Stichwortprotokoll zur Vorlesung Elementare Zahlentheorie, SS 2001

Kalenderwoche 17

Die Vorlesung beginnt mit

1. einer kurzen Erwähnung der Peano-Axiome für $\mathbb{N}$ sowie den Konstruktionen von $\mathbb{Z}$ und $\mathbb{Q}$ [1]

2. Bemerkungen zu zwei scheinbar unabhängigen Beispielen von Typen von in der Vorlesung zu studierenden Gleichungen

$$x^2 + y^2 = ?\,, \quad x, y, ? \in \mathbb{N}\,; \quad (p-1)! = p - 1 + vp\,, \quad v \in \mathbb{N}\,,\ p \text{ Primzahl}\,.$$

3. der Erinnerung an den Euklidischen Divisionsalgorithmus in $\mathbb{Z}$:

$$\forall\, a, b \neq 0\,, \in \mathbb{Z}\,, \exists\, v, r \in \mathbb{Z} : a = vb + r\,, \quad 0 \leq r < |b|$$

4. den Definitionen eines Ringes B und eines Homomorphismus $\mathbb{Z} \xrightarrow{f} B$:

   Ein Ring B ist eine Menge mit zwei ausgezeichneten Elementen, 0 und 1, und zwei Strukturen, $+$ und $\times$, die folgendes erfüllen

   Zu $a \in B$ existiert genau ein Element $-a \in B$ mit $a + (-a) = 0$.
   (Statt $a + (-b)$ schreiben wir einfacher $a - b$.)
   $a + b = b + a\,,\ a \times b = b \times a$
   $0 + a = a\,,\ 1 \times a = a$
   $a + (b + c) = (a + b) + c\,,\ a \times (b \times c) = (a \times b) \times c$
   $a \times (b + c) = a \times b + a \times c\,.$

   Es folgt: $a \times 0 = 0$ $(\forall\, a \in B)$ — aber es ist im allgemeinen falsch, aus $a \times b = 0$ das Verschwinden einer der beiden Faktoren, a oder b, zu folgern.
   B heißt endlich, falls es nur endlich viele Elemente in B gibt.

   Ein Homomorphismus $f : \mathbb{Z} \to B$ ist eine Abbildung von $\mathbb{Z}$ nach B, die $f(a + b) = f(a) + f(b)\,,\ f(a \times b) = f(a) \times f(b)$ $(\forall\, a, b \in \mathbb{Z})$ erfüllt. Es folgt $f(a - b) = f(a) - f(b)\,.$

Wir wollen algebraische Gleichungen über $\mathbb{Z}$, so wie $x^2 + y^2 = ?$, mittels Homomorphismen $f : \mathbb{Z} \to B$ in solche über B übertragen; dabei soll B endlich sein, so daß wir hier alle Lösungen "in endlicher Zeit" finden können. Für die Durchführung dieses Programms benötigen wir zuerst Kenntnisse über mögliche Paare (f, B). Ein Beispiel ist: $B = \{0, 1\}\,,\ 1 + 1 = 0\,;\quad f(a) = 0 \iff 2|a$ (d.h. a ist gerade).

LEMMA. $\ker f \stackrel{\text{def}}{=} \{a \in \mathbb{Z} : f(a) = 0\}$ *ist abgeschlossen unter* $+$
$z \in \mathbb{Z}\,, a \in \ker f \Longrightarrow za \in \ker f$
$\exists\, a_f \in \ker f : \ker f = \{za_f : z \in \mathbb{Z}\}\,.$

[1] $\mathbb{N}$ bezeicnet die Menge der natürlichen, $\mathbb{Z}$ die der ganzen, $\mathbb{Q}$ die der rationalen, $\mathbb{R}$ die der reellen und $\mathbb{C}$ die der komplexen Zahlen.

Bemerkung: $a_f = \{\pm \min\{a > 0 : a \in \ker f\}$; wir wählen immer die nicht-negative Zahl.

Das folgende n ist kurz für a_f:

DEFINITION. *Ist $n \geq 0$, so schreiben wir $\mathbb{Z}/n$ für $\mathbb{Z}$ mit der neuen Gleichheit*

$$a \equiv b \iff n \mid a - b\,.$$

(Ausführlicher schreiben wir auch $a \equiv b \bmod n$ statt nur $a \equiv b$.)

SATZ. *$\equiv$ ist verträglich mit $+$ und $\times$; $\mathbb{Z}/n$ ist für $n > 0$ ein endlicher Ring mit genau n Elementen.*

Die kleinstmöglichen B sind die Ringe $\mathbb{Z}/n$, $n > 0$, und $f(a) = a \bmod n$ ist ein zulässiges $f : \mathbb{Z} \to B = \mathbb{Z}/n$.

Kalenderwoche 18

Das Rechnen in $\mathbb{Z}/n$:

Wir schreiben $\overline{a}$ für die Gleichheitsklasse von $a \in \mathbb{Z}$ in $\mathbb{Z}/n$; bei 0 und 1 lassen wir allerdings oft den Querstrich weg. Des weiteren verwenden wir ab sofort den Punkt $\cdot$ für die Multiplikation (und also nicht mehr $\times$).

Beachte, daß $\mathbb{Z}/n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ für $n \neq 0$ gilt; $\mathbb{Z}/0 = \mathbb{Z}$.

LEMMA. *$\overline{a}$ ist invertierbar in $\mathbb{Z}/n$, d.h. $\exists\, \overline{b} \in \mathbb{Z}/n : \overline{a}\overline{b} = \overline{1}$, genau wenn a und n teilerfremd sind (also $\mathrm{ggT}(a, n) = 1$). Insbesondere ist $\mathbb{Z}/n$ ein Körper, genau wenn n eine Primzahl ist.*

Ein Ring B heißt ein Körper, wenn alle seine Elemente $\neq 0$ invertierbar sind. Ein $a \in B$ mit $ab = 0$ für ein $b \in B$, $b \neq 0$ heißt ein Nullteiler.

Obiges Lemma resultiert aus der Darstellbarkeit des größten gemeinsamen Teilers $d = \mathrm{ggT}(a, b)$ zweier ganzer Zahlen a, b als ganzzahlige Linearkombination von a und b:

LEMMA. $\exists\, v, w \in \mathbb{Z} : d = va + wb\,.$

Ist nämlich $\mathrm{ggT}(a, b) = d$, so kann d durch sukzessive Anwendung des Euklidischen Algorithmus berechnet werden:

Setze $b = a_0, a = a_1$. Dividiere zuerst a_0 durch a_1 mit Rest a_2, dann, falls $a_2 \neq 0$, a_1 durch a_2 mit Rest a_3, etc. Schließlich landet man bei einem Rest $a_{i+1} = 0$. Es folgt sofort $d = a_i$, und man sieht auch, wie v und w zu bilden sind. Man bemerke, daß damit zugleich ein explizites Verfahren zur Berechnung von $\overline{a}^{-1} \in \mathbb{Z}/n$ für $\mathrm{ggT}(a, n) = 1$ angegeben ist.

