Elementary Number Theory

Dr. Michael Woodbury

Inhaltsverzeichnis

Diese Notizen befinden sich die Definitionen und Sätze des Kurses: „Elementary Number Theory" des Sommersemesters an der Universität zu Köln. Hier findet man normalerweise keine Beweisen, aber manchmal die Idee dabei. Man kann die Beweisen aus fast jedem Zahlentheoriebuch finden, aber wäre es besser, wenn man ohne Hilfe zu beweisen versuchen würde. Auf jeden Fall, wir besprechen alles während der Vorlesungen.

1. 11 April

Man versucht in der Zahlentheorie Fragen über die natürlichen Zahlen $\mathbb{N} = \{1, 2, \ldots\}$ zu beantworten. Die ganzen Zahlen $\mathbb{Z}$, der Körper $\mathbb{Q}$, und oftmals andere Ringen und Körper sind oft hilfreich darum.

Zwei Fragen von Zahlentheorie:

- Welche $n \in \mathbb{N}$ können als Summe von zwei Quadrate geschrieben werden? (Einfacher: für welche Primzahlen p kann man $a, b \in \mathbb{Z}$ finden, damit $p = a^2 + b^2$ ist?)
- Kann man jeden PPT[1] (a, b, c) ausschreiben?[2] Definition: $(a, b, c) \in \mathbb{N}^3$ ist eine *PPT*, falls $a^2 + b^2 = c^2$ und $\mathrm{ggT}(a, b, c) = 1$.

2. 14 April

Bekanntes

- $\mathbb{Z}$ ist mit gewöhnlicher Addition und Multiplikation ein kommutativer Ring mit Eins 1.

  Zur Erinnerung
  Ein *Ring* R ist eine nichtleere Menge mit zwei binären Operationen $+$ und $\cdot$, so dass gilt

  (i) $(R, +)$ abelsche Gruppe
  - abg. bzgl. Addition
  - Assoziativitätsgesetz
  - Neutrales Element 0
  - Inverses
  - abelsch $a + b = b + a \qquad \forall a, b \in R$

[1] auf Englisch: PPT=primitive Pythagorean triple.

[2] Wir haben $(3, 4, 5)$ und $(5, 12, 13)$, die PPTs sind. Gibt es andere? Wie viele?

(ii) Assoziativitätsgesetz für Multiplikation

(iii) Distributivgesetz

$$(a+b)c = ac + bc$$

kommutativer Ring:

$$ab = ba \qquad \forall a, b \in R$$

Ring mit Eins 1:

$$1 \cdot a = a = a \cdot 1 \qquad \forall a \in R$$

- $\mathbb{Z}$ ist *Integritätsring*

$$a, b \in \mathbb{Z} \qquad ab = 0 \Rightarrow a = 0 \text{ oder } b = 0$$

(wenn dies nicht gelten würde, hießen a, b *Nullteiler.*)

- Wohlordnungsprinzip ($\mathbb{N}$ pos. ganze Zahlen)
Es sei $A \subset \mathbb{N}, A \neq \emptyset$
Dann gibt es ein kleinstes Element in A, d.h. $\exists a \in A$, so dass $a \leq x \quad \forall x \in A$.

Satz 2.1 (Divisionsalgorithmus)**.** *Für $a \in \mathbb{N}, b \in \mathbb{Z}$ existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $b = qa + r$ und $0 \leq r < a$.*

Idee des Beweises: Die Menge $A = \{b - qa \mid q \in \mathbb{Z}, b - qa \geq 0\}$ ist nicht leer. Sei $r \in A$ das kleinstes element. □

Definition. Es sei R ein kommutativer Ring, $a, b \in R$.
a heißt ein *Teiler von b* (*b ist durch a teilbar*, *b ist ein Vielfaches von a*), wenn es ein $q \in R$ gibt mit $b = qa$.
Zeichen:

$$a|b \leftrightarrow a \nmid b$$

Bemerkung. Falls R ein Integritätsring ist, $a \neq 0$, $a|b$, so gibt es genau ein $q \in R$, so dass $b = qa$.

Satz 2.2. *Es sei R ein kommutativer Ring mit Eins $1, a, b, c, d, u, v \in R$. Dann gilt:*

(1) $1 \mid a, a \mid a, a \mid 0$.

(2) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*

(3) *Aus $d \mid a$ und $d \mid b$ folgt $d \mid (ua + vb)$.*

(4) *Aus $a \mid b$ folgt $a \mid bc$ und $ac \mid bc$.*

(5) *Aus $0 \mid a$ folgt $a = 0$.*

Sei R nun ein Integritätsring. Dann gilt:

(6) *Aus* $av \mid bv$ *und* $v \neq 0$ *folgt* $a \mid b$.

In $R = \mathbb{Z}$ *gilt:*

(7) *Die einzigen Teiler von* 1 *sind* ± 1.

(8) *Wenn* $a \mid b$ *und* $b \mid a$, *dann gilt* $a = \pm b$.

(9) *Wenn* $a \mid b$ *und* $b \neq 0$, *dann* $|a| \leq |b|$.

Beweis: z.B. (6)

$$bv = qav \Rightarrow (b - qa)v = 0 \Rightarrow b - qa = 0 \Rightarrow b = qa \Rightarrow a \mid b.$$

□

Definition. Jede natürliche Zahl n hat die Teiler 1 und n. Falls $p > 1$ nur die Teiler 1 und p hat, so heißt p eine *Primzahl*.
(1 wird nicht als Primzahl angesehen. → Probleme z.B. bei eindeutiger Primzahlzerlegung, die wir später zeigen.)

Satz 2.3. *Jede natürliche Zahl* $n > 1$ *kann als Produkt von endlich vielen Primzahlen dargestellt werden.*

Beweis: Induktiv. $n = 2$ ist eine Primzahl. Sei $n > 2$ und jede Zahl $m \in \mathbb{N}$ mit $2 \leq m < n$ sei Produkt endlich vieler Primzahlen. Falls n eine Primzahl ist, sind wir fertig. Sonst hat n einen Teiler m_1 mit $2 \leq m_1 < n$, $n = m_1 m_2$, $2 \leq m_2 < n$. Nach Induktionsvorraussetzung sind sowohl m_1 und m_2 Produkte endlich vieler Primzahlen, also auch $n = m_1 m_2$. □

Satz 2.4. *Es gibt unendlich viele Primzahlen.*

Beweis (Euklid): Seien $p_1, \ldots, p_r$ Primzahlen. Dann ist $N = p_1 \cdots p_r + 1$ ist durch keine der Zahlen $p_1, \ldots, p_r$ teilbar. Nach Satz 2.3 besitzt N einen Primteiler, der von $p_1, \ldots, p_r$ verschieden ist. □

Definition. Es sei R ein kommutativer Ring mit $1, a_1, \ldots, a_m \in R$. Ein Element $d \in R$ heißt ein *gemeinsamer Teiler* von $a_1, \ldots, a_m$ falls $d \mid a_k$, $1 \leq k \leq m$. Gilt außerdem für jeden weiteren Teiler δ von $a_1, \ldots, a_r$, dass $\delta \mid d$, so heißt d **ein** *größter gemeinsamer Teiler* von $a_1, \ldots, a_m$. Man schreibt $d = \mathrm{ggT}(a_1, \ldots, a_m)$.
Ist 1 ein größter gemeinsamer Teiler von $a_1, \ldots, a_m$, so heißen $a_1, \ldots, a_m$ *teilerfremd*.
Man nennt $a_1, \ldots, a_m$ *paarweise teilerfremd* falls

$$\mathrm{ggT}(a_j, a_k) = 1 \quad j, k \in \{1, \ldots, m\}, j \neq k.$$

Ein $t \in R$ heißt *gemeinsames Vielfaches* von $a_1, \ldots, a_m$ falls $a_k \mid t$ für $1 \leq k \leq m$.
Falls außerdem für jedes gemeinsame Vielfache s von $a_1, \ldots, a_m$ auch $t \mid s$ gilt, so heißt t ein *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_m$. Man schreibt $t = \mathrm{kgV}(a_1, \ldots, a_m)$.

3. 18 April

Es sei R ein Ring mit 1. Ein element $u \in R$ heißt eine *Einheit* falls es $v \in R$ gibt, damit $uv = 1$ gilt. Die Menge aller Einheiten heißt die *Einheitengruppe*. Man schriebt

$$R^\times = \{u \in R \mid u \text{ ist eine Einheit}\}.$$

Ein *Körper* ist ein kommutativer Ring K mit $K^\times = K \setminus \{0\}$.

Beispiele von Ringen:

- $\mathbb{Z}$: die einzigen Einheiten sind ± 1.
- Die Gaußchen Zahlen: $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ mit $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
- Falls R ein Ring ist und $n \in \mathbb{N}$, dann ist

$$M_n(R) := \left\{ \left(\begin{array}{ccc} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \\ a_{n1} & \cdots & a_{nn} \end{array} \right) \middle| \, a_{ij} \in R \right\}.$$

  ein Ring.

- Falls R ein Ring ist, dann ist

$$R[x] := \{a_0 + a_1 x + \cdots a_n x^n \mid n \in \mathbb{N}_0, a_j \in R\}$$

  ein Ring. Wir nehnen $R[x]$ *Ring der Polynome in einer Variablen über* R.

Satz 3.1 (Euklidischer Algorithmus)**.** *Es seien $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Dann gibt es ganze Zahlen $k \geq 0$ und $r_1, \ldots, r_k,\ q_1, \ldots, q_{k+1}$ mit*

$$\begin{array}{lcll} a & = & bq_1 + r_1 & 0 < r_1 < b \\ b & = & r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 & 0 < r_3 < r_2 \\ & \vdots & & \\ r_{k-2} & = & r_{k-1} q_k + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} & = & r_k q_{k+1} & \end{array}$$

Es gilt: $r_k = \mathrm{ggT}(a, b)$.
Man erhält eine Lösung $x, y \in \mathbb{Z}$ von $ax + by = \mathrm{ggT}(a, b)$, indem man aus der Gleichungskette $r_{k-1}, r_{k-2}, \ldots, r_1$ eliminiert.

Idee des Beweises: Falls $g \mid a, b$, benutzt man mehrmalig Satz 2.2 um $g \mid r_k$ zu zeigen. Genauso, zeigt man dass $r_k \mid a, b$. □

Satz 3.2. *Es seien $a, b \in \mathbb{Z}$ und $a \neq 0$. Dann gilt*

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \mathrm{ggT}(a, b)\mathbb{Z} = \{n \,\mathrm{ggT}(a, b) \mid n \in \mathbb{Z}\}.$$

Satz 3.3. *Es seien $a, b \in \mathbb{Z}$, und $x_0, y_0 \in \mathbb{Z}$ so dass $ax_0 + by_0 = \mathrm{ggT}(a, b)$. Dann ist jede Lösung $(x, y) \in \mathbb{Z}^2$ der Form*

$$\left(x_0 - \frac{ak}{\mathrm{ggT}(a,b)}, y_0 + \frac{bk}{\mathrm{ggT}(a,b)}\right)$$

mit $k \in \mathbb{Z}$.

4. 21 April

Satz 4.1. *Es seien $a_1, \ldots, a_r \in \mathbb{Z}$, p Primzahl. Wenn $p \mid a_1 a_2 \cdots a_r$, dann folgt $a \mid a_j$ für einege $1 \leq j \leq r$.*

Idee des Beweises: Für $r = 1$ ist die Behauptung richtig. Sei $p \mid a_1 a_2 \cdots a_r$, $p \nmid a_1$. Schreibe $a = a_1$ und $b = a_2 \cdots a_r$. Nach Satz 3.1 gibt es $x, y \in \mathbb{Z}$, so dass $ax + py = 1$. Multiplikation mit b ergibt

$$abx + pby = b.$$

Nach Satz 2.3(3) folgt $p \mid b$. Nach Induktionsvorraussetzung folgt die Behauptung. □

Definition. Ein Integritätsring R heißt *euklidischer Ring*, falls es eine Gradfunktion $g : R \setminus \{0\} \to \mathbb{N}_0$ gibt, so dass in R der folgende Divisionsalgorithmus besteht:
Zu beliebigen $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit $a = qb + r$ wobei $r = 0$ oder $g(r) < g(b)$ ist.

Definition. Sei R ein kommutativer Ring mit 1. Ein $x \in R$ heißt *irreduzibel* oder *unzerlegbar*, falls $x \neq 0$ und $x \notin R^\times$ ist und falls jeder Teiler von x entweder Einheit oder assoziiert zu x ist. Ein $x \in R$ heißt *prim* oder *Primelement*, falls $x \neq 0$ und $x \notin R^\times$ und falls aus $a, b \in R$ und $x \mid ab$ stets folgt, dass $x \mid a$ oder $x \mid b$.

Bemerkungen.

(1) Jedes Primelement ist irreduzibel.

(2) Nach Satz 4.1 ist in $\mathbb{Z}$ jedes irreduzible Element prim, dies gilt auch in einem beliebigen euklidischen Ring.

Definition. Ist a eine ganze zu N teilerfremde Zahl, so heißt $\overline{a}$ eine *prime Restklasse* oder *teilerfremde Restklasse*. (Wohldefiniert, da mit a auch $a + rN$ teilerfremd zu N ist.) Bezeichne mit $\varphi(N)$ die Anzahl der primen Restklassen *Eulersche Phi-Funktion*.

Beispiel. Es sei $N = 6$. Dann sind $1, 5$ die primen Restklassen, also $\varphi(6) = 2$.

Es sei $N = 12$. Dann sind $1, 5, 7, 11$ die primen Restklassen, also $\varphi(12) = 4$.

Die Menge $\{a_1, , \ldots, a_r\} \subset \mathbb{Z}$, $(a_i, N) = 1$ heißt ein *primes Restsystem* oder *reduziertes Restsystem modulo N*, wenn es zu jedem $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, N) = 1$ genau ein $1 \leq j \leq r$ gibt, so dass $a \equiv a_j \pmod{N}$.

Beispiel. $\{1, 5, 7, 11\}$ ist ein primes Restsystem modulo 12.

Bemerkung. Man verwendet Restklassen um zu zeigen, dass es keine Lösungen $(x, y) \in \mathbb{Q}$ zu $x^2 + y^2 = 3$ gibt. Idee: eine Lösung existiert genauso wenn es $(a, b, c) \in \mathbb{Z}^3$ gibt mit $\text{ggT}(a, b, c) = 1$ und

$$a^2 + b^2 = 3y^2.$$

Die Restklassen von Quadraten modulo 4 sind:

$a \pmod 4$	$a^2 \pmod 4$
0	0
1	1
2	0
3	1

Nach $a^2 + b^2 \equiv 3c^2$ folgt $a^2, b^2, c^2 \equiv 0 \pmod 4$. Das ist troztdem ein Widerspruch, da a, b, c gerade sein müssen, um diese Kongruenzen zu gelten.

5. 25 April

Beispiel. Restklassen werden auch bunutzt zu zeigen: Sei $n \in \mathbb{N}$. Dann gilt $3 \mid n$, genauso wenn 3 die Summe der von n teilt. Dass heißt,

$$3 \mid n = \sum_{j=1}^{N} a_j 10^j (0 \leq a_j \leq 9) \quad \leftrightarrow \quad 3 \Big| \sum_{j=1}^{N} a_j$$

gilt.

Definition. Eine *Gruppe* $(G, \star)$ ist eine Menge G und eine binären Operation

$$\star : G \times G \to G \qquad (\text{man schreibt } g \star h := \star(g, h)),$$

so dass Folgendes gilt.

- (Associativitätsgesetz) $a \star (b \star c) = (a \star b) \star c$ für alle $a, b, c \in G$.
- (Neutrales Element) Es gibt $e \in G$, damit $e \star g = g \star e = g$ für alle $g \in G$ gilt.
- (Inverses) Für jedes $g \in G$ existiert es $g' \in G$, damit $g \star g' = g' \star g = e$.

Beispiel.

- Sei $N \in \mathbb{Z}$, $N > 1$. Dann ist $(\mathbb{Z}/N\mathbb{Z}, +)$ eine Gruppe mit $a + b := a + b \pmod N$.
- Sei $N \in \mathbb{Z}$, $N > 1$. Dann ist $(\mathbb{Z}/N\mathbb{Z}^\times, \cdot)$ eine Gruppe mit $a \cdot b := ab \pmod N$.

Satz 5.1.

(1) *G sei eine endliche Gruppe, e das neutrale Element und m ihre Ordnung. Dann gilt: $a^m = e$ für alle $a \in G$.*

(2) Eulerscher Satz
Für alle $N \in \mathbb{N}$ *und alle* $a \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a, N) = 1$ *gilt*

$$a^{\varphi(N)} \equiv 1 \pmod{N}.$$

(3) Kleiner Fermatscher Satz
Ist p *eine Primzahl, so gilt* $a^{p-1} \equiv 1 \pmod{p}$ *für alle* $a \in \mathbb{Z}$ *mit* $p \nmid a$ *und es gilt* $a^p \equiv a \pmod{p}$ *für alle* $a \in \mathbb{Z}$.

Idee des Beweises: Sei G eine abelsche Gruppe mit $n = \#G$ und $G = \{g_1, \cdots, g_n\}$. Für jedes $g \in G$ merkt man, dass $G = \{g \star g_1, \cdots, g \star g_n\}$. Dann findet man dass

$$g^n \star (g_1 \star g_2 \star \cdots \star g_n) = (g \star g_1) \star (g \star g_2) \star \cdots \star (g \star g_n) = g_1 \star g_2 \star \cdots \star g_n$$

gilt, da G abelsche ist. Es folgt $g^n = e$.

Teile (2) und (3) folgen nach (1) mit $(G, \star) = (\mathbb{Z}/N\mathbb{Z}^\times, \cdot)$ bzw. $(G, \star) = (\mathbb{Z}/p\mathbb{Z}^\times, \cdot)$. □

Bemerkung. Satz 5.1(1) gilt für *alle* endlichen Gruppen. Der Beweis davon ist nicht besonders schwer nur länger, aber wir brauchen in diesem Kurs so einen allgemeinen Satz nicht.

6. 28 April

Definition. Seien $n > 1$, $b > 1$ natürliche Zahlen. n heißt *pseudoprim zur Basis* b, falls n nicht prim ist und $b^n \equiv b \pmod{n}$. Man nennt n *pseudoprim*, falls n pseudoprim zur Basis 2 ist.

Beispiel. Alle Pseudoprimzahlen unter 2000 sind: $341, 561, 645, 1105, 1387, 1729, 1905$.
Lehmer (1950) fand die erste gerade Pseudoprimzahl: 161038.
Beeger (1951): Es gibt unendlich viele gerade Pseudoprimzahlen (wir werden dies später zeigen).

Definition. $n \in \mathbb{N}$ heißt *vollkommen*, falls n gleich der Summe seiner positiven Teiler $d < n$ ist. Also ist n vollkommen $\Leftrightarrow \sigma(n) = 2n$, wobei

$$\sigma(n) = \sum_{\substack{d|n \\ d>0}} d.$$

Beispiel.

$$6 = 1 + 2 + 3,$$
$$28 = 1 + 2 + 4 + 7 + 14.$$

Satz 6.1.

(1) *Wenn p eine Primzahl der Form $p = 2^N - 1$ mit $N \in \mathbb{N}$ ist, dann ist $n = 2^{N-1}p$ vollkommen.*

(2) *Wenn n eine gerade vollkommene Zahl ist, dann ist $n = 2^{N-1}(2^N - 1)$ mit $N \in \mathbb{N}$, wobei $2^N - 1$ prim ist.*

Beispiele.

$$6 = (2^2 - 1)2,$$
$$28 = (2^3 - 1)2^2,$$
$$496 = 31 \cdot 16 = (2^5 - 1)2^4.$$

Fragen.

(1) Gibt es ungerade vollkommene Zahlen?
Unklar. Vermutung, dass es keine gibt.

