz ist.

Eine wichtige Beobachtung bei der Lösung von Problemen, wo Gaussklammern involviert sind, ist folgende: Zwischen zwei aufeinanderfolgenden ganzen Zahlen liegt keine weitere. Dies führt auf folgendes erstaunliches Resultat:

Beispiel 16. *Seien α und β positive* irrationale *Zahlen mit $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Dann enthalten die beiden Folgen $\lfloor \alpha m \rfloor$ und $\lfloor \beta n \rfloor$ zusammen jede natürliche Zahl genau einmal.*

Lösung. Wir zeigen zuerst, dass die beiden Folgen disjunkt sind. Nehme also an, es gelte $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor = q$. Dann gilt $q < \alpha m < q+1$ sowie $q < \beta$n$< q+1$, dabei stehen die strikten Ungleichheitszeichen, da α und β irrational sind. Folglich gilt

$$\frac{m}{q+1} < \frac{1}{\alpha} < \frac{m}{q}, \qquad \frac{n}{q+1} < \frac{1}{\beta} < \frac{n}{q}.$$

Addition dieser Ungleichungen liefert

$$\frac{m+n}{q+1} < 1 < \frac{m+n}{q} \quad \Rightarrow \quad q < m+n < q+1,$$

was nicht möglich ist. Also gilt $\lfloor \alpha m \rfloor \neq \lfloor \beta n \rfloor$.
Nun zeigen wir, dass jede natürliche Zahl in einer der beiden Folgen vorkommt. Nehme an, die Zahl q komme nicht vor. Dann gibt es nichtneqative ganze Zahlen m und n mit

$$\alpha m < q < q+1 < \alpha(m+1), \qquad \beta n < q < q+1 < \beta(n+1).$$
$$\frac{m}{q} < \frac{1}{\alpha} < \frac{m+1}{q+1}, \qquad \frac{n}{q} < \frac{1}{\beta} < \frac{n+1}{q+1}.$$

Addition dieser Ungleichungen ergibt

$$\frac{m+n}{q} < 1 < \frac{m+n+2}{q+1} \quad \Rightarrow \quad m+n < q < q+1 < m+n+2.$$

Dies ist ein Widerspruch, da zwischen $m+n$ und $m+n+2$ keine zwei ganzen Zahlen Platz haben. □

Beispiel 17. *Zeige, dass die Folge $a_n = \lfloor n + \sqrt{n} + 1/2 \rfloor$ alle natürlichen Zahlen enthält, ausser die Quadratzahlen.*

Lösung. Nehme an, m komme in der monotonen Folge a_n nicht vor. Dann gibt es eine natürliche Zahl n mit

$$n + \sqrt{n} + \frac{1}{2} < m < m+1 < n+1+\sqrt{n+1} + \frac{1}{2}.$$

Daraus folgt der Reihe nach

$$\begin{aligned} & \sqrt{n} < m - n - \frac{1}{2} < \sqrt{n+1} \\ \Rightarrow \quad & n < (m-n)^2 - (m-n) + \frac{1}{4} < n+1 \\ \Rightarrow \quad & n - \frac{1}{4} < (m-n)^2 - (m-n) < n + \frac{3}{4}, \end{aligned}$$

und daher $(m-n)^2 - (m-n) = n$, also ist $m = (m-n)^2$ eine Quadratzahl. Der Beweis wird nun durch ein einfaches Zählargument abgeschlossen. Es gibt genau k positive Quadratzahlen $\leq k^2 + k$ und genau k^2 Zahlen der Form $\lfloor n + \sqrt{n} + 1/2 \rfloor$. Also ist $\lfloor n + \sqrt{n} + 1/2 \rfloor$ die n-te Nichtquadratzahl. □

Es gibt einige Grössen, die sich bequem mit Hilfe der Gaussklammer hinschreiben lassen.

- Die Anzahl natürlicher Zahlen $\leq n$, die durch a teilbar sind, ist gleich $\left\lfloor \frac{n}{a} \right\rfloor$.
- Sei p eine Primzahl. Die grösste p-Potenz, die $n!$ teilt, ist gleich

  $$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

  Denn es gibt genau $\left\lfloor \frac{n}{p} \right\rfloor$ Vielfache von p, die $\leq n$ sind. Jede dieser Zahlen liefert einen Faktor p in der Primfaktorzerlegung von $n!$. Nun sind aber genau $\left\lfloor \frac{n}{p^2} \right\rfloor$ dieser Zahlen sogar durch p^2 teilbar und liefern einen weiteren Faktor p, usw.

Natürlich ist die Gaussklammer nicht additiv, das heisst, im Allgemeinen ist $\lfloor x+y \rfloor \neq \lfloor x \rfloor + \lfloor x \rfloor$. Es gelten jedoch die wichtigen Hermitschen Identitäten:

Satz 3.1. *Für jede natürliche Zahl n und jede reelle Zahl x gilt*

$$\lfloor nx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \ldots + \left\lfloor x + \frac{n-1}{n} \right\rfloor.$$

Beweis. Wähle k so, dass gilt $\frac{k}{n} \leq \{x\} < \frac{k+1}{n}$. Die linke Seite hat dann den Wert $n\lfloor x \rfloor + k$. Auf der rechten Seite haben die ersten $n-k$ Summanden den Wert $\lfloor x \rfloor$, die übrigen k den Wert $\lfloor x \rfloor + 1$. Daraus folgt die Behauptung. □