LEMMA. $\mathrm{ggT}(a, n) = 1 \Longrightarrow \overline{a}^{\varphi(n)} = \overline{1}$ *mit $\varphi(n)$ als der Anzahl der Zahlen*

$$z : 1 \leq z \leq n\,,\ \mathrm{ggT}(z, n) = 1\,.$$

Insbesondere ist $\varphi(p) = p - 1$ für eine Primzahl p und es gilt

$$a^p \equiv a \bmod p \quad \forall\, a \in \mathbb{Z}\,.$$

Letztere Kongruenz wird auch *Kleiner Satz von Fermat* genannt. – φ ist die sogenannte *Eulersche Funktion*.

LEMMA. *1. φ ist multiplikativ in dem Sinne, daß*

$\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ *für* $n_1, n_2 \in \mathbb{N}$ *gilt, sofern nur* $\mathrm{ggT}(n_1, n_2) = 1$.

2. $\varphi(p^j) = (p-1)p^{j-1}$ *für Primzahlen* p *und Exponenten* $j \geq 1$.

BEMERKUNG. Die Abbildung $\mathbb{Z}/n_1 n_2 \to \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$, $a \bmod n_1 n_2 \mapsto (a \bmod n_1, a \bmod n_2)$ ist additiv, multiplikativ und, falls $\mathrm{ggT}(n_1, n_2) = 1$, auch injektiv, aus Ordnungsgründen dann auch surjektiv. Daraus fließen zwei Folgerungen:

a) die Multiplikativität der Eulerschen φ-Funktion, so wie im Lemma oben beschrieben

b) der *Chinesische Restsatz: Sind* n_1 *und* n_2 *teilerfremd und* a_1, a_2 *irgendwelche ganze Zahlen, so existiert ein* $z \in \mathbb{Z}$ *mit*

$$z \equiv a_1 \bmod n_1\,,\ z \equiv a_2 \bmod n_2\,.$$

Man spricht auch von dem Lösen *simultaner Kongruenzen*. Explizit tut man das so:

Finde $v, w \in \mathbb{Z}$ mit $vn_1 - wn_2 = 1$, multipliziere mit $a_2 - a_1$, also $(a_2 - a_1)vn_1 - (a_2 - a_1)wn_2 = a_2 - a_1$, und setze $z = a_1 + (a_2 - a_1)vn_1 = a_2 + (a_2 - a_1)wn_2$. – Anstelle von zwei Zahlenpaaren n_1, n_2 und a_1, a_2 darf man auch beliebige s-Tupel $n_1, \ldots, n_s$ und $a_1, \ldots, a_s$ vorgeben ($s \geq 2$) und erhält m.m. das gleiche Resultat vorausgesetzt, daß die n_i, $1 \leq i \leq s$, paarweise teilerfremd sind.

LEMMA. $(p-1)! \equiv -1 \bmod p$ *für Primzahlen* p.

Das Lemma wird meist als *Satz von Wilson* bezeichnet.

<u>Kalenderwoche 19</u>

Einige zahlentheoretische Funktionen:

Die Eulersche φ-Funktion ist eine solche. Eine andere ist die σ-Funktion, $\sigma(n) = \sum_{d|n} d$, die alle Teiler d der gegebenen natürlichen Zahl n aufsummiert. Es handelt sich also wieder um eine Funktion $\mathbb{N} \to \mathbb{N}$. Auch σ ist multiplikativ:

LEMMA. *1.* $\mathrm{ggT}(n_1, n_2) = 1 \Longrightarrow \sigma(n_1 n_2) = \sigma(n_1)\sigma(n_2)$

2. $\sigma(p^\nu) = \frac{p^\nu - 1}{p-1} + p^\nu$ *für primes* p *und natürlichen Exponenten* ν

DEFINITION. $n \in \mathbb{N}$ *heißt vollkommen, wenn* $\sigma(n) = 2n$ *gilt.*

Die Definition geht wohl auf Euklid zurück. Beachte $\sigma(6) = 12$, $\sigma(8) = 15 < 16$, $\sigma(12) = 28 > 24$; Primzahlpotenzen sind nie vollkommen.

SATZ. $n = 2^\nu(2^{\nu+1} - 1) = 2^\nu p$ *mit einer Primzahl* $p \Longrightarrow \sigma(n) = 2n$.
Dies sind die einzigen geraden vollkommenen Zahlen.

Eine ungerade vollkommene Zahl ist bis heute nicht bekannt. – Auf Primzahlen der Form $p = 2^j - 1$, den sogenannten *Mersenneschen Primzahlen*, kommen wir noch zu sprechen.

DEFINITION. *Ist* $n = p_1^{\nu_1} \cdot \ldots \cdot p_r^{\nu_r}$ *die Primzahlpotenz-Produktdarstellung der natürlichen Zahl* $n > 1$, *so sei*

$$\mu(n) = \begin{cases} (-1)^r & \text{wenn alle } \nu_i = 1 \\ 0 & \text{sonst} \quad . \end{cases}$$

Des weiteren sei $\mu(1) = 1$.

μ heißt die *Möbiussche Funktion*; sie ist offenkundig (im selben Sinn wie φ und σ) multiplikativ.

SATZ. 1. $\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$

2. *Erfüllen die beiden Funktionen* $f, g : \mathbb{N} \to \mathbb{N}$ *eine der beiden Gleichungen*

$$\sum_{d|n} f(d) = g(n) \quad \text{oder} \quad \sum_{d|n} \mu(n/d) g(d) = f(n) \ ,$$

so auch die andere.

Das ist die *Möbiussche Umkehrformel*. Eine erste Anwendung ist : $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$, nämlich weil $\sum_{d|n} \varphi(d) = n$. Diese letzte Gleichheit ist auch der Hauptbaustein im Beweis von dem wichtigen

SATZ. *Zu jeder Primzahl* p *gibt es eine Zahl* w, *so daß* $\{\overline{1}, \overline{w}, \overline{w}^2, \ldots, \overline{w}^{p-2}\} = \mathbb{Z}/p \setminus \{0\}$.

Ein solches w heißt eine *Primitivwurzel modulo* p. Wir kennen keine explizite $\mathbb{N}$-wertige Funktion auf der Menge der Primzahlen, deren Auswertung bei p eine Primitivwurzel modulo p liefert.