(2) Für welche n ist $2^n - 1$ prim?
(Satz 6.1 führt die Suche nach geraden vollkommenen Zahlen zurück auf Primzahlen der Form $2^n - 1$.)
Für $a > 1$, $b > 1$ gilt:

$$x^{ab} - 1 = (x^a - 1)\big(x^{a(b-1)} + x^{a(b-2)} + \ldots + x^a + 1\big).$$

Daher ist $2^{ab} - 1$ nicht prim. Für p Primzahl heißt $M_p = 2^p - 1$ *eine Mersennesche Zahl*. Falls M_p prim ist, heißt M_p *eine Mersennesche Primzahl*.

Beispiel. M_2, M_3, M_5, M_7 sind prim, aber $M_{11} = 2047 = 23 \cdot 89$ ist nicht prim.

Satz 6.2.

(1) *Es sei $n \in \mathbb{N}$ mit $2^n \equiv 2 \pmod{n}$. Dann ist auch $2^{M_n} \equiv 2 \pmod{M_n}$ für $M_n = 2^n - 1$.*

(2) *Ist p eine Primzahl, dann ist M_p prim oder pseudoprim.*

(3) *Ist n pseudoprim, dann ist auch M_n pseudoprim.*

(4) *Es gibt unendlich viele Pseudoprimzahlen (zur Basis 2).*

Beweis:

(1) $n = 1$ folgt, da $M_1 = 1$.
Sei nun $n > 1$ und $2^n = 2 \pmod{n}$. Das heißt $2^n = 2 + kn$ für ein $k \in \mathbb{N}$. Dann ist $2^{M_n} = 2^{2^n - 1} = 2 \cdot 2^{kn}$. Also

$$\begin{aligned} 2^{M_n} - 2 &= 2(2^{kn} - 1) = 2(2^n - 1)\big(2^{(k-1)n} + 2^{(k-2)n} + \ldots + 2^n + 1\big) \\ &= 2M_n\big(2^{(k-1)n} + \ldots + 2^n + 1\big) \equiv 0 \pmod{M_n}. \end{aligned}$$

Also gilt (1).

(2) Ist p prim, so gilt $2^p \equiv 2 \pmod{p}$ (Kleiner Fermatscher Satz).
Nach (1) ist daher M_p prim oder pseudoprim.

(3) folgt nach (1) und (2). (Nicht prim nach Vorbemerkung.)

(4) 341 ist pseudoprim, eine unendliche Folge von Pseudoprimzahlen ist gegeben durch

$$M_{341}, M_{M_{341}}, M_{M_{M_{341}}}, \ldots.$$

□

Definition. Für ganze Zahlen $n \geq 0$ heißen $F_n = 2^{2^n} + 1$ die *Fermatschen Zahlen*.

Bemerkung. Ist m keine Zweierpotenz, dann ist $2^m + 1$ nicht prim. Denn schreibe $m = vt$ mit $v \in \mathbb{N}$, $t \geq 3$ ungerade. Dann ist

$$2^m + 1 = 2^{vt} + 1 = (2^v + 1)\big(2^{v(t-1)} - 2^{v(t-2)} + \ldots - 2^v + 1\big)$$

mit Faktoren > 1.

Satz 6.3. *Für jedes $n \geq 0$ ist $2^{F_n} \equiv 2 \pmod{F_n}$ und F_n ist prim oder pseudoprim.*

Beweis: Es ist $F_n = 2^{2^n} + 1$, also $2^{2^n} \equiv -1 \pmod{F_n}$. Potenzieren ergibt

$$2^{a \cdot 2^n} \equiv (-1)^a \pmod{F_n} \quad \text{für alle } a \geq 0.$$

Es ist

$$2^{F_n} = 2^{k \cdot 2^n + 1} = 2 \cdot 2^{k \cdot 2^n}$$

mit $k \cdot 2^n = 2^{2^n}$ also $k = 2^{2^n - n} \in 2\mathbb{Z}$. Daher ist

$$2^{F_n} = 2 \cdot 2^{k \cdot 2^n} \equiv 2(-1)^k \equiv 2 \pmod{F_n}.$$

□

Definition. Eine natürliche Zahl $n > 1$ heißt eine *Carmichael-Zahl*, falls n nicht prim ist und $a^n \equiv a \pmod{n}$ für alle $a \in \mathbb{Z}$.

Setzt man $a = -1$ ein, so folgt, dass jede Carmichael-Zahl ungerade ist. Für Carmichael-Zahlen n und alle a mit $\mathrm{ggT}(a, n) = 1$ gilt $a^{n-1} \equiv 1 \pmod{n}$.

Satz 6.4. *Sei $n = p_1 \cdots p_r$, $r \geq 2$, $p_1, \ldots, p_r$ verschiedene ungerade Primzahlen. Für jedes $j = 1, \ldots, r$ sei $\varphi(p_j) = p_j - 1$ ein Teiler von $n - 1$. Dann ist n eine Carmichael-Zahl.*

Beweis: n ist nicht prim, da $r \geq 2$. Für jedes j ist $n - 1 = (p_j - 1)k_j$ mit $k_j \in \mathbb{N}$. Für $a \in \mathbb{Z}$, $p_j \nmid a$ folgt

$$a^{n-1} = \big(a^{p_j - 1}\big)^{kj} \equiv 1^{kj} \equiv 1 \pmod{p_j},$$

nach dem kleinen Fermatschen Satz. Es folgt $a^n \equiv a \pmod{p_j}$ für alle $a \in \mathbb{Z}$ und alle $j = 1, \ldots, r$, also $a^n \equiv a \pmod{n}$ für alle $a \in \mathbb{Z}$. □

Bemerkung. Es gibt genau drei Carmichael-Zahlen $n < 2000$, nämlich

$$561 = 3 \cdot 11 \cdot 17,$$
$$1105 = 5 \cdot 13 \cdot 17,$$
$$1729 = 7 \cdot 13 \cdot 19.$$

Idee eines Testes für Zusammengesetztheit
Wenn für $n - 1 = 2^s \cdot t$, t ungerade, $s \geq 1$ und ein $b \in \mathbb{N}$ die Fermat-Kongruenz $b^{n-1} \equiv b^{2^s t} \equiv 1 \pmod{n}$ erfüllt ist, dann prüfe man auch die „Quadratwurzeln".

$$b^{\frac{1}{2}(n-1)}, b^{\frac{1}{4}(n-1)}, \ldots, b^t \pmod{n}.$$

Definition. Es seien $n, b \in \mathbb{N}$, $n \geq 3$ ungerade, $\mathrm{ggT}(n, b) = 1$ und $n - 1 = 2^s t$ mit t ungerade. n heißt *stark pseudoprim* zur Basis b, falls entweder $b^t \equiv 1 \pmod{n}$ oder $b^{2^r t} \equiv -1 \pmod{n}$ für ein r mit $0 \leq r < s$ gilt.

Satz 6.5.

(1) *Ist n prim und $n \neq 2$, dann ist n stark pseudoprim zu jeder Basis b mit* $\mathrm{ggT}(b, n) = 1$.

(2) *Es sei $n \geq 3$ ungerade, quadratfrei und stark pseudoprim zu jeder Basis b mit* $\mathrm{ggT}(b, n) = 1$. *Dann ist n prim oder eine Carmichael-Zahl.*

Beweis:

(1) Sei $n \neq 2$ prim, $n - 1 = 2^s t$ mit t ungerade. Nach dem kleinen Fermatschen Satz gilt: $b^{2^s t} = b^{n-1} \equiv 1 \pmod{n}$. Im Körper $\mathbb{F}_n$ hat 1 nur die beiden Quadratwurzeln 1 und -1. Falls also $b^t \not\equiv 1 \pmod{n}$ ist, dann ist in der Folge der Restklassen von $b^t, b^{2t}, b^{2^2 t}, \ldots, b^{2^{s-1} t}$ modulo n die letzte von 1 verschiedene Restklasse gleich der Restklasse von -1. Also gibt es ein r mit $0 \leq r < s$ mit $b^{2^r t} \equiv -1 \pmod{n}$. Also ist n stark pseudoprim zu jeder Basis b mit $\mathrm{ggT}(b, n) = 1$.

(2) Durch wiederholtes Quadrieren folgt $b^{n-1} \equiv 1 \pmod{n}$ für alle $b \in \mathbb{Z}$ mit $\mathrm{ggT}(b, n) = 1$. Da n quadratfrei ist, folgt $b^n \equiv b \pmod{n}$ für alle $b \in \mathbb{Z}$. Also ist n prim oder eine Carmichael-Zahl.

□

Beispiel. Es sei $n = 561$. Dann ist $n - 1 = 2^4 \cdot \overbrace{35}^{t}$. Da $2^5 \equiv -2 \pmod{17}$ ist

$$2^{35} = (2^5)^7 \equiv (-2)^7 = -2^2 \cdot 2^5 \equiv 8 \pmod{17} \Rightarrow 2^{35} \not\equiv \pm 1 \pmod{n}.$$

Da

$$2^5 \equiv -1 \pmod{11} \Rightarrow 2^{35} \equiv -1 \pmod{11} \Rightarrow 2^{2^r \cdot 35} \equiv 1 \pmod{11}$$

für $r \in \{1, 2, 3\}$. Also ist n nicht stark pseudoprim zur Basis 2.

Definition. Ist n nicht stark pseudoprim zur Basis b, dann heißt b ein *Zeuge* für die Zerlegbarkeit von n.

Satz 6.6 (Satz von Rabin)**.** *Wenn $n > 9$ ungerade und zerlegbar ist, dann sind mindestens $\frac{3}{4}$ aller teilerfremden Reste $b \pmod{n}$ Zeugen für die Zerlegbarkeit von n.*

Beweis: entfällt □

Rabin-Miller-Test
Wähle ein „kleines“ k und Basen $b_1, \ldots, b_k$. Es sei ein „großes“ ungerades n vorgelegt. Man testet, ob n stark pseudoprim zu den Basen $b_1, \ldots, b_k$ ist. Falls nicht, dann ist n zusammengesetzt. Falls doch, wird n für „wahrscheinlich prim“ erklärt. Die Wahrscheinlichkeit, dass n fälschlicherweise für prim gehalten wird, ist nach dem Satz von Rabin kleiner als 4^{-k} (falls die Zeugen unabh. sind).

7. 2 Mai

Satz 7.1 (Chinesischer Restsatz)**.** *Es seien die natürlichen Zahlen m, n paarweise teilerfremd.*

Es seien $a, b \in \mathbb{Z}$ gegeben mit $\mathrm{ggT}(m, a) = \mathrm{ggT}(n, b) = 1$.

Das System der Kongruenzen $x \equiv a \pmod{m}$ und $x \equiv b \pmod{n}$ besitzt genau eine Lösung x modulo mn.

Idee des Beweises: Man benutzt die Abbildung:

$$f : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$
$$f(a \mod mn) \mapsto (a \mod m, a \mod n).$$

Man zeigt, dass f wohldefiniert und eine Bijektion ist, wenn $\mathrm{ggT}(m, n) = 1$ gilt. □

Satz 7.2. *Sei ϕ die Eulersche Phi-Funktion. Dann gilt $\phi(mn) = \phi(n)\phi(m)$, wenn $\mathrm{ggT}(m, n) = 1$, und $\phi(p^e) = p^e - p^{e-1}$, wenn p Primzahl ist.*

Idee des Beweises: Da $\phi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$ ist, folgt Satz 7.2 nach Satz 7.1. □

Idee der öffentlichen Verschlüsselungsmethoden

(1) Am Nachrichtenaustausch nimmt eine „große“ Menge $\mathcal{P}$ von Personen P teil. Jede Person hat einen öffentlichen Schlüssel E_P (E = encoding) und einen privaten Schlüssel D_P (D = decoding). Eine Nachricht ist eine Zahl $N \in \{0, 1, 2, \ldots, n-1\} = \mathcal{N}$, n fest vereinbart und E_P und D_P sind bijektive Abbildungen von $\mathcal{N}$ auf sich.

(2) Es gilt: $E_P \circ D_P = D_P \circ E_P = id$.

(3) E_P und D_P sind beide schnell ausführbar.

(4) Die Ermittlung von D_P aus dem bekannten E_P ist hoffnungslos zeitaufwändig.

Funktionsweise:
A will N an B senden. A besorgt sich das öffentlich zugängliche E_B, berechnet und sendet $E_B(N)$. Dann ist nur B in der Lage, $D_B\big(E_B(N)\big) = N$ zu lesen. Die Authentizität der Nachricht kann A durch Hinzufügen von $E_B\big(D_A(U)\big)$, U Unterschrift gewährleisten, dann liest B die Nachricht $D_A(U)$. Mittels des öffentlichen E_A wird dann $E_A\big(D_A(U)\big) = U$ gelesen.

Das RSA-Verfahren (Rivest, Shamir, Adleman, 1977)
(Der Computer von) A wählt zwei „große“ Primzahlen $p_A \neq q_A$ aus, berechnet $n = n_A = pq$, wählt dann ein $e = e_A \in \mathbb{N}$ mit $1 < e < (p-1)(q-1) = \varphi(n)$ mit $\mathrm{ggT}\,\big(e, \varphi(n)\big) = 1$ und berechnet (mit euklidischem Algorithmus) die Zahl $d = d_A \in \{1, \ldots, \varphi(n) - 1\}$ mit $de \equiv 1 \pmod{\varphi(n)}$.
Es sei $0 \leq N < n_A - 1$ und für solches sei $E_A(N) \equiv N^{e_A} \pmod{n_A}$ und $D_A(N) \equiv N^{d_A} \pmod{n_A}$.

Zu den Postulaten

(3) Ist erfüllt mit $O(\log n_A)$ Rechenoperationen.

(2) Es ist $ed = 1 + k\varphi(n)$ mit $k \in \mathbb{Z}$.
Mit dem Eulerschen Satz folgt also

$$\begin{aligned} D_A \circ E_A(N) = E_A \circ D_A(N) &\equiv N^{ed} \\ = N^{1+k\varphi(n)} = N \cdot N^{k\varphi(n)} &\equiv N \pmod{n_A} \end{aligned}$$

für alle $N \in \{0, 1, \ldots, n-1\}$.

(1) Die Wahl von p und q ist mit vertretbarem Aufwand möglich.

(4) Zur Ermittlung von D_A aus dem bekannten E_A genügt es, für das bekannte $n_A = n$ die Primteiler p und q oder die Eulersche Funktion $\varphi(n)$ zu berechnen.

8. 9 Mai

A will b an B senden. Um das RSA-Verfahren zu benutzen, B muss größe Primzahlen p und q finden, das Produkt $n = pq$ berechnen, und k mit $\text{ggT}(\phi(m), n) = 1$ wählen. Dann veröffentlicht B den Schlüssel (n, k). Dann berechnet A $a \equiv b^k \mod n$ mit $0 \leq a \leq m - 1$, und schickt an A die Zahl b. Es gibt zwei Probleme überzuwinden:

- Wie kann man schnell $a \equiv b^k \mod n$ berechnen?
- Wie kann man die Kongruenz $x^k \equiv b \mod n$ für x lösen?

Das Verfahren der sukzessiven Quadrate

- Sei N am größten damit $2^N \leq a$. Dann berechnet man

$$a_1 \equiv a^2 \mod n,\ a_2 \equiv (a^2)^2 \mod n,\ \ldots,\ a_N \equiv a^{2^N} \mod n.$$

- Sei $k = \sum_{j=0}^{N} c_j 2^j$ mit $c_j \in \{0, 1\}$.
- Sei $b_0 = 1$. Für jedes $1 \leq j \leq N$, sei $b_j = b_{j-1} a_j \mod n$.
- Dann ist $b = b_N \equiv a^k \pmod n$.

Beispiel. Wir berechnen$7^{327} \pmod{853}$. Zuerst das Berechnen von 7^{2^j} for $j = 0, 1, 2, 3, \ldots$:

$$\begin{aligned}
7^0 &= 1 \equiv && 1 \pmod{853}\\
7^1 &= 7 \equiv && 7 \pmod{853}\\
7^2 &= 49 \equiv && 49 \pmod{853}\\
7^4 &= (7^2)^2 = 49^2 = 2401 \equiv && 695 \pmod{853}\\
7^8 &= (7^4)^2 \equiv (695)^2 \pmod{853} \equiv 483025 \pmod{853} \equiv && 227 \pmod{853}\\
7^{16} &= (7^8)^2 \equiv (227)^2 \pmod{853} \equiv 51529 \pmod{853} \equiv && 349 \pmod{853}\\
7^{32} &= (7^{16})^2 \equiv (349)^2 \pmod{853} \equiv 121801 \pmod{853} \equiv && 675 \pmod{853}\\
7^{64} &= (7^{32})^2 \equiv (675)^2 \pmod{853} \equiv 455625 \pmod{853} \equiv && 123 \pmod{853}\\
7^{128} &= (7^{64})^2 \equiv (123)^2 \pmod{853} \equiv 15129 \pmod{853} \equiv && 628 \pmod{853}\\
7^{256} &= (7^{128})^2 \equiv (628)^2 \pmod{853} \equiv 394384 \pmod{853} \equiv && 298 \pmod{853}
\end{aligned}$$

Da

$$327 = 256 + 64 + 4 + 2 + 1,$$

merken wir, dass

$$\begin{aligned}7^{327} =& 7^{256+64+4+2+1} = 7^{256}7^{64}7^{4}7^{2}7^{1}\\ \equiv& 298 \cdot 123 \cdot 695 \cdot \underbrace{49 \cdot 7} \pmod{327}\\ \equiv& 298 \cdot 123 \cdot \underbrace{695 \cdot 343} \pmod{327}\\ \equiv& 298 \cdot \underbrace{123 \cdot 398} \pmod{327}\\ \equiv& \underbrace{298 \cdot 333} \pmod{327}\\ \equiv& 286 \pmod{327}\end{aligned}$$

ist.

Verfahren zum Finden einer k-ten Wurzel

- Man berechnet $\phi(n)$.
- Man findet $u, v > 0$, damit $ku - \phi(n)v = 1$ ist.
- Man berechnet $b^u \pmod{m}$. (Durch das verfahren der sukzessiven Quadrate)

Bemerkung. Wenn man kennt die Zahlen p, q, dabei $n = pq$ ist, ist es einfach dieses Verfahren zu benutzen. Wenn nicht, muss man zuerst n teilen, etwas schwieriger zu machen.

Beispiel. Wir lösen Folgendes:

$$x^{329} \equiv 452 \pmod{1147}.$$

Wir finden, dass $1147 = 31 \times 37$ ist, deshalb gilt

$$\phi(1147) = \phi(31)\phi(37) = 30 \times 36 = 1080.$$

Wir benutzen den Euklidischer Algorithmus, um

$$329u - 1080v = ku - \phi(m)v = 1 \tag{8.1}$$

zu lösen. Nach

$$\begin{aligned}1080 &= 3 \times 329 + 93\\ 329 &= 3 \times 93 + 50\\ 93 &= 1 \times 50 + 43\\ 50 &= 1 \times 43 + 7\\ 43 &= 6 \times 7 + 1\\ 7 &= 7 \times 1 + 0,\end{aligned}$$

finden wir, dass

$$-151k + 46\phi(m) = 1$$

ist. Leider, die Lösung $(u_0, v_0) = (-151, -46)$ geht nicht, da $u_0, v_0 < 0$. Nach Satz 3.3, finden wir andere Lösung

$$(u, v) = (-151 + \phi(m), -46 + k) = (929, 283).$$

Wir finden eine Lösung von

$$x = b^u \pmod{1147}$$

mit dem Verfahren der suksussiven Quadrate:

$$\begin{aligned}
452^1 &\equiv 452 \pmod{1147}\\
452^2 &\equiv 138 \pmod{1147}\\
452^4 &\equiv 692 \pmod{1147}\\
452^8 &\equiv 565 \pmod{1147}\\
452^{16} &\equiv 359 \pmod{1147}\\
452^{32} &\equiv 417 \pmod{1147}\\
452^{64} &\equiv 692 \pmod{1147}\\
452^{128} &\equiv 565 \pmod{1147}\\
452^{256} &\equiv 359 \pmod{1147}\\
452^{512} &\equiv 417 \pmod{1147}.
\end{aligned}$$

Da

$$u = 929 = 1 + 32 + 128 + 256 + 512,$$

finden wir endlich, dass

$$x = 452^{929} \equiv 452 \cdot 417 \cdot 565 \cdot 359 \cdot 417 \pmod{1147} \equiv 763 \pmod{1147}.$$

Idee des Beweises, dass dieses Verfahren klappt: Wenn $\gcd(k, \phi(m)) = 1$, haben wir nach Satz 3.1 eine Lösung $(u, v) \in \mathbb{Z}$, mit

$$ku - \phi(m)v = 1.$$

Nach Satz 3.3, gibt es eine mit $u, v > 0$. Dann berechnen wir:

$$\begin{aligned}
x^k =& (b^u)^k \pmod{m}\\
\equiv& b^{ku} \pmod{m}\\
\equiv& b^{1+\phi(m)v} \pmod{m}\\
\equiv& b \cdot (b^{\phi(m)})^v \pmod{m}\\
\equiv& b \cdot 1^v \pmod{m}\\
\equiv& b \pmod{m}.
\end{aligned}$$

□

9. 12 Mai

Sei $p > 2$ Primzahl, $a \in \mathbb{Z}$, $p \nmid a$. Wir suchen Lösungen x zu

$$x^2 \equiv a \pmod{p}. \tag{9.1}$$

Das Quadratische Reziprozitätsgesetz gibt eine Lösung dieser Gleichung. Ein vorerstes Ergebnis ist Folgendes.