FOLGERUNG. 1. *Die Teilmenge der Quadrate in* $\mathbb{Z}/p \setminus \{0\}$ *ist abgeschlossen unter der Multiplikation und der Inversenbildung.*

2. *Sei* $p \neq 2$. *Dann gilt* $0 \neq \alpha \in \mathbb{Z}/p$ *ist Quadrat* $\iff \alpha^{\frac{p-1}{2}} = 1$.

3. $-1 \in \mathbb{Z}/p$ *ist Quadrat* $\iff p \equiv 1 \bmod 4$ *(*$p \neq 2$ *ist vorausgesetzt).*

Beachte die Ähnlichkeit zwischen $\mathbb{Z}/p$ und $\mathbb{R}$ bezüglich Punkt 1. Die Verallgemeinerung von 3., nämlich die Frage, für welche Primzahlen p die vorgegebene Zahl $z \in \mathbb{Z}$ Quadrat modulo p ist, wird durch das *Gaußsche quadratische Reziprozitätsgesetz* beantwortet, auf das wir hier (seiner grundsätzlichen Bedeutung zum Trotz) zugunsten anderer Diskussionen nicht eingehen, sondern nur auf die Literatur (z.B. auf das Buch von Hasse) verweisen wollen.

In dem Zusammenhang machen wir auch die

DEFINITION. *Ist* $1 \leq n \in \mathbb{N}$ *und* $a \in \mathbb{Z}$ *teilerfremd zu* n, *so ist*

$$\operatorname{ord}_n(a) = \min\{1 \leq e \in \mathbb{N} : a^e \equiv 1 \bmod n\} \, .$$

LEMMA. 1. $a^k \equiv 1 \bmod n \iff \operatorname{ggT}(a, n) = 1 \ \& \ \operatorname{ord}_n(a) | k$

2. $\operatorname{ord}_n(a) | \varphi(n)$

3. w *ist Primitivwurzel modulo* $p \iff \operatorname{ord}_p(w) = p - 1$

Kalenderwoche 20

Periodenlängen :

Die rationalen Zahlen $z/n \in \mathbb{Q}, z \in \mathbb{Z}, 0 \neq n \in \mathbb{N}$ sind die periodischen unendlichen Dezimalbrüche. Der Grund dafür liegt im wesentlichen in der Konvergenz der *geometrischen Reihe*

$$\sum_{i=0}^{\infty} q^i = \frac{1}{1-q} \quad \text{falls} \quad 0 < q < 1$$

— und natürlich an der "Endlichkeit" der Reste nach Division durch n: $\{0, 1, \ldots, n-1\}$ sind alle diese Reste. Da wir uns im folgenden nur für das interessieren, was "hinter dem Komma" passiert, beschränken wir uns gleich auf das offene Einheitsintervall $(0, 1)$.

LEMMA. 1. *Ist* $0 < z < n$, $(z, n) = 1$, *die rationale Zahl* $0 < \frac{z}{n} < 1$ *also gekürzt geschrieben, so gilt:* $[\frac{z}{n}$ *ist rein periodisch, d.h. die Periode beginnt gleich hinter dem Komma* $\iff \mathrm{ggT}(10, n) = 1]$.

2. *In diesem Fall, nämlich wenn* $(10, n) = 1$, *ist die Periodenlänge von* $\frac{z}{n}$ *die* Ordnung *von 10 modulo n, i.e. die kleinste Zahl* $0 \neq k \in \mathbb{N}$ *mit* $10^k \equiv 1 \bmod n$ *(und damit ein Teiler von* $\varphi(n)$*).*

Die Periodenlänge ist in natürlicher Weise definiert. Beachte, daß sie nur vom Nenner, nicht vom Zähler abhängt. Beachte auch, daß bei primen Nennern $p \neq 2, 5$ der Bruch $0 < \frac{z}{p} < 1$ Periodenlänge $\ell \mid p-1$ hat. Darüber hinaus gilt: Ist $\ell = p-1$, so entsteht $\frac{z}{p}$ aus $\frac{1}{p}$ durch zyklische Vertauschung der Ziffern der Periode von $\frac{1}{p}$.

BEMERKUNG. Teiler 2 und 5 des Nenners führen zu den sogenannten Vorperiden; wie z.B. die 1 bei $\frac{1}{6} = 0,1\overline{6}$.

Kalenderwoche 21

Primzahlen :

Diese spielen gewiß die Hauptrolle beim Rechnen mit ganzen Zahlen; Grund ist die eindeutige Primzahlpotenz-Produktdarstellung

$$n = \prod_{i=1}^{r} p_i^{j_i} \quad p_i \text{ prim}, \; j_i, r \in \mathbb{N}$$

der natürlichen Zahlen n. Die selbst resultiert aus dem Euklidischen Divisionsalgorithmus :

DEFINITION. *Die natürliche Zahl* $u \neq 1$ *heißt unzerlegbar, wenn* $[u = n_1 n_2 \Longrightarrow n_1 = 1$ *oder* $n_2 = 1]$.
Die natürliche Zahl $1 \neq p$ *heißt prim, wenn* $[p \mid n_1 n_2 \Longrightarrow p | n_1$ *oder* $p | n_2]$.
n_1, n_2 *sind hier* $\in \mathbb{N}$.

LEMMA. 1. *Jede natürliche Zahl ist (endliches) Produkt von unzerlegbaren natürlichen Zahlen.*

2. prim *und* unzerlegbar *sind gleichbedeutend*

3. *Jedes* $n \in \mathbb{N}$ *läßt sich (bis auf die Reihenfolge der Faktoren) eindeutig als Produkt* $n = \prod_{i=1}^{r} p_i^{j_i}$ p_i prim, $j_i, r \in \mathbb{N}$ *schreiben.*

Zwei Fragen schließen sich direkt an: wie ist die Menge $\mathcal{P}$ der Primzahlen in $\mathbb{N}$ ausgezeichnet; wie findet man die obige Primzahlpotenz-Produktzerlegung von einem n ?

LEMMA. *$\mathcal{P}$ ist eine unendliche Menge. Sie ist "eher größer als" die Menge der Quadratzahlen.*

Ersteres folgt z.B. aus $p_i \nmid p_1 p_2 \cdot \ldots \cdot p_r + 1$ für $1 \leq i \leq r$ und r vorgegebene Primzahlen $p_1, \ldots, p_r$; also steckt in $p_1 p_2 \cdot \ldots \cdot p_r + 1$ eine weitere, neue Primzahl p_{r+1}. Allerdings sagt dieses Argument nichts über die Größe von $\mathcal{P}$ aus.

LEMMA. $\sum_{n=1}^{\infty} \frac{1}{n^s}, s \in \mathbb{R}_{\geq 1}$ *konvergiert für $s > 1$ und divergiert für $s = 1$. Es gilt*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}} \quad (\text{Euler} - \text{Produkt}) ;$$

insbesondere ist $\sum_{p \in \mathcal{P}} \frac{1}{p}$ divergent.

Auf genauere Aussagen über die Primzahlverteilung wird hier nicht eingegangen; wir möchten allerdings in dem Zusammenhang diejenigen, die aus der Analysis die ζ-Funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, s \in \mathbb{C}, \Re(s) > 1$$

kennen, an die berühmte, noch offene, Riemannsche Vermutung über die Lage der nichttrivialen Nullstellen von der auf ganz $\mathbb{C}$ fortgesetzten ζ-Funktion erinnern: die haben alle $\Re(s) = \frac{1}{2}$. Die ζ-Funktion ist übrigens auch Haupthilfsmittel bei den (nicht mehr elementaren) Beweisen von :

1. Für die natürliche Zahl x bezeichne $\pi(x)$ die Anzahl der Primzahlen $p \leq x$. Dann gilt

   $$\pi(x) \sim x / \log x ,$$

   i.e. $\lim_{x \to \infty} \pi(x) / \frac{x}{\log x} = 1$ (*Primzahlsatz*; i.w. bewiesen von Riemann) [2]

2. *Primzahlen in arithmetischen Progressionen*: Ist $1 \leq n \in \mathbb{N}$ und $a \in \mathbb{N}$ teilerfremd zu n, so existieren unendlich viele Primzahlen $p \equiv a \bmod n$, also der Form $p = a + z \cdot n$, z ganz (*Dirichletscher Primzahlsatz*).

Für das Auffinden der Primteiler einer gegebenen Zahl n hat man kaum andere Möglichkeiten, als eben alle Zahlen $< \sqrt{n}$ als Teiler zu testen, etwa mit dem Divisionsalgorithmus. (Die bekannten Regeln über Teilbarkeit durch 3, 9 oder 11, die auf die Teilbarkeit der Quersumme, bzw. der alternierenden Quersumme, durch 3, 9 bzw. 11 hinauslaufen, hängen mit den speziellen Kongruenzen von 10 modulo 9 bzw. 11 zusammen :

$$10 \equiv 1 \bmod 9 \Longrightarrow 10^i \equiv 1 \bmod 9 , \quad 10 \equiv -1 \bmod 11 \Longrightarrow 10^i \equiv (-1)^i \bmod 11 .)$$

[2] log ist der natürliche Logarithmus

Spezielle Primzahlen:

Die Mersenneschen Primzahlen p sind von der Form $p = 2^j - 1$, $j \geq 2$. Es folgt, daß j sogar selbst eine Primzahl sein muß. Beachte, daß $j = 2, 3, 5, 7, 13$ die Mersenneschen Primzahlen $3, 7, 31, 127, 8191$ liefert, daß aber $2^{11} - 1 = 2047 = 23 \cdot 89$ keine Primzahl ist. Es ist nicht bekannt, ob die Folge der Mersenneschen Primzahlen abbricht oder unendlich ist. Die größten heute bekannten Primzahlen sind jedenfalls Mersennesche Primzahlen. Vor ca. 20 Jahren war gerade diese gefunden worden: $2^{132\,049} - 1$.

Die *Fermatschen Primzahlen* p sind von der Form $p = 2^n + 1$. Für solche p muß n eine Potenz von 2 sein: $n = 2^\nu$. Es sind $p = 3, 5, 17, 257, 65537$ Fermatsche Primzahlen; $2^{2^5} + 1$ ist allerdings durch 641 teilbar. Wiederum ist unbekannt, ob die Folge der Fermatschen Primzahlen abbricht oder unendlich ist. Bemerkt sei noch (was man in einer Algebra-Vorlesung lernt), daß das regelmäßige p-Eck für eine ungerade Primzahl p genau dann mit Zirkel und Lineal konstruiert werden kann, wenn p eine Fermatsche Primzahl ist.

Kalenderwochen 22-24

Primzahltests:

LEMMA. *1. Ist $m > 1$ und $(m-1)! \equiv -1 \bmod m$, so ist m prim.*

2. Ist einmal $a^m \not\equiv a \bmod m$, so ist m nicht prim.

Tatsächlich ist 1. kein wirklich brauchbar Primzahltest; zu viele Multiplikationen werden gefordert. Dagegen liefert 2. schon einen probabilistischen Test mit nicht zu schlechter Treffsicherheit (siehe weiter unten); es gibt davon allerdings wesentlich bessere. Seit den 80-er Jahren verfügt man auch über einen exakten, bemerkenswert schnellen Test (weniger als eine Minute Rechenzeit bei 100-stelligen Zahlen), der auf tiefen zahlentheoretischen Ergebnissen beruht (Adleman, Pomerance und Rumely; Lenstra).

DEFINITION. *Eine natürliche Zahl c heißt Carmichaelzahl, falls c nicht prim ist, aber $a^{c-1} \equiv 1 \bmod c$ für alle $a \in \mathbb{Z}$, $(a, c) = 1$ erfüllt.*

Wir beobachten, daß Carmichaelzahlen weder gerade noch Primzahlpotenzen sein können. Letzteres ist eine Konsequenz von

$1 + p$ hat die Ordnung $p^{r-1} \bmod p^r$ für ungerade Primzahlen p und natürliche Exponenenten r. Auch für das nächste Lemma ist diese Aussage, leicht verschärft, entscheidend: *Ist p eine ungerade Primzahl, so existieren Primitivwurzeln $w_r \bmod p^r$ für alle $r \geq 1$.* Setze einfach $w_r = (w_1)^{p^{r-1}}(1 + p)$. Für $p = 2$ stimmt dies übrigens nicht.

LEMMA. *Sei $c = \prod_{i=1}^{r} p_i^{j_i}$ keine Primzahl. Dann gilt*

$$c \quad \text{ist Carmichaelzahl} \iff \varphi(p_i^{j_i}) \mid c - 1 \quad (\forall\, i)\,.$$

Also sind Carmichaelzahlen quadratfrei. – Die kleinste Carmichaelzahl ist $561 = 3 \cdot 11 \cdot 17$. Offen ist, ob es unendlich viele Carmichaelzahlen gibt.

Die Kryptographiemethode von Rivest/Shamir/Adleman (1977):

Hier ist das Problem. Eine Person P_1 will eine Botschaft B_1 so an eine Person P_2 schicken, daß ausschließlich die sie lesen kann.

So geht man vor. P_1 verschlüsselt gemäß einer Regel v_2 die Botschaft B_1 zu $B_2 = v_2(B_1)$ und teilt das Ergebnis B_2 dem P_2 mit. Dieser entschlüsselt nach einer Regel e_2 das empfangene B_2 und bekommt $B_1 = e_2(B_2)$ zurück.

Folgende Bedingungen werden gestellt. Nur P_2 soll in der Lage sein, $e_2(B_2)$ auswerten zu können. Botschaften sollen mit einer Unterschrift versehbar sein *(Authentizität)*.