Satz 9.1 (Eulersches Kriterium)**.** *Seien $p > 2$ Primzahl und $a \in \mathbb{Z}$, $p \nmid a$. Es gilt $a^{\frac{p-1}{2}} \equiv \pm 1$. Es gibt eine Lösung x von* (9.1) *gleich genau wenn $a^{\frac{p-1}{2}} \equiv 1$ gilt.*

Definition. Falls es x mit $x^2 \equiv a \pmod{p}$ gibt, dann nennt man a einen *quadratischen Rest modulo p*. Falls $x^2 \equiv a \pmod{p}$ nicht lösbar ist, nennt man a einen *quadratischen Nichtrest modulo p.*

Wir werden zwei Sätze beweisen, um Eulersches Kriterium beweisen zu können.

Satz 9.2 (Primitivelementsatz)**.** *Sei $p > 2$ Primzahl. Es gilt $g \in \mathbb{Z}$, damit*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{g}, \bar{g}^2, \ldots, \bar{g}^{p-1} = \bar{1}\}.$$

Solches g heißt ein Primitivelement *oder* Primitivwurzel.

Satz 9.3. *Sei k ein Körper, $f \in k[x]$, $f(x) = a_n x^n + \cdots + a_0$ mit $a_n \neq 0$, $n > 0$. Es gibt am meisten n Lösungen der Gleichung $f(x) = 0$.*

Bemerkung. Sei p Primzahl. Dann ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper.

Beweis des Eulerschen Kriterium: Sei $x \equiv a^{\frac{p-1}{2}} \pmod{p}$. Nach Kleinem Fermatschem Satz folgt $x^2 \equiv 1 \pmod{p}$. Nach Satz 9.3 folgt $x \equiv \pm 1 \pmod{p}$, da ± 1 Lösungen von $f(x) = x^2 - 1 \in \mathbb{F}_2[x]$ sind, und $1 \neq -1$ gilt. Wir bemerken hier, dass wir benutzen haben, dass $p > 2$ ist.

Sei $x^2 \equiv a \pmod{p}$. Nach Kleinem Fermatschem Satz, gilt es

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Andererseits sei $a \in Z$ mit $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Sei g ein Primativelement. Dass heißt, es gibt $r \in \mathbb{Z}$, damit es $g^r \equiv a \pmod{p}$ gilt. Dann rechnen wir

$$1 \equiv a^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^r \pmod{p}.$$

Da $g^{\frac{p-1}{2}} \in \pm 1$ ist, und g Primitivelement ist, folgt $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Dann erhält man, dass r gerade ist, deshalb ist a ein quadratischer Rest. □

Definition. Es sei G eine Gruppe. Falls es $g \in G$ gibt mit $G = \{g^n \mid n \in \mathbb{Z}\}$, nennt man G eine *zyklische Gruppe*. Ein Element g mit dieser Eingeschaft heißt ein *Primitivelement*.

Definition. Es seien $(G, \star_1)$ und $(H, \star_2)$ Gruppen. Das *direkte Produkt* $G \times H$ von G und H ist eine Gruppe mit Multiplikation

$$(g, h) \star (g', h') := (g \star_1 g', h).$$

Wenn $e_G \in G$ und $e_H \in H$ die neutralen Elementen von G und H sind, ist $e = (e_G, e_H)$ das neutrale Element von $G \times H$.

Es sei $(G, \star)$ eine Gruppe. Falls es $H \subset G$ gilt, damit $(H, \star)$ eine Gruppe ist, heißt H eine *Untergruppe*.

Beispiel. Folgende sind zyklisch.

- $(\mathbb{Z}, +)$
- $(\mathbb{Z}/m\mathbb{Z}, +)$
- Nach dem Primitivelementsatz ist $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ zyklisch.

Falls G, H Gruppe und $\#G, \#H > 1$ sind, ist $G \times H$ keine zyklische Gruppe.

Beispiel. Sei $G = \mathbb{Z}/13\mathbb{Z}^\times$. Man kann zeigen, dass Folgende ein kompletes Verzeichnis der Untergruppen von G sind.

$$\begin{aligned} H_1 &= \{\overline{1}\}, \\ H_2 &= \{\overline{-1}, \overline{1}\}, \\ H_3 &= \{\overline{3}, \overline{-4}, \overline{1}\}, \\ H_4 &= \{\overline{5}, \overline{-1}, \overline{-5}, \overline{1}\}, \\ H_6 &= \{\overline{4}, \overline{3}, \overline{-1}, \overline{-4}, \overline{-3}, \overline{1}\}, \\ H_{12} &= G. \end{aligned}$$

Bemerkung: Für jeden Teiler $d \mid 12$ gibt es eine eindeutige Untergruppe $H_d \subset \mathbb{Z}/13\mathbb{Z}^\times$. Es stimmt, dass jede endliche Gruppe mit dieser eigenschaft zyklisch ist.

Satz 9.4. *Sei G eine endliche abelsche Gruppe. Dann ist G zyklisch genau wenn für jeden Teiler $r \mid \#G$, es eine eindeutige Untergruppe $H_r \subset G$ gibt mit $\#H_r = r$.*

Idee des Beweises: Es sei G zyklisch, mit neutrales Element $e \in G$ und $n = \#G$, so dass $G = \{g, g^2, \ldots, g^n = e\}$ ist. Wenn $n = dr$ mit $d, r \in \mathbb{N}$ gilt, definieren wir die Untergruppe

$$H_d := \{g^r, g^{2r}, \ldots, g^{dr} = e\}.$$

Für jedes $x \in G$ mit $x^d = e$ behaupten wir, dass $x \in H_d$. Da $x = g^s$, erhält man, dass $g^{sr} = e$, so folgt $sr = tn$ und dann $s = td$. Das heißt, H_d ist eindeutig.

Sei G eine endliche abelsche Gruppe, so dass für jeden Teiler $r \mid \#G$, es eine eindeutige Untergruppe $H_r \subset G$ gibt mit $\#H_r = r$. Die Hauptschritte sind Folgende.

(a) Sei ϕ die Eulersche Phi-Funktion. Man zeigt, dass $F(m) := \sum_{d|m} \phi(m)$ multiplikativ ist. Dass heißt, $F(mn) = F(m)F(n)$ für $m, n \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$.

(b) Nach Satz 7.2 und (a), folgt $F(m) = m$.

(c) Sei $h \in G$. Dann definieren wir

$$\langle h \rangle := \{h^n \in H \mid n \in \mathbb{Z}\} \subset G.$$

Sei $\mathrm{gen}(H) = \{h \in G \mid \langle h \rangle = H\}$. Man zeigt, dass $\#\,\mathrm{gen}(\langle h \rangle) = \phi(\#H)$ gilt.

Jedes $h \in G$ ist das Primitivelement von einer eindeutigen zyklischen Untergruppe von G, so dass

$$\begin{aligned}
\#G &= \sum_{\substack{H \subset G \\ H \text{ zyklisch}}} \#\,\mathrm{gen}(H) \\
&= \sum_{\substack{H \subset G \\ H \text{ zyklisch}}} \phi(\#H) && \text{(nach (c))} \\
&= \sum_{\substack{d|\#G \\ H_d \text{ ist zyklisch}}} \phi(\#H_d) && \text{(nach der Annahme von } G\text{)} \\
&\leq \sum_{d|\#G} \phi(d) = \#G && \text{(nach (b))}.
\end{aligned}$$

So ist jede Untergruppe von G zyklisch, insbesondere G selbst. □

10. 23 Mai

Zur Erinnerung

- Ein *Körper* ist ein kommutativer Ring k, so dass $k^\times = k \setminus \{0\}$.
- Der *Ring der Polynome über k*

  $$k[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}_0, a_j \in k\}$$

  ist ein Ring mit den üblichen Operationen von Multiplikation und Addition von Polynomen.
- Der *Gradfunktion*

  $$\mathrm{grad} : k[x] \setminus \{0\} \to k$$

  ist definiert als

  $$\mathrm{grad}\, f = n, \qquad \text{falls } f = a_0 + \cdots + a_n x^n \in k[x] \text{ mit } a_n \neq 0 \text{ gilt.}$$

  Dann gilt es $\mathrm{grad}(fg) = \mathrm{grad}(f) + \mathrm{grad}(g)$, Falls $f, g \neq 0$. (Manchmal definiert man $\mathrm{grad}(0) = -\infty$. Mit dieser Definition, gilt $\mathrm{grad}(fg) = \mathrm{grad}(f) + \mathrm{grad}(g)$ für alle $f, g \in k[x]$.)

- Ein Element $f \in k[x]\backslash\{k\}$ ist *reduzible* oder *zerlegbar*, falls es $g, h \in k[x]\backslash\{k\}$ gibt, so dass $f = gh$. Ansonsten, man heißt f *irreduzible* oder *unzerlegbar*.
- Durch Polynomdivision hat $k[x]$ ein Divisionsalgorithmus. Dass heißt, $k[x]$ ist Euklidischer Ring, und es gibt einen Analog zum Fundementalsatz der Arithmetik.
- Ein Element $f = a_0 + \cdots + a_n x^n \in k[x]$ mit $a_n \neq 0$ ist *normiertes Polynom* falls $a_n = 1$ gilt. Nach dem letzten Punkt, hat jedes monierte Polynom f mit $\text{grad}(f) \geq 1$ eine eindeutige Factorzerlegung von unzerlegbaren Elementen.
- Jedes $f \in k[x]$ kann als Funktion $f : k \to k$ gebildet werden. Ein Element $\alpha \in k$ ist *Nullstelle* von f, falls $f(\alpha) = 0$ gilt.
- Beispiele: $\mathbb{C}$, $\mathbb{R}$ und $\mathbb{Q}$ sind Körper. Falls p Primzahl ist, dann ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ auch ein Körper.

Satz 10.1. *Sei k ein Körper, $0 \neq f \in k[x]$. Ein Element $\alpha \in k$ ist eine Nullstelle von f, genau wenn $x - \alpha \mid f$.*

Beweis: Nach dem Divisionsalgorithmus haben wir, dass $q, r \in k[x]$ mit $\text{grad}(r) < \text{grad}(x - \alpha) = 1$ existieren, so dass $f(x) = q(x)(x - \alpha) + r(x)$ gilt. Das heißt, $r(x) = r \in k$. Falls α eine Nullstelle von f ist, finden wir dass

$$0 = f(\alpha) = q(\alpha) \cdot 0 + r = r$$

gilt. Also, $x - \alpha \mid f$.

Falls $x - \alpha \mid f$, haben wir $g \in k[x]$, damit $f(x) = (x - \alpha)g(x)$ gilt. Es folgt, dass $f(\alpha) = 0$ ist. □

Sei $f \in k[x] \setminus k$. Man definiert eine Äquivalenzrelation durch $g \sim h$, falls $f \mid g - h$.

Definition. Für $a \in \mathbb{Z}$ und $p \neq 2$ prim definieren wir das *Legendresymbol* $\left(\frac{a}{p}\right)$ durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } p \nmid a \text{ und } x^2 \equiv a \pmod{p} \text{ lösbar,} \\ -1 & \text{falls } p \nmid a \text{ und } x^2 \equiv a \pmod{p} \text{ nicht lösbar,} \\ 0 & \text{falls } p \mid a. \end{cases}$$

Im jedem Fall ist $1 + \left(\frac{a}{p}\right)$ die Anzahl der Lösungen von $x^2 \equiv a \pmod{p}$.

Mit dieser Definition, ist Satz Folgendes.

Satz 10.2 (Legendre)**.** *Für $a \in \mathbb{Z}$ und $p \neq 2$ prim gilt es*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

11. 30 Mai

Wir können nun den Beweis von Satz 9.3 geben.

Beweis von Satz 9.3: Der Beweis ist induktiv. Falls $\operatorname{grad}(f) = 0$, dann ist $f = c \in k^\times$. Falls $\operatorname{grad}(f) = n > 0$, entweder hat f eine Nullstelle oder nicht. Wenn nicht, folgt die Behauptung. Wenn $\alpha \in k$ eine Nullstelle ist, nach Satz 10.1 finden wir, dass $f = (x - \alpha)g$ mit $\operatorname{grad}(g) = n - 1$ gilt. Es gilt

$$\{\beta \in k \mid f(\beta) = 0\} = \{\alpha\} \cup \{\beta \in k \mid g(\beta) = 0\},$$

also f hat höchstens $1 + (n - 1) = n$ Nullstellen. □

Wir können auch eine Verallgemeinerung von dem Primitivelement Satz (Satz 9.2) beweisen.

Satz 11.1. *Es sei k ein Körper und G eine endliche Untergruppe der multiplikativen Gruppe $(k^\times, \cdot)$. Dann ist G zyklisch.*

Beweis: Sie $H_d \subset G$ eine Untergruppe, so dass $\#H_d = d$. Es sei $f = x^d - 1 \in k[x]$. Für jedes element $\alpha \in H_d$, gilt es $f(\alpha) = 0$, so dass $H \subset \{\alpha \in k \mid f(\alpha) = 0\}$. Gilt außerdem nach Satz 9.3, dass

$$d = \#H_d \leq \#\{\alpha \in k \mid f(\alpha) = 0\} \leq d$$

gilt. Das heißt H_d ist eindeutig. Also der Satz folgt nach Satz 9.4. □

Satz 11.2 (Quadratrisches Reziprozitätsgesetz)**.** *Sei p, q ungerade Primzahlen. Dann gilt Folgendes.*

(0) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, *falls* $a \equiv b \pmod{p}$

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(2) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(3) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(4) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Beweis von (1), (2): Nach dem Eulerschen Kriterium gilt

$$\begin{aligned}\left(\frac{ab}{p}\right) \equiv & (ab)^{\frac{p-1}{2}} \pmod{p} \\ \equiv & a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p} \\ \equiv & \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.\end{aligned}$$

und (2) ist eine direkte Verwendung des Eulerschen Kriterium. □

Definition. Es sei $p \neq 2$ prim und $a \in \mathbb{Z}$ mit $p \nmid a$. Das Element $a \in \mathbb{Z}$ mit $p \nmid a$ heißt *negativ modulo p* (bzw. *positiv modulo p*), wenn $\bar{a} \in \{\overline{-1}, \overline{-2}, \ldots, \overline{-\frac{p-1}{2}}\}$ (bzw. $\bar{a} \in \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\}$).

Satz 11.3 (Lemma von Gauß)**.** *Es sei $p \neq 2$ prim, $a \in]Z$, $p \nmid a$. Es Sei*

$$M = \{\overline{2a} \mid 1 \leq a \leq \frac{p-1}{2}\},$$

und $\mu = \#\{x \in M \mid x \text{ negativ}\}$. Dann gilt

$$\left(\frac{2}{p}\right) = (-1)^{\mu}.$$

Beweis: Wir definieren $\sigma : M \to \{\pm 1\}$ durch $\sigma(a) = -1$, wenn $\overline{2a}$ negativ ist, sonst $\sigma(a) = 1$.

Es ist nicht möglich, dass $\{\overline{2a}, \overline{2b}\} = \{\pm x\}$ gilt für $x \in \mathbb{Z}/p\mathbb{Z}$ and $1 \leq a, b \leq \frac{p-1}{2}$, da $0 < 2(a+b) < p$. Sonst wäre $a+b$ Teilbar durch p, ein Widerspruch. Also, dann gilt

$$\begin{aligned}
(\frac{p-1}{2})! \equiv & \prod_{a=1}^{\frac{p-1}{2}} (-1)^{\sigma(a)} \left(\overline{2a}\right) \pmod{p} \\
\equiv & (-1)^{\mu} 2^{\frac{p-1}{2}} (\frac{p-1}{2})! \pmod{p} \\
\equiv & (-1)^{\mu} \left(\frac{2}{p}\right) (\frac{p-1}{2})! \pmod{p} \qquad \text{(nach dem Eulerschen Kriterium).}
\end{aligned}$$

Da $p \nmid (\frac{p-1}{2})!$ dürfen wir $(\frac{p-1}{2})!$ eliminieren. Die Behauptung des Satzes folgt. □

Beweis des Satzes 11.2(3): Falls $x \in \mathbb{R}$ gilt definieren wir $\lfloor x \rfloor$ als die größte Zahl $n \in \mathbb{Z}$ mit $n \leq x$. Also, die Elementen der Menge

$$P = \left\{2 \cdot 1, 2 \cdot 2, \ldots, 2 \cdot \left\lfloor \frac{p-1}{4} \right\rfloor\right\}$$

sind positiv modulo p, und die Elementen der Menge

$$M \setminus P = N = \left\{\left\lfloor \frac{p-1}{4} \right\rfloor + 2, \left\lfloor \frac{p-1}{4} \right\rfloor + 4, \ldots p-1\right\}$$

negativ modulo p sind.

Der Anzahl von N ist

$$\mu = \begin{cases} \frac{p-1}{4} & \text{falls } p \equiv 1 \pmod 4 \\ \frac{p+1}{4} & \text{falls } p \equiv 3 \pmod 4. \end{cases}\}$$

Falls $p \equiv 1 \pmod 4$ gilt, finden wir nach dem Lemma von Gauß

$$p \equiv 1 \pmod 4 \quad \Longrightarrow \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 8 \\ -1 & \text{falls } p \equiv 5 \pmod 8. \end{cases}$$

Wir finden ähnlich falls $p \equiv 3 \mod 4$, dass

$$p \equiv 3 \pmod 4 \quad \Longrightarrow \quad \left(\frac{2}{p}\right) = \begin{cases} -1 & \text{falls } p \equiv 3 \pmod 8 \\ 1 & \text{falls } p \equiv 7 \pmod 8 \end{cases}$$

gilt. Auf jedem Fall ist $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. □

12. 2 Juni

Man kann mit der Hilfe der Lemma von Gauß Teil (4) des Satzes 11.2 beweisen.

Satz 12.1. *Es seien p, a und N wie in Satz 11.3 gegeben. Dann gilt:*

$$N \equiv \sum_{1 \le \ell \le \frac{1}{2}(p-1)} \left\lfloor \frac{\ell a}{p} \right\rfloor + (a-1)\frac{p^2-1}{8} \pmod 2.$$

Für ungerades a gilt:

$$N \equiv \sum_{1 \le \ell \le \frac{1}{2}(p-1)} \left\lfloor \frac{\ell a}{p} \right\rfloor \pmod 2.$$

Dabei wird für $x \in \mathbb{R}$ mit $\lfloor x \rfloor$ die größte ganze Zahl $\le x$ bezeichnet.