Ein Lösungsvorschlag. Jede Person P wird öffentlich in einer Art Telefonbuch mit einem Nummernpaar (n, v) geführt. Im Unterschied zur Telefonnummer wird allerdings dieses Paar dem P nicht von der buchführenden Stelle zugewiesen, sondern von ihm selbst gewählt und jener mitgeteilt. Er sucht es so aus [3]: Zunächst wählt er zwei etwa 100-stellige Primzahlen q und t und setzt $n = q \cdot t$. Des weiteren wählt er eine Zahl $e < (q-1) \cdot (t-1) = \varphi(q) \cdot \varphi(t)$, die teilerfremd zu $q-1$ und zu $t-1$ ist. Sowohl über q, t als auch über e hüllt sich P in Schweigen; er teilt nach außen allein n sowie diejenige Zahl v zwischen 1 und $(q-1) \cdot (t-1)$ mit, die folgendes erfüllt: $e \cdot v$ *läßt nach Division durch* $(q-1) \cdot (t-1)$ *den Rest 1*. Wir wissen, daß es genau ein solches v gibt.

Wie korrespondiert nun P_1 mit P_2?

> P_1 schlägt das Nummernpaar (n_2, v_2) von P_2 nach.
>
> Mithilfe von (n_2, v_2) verschlüsselt P_1 seine Botschaft B_1 zu $v_2(B_1) = B_2$. Dazu ersetzt er zunächst die Buchstaben in B_1 durch ihre Stellen im Alphabet $(a = 01, b = 02, \ldots)$ und verfährt dann mit jeder Buchstabenzahl z wie folgt: er berechnet den Rest $r(z)$ von der Potenz z^{v_2} nach Division durch n_2. Alle so für die einzelnen z gewonnenen Ergebnisse schickt er in der richtigen Reihenfolge an P_2.
>
> P_2 entschlüsselt B_2 zu $e_2(B_2) = B_1$, indem er die empfangenen Zahlen $r(z)$ in die e_2-te Potenz $r(z)^{e_2}$ hebt, durch n_2 dividiert und dann den Rest nimmt. Wir wissen, daß man so das z zurückgewinnt.

Nun sind folgende Bemerkungen am Platz:

1. Im Mittel ist jede 115-te ungerade Zahl mit 100 Stellen eine Primzahl. Das folgt aus dem Primzahlsatz. In dem Zusammenhang sei allerdings bemerkt, daß es beliebig lange Zahlenreihen $m, m+1, m+2, \ldots, m+n-2$ ohne eine einzige Primzahl darin gibt : setze, für vorgegebenes großes n, einfach $m = n! + 2$.

2. Es gibt heute Verfahren, die gestatten, von einer Zahl q zu entscheiden, ob sie Primzahl ist oder nicht, ohne dabei Faktorisierungen zu testen. Wir erinnern daran, daß zum Beispiel Primzahlen q diese Eigenschaft haben: ist $1 < a < q$, so läßt a^{q-1} nach Division durch q den Rest 1. Ein auf solch ausgezeichneten Eigenschaften aufgebauter Primzahltest dauert auf modernen Rechnern bei einer 100-stelligen Zahl nicht einmal mehr eine Minute.

[3] zu den angesprochenen Rechnungen vergleiche das numerische Beispiel am Schluß

3. Potenzieren mit gleichzeitiger Divisionsrestbildung läßt sich äußerst schnell auf einem Computer realisieren. Das beruht auf zweierlei. Erstens darauf, daß Rechner sozusagen 2-adisch arbeiten und deshalb das Quadrieren (und damit zugleich jede Potenzbildung) eine einfach durchzuführende Operation ist, und zweitens darauf, daß wegen der steten Restbildungen die Zahlen relativ klein bleiben.

Diese drei Bemerkungen lassen erkennen, daß das hier vorgestellte Ver- und Entschlüsselungsverfahren bei hinreichendem Einsatz von Technik nicht viel Zeit verbrauchen wird.

4. Um das Verfahren knacken zu wollen, muß man e_2 kennen. Dann kennt man aber auch schon q_2 und t_2 (was aber nur für P_2 zutrifft). Die heute schnellste Methode, eine 200-stellige Zahl n_2 zu faktorisieren, also in unserem Fall als Produkt $n_2 = q_2 \cdot t_2$ zu schreiben, erfordert 10^{23} Operationen. Die auszuführen dauert auch auf Computern immer noch 10^9 Jahre (1 Operation = 1 Microsekunde).

5. Zur Authentizität: Will man das, so geht man auf die folgende Weise vor. P_1 bildet zunächst (was nur er allein kann) $e_1(B_1)$ und verschlüsselt sodann dies zu $v_2(e_1(B_1))$. P_2 entschlüsselt zu $e_2(v_2(e_1(B_1))) = e_1(B_1)$ und nimmt das v_1 von P_1, um zu $B_1 = v_1(e_1(B_1))$ zu gelangen. Wir wissen, daß tatsächlich sowohl $e_2 v_2$ als auch $v_1 e_1$ Botschaften unverändert lassen.

Alle hier eingehenden theoretischen Ergebnisse entstammen der Zahlentheorie und sind seit Gauß, spätestens Riemann bekannt. Einzig die schnellen Primzahltests sind neu und nützen zahlentheoretische Erkenntnisse des 20. Jahrhunderts aus.

Ich schließe mit einem numerischen Beispiel mit allerdings einstelligen statt 100-stelligen Primzahlen.

$P_1 \leftrightarrow (n_1 = 15, v_1 = 3)$, $q_1 = 3$, $t_1 = 5$, also ist wirklich $n_1 = 15$; $v_1 = 3$ ist teilerfremd zu $q_1 - 1 = 2$ und $t_1 - 1 = 4$ und $< 2 \cdot 4 = 8$. Man überprüft, daß $e_1 = 3$, denn $3 \cdot 3 = 9 = 1 \cdot 8 + 1$.

$P_2 \leftrightarrow (n_2 = 14, v_2 = 5)$, $q_2 = 2$, $t_2 = 7$, also ist wirklich $n_2 = 14$; $v_2 = 5$ ist teilerfremd zu $q_2 - 1 = 1$ und $t_2 - 1 = 6$ und $< 1 \cdot 6 = 6$. Man überprüft, daß $e_2 = 5$, denn $5 \cdot 5 = 25 = 4 \cdot 6 + 1$.

B_1 sei die frohe Zustimmung *ja* zum Vorschlag, ins Kino zu gehen. Also $j = 10, a = 1$. Die Potenzbildungen und Rechnungen in Resten sind vertauschbar, mithin kann $z^{v_2} = 10^5 = s \cdot 14 + r$ mit $0 \leq r \leq 13$ auch so berechnet werden: $10^5 = (10^2)^2 \cdot 10 = (100)^2 \cdot 10$, 100 läßt nach Division durch 14 den Rest 2 ($100 = 7 \cdot 14 + 2$), also $(100)^2 \cdot 10$ den Rest $4 \cdot 10 = 40 = 2 \cdot 14 + 12$; i.e. $12 = r(z)$ für $z = j = 10$.
$1^5 = 1$ läßt den Rest 1 ($1 = 0 \cdot 14 + 1$). Somit besteht B_2 aus den beiden Zahlen 12 und 1.

Nun beginnt die Entschlüsselung mithilfe von $e_2 = 5$.
$12^5 = (12^2)^2 \cdot 12 = 144^2 \cdot 12$, $144 = 10 \cdot 14 + 4$. Also läßt 12^5 nach Division durch 14 denselben Rest wie $4^2 \cdot 12 = 16 \cdot 12$. Nun ist $16 = 1 \cdot 14 + 2$, womit $16 \cdot 12$ den gleichen Rest wie $2 \cdot 12 = 24 = 1 \cdot 14 + 10$ hat. Wir erhalten $10 = j$ zurück und analog $1 = a$.

Kalenderwoche 25

Die Gleichungen (1) $x^2 + y^2 = ?$ und (2) $x^3 + y^3 = z^3$ über $\mathbb{Z}$

Die Spezifizierung von "?" in (1) erlaubt die Antwort auf die Frage, welche natürlichen Zahlen Summe zweier Quadrate sind. Gleichung (2) ist die Fermatsche Gleichung zum Exponenten 3 .

Für das Studium der Gleichungen (1) und (2) führen wir die folgenden Ringe ein

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}\,, \text{ mit } i^2 = -1$$

beziehungsweise $\mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\} \subset \mathbb{C}\,,$ mit $\zeta = e^{2\pi i/3}\,,$ also $\zeta^2 + \zeta + 1 = 0\,.$

An dieser Stelle scheint es angebracht, ein paar wenige Worte über den Körper $\mathbb{C}$ der komplexen Zahlen einzufügen.

$$\mathbb{C} = \{(a,b) : a, b \in \mathbb{R}\} \text{ mit } \begin{cases} (a_1, b_1) = (a_2, b_2) & \overset{\text{def}}{\iff} & a_1 = a_2\,,\ b_1 = b_2 \\ (a_1, b_1) + (a_2, b_2) & \overset{\text{def}}{=} & (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1) \cdot (a_2, b_2) & \overset{\text{def}}{=} & (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)\,. \end{cases}$$

Diese Regeln weisen $\mathbb{C}$ als einen Körper aus: Addition und Multiplikation sind kommutativ und assoziativ; es gilt das Distributivgesetz; die Null ist $(0,0)$; $-(a,b) = (-a,-b)$; die Eins ist $(1,0)$ und es gilt $(a,b)^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$, falls $(a,b) \neq (0,0)$, also $a^2 + b^2 > 0$ ist.

Schreibt man einfach a statt $(a,0)$ und bi statt $(0,b)$, so wird $(a,b) = a + bi$ und es gilt die Regel $i^2 = -1$. Beachte, daß schon deswegen, nämlich wegen dieser letzten Gleichung, $\mathbb{C}$ keine im gewohnten Sinne mit der Multiplikation verträgliche Ordnungsbeziehung "$>$" besitzt.

Der Körper $\mathbb{R}$ wird als Teilkörper von $\mathbb{C}$ über $\mathbb{R} \ni a \leftrightarrow (a,0) = a + 0i$ angesehen. Wir beobachten schließlich, daß $\mathbb{C}$ als die reelle Ebene aufgefaßt werden kann – mit der reellen Koordinate a von $(a,b) = a + bi$ und der imaginären Koordinate b. Der Addition entspricht hier die übliche Vektoraddition (Kräfteparallelogramm), dem Produkt von $a_1 + b_1 i$ mit $a_2 + b_2 i$ der Vektor $a_3 + b_3 i$, dessen Länge $\sqrt{a_3^2 + b_3^2}$ (Pythagoras) das Produkt aus den beiden Längen $\sqrt{a_1^2 + b_1^2}$ und $\sqrt{a_2^2 + b_2^2}$ und dessen Winkel φ_3 (zur positiven reellen Achse) die Summe aus den entsprechenden Winkeln φ_1, φ_2 der Vektoren $a_1 + b_1 i\,,\ a_2 + b_2 i$ ist. In der Tat, die geometrische Definition von sin und cos impliziert unmittelbar $a + bi = \sqrt{a^2 + b^2}(\cos\varphi + i \sin\varphi)$.

Wir erwähnen schließlich die *komplexe Konjugation*

$$\gamma : \mathbb{C} \to \mathbb{C}\,, \quad a + bi \mapsto a - bi\,.$$

Dies ist ein Körperautomorphismus, also verträglich mit $+$ und $\cdot$, sowie injektiv und surjektiv. Aus γ resultieren zwei Abbildungen

1. $\mathrm{tr} : \mathbb{C} \to \mathbb{R}\,, \quad a + bi \mapsto 2a = (a+bi) + \gamma(a+bi)\,.$ Dies ist eine $\mathbb{R}$-Linearform, also additiv und dazu verträglich mit reeller Skalierung.

2. $\mathrm{n} : \mathbb{C} \to \mathbb{R}_{\geq 0}\,, \quad a + bi \mapsto a^2 + b^2\,.$ Dies ist eine multiplikative Abbildung, die 0 nur für $a + bi = 0$ wird.

Unsere Teilbereiche $\mathbb{Z}[i]$ und $\mathbb{Z}[\zeta]$ von $\mathbb{C}$ sind abgeschlossen unter $+$ und $\cdot$, nicht aber gegenüber der multiplikativen Inversenbildung; es handelt sich also wirklich um *Ringe* in $\mathbb{C}$. Die Abbildungen $\mathrm{tr}\,, \mathrm{n}$, eingeschränkt auf $\mathbb{Z}[i]$ oder $\mathbb{Z}[\zeta]$, nehmen Werte in $\mathbb{Z}$ an.

Was führt uns überhaupt zu diesen beiden Ringen? Bei Gleichung (1) die Beobachtung, daß

$$x^2 + y^2 = (x + yi)(x - yi) = \mathrm{n}(x + yi)\,,$$

bei Gleichung (2), daß

$$x^3 + y^3 = (x + y)(x + y\zeta)(x + y\zeta^2)$$

gilt. In den neuen Ringen werden unsere Ausgangsgleichungen somit in multiplikative Gleichungen transferiert und wir können Teilbarkeiten studieren. Dazu überlegen wir uns zuerst, daß $\mathbb{Z}[i]$ und $\mathbb{Z}[\zeta]$, wie $\mathbb{Z}$ selbst, einen Euklidischen Divisionsalgorithmus erlauben:

Sind $0 \neq t, s \in R \overset{\text{def}}{=} \left\{ \begin{array}{c} \mathbb{Z}[i] \\ \mathbb{Z}[\zeta] \end{array} \right.$, so existieren $v, r \in R$ mit $s = vt + r$ und $\mathrm{n}(r) < \mathrm{n}(t)$.