Beweis: Für $\ell \in S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ wird m_ℓ wie im Beweis von Satz 11.3 erklärt. Es ist $\ell a \equiv m_\ell \pmod p$ und $|m_\ell| < \frac{p}{2}$. Mit $s_1, \ldots, s_M$ werden die positiven und mit $r_1, \ldots, r_N$ die negativen unter den m_ℓ bezeichnet. Dann gilt:

$$\sum_{\ell \in S} \ell a = \sum_{\ell \in S} p \left\lfloor \frac{\ell a}{p} \right\rfloor + s_1 + \ldots + s_M + (p + r_1) + \ldots + (p + r_N).$$

Außerdem gilt, da $\ell \mapsto |m_\ell|$ eine Permutation von S ist, dass

$$\sum_{\ell \in S} \ell = \sum_{\ell \in S} |m_\ell| = (s_1 + \ldots + s_M) - (r_1 + \ldots + r_N).$$

Subtraktion der beiden Gleichungen liefert

$$p \sum_{\ell \in S} \left\lfloor \frac{\ell a}{p} \right\rfloor + pN + 2(r_1 + \ldots + r_N) = \sum_{\ell \in S} (\ell a - \ell) = (a-1) \sum_{\ell \in S} \ell = (a-1)\frac{p^2-1}{8}.$$

Da p ungerade ist, folgt

$$N \equiv pN \equiv \sum_{\ell \in S} \left\lfloor \frac{\ell a}{p} \right\rfloor + (a-1)\frac{p^2-1}{8} \pmod 2.$$

Dies liefert die erste Behauptung des Satzes.
Für ungerades a ist $(a-1)\frac{p^2-1}{8} \equiv 0 \pmod 2$. □

Erster Beweis des Satzes 11.2(4): Es sei

$$T = \left\{ (x,y) \in \mathbb{N}^2 \middle| 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2} \right\}.$$

Außerdem seien

$$T_1 = \left\{ (x,y) \in T \middle| y < \frac{q}{p}x \right\},$$
$$T_2 = \left\{ (x,y) \in T \middle| x < \frac{p}{q}y \right\}.$$

Dann gilt: $T = T_1 \cup T_2, T_1 \cap T_2 = \emptyset$. Es folgt:

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \#T = \#T_1 + \#T_2 = \sum_{1 \le x \le \frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{1 \le y \le \frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor.$$

Nach Satz 12.1 und Satz 11.3 gilt

$$(-1)^{\sum_x \left\lfloor \frac{qx}{p} \right\rfloor} = (-1)^N = \left(\frac{q}{p}\right).$$

Die Rollen von p und q können getauscht werden. Also folgt

$$(-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

□

Sei G eine abelsche Gruppe und $H \subset G$ eine Untergruppe. Man definiert eine Äquivalenzrelation auf G durch $g' \sim_H g$ falls $g^{-1}g' \in H$. Für $g \in G$ schreiben wir

$$gH := \{g' \in G \mid g' \sim_H g\},$$

so dass gH *die Äquivalenzklass von* g ist.

Satz 12.2. *Die Relation* $\sim_H$ *is eine Äquivalenzrelation. Außerdem ist die Menge*

$$G/H := \{gH \mid g \in G\}$$

durch die Operation $gH \cdot g'H := (gg')H$ *eine Gruppe.*

Beweis: Aufgabe. □

Bemerkung. Falls G keine abelsche Gruppe ist, kann es sein, dass G/H keine Gruppe wäre. Es wird gebracht, damit G/H eine Gruppe wäre, dass H *normale Untergruppe* oder *Normalteiler* ist. Das heißt, es gilt

$$gH = Hg := \{hg \mid h \in H\}.$$

Satz 12.2 gilt für allgemeine Gruppen G und Normalteiler H.

Satz 12.3. *Sei G eine endliche Gruppe und $H \subset G$ Untergruppe. Dann gilt*

$$\#(G/H) = \frac{\#G}{\#H}.$$

Beweis: Da die Relation $g \sim_H g'$ eine Äquivalenzrelation ist, sind die Menge gH und $g'H$ entweder gleich oder disjunkt. Also, es existieren $g_1, \ldots, g_r \in G$, damit

$$G/H = \{g_1H, g_2H, \ldots, g_rH\}$$

gilt, und $g_iH = g_jH$, genau wenn $i = j$, das heißt $\#G = r$. Jedes g_iH besitzt genau $\#H$ Elementen. Es folgt

$$G = \bigsqcup_{j=1}^{r} g_jH \implies \#G = r\#H,$$

was zu zeigen war. □

Definition. Die Menge $R = \{g_1, \ldots, g_r\}$ des letzten Beweises heißt ein *vollständiges System von Repräsentanten der Gruppe G/H.*

Beispiel. Es sei $G = (\mathbb{Z}, +)$ und $H = (n\mathbb{Z}, +)$. Dann gilt

$$G/H = \mathbb{Z}/n\mathbb{Z}.$$

Beispiel. Es sei $p \neq q$ ungerade Primzahlen, $G = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ und $H = \{(\overline{1}, \overline{1}), (\overline{-1}, \overline{-1})\}$. Jedes Element aus G/H hat als Repräsentant $(i, j) \in \mathbb{Z}^2$ mit $p \nmid i$ und $q \nmid j$, welche Elementen durch drei verschiedene Arten äquivalent sein können .

(a) Durch die Äquivalenzrelation bei $\mathbb{Z}/pZ$:

$$(i, j) \equiv (i + pn, j) \qquad \text{für jedes } n \in \mathbb{Z}.$$

(b) Durch die Äquivalenzrelation bei $\mathbb{Z}/qZ$:

$$(i, j) \equiv (i, j + qm) \qquad \text{für jedes } m \in \mathbb{Z}.$$

(c) Durch die Äquivalenzrelation von H:

$$(i, j) \sim_H (-i, -j).$$

Wir behaupten, dass

$$R_1 = \left\{(i, j) \mid 1 \leq i \leq q - 1, 1 \leq j \leq \frac{q-1}{2}\right\}$$

ein vollständiges System von Repräsentanten der Gruppe G/H ist. Nach dem Satz 12.3 hat R_1 den richtigen Anzahl. Also, wir müssen zeigen, dass jedes $(i, j) \in \mathbb{Z}^2$ mit $p \nmid i$ und $q \nmid j$ äquivalent zu einem Element aus R_1 ist.

Sei $(i, j) \in \mathbb{Z}^2$ mit $p \neq i$, $q \nmid j$. Zuerst, nach (b) merken wir, dass

$$(i, j) \sim (i, j + qm)$$

gilt. Also, wir wählen m aus, damit $1 \leq j' = j + qm \leq q - 1$. Falls $1 \leq j \leq \frac{q-1}{2}$, können wir auch nach (b) $i' = j + pn$ auswählen, damit $(i', j') \in R_1$ gilt.

Falls $\frac{q-1}{2} < j' < q$, finden wir nach (c) und (b)

$$(i, j') \sim (-i, -j') \sim (-i, q - j') = (-i, j'')$$

und $1 \leq j'' \leq \frac{q-1}{2}$. Dann wählen wir $n \in \mathbb{Z}$ aus, damit

$$(-i, j'') \sim (-i + pn, j'') = (i'', j'')$$

mit $1 \leq i'' \leq p$ gilt, so dass $(i'', j'') \in R_1$ gilt.

Die Menge

$$R_2 = \left\{ (a, a) \mid 1 \leq a \leq \frac{pq - 1}{2}, \mathrm{ggT}(a, pq) = 1 \right\}$$

ist auch ein vollständiges System von Repräsentanten der Gruppe G/H. Das zu zeigen, lassen wir als Aufgabe. Man benutzt den chinesischen Restsatz, um diese Behauptung zu beweisen.

13. 6 Juni

Als eine Erklärung der Notation bemerken wir, dass es unterschiedliche Arten gibt, um Äquivalenzklassen zu schreiben. Falls G eine Gruppe ist und H eine Untergruppe, Folgendes werden benutzt:

$$\overline{g} = gH = [g] = \{g' \in G \mid g' \sim_H g\} = \{gh \mid h \in H\}.$$

Wir schreiben hier $g' \sim_H g$, falls $g^{-1}g \in H$ gilt.

Beweis des Satzes 11.2(4): Sei $G = (\mathbb{Z}/pZ)^\times (\mathbb{Z}/q\mathbb{Z})^\times$, $H = \{(\overline{1}, \overline{1}), (\overline{-1}, \overline{-1})\} \subset G$. Wir schreiben $(i, j) \in \mathbb{Z}^2$ als ein Repräsentant von einem Element der Gruppe G. Das heißt, ein Element aus G wird als

$$(\overline{i}, \overline{j}) = \{(i + pm, j + qn) \mid n, m \in \mathbb{Z}\} = (i \pmod p, j \pmod q)$$

geschrieben.

Es Seien R_1 und R_2 wie letztes Mal. Zuerst findet man das Produkt von $(i, j) \in R_1$:

$$\begin{aligned}
\prod_{(i,j) \in R_1} (i, j) &= \prod_{i=1}^{p-1} \prod_{j=1}^{\frac{q-1}{2}} (i, j) \\
&= \prod_{i=1}^{p-1} \left(i^{\frac{q-1}{2}}, \left(\frac{q-1}{2} \right)! \right) \\
&= \left((p-1)!^{\frac{q-1}{2}}, \left(\frac{q-1}{2} \right)!^{p-1} \right)
\end{aligned}$$

Es wird als Hausaufgabe beweisen, dass

$$\left(\frac{q-1}{2}\right)!^2 \equiv (-1)^{\frac{q-1}{2}}(q-1)! \pmod{q}$$

gilt, so dass

$$\prod_{(i,j)\in R_1}(i,j) \equiv \left((p-1)!^{\frac{q-1}{2}} \pmod{p}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}} \pmod{q}\right). \tag{13.1}$$

in G. Änlicherweise, findet man das Produkt

$$\begin{aligned}\prod_{(a,a)\in R_2} a =& \frac{\left(\prod_{i=1}^{p-1} i(p+i)(2p+i)\cdots(\frac{q-3}{2}p+i)\right)\prod_{i=1}^{\frac{q-1}{2}}(\frac{q-1}{2}p+i)}{q\cdot(2q)\cdots(\frac{p-1}{2}q)}\\ \equiv& (p-1)!^{\frac{q-1}{2}}\frac{1}{q^{\frac{p-1}{2}}} \pmod{p}\\ \equiv& (p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod{p}.\end{aligned}$$

Im letzten Schritt haben wir Eulersches Kriterium verwendet.

Wenn wir die Teile von p und q umtauschen, folgt es

$$\prod_{(a,a)\in R_2}(\overline{a},\overline{a}) \equiv \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod{p}, (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right) \pmod{q}\right). \tag{13.2}$$

Es folgt aus (13.1) und (13.2), dass

$$\left(1 \pmod{p}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod{q}\right)$$

und

$$\left(\left(\frac{q}{p}\right) \pmod{p}, \left(\frac{p}{q}\right) \pmod{q}\right)$$

das gleiche Element aus G/H repräsentieren. Da

$$\overline{\left(\left(\frac{q}{p}\right) \pmod{p}, \left(\frac{p}{q}\right) \pmod{q}\right)} = \overline{\left(1 \pmod{p}, \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \pmod{q}\right)}$$

in G/H gilt, so finden wir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

wie behauptet wurde. □

Wir möchten jetzt erklären, wie man eine Lösung von der Gleichung

$$x^2 \equiv a \pmod{p}$$

finden kann. Zuerst, nach dem Satz 13.1, kann man ziemlich einfach entscheiden, ob eine Lösung existiert, weil es einem erlaubt, $\left(\frac{m}{n}\right)$ zu berechnen, ohne dass n prim sein muss. Um dieses Ziel zu erreichen, brauchen wir Folgendes.

Definition. Sei $m = p_1 p_2 \cdots p_r \in \mathbb{N}$ mit p_i prim für alle $1 \leq i \leq r$. Dann definiert man das *Jakobisymbol*

$$\left(\frac{n}{m}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots\left(\frac{m}{p_r}\right).$$

Am rechten Siete ist jeder Begriff das Legendresymbol.

Satz 13.1 (Allgemeines Quadratisches Reziprozitätsgesetz)**.** *Es seien $m, n \in \mathbb{N}$ ungerade. Es gilt Folgendes.*

(1) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{m}\right)$, *für alle* $a, b \in \mathbb{Z}$

(2) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

(3) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{2}}$

(4) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$

Bemerkung. Falls $\left(\frac{m}{n}\right) = -1$, die Gleichung $x^2 \equiv m \pmod{n}$ keine Lösung hat. Falls n nicht prim ist, kann es sein, dass keine Lösung existiert, sogar $\left(\frac{m}{n}\right) = 1$ gilt. Beispeil: $\left(\frac{-1}{21}\right) = 1$, aber -1 kein Quadrat modulo 21 ist.

Nach mehrmalige Verwendungen vom Allgemeinen Quadratischen Reziprozitätsgesetz kann man $\left(\frac{a}{p}\right)$ berechnen. Falls, das Ergebnis $+1$ ist, benutzt man folgenden Satz, um eine Lösung zu $x^2 \equiv a \pmod{p}$ zu finden.

Satz 13.2 (Algorithmus von Tonelli)**.** *Es sei $p > 3$ prim $a \in \mathbb{Z}$ ($p \nmid a$), damit $x^2 \equiv a \pmod{p}$ eine Lösung hat. Falls x_0 ein quadratischen Nichtrest ist und $p = 2^s m + 1$ mit $m \in \mathbb{Z}$ ungerade gilt, gibt es $0 \leq j < 2^s$, so dass $x = a^{\frac{m+1}{2}} x_0^{mj}$ eine Lösung ist.*

Um diesen Algorithmus zu verwenden, folgt man Folgendes.

- Die Wert von $\left(\frac{a}{p}\right)$ kann berechnet werden nach Verwendung des Quadratischen Restgesetzes. Falls $\left(\frac{a}{p}\right) = -1$ gilt, hat $x^2 \equiv a \pmod{p}$ keine Lösungen.
- Anderenfalls findet man die Darstellung $p = 2^s m + 1$ mit m ungerade.
- Man probiert für verschiedene Primzahlen $q = 2, 3, \ldots$, ob q ein Nichtrest modulo p ist. Sobald $\left(\frac{q}{p}\right) = -1$ gilt, sei $x_0 = q$.
- Sei $r \equiv a^{\frac{m+1}{2}} \pmod{p}$.
- Sei $b \equiv x_0^m \pmod{p}$.

- Für das kleinste nichtnegative j, damit $(b^j r)^2 \equiv a \pmod{p}$ ist, sind $x \equiv \pm b^j r$ die gesuchten Lösungen zur Gleichung $x^2 \equiv a \pmod{p}$.

14. 9 Juni

Beweis von Tonellis Algorithmus: Sei x_0 ein quadratischer Nichtrest modulo $p = 2^s m+1$ mit m ungerade. Sei $b = x_0^m$. Dann mussen wir zeigen, dass es $0 \leq j < 2^s$ gibt, damit $a^{\frac{m+1}{2}} b^j$ eine Lösung zur Gleichung $x^2 \equiv a \pmod{p}$ ist.

Sei $G = (\mathbb{Z}/p\mathbb{Z})^\times$ und $H \subset G$ die eindeutige Untergruppe mit $\#H = 2^s$. Wir behaupten, dass $H = \langle b \rangle = \{b^n \pmod{p} \mid n = 1, 2, \ldots\}$ gilt. Da $b^{2^s} = x_0^{m2^s} = x_0^{p-1} \equiv 1 \pmod{p}$ folgt $b \in H$. Falls $b^{2^r} \equiv 1 \pmod{p}$ für $1 \leq r < s$, dann folgt

$$\begin{aligned}\left(\frac{x_0}{p}\right) \equiv & x_0^{\frac{p-1}{2}} \pmod{p} \\ \equiv & \left((x_0^m)^{2^r}\right)^{2^{s-r-1}} \pmod{p} \\ \equiv & 1 \pmod{p}\end{aligned}$$

da $s - r - 1 \geq 0$ ist. Das widerspricht die Annahme, dass x_0 ein Nichtrest ist.

Genauso wie es gezeigt wurde, dass $x_0^m \in H$ gilt, ist $a^m \in H$. Da $a \equiv x^2 \pmod{p}$ nur eine Lösung hat, finden wir außerdem $a^m \in \langle b^2 \rangle$. Das heißt, es gibt $0 \leq j < 2^s$, damit $a^m b^{2j} \equiv 1 \pmod{p}$. Danach folgt

$$(a^{\frac{m+1}{2}} b^j)^2 = a \cdot a^m b^{2j} \equiv a \pmod{p}.$$

□

Satz 14.1. *Es gibt unendliche Primzahlen $p \equiv 1 \pmod{4}$. Es gibt unendliche Primzahlen $p \equiv 3 \pmod{4}$.*

Idee des Beweises: Sei $P = \{3, p_1, \ldots, p_r\}$ eine Menge von verschiedenen Primzahlen mit $p_j \equiv 3 \pmod{4}$ für jedes $1 \leq j \leq r$. Sei $M = 4p_1 \cdots p_r + 3$. Falls alle p, damit $p \mid M$, wären äquivelent zu 1 modulo r, dann wäre auch $M \equiv 1 \pmod{4}$. Das heißt, es gibt $p \neq 3$, damit $p \mid M$ und $p \equiv 3 \pmod{4}$ gelten. Für dieses p ist $p \notin P$. Also keine endliche Bezeichnung von Primzahlen $p \equiv 3 \pmod{4}$ wäre komplet.

Sei $Q = \{q_1, \ldots, q_r\}$ eine Menge von Primzahlen mit $p_j \equiv 1 \pmod{4}$ für jedes $1 \leq j \leq r$. Es sei $N = (2p_1 \cdots p_r)^2 + 1$. Für jedes $q \mid N$ folgt es $q \notin Q$ und $(\frac{-1}{q}) = 1$. □

Satz 14.2. *Eine Primzahl p kann als Produkt $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ geschriben werden, genau wenn $p = 2$ oder $p \equiv 1 \pmod{4}$.*

Beweis: Sei p prim und $a, b \in \mathbb{Z}$ damit $p = a^2 + b^2$. Da $p \nmid a, b$ folgt es

$$a^2 \equiv -b^2 \pmod{p} \quad \Longrightarrow \quad c^2 \equiv -1 \pmod{p},$$

so dass $\left(\frac{-1}{p}\right) = 1$. Nach dem quadratischen Reziprozitätsgesetz ist $p \equiv 1 \pmod 4$.

Da $2 = 1^2 + 1^2$ deutlich ist, mussen wir nun zeigen, dass jedes $p \equiv 1 \pmod 4$ als Produkt $p = a^2 + b^2$ geschrieben werden kann. Da $p \equiv 1 \pmod 4$ ist, finden wir $\left(\frac{-1}{p}\right) = 1$, so dass es $x_0 \in \mathbb{Z}$ gibt, damit $p \mid x_0 + 1$. Wir benutzen den Ring $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ der Gaußchen Zahlen. Da R ein Divisionsalgorithmus besitzt gilt es eindeutige Faktorzerlegung von unzerlegbaren Elementen dabei.

Also es gilt

$$p \mid x_0^2 + 1 = (x_0 + i)(x_0 - i).$$

Wäre p unzerlegbar, dann wäre p Teiler von $x_0 + \epsilon i$ für $\epsilon \in \{1, -1\}$, dann hätten wir $x_0 + \epsilon i = p\alpha$ für $\alpha \in \mathbb{Z}[i]$. Nach komplexer Konjugation, hätten wir auch dass $x_0 - \epsilon i = p\overline{\alpha}$, so dass p auch Teiler von $x_0 - \epsilon p$ wäre. Das würde implizieren

$$p \mid (x_0 + i) + (x_0 - i) = 2x_0.$$

Nochmal nach eindeutiger Primfaktorzerlung, dann wäre p Teiler von entweder 2 oder x_0, ein Widerspruch. Also es existieren $\alpha, \beta \in R$, die keine Einheiten sind, damit $p = \alpha\beta$. Nach der Normfunktion

$$N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}, \qquad a + ib \mapsto a^2 + b^2$$

folgt es $p^2 = N(\alpha)N(\beta)$. Da α, β kiene Einheiten sind, nach eindeutiger Primfaktorzerlung der Zahlen $\mathbb{Z}$ gilt es $N(\alpha) = N(\beta) = p$. Dass heißt, es gibt $\alpha = a + bi \in \mathbb{Z}[i]$, damit $p = N(\alpha) = a^2 + b^2$. □

Idee des Beweises des Allgemeinen Quadratischen Reziprozitätsgesetzes: Als erster Schritt zeigt man

$$\frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \ldots + \frac{p_r - 1}{2} \equiv \frac{p_1 p_2 \cdots p_r - 1}{2} \pmod 2$$

für ungerade Primzahlen $p_1, p_2, \ldots, p_r$.

Dann folgt es für $n = p_1 p_2 \cdots p_r$, dass

$$\left(\frac{-1}{n}\right) = (-1)^{\sum \frac{p_j - 1}{2}} = (-1)^{\frac{n-1}{2}}$$

gilt. Die andere Fälle sind ähnlich. □

15. 13 Juni

Satz 15.1. *Es sei $R = \mathbb{Z}[i]$ der Ring der ganzen Gaußschen Zahlen mit Norm $N(z) = z\overline{z} = a^2 + b^2$ für $z = a + bi \in R$. Für $n \in \mathbb{N}$ sei*

$$r_2(n) = \#\left\{(x, y) \in \mathbb{Z}^2 \middle| x^2 + y^2 = n\right\}$$

und $\rho_2(n) = \frac{1}{4}r_2(n)$. *Dann die Funktion* $\rho_2 : \mathbb{N} \to \mathbb{Z}$ *ist multiplikativ. Für Primzahlpotenzen* p^k *gilt:*

$$\rho_2(p^r) = \begin{cases} k+1 & \text{für } p \equiv 1 \pmod 4, \\ 0 & \text{für } p \equiv 3 \pmod 4 \text{ und } r \text{ ungerade}, \\ 1 & \text{für } p \equiv 3 \pmod 4 \text{ und } r \text{ gerade}, \\ 1 & \text{für } p = 2. \end{cases}$$

Beweis: In R gilt der Satz von der eindeutigen Faktorzerlegung von irreduzibelen Elementen. Dass heißt, jedes Element $r \in R$ kann als produkt $r = \mathfrak{p}_1\mathfrak{p}_2 \cdot \mathfrak{p}_r \in R$ geschrieben werden, mit jedes $\mathfrak{p}_j$ unzerlegbar. Außerdem, ist diese Darstellung eindeutig bis auf Reihenfolge und Multiplikation von Einheiten. Die Einheiten von R sind

$$R^\times = \{1, -1, i, i\}.$$

Sei $X_n = \{(a, b) \mid n = a^2 + b^2\}$, so dass $r_2(n) = \#X_n$. Man merkt, falls $(a, b) \in X_n$, dass $\{(a, b), (-a, -b), (-b, a), (b, -a)\}$ eine Untermenge von vier verschiedenen Elementen aus X_n ist. (Hier benutzen wir $n > 0$.) Also, wir definieren eine Äquivzlenzrelation $\sim$ in X_n nach $(a, b) \sim (-a, -b) \sim (-b, a) \sim (b, -a)$. Dann gilt $r_2(n) = \#X_n$ und $\rho_2(n) = \#(X_n/\sim)$.

Sei Y_n die Menge von Facktorlerzungen $n = \alpha\overline{\alpha}$ für $\alpha \in R$, damit für jedes $r \in R^\times$ wir $\alpha \cdot \overline{\alpha}$ mit $\alpha \cdot \overline{\alpha}$ identifizieren. Nach der eindeutigen Faktorzerlegung in R, ist $\#Y_{nm} = (\#Y_n)(\#Y_m)$, falls $\mathrm{ggT}(n, m)$ gilt. Da die Abbildung $(a, b) \mapsto \alpha \cdot \overline{\alpha}$ mit $a + bi$ ein Isomorphismus ist, folgt es, dass ρ_2 multiplikativ ist.

Sei $p \in \mathbb{Z}$ prim. Falls p als Element aus R reduzibel ist, dann folgt $p \equiv \alpha\beta$ für $\alpha, \beta \in R$ mit $N(\alpha) = N(\beta) = p$. Es folgt $p = a^2 + b^2$ hat eine Lösung $(a, b) \in \mathbb{Z}^2$. Also, nach Satz 14.2, ist p unzerlegbar in R, genau wenn $p \equiv 3 \pmod 4$ gilt. Dann folgt es $r_2(p^k) \neq 1$ für $p \equiv 3 \pmod 4$, genau wenn k ungerade ist.

Sei $p \equiv 1 \pmod 4$. Letztes mal haben wir gezeigt, dass $p = a^2 + b^2 = \alpha \cdot \overline{\alpha}$ für $\alpha \in R$. Danach finden wir

$$p^k = (\alpha^{k-i}\overline{\alpha}^i)(\overline{\alpha^{k-i}\overline{\alpha}^i}). \tag{15.1}$$

Da $a \neq b$, gibt es keine $\epsilon \in R^\times$, damit $\alpha = \epsilon\overline{\alpha}$. Also für jedes $0 \leq i \leq k$ repräsentiert die rechte Seite von (15.1) verschiedene Elementen aus Y_{p^k}. Es folgt $\rho_2(p^k) = k + 1$.

Dagegen, weil $2^k = (1 + i)^k(1 - i)^k$ gilt und $\overline{1 + i} = -i(1 + i)$ ist, besitzt Y_{2^k} nur ein Element deswegen ist $\rho_2(2^k) = 1$. □

16. 16 Juni

Falls $p \equiv 1 \pmod 4$, dann möchten wir die Lösungen $(a, b) \in X_p$ finden. Für p nicht gross, kann man einfact probieren, ob für $1 \leq a \leq \sqrt{p}$ $p - a^2$ ein Quadrat ist. Für grosseres Primzahlen ist Folgendes besser.

- Man sucht n damit $(\frac{n}{p}) = 1$, so dass für $n = a^{\frac{p-1}{4}}$
$$n^2 \equiv -1 \pmod p$$
gilt.
- In der Ring $\mathbb{Z}[i]$ ermittelt man $\mathrm{ggT}(n + i, p) = a + ib$.

Beispiel. Wir folgen dem vorhergegehendem Algorithmus mit $p = 4649$. Nach dem Verfahren der sukzessiven Quadrate kann man ermitteln, dass $(\frac{3}{p}) = 1$, so dass $3^{\frac{p-1}{4}} \equiv 1846 \pmod p$ eine Lösung von $x^2 \equiv -1 \pmod p$ ist. Um $\mathrm{ggT}(n + i, p)$ auszurechnen, nutzen wir

$$\frac{p}{1846i + 1} = \frac{p}{1846i + 1}\frac{1846 - i}{1846 - i} = \frac{1846}{733} - \frac{i}{733} = (2 + 0i) + \left(\frac{380}{733} - \frac{i}{733}\right),$$

so dass

$$p = (2 + 0i)(1846 + i) + r_1$$

mit $r_1 = 957 - 2i$ gilt. Wir teilen nochmal

$$\frac{1846 + i}{957 - 2i} = (2 + 0i) + \left(\frac{-14}{197} + \frac{i}{197}\right),$$

so dass

$$1846 + i = (2 + 0i)r_1 + r_2$$

mit $r_2 = -68 + 5i$. Da $r_1 = (-14 - i)r_2$, finden wir $\mathrm{ggT}(1846 + i, p) = -68 + 5i$ und

$$p = 4649 = 68^2 + 5^2.$$

Beispiel. Um die Lösungen (a, b) damit $a^2 + b^2 = n = 60437 = 13 \cdot 4649$ zu finden, benutzen wir die Faktorzerlegung $13 = \mu\overline{\mu}$ mit $\mu = 2 + 3i$ und $4649 = \lambda\overline{\lambda}$ mit $\lambda = 5 + 68i$. Die Elementen aus Y_n sind

$$(\mu\lambda)(\overline{\mu\lambda}), \quad (\mu\overline{\lambda})(\overline{\mu\overline{\lambda}}), \quad (\overline{\mu\lambda})(\mu\lambda), \quad (\overline{\mu\overline{\lambda}})(\mu\overline{\lambda}).$$

Die ersten zwei Beispiele davon führen nach

$$\mu\lambda = -194 + 151i, \qquad \mu\overline{\lambda} = 214 + i121.$$

Also finden wir

$$X_n = \{(\pm 151, \pm 194), (\pm 121, \pm 214), (\pm 194, \pm 151), (\pm 214, \pm 121)\}.$$

Es gibt viele Verallgemeinerungen der Frage, ob n als Summe von zwei Quadraten geschrieben werden können. Folgendes sind Beispiele davon.

Satz 16.1 (Gauss)**.** *Eine positive Zahl kann also Summe geschrieben werden, genau wenn sie nicht der Form* $4^\ell(8k+7)$ *für* $k \in \mathbb{N}$ *ist.*

Folgerung 16.2 (Gauss)**.** *Jedes* $n \in N$ *kann als Summe von drei dreieckige Zahlen geschrieben werden.*

Die *drieeckige Zahlen* sind,

$$0, 1, 3, 6, \ldots, \frac{n(n-1)}{2}, \ldots$$

Beweis der Folgerung: Sei $n \in \mathbb{N}$. Nach dem Satz 16.1 gibt es $p, q, r \in \mathbb{Z}$ damit $8n+3 = p^2+q^2+r^2$. Da $p^2+q^2+r^2 \equiv 3 \pmod 4$, folgt es, dass p, q, r ungerade sind, so dass

$$8n+3 = p^2+q^2+r^2 = (2a+1)^2+(2b+1)^2+(2c+1)^2 = 4a(a-1)+4b(b-1)+4c(c-1)+3$$

gilt. Es folgt

$$n = \frac{a(a-1)}{2} + \frac{b(b-1)}{2} + \frac{c(c-1)}{2}.$$

□

Satz 16.3 (Lagrange)**.** *Jedes* $n \in \mathbb{N}$ *kann als Summe von vier Quadraten geschrieben werden.*

Eine *k-eckige Zahl* ist eine der Form $(k-2)\binom{n}{2} + n$.

Satz 16.4 (Cauchy)**.** *Jedes* $n \in \mathbb{N}$ *kann als Summe von* k *k-eckige Zahlen geschrieben werden.*

Bemerkung. Die 4-eckige Zahlen sind die Quadrate. Das heißt, die Fälle $k = 3, 4$ von Cauchys Satz verallgemeinern die vorgegehenden Sätze von Gauss und Lagrange.

17. 20 Juni

Wir haben behauptet, dass die ganze Quaternionen

$$B = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$$

ein Ring erschaffen, wenn wir Folgendes definieren:

$$i^2 = j^2 = k^2 = ijk = -1, \quad ax = xa \; \forall x \in \{i, j, k\}, a \in \mathbb{Z}.$$

Die Quaternionen besitzt eine *Konjugation*

$$\overline{a + bi + cj + dk} = a - bi - cj - dk$$

und *Norm*

$$N(a + bi + cj + dk) = (a + bi + cj + dk)(\overline{a + bi + cj + dk}) = a^2 + b^2 + c^2 + d^2.$$

Davon kann man relativ einfach beweisen, dass

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = \alpha^2+\beta^2+\gamma^2+\delta^2 \tag{17.1}$$

mit

$$\begin{aligned}\alpha &= aA+bB+cC+dD\\ \beta &= -aB+bA-cD+dC\\ \gamma &= -aC+bD+cA-dB\\ \delta &= -aD-bc+cB+dA\end{aligned}$$

gilt. (Wir bemerken, dass die Eulersche Identität und $N(\mu)N(\lambda) = N(\mu\overline{\lambda})$ für $\mu, \lambda \in B$ sind äquivalent.) Gleichung (17.1) heißt *Eulersche Identität*.

Beweis des Satzes von Lagrange: Wir mussen zeigen, dass jedes $n \in \mathbb{N}$ als Summe von vier Quadraten geschrieben werden können. Nach der Eulerschen Identität müssen wir nur zeigen, dass der Satz für $n = p$ eine Primzahl gilt. Sei

$$X = \{i^2 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \le i \le \frac{p-1}{2}\}$$

und

$$Y = \{i^2 \in \mathbb{Z}/p\mathbb{Z} \mid 0 \le i \le \frac{p-1}{2}\}.$$

Da $c^2 \equiv d^2 \pmod p$ gilt, genau wenn $c \equiv \pm d \pmod p$, gilt es $\#X = \#Y = \frac{p+1}{2}$, so dass $X \cap Y \neq \emptyset$. Also finden wir $0 \le x, y \le \frac{p-1}{2}$, so dass $x^2 = -1 - y^2 \pmod p$ und

$$p \mid x^2+y^2+1 \implies pm_0 = x^2+y^2+1^+0^2$$

mit

$$0 < m_0 \le \frac{x^2+y^2+1}{p} \le \frac{p}{4}+\frac{p}{4}+\frac{1}{p} < p.$$

Sei m die kleinste positive Zahl damit

$$pm = a^2+b^2+c^2+d^2.$$

Nach was wir gerade gezeigt habe, dürfen wir annehmen, dass solche m existiert und $1 \le m < p$ gilt. Setzen wir $m > 1$ voraus. Es seien $a \equiv A \pmod m$, $b \equiv B \pmod m$, $c \equiv C \pmod m$ und $d \equiv D \pmod m$ mit $A, B, C, D \in (-\frac{m}{2}, \frac{m}{2}]$. Es folgt

$$pm = a^2+b^2+c^2+d^2 \equiv A^2+B^2+C^2+D^2 \pmod m, \tag{17.2}$$

so dass $m \mid A^2+B^2+C^2+D^2$ gilt. Außerdem finden wir

$$rm = A^2+B^2+C^2+D^2 \implies 0 \le r = \frac{A^2+B^2+C^2+D^2}{m} \le m. \tag{17.3}$$

Falls $r = 0$ gilt dann folgt es $A = B = C = D = 0$, so dass $m \mid a, b, c, d$. Es folgt davon, dass $pm = m^2(a'^2 + b'^2 + c'^2 + d'^2)$ gilt, so $m \mid p$. Für $m > 1$ ist das ein Widerspruch. Falls $r = m$ gilt dann folgt $A = B = C = D = \frac{m}{2}$. So finden wir

$$pm = a^2 + b^2 + c^2 + d^2 \equiv A^2 + B^2 + C^2 + D^2 \equiv 0 \pmod{m^2},$$

so dass $m^2 \mid mp$, nochmal ein Widerspruch. So haben wir gezeigt, dass $0 < r < m$. Nach (17.2), (17.3) und der Eulerschen Identität finden wir

$$pm^2 r \equiv \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

Außerdem folgt es nach der Eulerschen Identität, dass

$$\begin{aligned}
\alpha =& aA + bB + cC + dD \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m},\\
\beta =& -aB + bA - cD + dC \equiv -ab + ba - cd + dc \equiv 0 \pmod{m},\\
\gamma =& -aC + bD + cA - dB \equiv -ac + bd + ca - db \equiv 0 \pmod{m},\\
\delta =& -aD - bc + cB + dA \equiv -ad - bc + cb + da \equiv 0 \pmod{m}
\end{aligned}$$

gilt. Das heißt $m \mid \alpha, \beta, \gamma, \delta$. Es folgt

$$pr = \alpha'^2 + \beta'^2 + \gamma'^2 + \delta'^2,$$

ein Widerspruch zur Minimalität von m. □

Es seien $x_0, x_1, \ldots, x_k \in \mathbb{R}$ mit $x_j > 0$ für $1 \leq j \leq r$. Dann heißt

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots + \cfrac{1}{x_{n-1} + \cfrac{1}{x_n}}}}} = [x_0, x_1, \ldots, x_k]$$

ein *allgemeiner (endlicher) Kettenbruch*. Falls $a_0 \in \mathbb{Z}$ und $a_1, \ldots, a_k \in \mathbb{N}$ ist, dann heißt der Kettenbruch *einfach* oder *regelmäßig*. Ähnlicherweise definiert man *unendlicher Kettenbruch* $[a_0, a_1, \ldots]$.

Es sei $x \in \mathbb{R}$, $x \neq 0$. Dann ist die *Kettenbruchdarstellung* von x nach Folgendem definiert. Sei $a_0 = \lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$ und $\delta_0 = x - a_0$. Wenn a_n und δ_n definiert sind, setzen wir dann $\delta_{n+1} = \frac{1}{\delta_n - a_n}$. Solange wie $\delta_{n+1} \neq 0$ gilt setzen wir $a_{n+1} = \lfloor \delta_{n+1} \rfloor$. Es folgt

$$x = a_0 + (\delta_0 - a_0) = a_0 + \frac{1}{\delta_1} == a_0 + \cfrac{1}{a_1 + \cfrac{1}{\delta_2}} == a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\delta_2}}} = [a_0, a_1, a_2 \ldots]$$

Die Kettenbruch ist unendlich, falls $x \notin \mathbb{Q}$.

Beispiel. Sei $x = \sqrt{2} + \sqrt{3}$. Dann finden wir

$$x = [3, 6, 1, 5, 7, 1, 1, \ldots].$$

Definition. Es seien $a_0 \in \mathbb{Z}$ und eine Folge $a_1, a_2, \ldots$ in $\mathbb{N}$ gegeben, so dass $[a_0, a_1, \ldots]$ ein unendlicher regelmäßiger Kettenbruch ist. Man nennt $r_n = \frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n] \in \mathbb{Q}$ den *n-ten Näherungsbruch* von $[a_1, a_1, \ldots]$.

18. 23 Juni

Bemerkung. Falls $\frac{a}{b} \in \mathbb{Q}$ mit $\mathrm{ggT}(a, b) = 1$. Die Zahlen $q_n \in \mathbb{Z}$, die man durch die Kettenbruchdarstellung von $\frac{p}{q}$ findet, sind die „Quotienten", die man durch den Euklidischen Algorithmus findet:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

mit $0 \neq r_n = \mathrm{ggT}(a, b)$. Dass heißt, falls $\frac{a}{b} \in \mathbb{Q}$ gilt, ist die Kettenbruchdarstellung von $\frac{a}{b}$ endlich. Und zwar, es gilt

$$\frac{a}{b} = [q_0, q_1, \ldots, q_{n+1}]$$

mit $q_{n+1} \neq 1$.

Bemerkung. Jedes $x \in \mathbb{Q}$ hat verschiedene Kettenbruchdarstellungen. Falls $x = [a_0, a_1, \ldots, a_k]$ gilt, dann folgt, z.B.,

$$[a_0, a_1, \ldots, a_k] = [a_0, a_1, \ldots, a_{k-1} + \frac{1}{a_k}] = [a_0, a_1, \ldots, a_k - 1, 1]. \tag{18.1}$$

Die Elementen von diesen Darstellungen könnten alles ganze Zahlen sein, genau wenn $a_j \in \mathbb{Z}$ für jedes j und $a_k = 1$.