Kalenderwoche 26

Als unmittelbare Folgerung erhalten wir:

In $R \overset{\text{def}}{=} \left\{ \begin{array}{c} \mathbb{Z}[i] \\ \mathbb{Z}[\zeta] \end{array} \right.$ *ist jedes Element "eindeutig" als Produkt von Primelementen darstellbar.*

Dabei nennen wir

$\pi \in R$ ein Primelement, wenn $[\,\pi | ab \Longrightarrow \pi | a$ oder $\pi | b\,]$ für $a, b \in R$ gilt.

Wir nennen $\varepsilon \in R$ eine Einheit, wenn $\varepsilon | 1$ in R gilt, wenn es also ein $\varepsilon' \in R$ mit $\varepsilon\varepsilon' = 1$ gibt. Obige Eindeutigkeit bedeutet dann "eindeutig bis auf Einheitsfaktoren".

LEMMA. *$\varepsilon \in R$ ist Einheit* $\iff \mathrm{n}(\varepsilon) = 1$.

Insbesondere sind $\pm 1, \pm i$ die Einheiten von $\mathbb{Z}[i]$ und $\pm 1, \pm\zeta, \pm\zeta^2$ die von $\mathbb{Z}[\zeta]$. Des weiteren: Ist ε Einheit, so ist $\varepsilon^{-1} = \gamma(\varepsilon)$.

SATZ. *Sei p eine ganzrationale Primzahl.*

1. *p ist nicht prim in $\mathbb{Z}[i]$* $\iff$ *p ist Summe von zwei Quadraten in $\mathbb{Z}$*
2. *p ist prim in $\mathbb{Z}[i]$* $\iff p \equiv 3 \bmod 4$
3. *p ist nicht prim in $\mathbb{Z}[\zeta]$* $\iff p \equiv 1 \bmod 3$ *oder* $p = 3 = (1 - \zeta)^2(-\zeta^2)$.

SATZ. *$a \in \mathbb{N}$ ist genau dann Summe zweier Quadrate in $\mathbb{Z}$, wenn jeder Primteiler $\equiv 3 \bmod 4$ von a gerade Vielfachheit in der Primfaktorzerlegung von a hat.*

BEMERKUNGEN:

1. Mit etwas feineren Methoden kann man beweisen, daß jede natürliche Zahl Summe von vier Quadraten ist.
2. So wie weiter unten für $\mathbb{Z}[\zeta]$ ausgeführt, zeigt man auch für $\mathbb{Z}[i]$: Sei π prim in $\mathbb{Z}[i]$, also $\mathbb{Z}[i]/\pi$ ein Körper k. Ist nun $\pi = 1 - i$ oder $\pi = p \equiv 3 \bmod 4$, so ist $k = \mathbb{Z}/2$ beziehungsweise $k = \mathbb{Z}/p$; ist aber $\mathrm{n}(\pi) = p \neq 2$, so ist k ein Körper mit p^2 Elementen.

3. Analog zur Übungsaufgabe

$$-1 \text{ ist Quadrat } \bmod p \iff p = 2 \text{ oder } p \equiv 1 \bmod 4$$

fragen wir, wie es mit 2 (statt -1) in diesem Zusammenhang steht. Die folgende Schlußkette gibt die Antwort; die Rechnungen finden in $\mathbb{Z}[i]$ statt, p ist eine ungerade Primzahl.

Setze $(\frac{2}{p}) = \begin{cases} 1 & \iff & 2 \text{ ist Quadrat } \bmod p \\ -1 & \iff & 2 \text{ ist kein Quadrat } \bmod p\,. \end{cases}$ Dann folgt (unter Ausnützung einer Primitivwurzel mod p), daß $(\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \bmod p$. Des weiteren

$$(1+i)^2 = 2i\,;\ (1+i)^{p-1} = (1+i)^{2\frac{p-1}{2}} = 2^{\frac{p-1}{2}} i^{\frac{p-1}{2}}$$
$$1 + i^p \equiv (1+i)^p = 2^{\frac{p-1}{2}} i^{\frac{p-1}{2}} (1+i) \bmod p$$
$$(1+i^p)(1+i) = \left\{ \begin{array}{c} 2i \iff p \equiv 1 \bmod 4 \\ 2 \iff p \equiv 3 \bmod 4 \end{array} \right\} \equiv (\tfrac{2}{p}) i^{\frac{p-1}{2}} 2i \bmod p\,.$$

Somit, erstens,

$$p \equiv 1 \bmod 4 \implies (\tfrac{2}{p}) = (-i)^{\frac{p-1}{2}}$$
$$p \equiv 3 \bmod 4 \implies 2 = (\tfrac{2}{p}) 2 \cdot i^{\frac{p-1}{2}+1}\,,$$

und zweitens dann, weil die beiden i-Potenzen gerade sind, es sich also um Kongruenzen in $\mathbb{Z}$ handelt, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

4. Entsprechend, mit $\mathbb{Z}[i]$ ersetzt durch $\mathbb{Z}[\zeta]$, zeigt man:

   $x^2 - xy + y^2 = z$ *ist lösbar in* $\mathbb{Z} \iff z \geq 0 \quad \& \quad [p|z\,,\ p \equiv 2 \bmod 3 \implies p$ *teilt* z *mit gerader Vielfachheit*]

Das Rechnen im Ring $\mathbb{Z}[\zeta]$ in bezug auf die Fermatsche Gleichung ist etwas schwieriger. Allerdings machen wir da zunächst noch die leichte

BEOBACHTUNG: Rechnet man modulo 9, so sieht man, daß $x^3 + y^3 = z^3$ unlösbar in den Zahlen $xyz \not\equiv 0 \bmod 3$ ist.

Kalenderwochen 27/29

$\mathbb{Z}[\zeta]$:

Wir untersuchen die drei folgenden Arten von Primzahlen $p \in \mathbb{Z}$.