Satz 18.1. *Gilt für zwei regelmäßige Kettenbrüche $[a_0, a_1, \ldots, a_k] = [b_0, b_1, \ldots, b_n]$ und $a_k > 1$, $b_n > 1$, so folgt $k = n$ und $a_j = b_j$ für $0 \leq j \leq k$. Jede rationale Zahl q besitzt genau eine Darstellung $q = [a_0, a_1, \ldots, a_k]$ als regelmäßiger Kettenbruch mit $a_k > 1$.*

Idee des Beweises: Man setzt $x_j = [a_j, a_{j+1}, \ldots, a_k]$, $y_j = [b_j, b_{j+1}, \ldots, b_n]$ für $0 \leq j \leq k$ bzw. n. Für $j \geq 1$ ist $x_j > 0$, $y_j > 0$. Es gilt

$$x_j = a_j + \frac{1}{[a_{j+1}, \ldots, a_k]} = a_j + \frac{1}{x_{j+1}}.$$

Es folgt $x_j > 1$ für $1 \leq j \leq k-1$ und $a_j < x_j < a_j + 1$ für $0 \leq j \leq k-1$. Es ist $x_k = a_k > 1$. Daher gilt $a_j = \lfloor x_j \rfloor$ für $0 \leq j \leq k$. Ebenso gilt $y_j = b_j + \frac{1}{y_{j+1}}$, $b_j < y_j < b_j + 1$, $0 \leq j \leq n-1$ und $b_j = \lfloor y_j \rfloor$ für $0 \leq j \leq n$. Nach Voraussetzung gilt $x_0 = y_0$. Daher folgt

$$a_0 = \lfloor x_0 \rfloor = \lfloor y_0 \rfloor = b_0.$$

Nach Induktion, kann man zeigen, dass $x_j = y_j$, $a_j = b_j$ für alle $0 \leq j \leq \min\{k, n\}$ gilt. Angenommen, es wäre $k < n$. Dann folgt $x_k = y_k$,

$$a_k = b_k = y_k - \frac{1}{y_{k+1}} < y_k = x_k,$$

ein Widerspruch zu $a_k = x_k$. Damit folgt $k = n$. □

Satz 18.2. *Es seien ein $a_0 \in \mathbb{Z}$ und eine Folge $(a_\nu)_{\nu \geq 1}$ von Zahlen $a_\nu \in \mathbb{Z}$ gegeben. Die Folgen $(p_n)_{n \geq -2}$ und $(q_n)_{n \geq -2}$ werden rekursiv definiert durch*

$$\begin{array}{rclrclrcl} p_{-2} & = & 0, & p_{-1} & = & 1, & p_n & = & a_n p_{n-1} + p_{n-2}, \\ q_{-2} & = & 1, & q_{-1} & = & 0, & q_n & = & a_n q_{n-1} + q_{n-2}. \end{array} \qquad n \geq 0$$

Man setze $r_n = [a_0, a_1, \ldots, a_n]$ für $n \geq 0$. Für alle $n \geq 1$ gilt dann:

(1) *Für alle $x \in \mathbb{R}$, $x > 0$ gilt*

$$[a_0, a_1, \ldots, a_{n-1}, x] = \frac{x h_{n-1} + h_{n-2}}{x q_{n-1} + q_{n-2}}.$$

(2) *Es gilt $r_n = \frac{p_n}{q_n}$ mit $\mathrm{ggT}\,(p_n, q_n) = 1$.*

(3) *Es gilt für $n \geq -1$*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

und

$$r_n - r_{n-1} = (-1)^{n-1} \frac{1}{q_n q_{n-1}}.$$

(4) *Für $n \geq 0$ gilt*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$$

und

$$r_n - r_{n-2} = (-1)^n \frac{a_n}{q_n q_{n-2}}.$$

Beweis:

(1) Für $n = 0$ steht rechts x, links $[x] = x$. Für $n = 1$ steht links

$$[a_0, x] = a_0 + \frac{1}{x},$$

rechts

$$\frac{x p_0 + p_{-1}}{x q_0 + q_{-1}} = \frac{x a_0 + 1}{x} = a_0 + \frac{1}{x}.$$

Für ein $n \geq 1$ und alle $x > 0$ sei (1) gültig. Dann folgt:

$$[a_0, a_1, \ldots, a_n, x] = \left[a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{x}\right] = \frac{\left(a_n + \frac{1}{x}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{x}\right) q_{n-1} + q_{n-2}}$$
$$= \frac{x\left(a_n p_{n-1} + p_{n-2}\right) + p_{n-1}}{x\left(a_n q_{n-1} + q_{n-2}\right) + q_{n-1}} = \frac{x p_n + p_{n-1}}{x q_n + q_{n-1}}.$$

(2) Man setzt $x = a_n$ in (1) ein und erhält

$$r_n = [a_0, a_1, \ldots, a_n] \overset{(1)}{=} \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

(Teilerfremdheit folgt (3)).

(3) Aufgabe für den Student.

(4) Es ist

$$p_0 q_{-2} - p_{-2} q_0 = a_0$$

und

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= \left(a_n p_{n-1} + p_{n-2}\right) q_{n-2} - p_{n-2}\left(a_n q_{n-1} + q_{n-2}\right) \\ &= a_n\left(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}\right) = (-1)^n a_n. \end{aligned}$$

Sowie

$$r_n - r_{n-2} = \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}.$$

□

Satz 18.3. *Es seien ein $a_0 \in \mathbb{Z}$ und eine Folge $a_1, a_2, a_3, \ldots$ in $\mathbb{N}$ gegeben. Man setze $r_n = [a_0, a_1, \ldots, a_n]$ für $n \geq 0$. Dann gilt $r_0 < r_2 < r_4 < \ldots < r_5 < r_3 < r_1$ und es existiert* $\lim_{n\to\infty} r_n$.

Beweis: Nach Satz 18.2 (4) gilt $r_n - r_{n-2} > 0$ für gerade n und $r_n - r_{n-2} < 0$ für ungerade n. Nach Satz 18.2 (3) gilt $r_{2n} - r_{2n-1} < 0$. Daher folgt

$$r_{2n} < r_{2n+2\nu} < r_{2n+2\nu-1} < r_{2n-1} \quad \forall n, \nu \in \mathbb{N}.$$

Nach Satz 18.2 (3) ist

$$r_n - r_{n-1} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$$

und $q_n \to \infty$. Daher sind die Grenzwerte gleich und es existiert $\lim_{n\to\infty} r_n$. □

19. 27 Juni

Jetzt wissen wir, dass für jeden regelmäßigen Kettenbruch $[a_0, \ldots]$, der Grenzwert von $r_n = [a_0, \ldots, a_n]$ als $n \to \infty$ zu einer reellen Zahl konvergiert. Einige Fragen, die wir noch beatworten müssen, sind Folgende.

- Es sei $x \in \mathbb{R}$. Gibt es einen regelmäßigen Kettenbruch $[a_0, \ldots]$ damit $x = \lim_{n\to\infty}[a_0, \ldots, a_n]$?
- Als Beispiel von der letzten Frage: gibt es einen unendlichen regelmäßigen Kettenbruch $[a_0, a_1, \ldots]$, damit $\lim_{n\to\infty}[a_0, \ldots, a_n] \in \mathbb{Q}$?
- Für $x \in \mathbb{R}$ damit $x = \lim_{n\to\infty}[a_0, \ldots, a_n]$, in welchem Art ist der Kettenbruch $[a_0, \ldots]$ eindeutig?

Satz 19.1. *Der Grenzwert eines jeden unendlichen regelmäßigen Kettenbruchs ist irrational.*

Idee des Beweises: Es sei $x = [a_0, a_1, a_2, \ldots]$ und p_n, q_n, r_n seien wie in Satz 18.2 erklärt. Nach Satz 18.3 gilt $r_{2n} < x < r_{2n+1}$, also

$$0 < |x - r_n| < |r_{n+1} - r_n|.$$

Aus Satz 18.2 (2), (3) folgt daher

$$0 < \big|q_n x - p_n\big| < q_n\big|r_{n+1} - r_n\big| = \frac{1}{q_{n+1}}.$$

Man kann damit zeigen, dass ein Widerspruch wäre, falls $x = \frac{a}{b} \in \mathbb{Q}$ wäre. □

Hilfssatz 19.2. *Es sei $x = [a_0, a_1, a_2, \ldots]$ ein unendlicher Kettenbruch und es sei $x_1 = [a_1, a_2, a_3, \ldots]$. Dann gilt $a_0 = \lfloor x \rfloor$ und $x = a_0 + \frac{1}{x_1}$.*

Beweis: Es gilt $r_0 < x < r_1$, also

$$a_0 < x < a_0 + \frac{1}{a_1} \leq a_0 + 1.$$

Also gilt $a_0 = \lfloor x \rfloor$. Aus Satz 18.3 folgt

$$\begin{aligned} x &= \lim_{n\to\infty}[a_0, a_1, \ldots, a_n] = \lim_{n\to\infty}\left(a_0 + \frac{1}{[a_1, \ldots, a_n]}\right) \\ &= a_0 + \frac{1}{\lim_{n\to\infty}[a_1, \ldots, a_n]} = a_0 + \frac{1}{x_1}. \end{aligned}$$

□

Satz 19.3. *Je zwei verschiedene unendliche regelmäßige Kettenbrüche haben verschiedene Grenzwerte.*

Beweis: Mit $a_0, b_0 \in \mathbb{Z}$, $a_n, b_n \in \mathbb{N}$ für $n \geq 1$ wird

$$[a_0, a_1, \ldots] = x = [b_0, b_1, \ldots]$$

vorausgesetzt. Aus Hilfssatz 19.2 folgt dann $a_0 = \lfloor x \rfloor = b_0$ und

$$[a_1, a_2, \ldots] = \frac{1}{x - a_0} = x_1 = \frac{1}{x - b_0} = [b_1, b_2, \ldots].$$

Induktiv folgt somit $a_n = b_n$ für alle $n \geq 0$. □

Satz 19.4 (Kettenbruchalgorithmus)**.** *Jede irrationale reelle Zahl besitzt genau eine Entwicklung in einen unendlichen regelmäßigen Kettenbruch $x = [a_0, a_1, \ldots]$. Man erhält die a_n rekursiv aus*

$$\begin{array}{lllll} \alpha_0 & = & \alpha, & a_0 & = & \lfloor \alpha_0 \rfloor, \\ \alpha_{n+1} & = & \frac{1}{\alpha_n - a_n}, & a_{n+1} & = & \lfloor \alpha_{n+1} \rfloor \quad \textit{für } n \geq 0. \end{array}$$

Beweis: Die Eindeutigkeit ergibt sich aus Satz 19.3. Wegen $\alpha \notin \mathbb{Q}$ ist durch die Rekursionsformel im Satz eine Folge $(a_n)_{n \geq 0}$ mit $a_n \in \mathbb{Z}$ wohldefiniert, denn es ist $\alpha_n \notin \mathbb{Z}$ für alle n. Offenbar gilt $a_n \in \mathbb{N}$ für alle $n \geq 1$. Es gilt:

$$\alpha = \alpha_0 = a_0 + \frac{1}{\alpha_1} = [a_0, \alpha_1] = \left[a_0, a_1 + \frac{1}{\alpha_2}\right] = [a_0, a_1, \alpha_2]$$

und induktiv folgt $\alpha = [a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n]$ für alle $n \geq 1$. Aus Satz 18.2 (1) folgt

$$\alpha = [a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}.$$

Aus Satz 18.2 (2), (3) folgt nun

$$\alpha - r_{n-1} = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_{n-2} q_{n-1} - p_{n-1} q_{n-2}}{q_{n-1} \left(\alpha_n q_{n-1} + q_{n-2}\right)} = \frac{(-1)^{n+1}}{q_{n-1} \left(\alpha_n q_{n-1} + q_{n-2}\right)}.$$

Wegen $\alpha_n > 1$ und $q_n \to \infty$ folgt hieraus $\lim_{n \to \infty} r_n = \alpha$, also $\alpha = [a_0, a_1, \ldots]$. □

20. 30 Juni

Definition. Es sei $\alpha \in \mathbb{Q}$ gegeben, $\alpha = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $\mathrm{ggT}(a, b) = 1$, $0 < \alpha < 1$. Die Dezimaldarstellung

$$\alpha = 0, a_1 a_2 a_3 \ldots = \sum_{\nu=1}^{\infty} a_\nu 10^{-\nu}$$

mit $a_\nu \in \{0, 1, \ldots, 9\}$ ist eindeutig, wenn man „Neunerenden“ ausschließt. Man nennt diese Darstellung *periodisch*, wenn es ganze Zahlen $m \geq 0$, $\ell > 0$ gibt mit $a_{\nu+\ell} = a_\nu$ für alle $\nu > m$. Wählt man dann m und ℓ minimal, so heißt m die *Länge der Vorperiode*, ℓ die *Länge der Periode*, $a_1 \ldots a_m$ die *Vorperiode* von α und $a_{m+1} \ldots a_{m+\ell}$ die *Periode* von α. Man schreibt dann $\alpha = 0, a_1 \ldots a_m \overline{a_{m+1} \ldots a_{m+\ell}}$.

Beispiele.

$$\frac{1}{15} = 0,0\overline{6} \qquad\qquad \frac{1}{7} = 0,\overline{142857}.$$

Satz 20.1. *Eine Dezimaldarstellung stellt genau dann eine rationale Zahl dar, wenn sie periodisch ist.*

Beweis: Die Dezimaldarstellung von $\alpha = \frac{a}{b}$ gekürzt, $0 < \alpha < 1$ erhält man wie folgt:

$$\begin{aligned} a &= r_1, \quad 0 < r_1 < b, \\ 10r_1 &= a_1 b + r_2, \quad 0 \le r_2 < b, \\ 10r_2 &= a_2 b + r_3, \quad 0 \le r_3 < b, \\ &\vdots \end{aligned}$$

Damit wird

$$\alpha = \frac{a}{b} = \frac{10r_1}{10b} = \frac{a_1}{10} + \frac{r_2}{10b} = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{r_3}{10^2 b} = \ldots = 0, a_1 a_2 a_3 \ldots.$$

Wegen $r_\nu \in \{0, 1, \ldots, b-1\}$ existieren μ, ν mit $\mu < \nu$ und $r_\mu = r_\nu$. Dann folgt $a_k = a_{k+(\nu-\mu)}$ für alle $k \ge \mu$. Also ist die Entwicklung von α periodisch (mit $r \le b$, $s \le b$).
Der Rest des Beweises wird für den Student als Hausaufgabe gelassen. □

Wir definieren ähnlicherweise, was ein *periodischer Kettenbruch* ist.

Definition. Ein unendlicher regelmäßiger Kettenbruch $[a_0, a_1, \ldots]$ heißt *periodisch*, falls es ganze Zahlen $m \ge 0$ und $\ell > 0$ gibt, so dass $a_{k+\ell} = a_k$ für alle $k \ge m$ gilt. Man schreibt dann

$$[a_0, a_1, a_2, \ldots] = [a_0, a_1, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+\ell-1}}].$$

Ein Beispiel ist

$$\frac{1}{2}\left(\sqrt{5}+1\right) = [1, 1, 1, \ldots] = [\overline{1}].$$

Im Falle $m = 0$ heißt der Kettenbruch *rein periodisch*.

Definition. Eine Zahl $\alpha \in \mathbb{C}$ heißt *algebraisch*, falls es ein Polynom $p \in \mathbb{Z}[x]$, $p \neq 0$ gibt mit $p(\alpha) = 0$. Der Grad des kleinsten Polynoms mit $p(\alpha) = 0$ heißt der *Grad von* α.

Eine Zahl $x \in \mathbb{R} \setminus \mathbb{Q}$ heißt *irrational*. Falls $\alpha \in \mathbb{C}$ nicht algebraisch ist, heißt x *transzendent*. Falls der Grad von α zwei ist, nennt man α ein *quadratische Irrationalzahl*.

Bemerkung. Jede reelle quadratische Irrationalzahl α ist der form

$$\alpha = \frac{a + \sqrt{b}}{d}$$

für $a, b, c \in \mathbb{Z}$, $d \neq 0$, b kein Quadrat.

Satz 20.2 (Euler, Lagrange)**.** *Jeder periodische Kettenbruch stellt eine reelle quadratische Irrationalzahl dar. Jede reelle quadratische Irrationalzahl besitzt eine periodische Kettenbruchentwicklung.*

Bemerkung. Es sei $x \in \mathbb{R}$. Nach dem Kettenbruchalgorithmus haben wir

$$\alpha_0 = x, \quad \text{und} \quad a_0 = \lfloor \alpha_0 \rfloor,$$
$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \quad \text{und} \quad a_{n+1} = \lfloor \alpha_{n+1} \rfloor$$

für $n \geq 0$. Nehmen wir an, dass $\alpha_m = \alpha_{m+\ell}$ für $m \geq$ und $\ell \geq 1$ gilt. Dann gilt es

$$a_{m+\ell} = \lfloor \alpha_{m+\ell} \rfloor = \lfloor \alpha_m \rfloor = a_m$$

und

$$\alpha_{m+\ell+1} = \frac{1}{\alpha_{m+\ell} - a_{m+\ell}} = \frac{1}{\alpha_m - a_m} = \alpha_{m+1}.$$

Induktiv ist damit $x = [a_0, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+\ell-1}}]$ periodisch.

Beispiel. Es sei $x = \frac{1+2\sqrt{5}}{3}$. Da $\sqrt{5} \approx 2.2$ ist, finden wir dann

$$\begin{aligned}
\alpha_0 &= \tfrac{1+2\sqrt{5}}{3} & a_0 = 1 &\Longrightarrow \alpha_0 - a_0 = \tfrac{2(\sqrt{5}-1)}{3} \\
\alpha_1 &= \tfrac{3}{2(\sqrt{5}-1)} = \tfrac{3(1+\sqrt{5})}{8} & a_1 = 1 &\Longrightarrow \alpha_1 - a_1 = \tfrac{3\sqrt{5}-5}{8} \\
\alpha_2 &= \tfrac{3}{3\sqrt{5}-5} = \tfrac{2(5+3\sqrt{5})}{5} & a_2 = 4 &\Longrightarrow \alpha_2 - a_2 = \tfrac{2(3\sqrt{5}-5)}{5} \\
\alpha_3 &= \tfrac{5}{2(3\sqrt{5}-5)} = \tfrac{5+3\sqrt{5}}{8} & a_3 = 1 &\Longrightarrow \alpha_3 - a_3 = \tfrac{3(\sqrt{5}-1)}{8} \\
\alpha_4 &= \tfrac{8}{3(\sqrt{5}-1)} = \tfrac{2(1+\sqrt{5})}{3} & a_4 = 2 &\Longrightarrow \alpha_4 - a_4 = \tfrac{2(\sqrt{5}-2)}{3} \\
\alpha_5 &= \tfrac{3}{2(\sqrt{5}-2)} = \tfrac{3(\sqrt{5}+2)}{2} & a_5 = 6 &\Longrightarrow \alpha_5 - a_5 = \tfrac{3(\sqrt{5}-2)}{2} \\
\alpha_6 &= \tfrac{2}{3(\sqrt{5}-2)} = \tfrac{2(\sqrt{5}+2)}{3} & a_6 = 2 &\Longrightarrow \alpha_6 - a_6 = \tfrac{2(\sqrt{5}-1)}{3} \\
\alpha_7 &= \tfrac{3}{2(\sqrt{5}-1)} = \tfrac{3(1+\sqrt{5})}{8} = \alpha_1
\end{aligned}$$

Nach der Bermerkung folgt es, dass

$$\frac{1+2\sqrt{5}}{3} = [1, \overline{4, 1, 2, 6, 2}]$$

gilt.

Beweis von Satz 20.2 $\Longrightarrow$: Es sei $\alpha = [a_0, \ldots, a_{m-1}, \overline{b_0, \ldots, b_{m+\ell-1}}]$. Man setze

$$B = [\overline{b_0, \ldots, b_{m+\ell-1}}]$$

Dann gilt es nach Satz 18.2 (1)

$$\alpha = [a_0, \ldots, a_{m-1}, B] = \frac{Bp'_{m-1} + p'_{m-2}}{Bq'_{m-1} + q'_{m-2}}$$

für bestimmte $p'_j, q'_j \in \mathbb{Z}$. Falls $B = \frac{a+\sqrt{d}}{c}$ kann man einfach zeigen, dass α auch der richtigen Form ist.

Nun seien p_n und q_n zu B wie in Satz 18.2, damit

$$B = [b_0, \ldots, b_{\ell-1}, B] = \frac{Bp_{m-1} + p_{m-2}}{Bq_{m-1} + q_{m-2}}$$

und

$$q_{n-1}B^2 + (q_{n-2} - p_{n-1})B - p_{n-2} = 0$$

gilt. Somit löst B eine quadtratische Gleichung über $\mathbb{Z}$ und wegen $B \in \mathbb{R} \setminus \mathbb{Q}$ ist B eine reelle quadratische Irrationalzahl. □

Satz 20.3. *Es sei $d \in \mathbb{N}$ kein Quadrat und ℓ die Länge der kürzesten Periode in der Kettenbruchentwicklung von $a = \sqrt{d}$. Dann gilt*

$$\sqrt{d} = [a_0, \overline{a_1, \ldots, a_{\ell-1}, a_\ell}]$$

mit $a_0 = \lfloor \sqrt{d} \rfloor$.

Satz 20.4. *Es sei $d \in \mathbb{N}$ kein Quadrat, $\frac{p}{q} = \frac{p_{\ell-1}}{q_{\ell-1}}$ die Näherungsbrüche für ℓ die kürzeste Periode der Kettenbruchentwicklung von $\sqrt{d}$. Dann ist*

$$(x, y) = \begin{cases} (p, q) & \text{falls } \ell \text{ gerade ist,} \\ (p^2 + dq^2, 2pq) & \text{falls } \ell \text{ ungerade ist.} \end{cases}$$

21. 4 Juli

Beweis von Satz 20.2 $\Longleftarrow$: Es sei $\alpha = \frac{a+\sqrt{b}}{c}$ für $a, b, c \in \mathbb{Z}$, $c \neq 0$ und $b > 0$ kein Quadrat. Dann gilt es

$$\alpha = \begin{cases} \frac{ac+\sqrt{c^2 b}}{c^2} & \text{falls } c > 0, \\ \frac{-ac+\sqrt{c^2 b}}{-c^2} & \text{falls } c < 0. \end{cases}$$

In jedem Fall gilt es $\alpha = \frac{m_0+\sqrt{d}}{s_0}$ mit $s_0 \mid d - m_0^2$. Es seien

$$m_{n+1} = a_n s_n - m_n,$$
$$s_{n+1} = \frac{d - m_{n+1}^2}{s_n}$$

für $n \geq 0$.

Zur Erinnerung: Nach dem Kettenbruchalgorithmus gilt es $\alpha = [a_0, a_1, \ldots]$ für $\alpha_0 = \alpha$, $a_0 = \lfloor \alpha_0 \rfloor$,

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} \quad \text{und} \quad a_{n+1} = \lfloor \alpha_{n+1} \rfloor.$$

Wir behaupten, dass

$$\alpha_n = \frac{m_n + \sqrt{d}}{s_n}$$

gilt. Die Behauptung ist klar für $n = 0$. Nehmen wir an, dass sie für ein beliebeges n gilt. Dann ist

$$s_{n+1} = \frac{d - m_n^2}{s_n} = \frac{d - (a_n s_n - m_n)^2}{s_n} = \frac{d - m_n^2}{s_n}$$

nach Voraussetzung eine ganze Zahl und

$$\begin{aligned}\alpha_{n+1} =& \frac{1}{\alpha_n - a_n} = \frac{1}{\frac{m_n+\sqrt{d}}{s_n} - a_n} = \frac{s_n}{m_n - a_n s_n + \sqrt{d}} \\ =& \frac{s_n}{\sqrt{d} - m_{n+1}} = \frac{s_n(m_{n+1} + \sqrt{d})}{d - m_{n+1}^2} = \frac{m_{n+1} + \sqrt{d}}{q_{n+1}}.\end{aligned}$$

So wird die Behauptung nach Induktion beweisen.

Es gilt dann

$$\alpha = \alpha_0 = [a_0, \ldots, a_{m-1}, \alpha_n] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

für p_k, q_k wie in Satz 18.2 erklärt. Die zu α_n konjugierten Zahlen sind $\alpha_n' = \frac{m_n - \sqrt{d}}{s_n}$ und es gilt

$$\alpha' = \left(\frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}\right)' = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}.$$

Auflösen nach α_n' ergibt

$$\frac{m_n - \sqrt{d}}{s_n} = \alpha_n' = -\frac{\alpha' q_{n-2} - p_{n-2}}{\alpha' q_{n-1} - p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}} \frac{\alpha' - r_{n-2}}{\alpha' - r_{n-1}}.$$

Da $q_k > 0$ für jedes $k \in \mathbb{N}$ und

$$\lim_{n\to\infty} \frac{\alpha' - r_{n-2}}{\alpha' - r_{n-1}} = \frac{\alpha' - \alpha}{\alpha' - \alpha} = 1 > 0.$$

gilt, daher folgt die Existenz eines N mit $\alpha_n' < 0$ für alle $n \geq N$.

Nach dem Kettenbruchalgorithmus ist $\alpha_n > 0$ für alle $n \geq 1$. Es folgt

$$\frac{2\sqrt{d}}{s_n} = \alpha_n - \alpha_n' > 0$$

für alle $n \geq N$ und somit $s_n > 0$ für alle $n \geq N$.

Nun folgt

$$0 < q_n \leq q_n q_{n+1} = d - m_{n+1}^2 \leq d$$

für alle $n \geq N$, sowie

$$m_{n+1}^2 = d - q_n q_{n+1} < d,$$

also $|m_{n+1}| < \sqrt{d}$ für alle $n \geq N$.

Für $n \geq N$ können also s_n und m_{n+1} nur endlich viele Werte annehmen. Daher ist $\{\alpha_n \mid n \in \mathbb{N}\}$ endlich und existieren m und ℓ mit $m < \ell$ und $\alpha_m =$

α_ℓ. Es folgt nach der Bemerkung nach der Aussage des Satzes 20.2, dass $\alpha = [a_0, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+\ell-1}}]$ periodisch ist. □

Satz 20.3 und Satz 20.4 sind Konsequenzen des folgenden Satzes von Galois.

Die Beide Sätze hängen vom folgenden ab.

Satz 21.1 (Galois)**.** *Es sei α eine reelle quadratische Irrationalzahl. Die Kettenbruchentwicklung von α ist genau dann rein periodisch, wenn $\alpha > 1$ und $-1 < \alpha' < 0$ ist.*

Beweis: Hausaufgabe für den Student. □

Beweis von Satz 20.3: Es sei $\alpha = \sqrt{d} = [a_0, a_1 \ldots]$, $d \in \mathbb{N}$ kein Quadrat. Es sei $\gamma = \lfloor\sqrt{d}\rfloor + \sqrt{d} = [c_0, c_1, \ldots]$. Da $c_0 = 2\lfloor\sqrt{d}\rfloor = 2a_0 > 1$ und $-1 < \gamma' = \lfloor\sqrt{d}\rfloor - \sqrt{d} < 0$ gelten, finden wir nach Satz 21.1, dass $\gamma = [\overline{2a_0, c_1, \ldots, c_{\ell-1}}]$ rein periodisch ist. So folgt es

$$\alpha = \gamma - a_0 = [a_0, \overline{c_1, \ldots, c_{\ell-1}, 2a_0}].$$

□

In statt Satz 20.4 zu beweisen, beweisen wir das folgende allgemeinere Ergebnis.

Satz 21.2. *Es sei $\alpha = \sqrt{d}$ für $d \in \mathbb{N}$ kein Quadrat. Es seien p_n, q_n wie in Satz 18.2 und s_n wie im Beweis von Satz 20.2 und ℓ wie in Satz 20.3. Dann gilt $s_n = 1$ genau wenn $\ell \mid n$ und $s_n \neq -1$ für jedes $n \in \mathbb{N}$. Außerdem gilt es für jedes $n \geq -1$*

$$p_n^2 - dq_n^2 = (-1)^{n+1} s_{n+1}.$$

Insbesondere

$$p_{n\ell-1}^2 - dq_{n\ell-1}^2 = (-1)^{n\ell}.$$

Bemerkung. Falls (p, q) eine Lösung von $x^2 - dy^2 = -1$ ist, folgt es

$$(p - q\sqrt{d})(p + q\sqrt{d}) = p^2 - q^2 d = -1.$$

Wir können beide Seite quadraten. Daraus kommt

$$\big((p^2 + q^2 d) - 2pq\sqrt{d}\big)\big((p^2 + q^2 d) + 2pq\sqrt{d}\big) = (p - q\sqrt{d})^2 (p + q\sqrt{d})^2 = 1.$$

So folgt Satz 20.4 nach Satz 21.2.

Satz 21.2 bedeutet, dass die Näherungsbrüche der Kettenbruchentwicklung von $\sqrt{d}$ Lösungen von den Pellschen Gleichungen sind. Folgendes ist die Rückrichtung.

Satz 21.3. *Es sei $d \in \mathbb{N}$ kein Quadrat. Es seien $\frac{p_n}{q_n}$ die Näherungsbrüche der Kettenbruchentwicklung von $\sqrt{d}$. Es sei $N \in \mathbb{Z}$ mit $0 < |N| < \sqrt{d}$.*

Zu jeder Lösung $x, y \in \mathbb{N}$ der Pelleschen Gleichung $x^2 - dy^2 = N$ mit $\mathrm{ggT}(x, y) = 1$ gibt es dann ein n mit $x = p_n$, $y = q_n$.

22. 7 Juli

Satz 22.1. *Es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Für alle $n \geq 1$ gilt dann*

$$\left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

Idee des Beweises: Mit den α_n, a_n aus dem Kettenbruchalgorithmus (Satz 19.4) für α gilt

$$\left|\alpha - r_n\right| = \frac{1}{q_n\left(\alpha_{n+1}q_n + q_{n-1}\right)} < \frac{1}{q_n\left(a_{n+1}q_n + q_{n-1}\right)} = \frac{1}{q_n q_{n+1}}.$$

Multiplikation mit k_n ergibt

$$|\alpha q_n - p_n| < \frac{1}{q_{n+1}}. \tag{22.1}$$

Danach zeigt man, dass $\alpha_{n+1}q_n + p_{n-1} < q_{n+2}$, also

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n\left(\alpha_{n+1}q_n + q_{n-1}\right)} > \frac{1}{q_n q_{n+2}}.$$

Multiplikation mit q_n und Anwendung von (22.1) liefert

$$\left|\vartheta k_n - h_n\right| > \frac{1}{k_{n+2}} > \left|\vartheta k_{n+1} - h_{n+1}\right|.$$

Damit kann man zeigen, dass

$$\left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\alpha - \frac{p_n}{q_n}\right|$$

gilt. □

Satz 22.2. *Es sei $\vartheta \in \mathbb{R}$, $\vartheta \notin \mathbb{Q}$ und $\frac{a}{b}$ ein gekürzter Bruch mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Dann gilt:*

(1) *Wenn $\left|\vartheta - \frac{a}{b}\right| < \left|\vartheta - \frac{h_n}{k_n}\right|$ für ein $n \geq 1$, dann ist $b > k_n$.*

(2) *Wenn $|\vartheta b - a| < |\vartheta k_n - h_n|$ für ein $n \geq 1$, dann ist $b \geq k_{n+1}$.*

Idee des Beweises: Wenn (1) nicht wahr wäre, folgt es, dass (2) auch nicht wahr ist. Das, heißt, man muss nur (2) beweisen.

Wir nehman an, dass es $\frac{a}{b}$ und n gibt, so dass $b < q_n$ und $|\alpha b - a| < |\alpha q_n - p_n|$. Man benutzt Satz 18.2 um zu zeigen, dass die Gleichungen

$$xq_n + yq_{n+1} = b$$
$$xp_n + yp_{n+1} = a$$

genau eine Lösung $x, y \in \mathbb{Z}$ haben. Nach der Annahme, gilt $xy < 0$. Da $r_0 < r_2 < \cdots < \alpha < \cdots < r_3 < r_1$, haben $x(\alpha q_{n+1} - p_{n+1})$ und $y(\alpha q_n - p_n)$ das gleiche Verzeichen. Es ist

$$x\,(\alpha q_n - p_n) + y\,(\alpha q_{n+1} - p_{n+1}) = \alpha b - a,$$

also

$$\begin{aligned} |\alpha b - a| &= |x\,(\alpha q_n - p_n)| + |y\,(\alpha q_{n+1} - p_{n+1})| \\ &> |x\,(\alpha q_n - p_n)| \geq |\alpha q_n - p_n| \end{aligned}$$

im Widerspruch zur Annahme. □

Satz 22.3. *Es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\frac{a}{b} \in \mathbb{Q}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\mathrm{ggT}(a, b) = 1$. Wenn*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

gilt, dann ist $\frac{a}{b}$ ein Näherungsbruch der Kettenbruchentwicklung von α.

Beweis: Es sei

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}.$$

Man nimmt an, es wäre $\frac{a}{b} \neq r_m = \frac{p_m}{q_m}$ für alle $m \geq 0$.

Man definiert $n \in \mathbb{N}_0$ durch $q_n \leq b < q_{n+1}$. Aus Satz 22.2 folgt dann

$$\Big|\alpha b - a\Big| \geq \Big|\alpha q_n - p_n\Big|,$$

also

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{b}{q_n}\left|\alpha - \frac{a}{b}\right| < \frac{1}{2bq_n}.$$

Wegen $\frac{a}{b} \neq r_n$ ist $bp_n - aq_n \in \mathbb{Z} \setminus \{0\}$, also $|bp_n - aq_n| \geq 1$. Es folgt

$$\frac{1}{bq_n} \leq \frac{|bp_n - aq_n|}{bq_n} = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2},$$

also $\frac{1}{2bq_n} < \frac{1}{2b^2}$, also $\frac{1}{q_n} < \frac{1}{b}$, also $b < q_n$ im Widerspruch zur Wahl von n. Somit folgt $\frac{a}{b} = r_n$. □

23. 11 Juli

Letztes Mal haben wir gesehen, wenn $\frac{a}{b} \in \mathbb{Q}$ eine „gute Approximation" von $x \in \mathbb{R} \setminus \{\mathbb{Q}\}$ ist, gilt dann, dass $\frac{a}{b}$ ein Näherungsbruch der Kettenbruchentwicklung von x ist. Die Worte „gute Approximation" bedeuten, dass $|\frac{a}{b} - x| < \frac{1}{2b^2}$. Das Problem ist leider, wir haben nicht gezeigt, dass beliebige $\frac{a}{b}$ existieren, die diese Eigenschaft entsprechen, sogar die Näherungsbruch der Kettenbruchentwicklung selbst. Folgendes berichtigt die Situation.

Satz 23.1 (Satz von Hurwitz)**.** *Zu jeder irrationalen reellen Zahl α gibt es unendlich viele rationale Zahlen $\frac{a}{b}$ mit*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{\sqrt{5}b^2}.$$

Von je drei aufeinanderfolgenden Näherungsbrüchen der Kettenbruchentwicklung von α erfüllt mindestens einer diese Ungleichung.

Beweis: Der Beweis ist nicht besonders schwer. Wegen der Zeit, beweisen wir diesen Satz nicht. □

Man kann auch zeigen dass die Zahl $\sqrt{5}$ von Satz 23.1 ist die beste, darauf man erwarten kann.

Satz 23.2. *Zu jedem $c > \sqrt{5}$ gibt es reelle irrationale Zahlen α, so dass*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{cb^2}$$

nur für endlich viele rationale Zahlen $\frac{a}{b}$.

Kein Beweis von Satz 23.2 wird gegeben. Jeder, der sich für dieses Ergebnis interessiert würde, söllte an $\alpha = \frac{1+\sqrt{5}}{2}$ denken.

Folgengder Satz von Liouville wurde genutzt, um zu zeigen, dass es transzendente Zahle gibt.

Satz (Liouville, 1844)**.** *Ist $\alpha \in \mathbb{R}$ algebraisch vom Grad n, dann gibt es ein $\delta > 0$, so dass nur endlich viele $\frac{h}{k} \in \mathbb{Q}$ gibt mit*

$$\left|\alpha - \frac{h}{k}\right| < \frac{\delta}{k^n}.$$

Bemerkung. Nach Cantors Beweis von 1891, dass die reellen Zahlen überabzählbar sind, ist die Existenz von transzendenten Zahlen einfach. In der Geschichte kommt Liouville ganz früher.

Verbesserung des Satzes von Liouville durch Thue (1909), Siegel (1921), Roth (1955).

Satz (Satz von Roth)**.** *Ist $\vartheta \notin \mathbb{Q}$ reell und algebraisch und $\varepsilon > 0$, dann gibt es ein $\delta > 0$, so dass für alle $\frac{h}{k} \in \mathbb{Q}$ gilt:*

$$\left|\vartheta - \frac{h}{k}\right| > \frac{\delta}{k^{2+\varepsilon}}.$$

Obwohl wir Sätze 21.2 und 21.3 wahrend der Klase nicht beweisen haben, schreiben wir den Beweis auf.

Beweis des Satzes 21.3: Es seien $\rho, \sigma \in \mathbb{R}$ und $X, Y \in \mathbb{N}$ und es sei $0 < \sigma < \sqrt{\rho}$, $\rho \notin \mathbb{Q}$, $\mathrm{ggT}(X, Y) = 1$ und $X^2 - \rho Y^2 = \sigma$. Dann folgt

$$\frac{X}{Y} - \sqrt{\rho} = \frac{\sigma}{Y(X + \sqrt{\rho}\, Y)} > 0,$$

also $\frac{X}{Y\sqrt{\rho}} > 1$ und da $\sigma < \sqrt{\rho}$

$$0 < \frac{X}{Y} - \sqrt{\rho} = \frac{\sigma}{Y(X + \sqrt{\rho}\, Y)} < \frac{\sqrt{\rho}}{Y(X + \sqrt{\rho}\, Y)} = \frac{1}{Y^2\left(\frac{X}{Y\sqrt{\rho}} + 1\right)} < \frac{1}{2Y^2}.$$

Nach Satz 22.3 ist daher $\frac{X}{Y}$ ein Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{\rho}$.

Im Falle $N > 0$ wählt man $\sigma = N$, $\rho = d$, $X = x$, $Y = y$. Dann folgt $x = h_n$, $y = k_n$ für ein passendes n.

Im Falle $N < 0$: Für $x^2 - dy^2 = N$ schreibt man $y^2 - \frac{1}{d}x^2 = -\frac{N}{d}$.

Man wählt $\sigma = -\frac{N}{d}$, $\rho = \frac{1}{d}$, $X = y$, $Y = x$. Dann gilt $0 < \sigma < \sqrt{\rho}$, und $\frac{y}{x}$ ist ein Näherungsbruch für $\frac{1}{\sqrt{d}}$. Ist $\sqrt{d} = [a_0, a_1, a_2, \ldots]$, so ist

$$\frac{1}{\sqrt{d}} = \left[0, \sqrt{d}\right] = [0, a_0, a_1, \ldots]\,.$$

Aus Satz 18.2 folgt, dass der n-te Näherungsbruch von $\frac{1}{\sqrt{d}}$ gleich $\frac{p_{n-1}}{q_{n-1}}$ ist. Für ein n ist also $\frac{y}{x} = \frac{p_n}{q_n}$, also $x = p_n$, $y = q_n$. □

Idee des Beweises von Satz 21.2: Es sei $d \in \mathbb{N}$ kein Quadrat, $\sqrt{d} = [a_0, a_1, \ldots]$ und $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$. Zuerst zeigt man, dass für alle $n \geq -1$

$$p_n^2 - dq_n^2 = (-1)^{n+1} s_{n+1}$$

gilt. Darum zu beweisen, benutzt man

$$\sqrt{d} = [a_0, \ldots, a_n, \tfrac{m_n + \sqrt{d}}{s_n}] = \frac{\left(\frac{m_n + \sqrt{d}}{s_n}\right) p_n + s_{n+1} p_{n-1}}{\left(\frac{m_n + \sqrt{d}}{s_n}\right) q_n + s_{n+1} q_{n-1}}.$$

Vergleich von rationalen und irrationalen Anteilen liefert

$$m_{n+1} q_n + s_{n+1} q_{n-1} - p_n = 0,$$
$$m_{n+1} p_n + s_{n+1} p_{n-1} - d q_n = 0.$$

Damit findet man unter Verwendung von Satz 18.2 die Behauptung.

Man muss jetzt beweisen, dass $s_n \neq -1$ für alle n.

Zur Erinnerung: $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_{\ell-1}, 2a_0}]$ und

$$\gamma = a_0 + \sqrt{d} = [\overline{2a_0, a_1, \ldots, a_{\ell-1}}]$$

ist rhein periodisch. Man schreibt $\gamma_n = \frac{m'_n+\sqrt{d}}{s'_n}$ wie im Beweis von Satz 20.2. Dann ist $\gamma_0 = a_0 + \sqrt{d}$, also $s'_0 = 1$. Wegen

$$\frac{m'_{r\ell} + \sqrt{d}}{s'_{r\ell}} = \gamma_{r\ell} = \gamma_0 = a_0 + \sqrt{d}$$

folgt es, dass $s'_{r\ell} = 1$ gilt. Da ℓ ist die kleinste Zahl damit $\gamma_0 = \gamma_\ell$, zeigt mann ähnlischerweise, dass $s'_n = 1$ genau wenn $\ell \mid n$.

Nach $\alpha_n = \gamma_n - a_0$ folgt $s_n = s'_n$ und $m'_n = mn - a_0 s_n$.

Dass $s_n \neq -1$ gilt, wird nach Widerspruch beweisen. □

Eine *elliptische Kurve* ist eine (projektive) Kurve von Grad 3 ohne Singularitäten zusammen mit einem Punkt $\mathcal{O}$. Solche Kurve kann geschrieben werden, als die Lösungen von einer Gleichung

$$y^2 = f(x) \qquad f(x) = x^3 + ax^2 + bx + c,$$

dabei f drei verschiedene Nullstellen hat. Dass heißt, falls k ein Körper ist, $a, b, c \in k$, ist $E(k) = \{(x, y) \in k^2 \mid y^2 = f(x)\} \cup \{\mathcal{O}\}$. Der sogenannte „Punkt auf ∞" $\mathcal{O}$ wird später erklärt werden.

Zwei Zahlentheoretische Fragen:

- Fermats Letzter Satz: Es sei $a, b, c \in \mathbb{Z}$ und $\ell \geq 3$ damit $abc \neq 0$ und $a^\ell + b^\ell = c^\ell$. Dann betrachten wir die elliptische Kurve $E_{a,b,c} : y^2 = x(x - a^\ell)(x + b^\ell)$. Der Beweis von Fermats Letzten Satz hängt von den Eigenschaften dieser Kurve ab.
- Dreieckszahlen: Eine Zahl $n \in \mathbb{N}$ heißt *Dreieckszahl* (engl. *congruent number*), falls es $a, b, c \in \mathbb{Q}$ gibt, damit

  $$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}.$$

  Dass heißt, n ist die Fläche eines rechtwinkligen Dreiecks mit rationalen Seitenlängen. Die elliptische Kurve $E_n : y^2 = x^3 - n^2 x$ hat mehr rationale Punkte außerdem $\{(0, 0), (\pm n, 0), \mathcal{O}\}$, genau wenn n Dreieckszahl ist.

24. 14 Juli

Definition. Es sei k ein Körper. Der *projektive Raum von Dimension n* (über k) ist

$$\mathbb{P}^n_k = \{(X_0, X_1, \ldots, X_n) \in k^{n+1} \setminus \{(0, 0, \ldots, 0)\}\}/\sim$$

und $(X_0, X_1, \ldots, X_n) \sim (X'_0, X'_1, \ldots, X'_n)$ gilt genau wenn es $t \in k^\times$ gibt, damit $tX_j = X'_j$ für alle $0 \leq j \leq n$. Man schreibt $[X_0 : X_1 : \cdots : X_n]$ als Repräsentant einer Äquivalenzklass.

Man nennt $\mathbb{P}^1_k$ die projektive Gerade und $\mathbb{P}^2_k$ die projektive Ebene.

Bemerkung. Manchmal ist es einfacher die projektive Gerade betrachten wie die Menge von Geraden aus k^2, die die Ursprung enthalten. Ähnlicherweise ist die projektive Ebene die Menge von Ebene aus k^3, die die Ursprung enthalten.

Für jedes $0 \leq i \leq n$ hat man die Menge

$$X_i = \{[X_0 : X_1 : \cdots : X_n] \in \mathbb{P}^n_k \mid X_i \neq 0\}.$$

Durch die Abbildung

$$X_i \to k^n, \qquad [X_0 : X_1 : \cdots : X_n] \mapsto (\tfrac{X_0}{X_i}, \ldots, \tfrac{X_{i-1}}{X_i}, \tfrac{X_{i+1}}{X_i}, \ldots, \tfrac{X_n}{X_i}).$$

Die Umkehrabbildung ist

$$k^n \to X_i, \qquad (x_1, x_2, \ldots, x_n) \mapsto [x_1 : \ldots : x_i : 1 : x_{i+1} : \cdots : x_n].$$

So gilt es, dass die projektive Gerade

$$\mathbb{P}^1_k = X_1 \sqcup \{[0 : Y] \mid Y \in k^\times\}$$

ist. Da $[0 : Y] = [0 : 1]$ für alle $Y \in k^\times$, haben wir $\mathbb{P}^1_k = X_1 \sqcup \{[0 : 1]\} \simeq k \cup \{\infty\}$. Also, die Projektive Gerade ist gleich als die normalle[3] Gerade plus ein Punkt mehr „aus Unendlichkeit".

Man findet auch, dass

$$\mathbb{P}^2_k = X_2 \sqcup \{[X : Y : 0] \in \mathbb{P}^2_k\} \simeq k^2 \sqcup \mathbb{P}^1_1.$$

Die Menge $\{[X : Y : Z] \in \mathbb{P}^2_k \mid Z = 0\}$ heißt die *Gerade aus Unendlichkeit*. So kann man dass, dass die projektive Ebene eine „Affin Ebene plus eine Gerade aus Unendlichkeit" ist.

Definition. Ein Polynom $F(X, Y, Z) \in k[X, Y, Z]$ heißt *homgen von Grad d*, falls $F(tX, tY, tZ) = t^d F(X, Y, Z)$. Das heißt, jedes Monom $X^j Y^k Z^\ell$ von F hat den gleichen Grad $d = j+k+\ell$. Falls $F(X, Y, Z)$ ein nicht konstantes homogenes Polynom von Grad d ist, nennt man die Menge $C = C_F = \{[X : Y : Z] \in \mathcal{P}^2_k$ eine *projektive Kurve von Grad d*. Eine Kurve von Grad 1 heißt eine Gerade.

Beispiel. Die projective Gerade von $F(X, Y, Z) = Z$ ist genau die vorher sogenannte Gerade aus Unendlichkeit der projektiven Ebene.

Eine affine Kurve ist die Menge von Lösungen zu einem Polynom $f \in k[x, y]$. Der Grad von f ist der größte (ganz) Grad von jedem Monom aus f. Man kann durch Folgendes zwischen affine und homogene Kurven wechseln. Falls $f \in k[x, y]$ von Grad d gilt, nimmt man $F(X, Y, Z) = Z^d f(\frac{X}{Z}, \frac{Y}{Z})$. Falls $F(X, Y, Z) \in k[X, Y, Z]$

[3] Man nennt k die *affine Gerade*.

homegen von Grad d gilt, nimmt man $f(x,y) = F(x,y,1)$. So ist jede Kurve aus der affinen Ebene das affine Teil von einer projektiven Kurve.

Beispiel. Es sei E eine elliptische Kurve. Also, wir haben ein Polynom $g \in k[x]$ von Grad 3, das unterschiedliche Nullstellen hat. Dann wird die affine Punkte von E durch $f(x,y) = y^2 - f(x)$ ermittelt. Die projektive Kurve E wird nach entweder

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

oder $F(X,Y,Z) = Y^2Z - X^3 + aX^2Z + bXZ^2 + cZ^3$ ermittelt. Wir können bestimmen, welche Punkte aus der entsprechenden projektiven Kurve auf der Gerade aus Unendlichkeit liegen, wenn wir $Z = 0$ in $F(X,Y,Z)$ einsetzen. Dann finden wir, dass $0 = X^3$ gilt für jeden Punkt der Kurve aus Unendlichkeit. Das heißt, $[0:1:0] = \mathcal{O}$ ist der einzige Punkt auf der Kurve aus Unendlichkeit.

Satz 24.1 (Bezout)**.** *Es seien C_1 und C_2 projektive Kurve von $\mathbb{P}^2_{\mathbb{C}}$ ohne gleichen Komponenten.*[4] *Falls d_j der Grad von C_j ist, gilt es, dass $C_1 \cap C_2$ genau d_1d_2 Punkte hat, wenn man richtig die Vielfachheit von jedem Punkt zählt.*

Beweis: entfällt □

Bemerkung. Eine elliptische Kurve E und die Gerade $Z = 0$ sollen nach diesem Satz drei Schnittpunkten haben. Wir haben gezeigt, dass es nur einen gibt. Das ist kein Widerspruch zum Satz. Allerdings haben wir gesehen, dass die Gleichung $X^3 = 0$ aus den Schnittpunkt davon erscheint. Deswegen ist die Vielfachheit 3.

25. 18 Juli

Definition. Es sei E eine elliptische Kurve über einen Körper k. Man definiert eine binäre Operation $+ : E(k) \times E(k) \to E(k)$ nach Folgendem. Es sei $P, Q \in E(k)$.

- Es sei $\overline{PQ}$ die Gerade durch P und Q. Falls $P \neq Q$ gilt, ist $\overline{PQ}$ eindeutig. Ansonsten definiert man, dass $\overline{PQ}$ die Gerade sei, die Tangent zu $E(k)$ ist.
- Es sei $R = P \star Q$ der dritte Punkt von $E(k) \cap \overline{PQ}$. Nach dem Satz von Bezout ist $P \star Q$ wohldefiniert.
- Es sei $\overline{\mathcal{O}R}$ die Gerade durch $\mathcal{O}$ und R. Sie ist nochmal die Tangente, falls $R = \mathcal{O}$.
- Es sei $P + Q$ der dritte Punkt von $E(k) \cap \overline{\mathcal{O}R}$.

Satz 25.1. *Es sei $E : y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve. Die Menge $E(k)$ ist durch die Operation $+$ eine abelsche Gruppe mit neutralem Element $\mathcal{O}$.*

[4] Es seien F_1 und F_2 homogene Polynome. So ist $F = F_1F_2$ ein homogenes Polynom. Die entsprechende Kurve $C = C_1 \cup C_2$ wohin C_1 und C_2 die Kurven nach F_1 und F_2 sind. Die C_1 und C_2 heißen *Komponenten* von C.

Idee des Beweises: (Wohldefiniert) Es seien $P = (x_1, y_1)$ und $Q = (x_2, y_2)$. Man leitet es ab, dass $P + Q = (x_0, y_0) = (\Phi, \Psi)$ für bestimmte rationale Abbildungen $\Phi, \Psi \in k(x_1, x_2, y_1, y_2, a, b, c)$. Das heißt, wenn $x_1, y_1, x_2, y_2 \in k$ gilt, so gilt es auch, dass $x_0, y_0 \in k$. Bemerkung: man muss vorsichtig mit $\mathcal{O}$ sein.

(Abelsch) Dass $P + Q = Q + P$ ist klar, weil $\overline{PQ} = \overline{QP}$. Also, $+$ ist abelsch.

(Neutrales Element) Es sei $P = (x_0, y_0) \neq \mathcal{O}$. Also, die Gerade $\overline{\mathcal{O}P}$ ist vertikal. Das heißt, der dritte Punkt von $E(k) \cap \overline{\mathcal{O}P}$ ist $R = (x_0, -y_0)$. Natürlich ist P der dritte Punkt von $E(k) \cap \overline{\mathcal{O}P}$. Dass heißt, $\mathcal{O} + P = P$. Falls $P = \mathcal{O}$ verwendet man, dass die Tangente durch $\mathcal{O}$ Schnittpunkt von Vielfachheit 3 hat.

(Inverses) Die Inverse von $P = (x_0, y_0)$ ist $-P = (x_0, -y_0)$.

(Assoziativitätsgesetz) Es seien $P, Q, R \in E(k)$. Man muss zeigen, dass $(P+Q)\star R = P \star (Q + R)$ gilt. Man verwendet Satz 25.2 mit

$$C = E, \quad C_1 = \overline{PQ} \cdot \overline{(P+Q)R} \cdot \overline{\mathcal{O}(Q \star R)}, \quad C_2 = \overline{P(Q+R)} \cdot \overline{QR} \cdot \overline{\mathcal{O}(P \star Q)}.$$

Die 8 Punkte des Schnittpunkts sind $\{P, Q, P \star Q, P + Q, R, R \star Q, R + Q, \mathcal{O}\}$. □

Satz 25.2 (Cayley-Bacharach)**.** *Es seien C, C_1, C_2 Kurve aus $\mathcal{P}^2_k$ von Grad 3, die keine gemeinsamen Komponenten haben. Falls $C \cap C_1$ und $C \cap C_2$ 8 gemeinsame Punkte enthalten, ist der neunte von Beiden das Gleiche.*

Beweis: entfällt □

Definition. Es sei E eine elliptische Kurve über einen Körper k. Die *Torsionuntergruppe von $E(k)$* ist

$$E(k)_{\text{tor}} := \{P \in E(k) \mid nP = \mathcal{O}, \text{ für einiges } n \in \mathbb{N}\}.$$

Satz 25.3. *Sei $E : y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve mit ganzzahligen Koeffizienten a, b, c. Es sei $P = (x_0, y_0) \in E(\mathbb{Q})_{\text{tor}}$. Es sei $\Delta = \Delta(E)$ die Diskriminante.*

(1) *(Satz von Nagell-Lutz, 1935/37)*
Es gilt $x_0, y_0 \in \mathbb{Z}$ und falls $y_0 \neq 0$, dann gilt $y_0^2 \mid \Delta$.

(2) *(Satz von Mazur, 1977)*
Die Gruppe $E(\mathbb{Q})_{\text{tor}}$ ist isomorph zu einer der Folgenden.

$\mathbb{Z}/N\mathbb{Z}$, $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$, $\quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, $N \in \{2, 3, 4\}$.

Beweis: entfällt □

Sei $E : y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve mit ganzzahligen Koeffizienten a, b, c. Es sei p Primzahl damit $p \nmid \Delta(E)$. Dann definiert E eine elliptische Kurve über den endlichen Körper $\mathbb{F}_p$ mit p Punkten. Dass heißt, wir können alles modulo p betrachten. Natürlich ist $E(\mathbb{F}_p)$ eine endliche Gruppe.

Satz 25.4. *Es sei $E : y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve mit ganzzahligen Koeffizienten a, b, c. Für jede Primzahl p damit $p \nmid \Delta(E)$ gibt es eine injektive Abbildung $E(\mathbb{Q})_{\text{tor}} \to E(\mathbb{F}_p)$. Diese Abbildung ist ein Homöomorphismus von Gruppen.*

Beweis: entfällt □

Beispiel. Die elliptische Kurve $E : y^2 = x^3 + x$ hat die zwei Punkte $(0,0), \mathcal{O} \in E(\mathbb{Q})_{\text{tor}}$. Gibt es sonst mehr?

Da $\Delta = -32$, ist E eine elliptische Kurve über $\mathbb{F}_p$ für jede Primzahl $p > 2$. Man zeigt, dass

$$E(\mathbb{F}_3) = \{(0,0), (-1,1), (-1,-1), \mathcal{O}\} \simeq \mathbb{Z}/4\mathbb{Z},$$
$$E(\mathbb{F}_5) = \{(0,0), (2,0), (-2,0), \mathcal{O}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Nach Satz 25.4 folgt es $E(\mathbb{Q})_{\text{tor}} = \{(0,0), \mathcal{O}\}$.

Man könnte den Satz von Nagell-Lutz benutzen anstatt Satzes 25.4. Dadurch finden wir für einen Punkt $(x_0, y_0) \in E(\mathbb{Q})_{\text{tor}}$, dass $y_0 \in \{0, 2, 4\}$ gilt. Wenn $x_0 \in \mathbb{Z}$ auch sein muss, gibt es nur eine Lösung: $(x_0, y_0) \in E(\mathbb{Q})$. Also, $E(\mathbb{Q})_{\text{tor}} = \{(0,0), \mathcal{O}\}$.

Satz 25.5 (Mordell (1922))**.** *Sei $E : y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve worin $a, b, c \in \mathbb{Z}$. Dann ist die Gruppe $E(\mathbb{Q})$ von endlich viele Punkte erzeugt. Das heißt, es gibt endlich viele Punkte, so dass jede rationale Lösung von E aus diesen erhalten werden kann, indem man den dritten Punkt auf E auf einer Gleichung durch zwei Punkte berechnet und reflektiert, um neue Punkte zu erhalten.*

Beweis: entfällt □

Bemerkung. Der Satz von Mordell sagt, dass $E(\mathbb{Q})_{\text{tor}}$ endlich ist und es $r \geq 0$ gibt, damit $E(\mathbb{Q}) \simeq \mathbb{Z}^r + E(\mathbb{Q})_{\text{tor}}$ gilt. Die Zahl r heißt der *Rang von E*.

26. 21 Juli

Wir betrachten eine elliptische Kurve E gegeben durch die Gleichung $y^2 = f(x) = x^3 + ax^2 + bx + c$, $a, b, c \in k$ so dass $\Delta(E) \neq 0$. Dann haben wir den Punkt $\mathcal{O} = [0 : 1 : 0]$ aus Unendlichkeit, der das neutrale Element von $E(k)$ ist.

Für einen Punkt $P \neq \mathcal{O}$, damit es $2P = \mathcal{O}$ gilt muss die Tangente auf P durch $\mathcal{O}$ liegen. Das heißt, die Gerade $\overline{PP}$ ist vertikal. Man sieht dann, dass $P = (x_0, 0)$ und $f(x_0) = 0$ gilt. Für $P = (x_0, y_0)$, merkt man auch, dass $-P$, der Punkt damit $P + (-P) = \mathcal{O}$ gilt, $-P = (x_0, -y_0)$ ist, weil $\overline{P(-P)}$ nochmal durch $\mathcal{O}$ liegen muss.

Falls $3P = \mathcal{O}$ gilt, muss dann $2P = -P$. Dass heißt, falls R der andere Punkt aus $\overline{PP} \cap E(k)$ ist, liegt $-P$ auf $\overline{R\mathcal{O}}$. Das kann nur sein, wenn $R = P$ ist. Also, die Tangente duch P ist ein dreimaler Schnittpunk. Solcher Punkt heißt ein *Wendepunkt*. Bemerkung: Wir haben schon gesehen, dass $\mathcal{O}$ ein Wendepunkt ist.

Satz 26.1. *Sei $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ eine elliptische Kurve. Es seien $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ damit $y_1 + y_2 \neq 0$. Dann gilt es*

$$P + Q = \big(\lambda^2 - a - x_1 - x_2, -\lambda x_3 - \nu\big),$$

wohin

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q, \\ \\ \dfrac{f'(x_1)}{2y_1} & \text{if } P = Q, \end{cases}$$

und

$$\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Beweis: Sei L die Gerade $\overline{PQ}$. Dann ist λ die Steigung davon und L wird nach $y = \lambda x + \nu$ gegeben. Man setzt dies in die Gleichung für E ein und findet

$$\begin{aligned} 0 &= f(x) - y^2 \\ &= (x^3 + ax^2 + bx + c) - (\lambda x + \nu)^2 \\ &= (x - x_1)(x - x_2)(x - x_0). \end{aligned}$$

Die letze Gleichung daher folgt, weil P, Q und $P + Q$ der Schnittpunkt $E(k) \cap L$ sind und so ihre x-Koordinaten Nullstellen sind.

Nun betrachtet man die x^2 Koeffizienten von $(x^3 + ax^2 + bx + c) - (\lambda x + \nu)^2$ und $(x - x_1)(x - x_2)(x - x_0)$. Dadurch findet man

$$x_3 = \lambda^2 - a - x_1 - x_2.$$

Die y-Koordinate von $P \star Q$ wird durch $\lambda x_3 + \nu$ gegeben. Also, die Negation davon ist die y-Koordinate von $P + Q$. □

Bemerkung. Man soll sich die Ableitung von Satz 26.1 erinnern. Dann kann man alles schnell und einfach wiederfinden, ohne die Gleichung in Gedächtnis behalten müssen.