1. $p \equiv 1 \bmod 3 \implies p = \pi\pi'$ mit π prim in $\mathbb{Z}[\zeta]$ und $\pi' = \gamma(\pi)$
2. $p \equiv 2 \bmod 3 \implies p$ prim in $\mathbb{Z}[\zeta]$
3. $p = 3 \implies p = (1-\zeta)^2(-\zeta^2)$

Ist π prim in $\mathbb{Z}[\zeta]$, so ist $\mathbb{Z}[\zeta]/\pi$ ein Körper. (Erinnerung: $\mathbb{Z}[\zeta]/\pi$ ist $\mathbb{Z}[\zeta]$ mit der neuen Gleichheit "$\alpha \equiv \beta \iff \pi|\alpha - \beta$" für $\alpha, \beta \in \mathbb{Z}[\zeta]$. Wir schreiben genauer $\alpha \equiv \beta \bmod \pi$. Ist $\alpha \not\equiv 0 \bmod \pi$, also $\mathrm{ggT}(\alpha, \pi) = 1 = \sigma\alpha + \tau\pi$ für geeignete $\sigma, \tau \in \mathbb{Z}[\zeta]$ (Divisionsalgorithmus), so gilt $\sigma\alpha \equiv 1 \bmod \pi$.) Welche Körper erhalten wir in den obigen Fällen?

1. $\mathbb{Z}[\zeta]/\pi$ ist der Körper $\mathbb{Z}/p$ mit $p = \mathrm{n}(\pi)$ Elementen:

$$\pi = a + b\zeta \Longrightarrow b\zeta \equiv -a \bmod \pi$$
$$up + vb = 1 \Longrightarrow vb \equiv 1 \bmod \pi \Longrightarrow \zeta \equiv -av \bmod \pi$$
$$n, m \in \mathbb{Z}: \quad n \equiv m \bmod \pi \iff n \equiv m \bmod p$$

2. $\mathbb{Z}[\zeta]/p$ ist ein Körper mit p^2 Elementen:

$$x + y\zeta \equiv x_1 + y_1\zeta \bmod p \text{ mit } 0 \le x_1, y_1 \le p-1$$
$$x_1 + y_1\zeta \equiv x_2 + y_2\zeta \bmod p \iff x_1 - x_2 + (y_1 - y_2)\zeta \equiv 0 \bmod p \iff x_1 = x_2\,,\ y_1 = y_2$$

3. $\mathbb{Z}[\zeta]/1-\zeta$ ist der Körper $\mathbb{Z}/3$ mit 3 Elementen:

$$x + y\zeta \equiv x + y \bmod 1 - \zeta$$

Die Unlösbarkeit von $x^3 + y^3 = z^3$ in $\mathbb{Z} \setminus \{0\}$:

Wir beweisen (stärker) die Unlösbarkeit von $\alpha^3 + \beta^3 + \delta^3 = 0$ in $\mathbb{Z}[\zeta] \setminus \{0\}$.

Schritt 1. Falls $\alpha\beta\delta \not\equiv 0 \bmod 1-\zeta$, so ist $\alpha^3 + \beta^3 + \delta^3 = 0$ unlösbar.
(Rechne modulo $(1-\zeta)^3$ und beachte, daß $\mathbb{Z}[\zeta]/1-\zeta = \mathbb{Z}/3$.)

Schritt 2. Es gelte $1-\zeta \nmid \alpha\beta$, $1-\zeta | \delta$ und es seien α, β, δ paarweise teilerfremd. Wir nehmen $\alpha^3 + \beta^3 + \varepsilon\delta^3 = 0$ mit einer Einheit ε an und suchen sogar dazu einen Widerspruch.

2a. α und β können durch Multiplikation mit Potenzen von ζ so abgeändert werden, daß $\alpha \equiv 1 \bmod 3$ und $\beta \equiv -1 \bmod 3$.
($\mathbb{Z}[\zeta]/3 = \{\overline{a + b\zeta} : a, b \in \{0,1,2\}\}$, $\zeta^2 + \zeta + 1 = 0$)

2b. $1-\zeta$ teilt $\alpha + \beta\zeta$, $\alpha\zeta + \beta$ und $(\alpha + \beta)\zeta^2$; nenne die Quotienten $\alpha_1, \beta_1, \delta_1$.
(Multipliziere geschickt mit Potenzen von ζ.)

2c. $\alpha_1, \beta_1, \delta_1$ sind paarweise teilerfremd, bis auf eventuelle Einheitsfaktoren $(\pm 1, \pm\zeta, \pm\zeta^2)$ dritte Potenzen und $\alpha_1 + \beta_1 + \delta_1 = 0$.
($\alpha_1\beta_1\delta_1 = \frac{\alpha^3+\beta^3}{(1-\zeta)^3} = (\frac{-\delta}{1-\zeta})^3$, $\alpha = -\zeta\alpha_1 + \zeta^2\beta_1$ usw.)

2d. Es gibt eine Gleichung $\alpha_2^3 + \varepsilon'\beta_2^3 + \varepsilon''\delta_2^3 = 0$ mit Einheitsfaktoren $\varepsilon', \varepsilon''$ und $1-\zeta \mid \delta_2$, aber: δ_2 ist nur durch eine niedrigere Potenz von $1-\zeta$ als δ teilbar.
($\alpha_2^3 \approx \alpha_1$ usw.)

2e. $\varepsilon' = 1$ (rechne modulo 3 – so daß also ε' "ganzrational" wird).

2f. Setze jetzt ein Induktionsargument an.

Kalenderwoche 30

Darstellungen natürlicher Zahlen als Summe ausgezeichneter natürlicher Zahlen:

1. Die *Goldbachvermutung* besagt, daß *jede natürliche Zahl > 5 Summe von drei Primzahlen ist* (so 1742 in einem Brief an Euler). Gleichbedeutend ist, daß jede gerade Zahl > 2 Summe zweier Primzahlen ist. Die Vermtung ist offen; sie ist richtig für alle Zahlen $\le 10^8$.

2. *Warings Problem (1782)* Gegeben sei $2 \leq k \in \mathbb{N}$. Definiere $r \in \mathbb{N}$ durch

   jede natürliche Zahl ist Summe von höchstens r k-ten Potenzen.

   Von vornherein ist nicht ersichtlich, daß so ein r existiert; dies ist tatsächlich ein Ergebnis von Hilbert (1909). Nenne $g(k)$ das Minimum aller möglichen r.

$g(2) = 4$	Lagrange 1770
$g(3) = 9$	Wieferich 1909
$g(4) = 19$	Balasubramanian, Dress, Deshouillers $\sim$ 1990

   des weiteren $g(5) = 37$, $g(6) = 73$, $143 \leq g(7) \leq 3806$, etc., $g(10) \geq 1079$.

3. Fermat vermutete, daß *jede natürliche Zahl Summe von höchstens drei triangulären Zahlen, vier Quadratzahlen, fünf pentagonaler Zahlen, r r-gonaler Zahlen sei.*

   Die trianguläre Zahlen sind $1, 3, 6, 10, \ldots$, also die Werte von $f_3(x) = \frac{x(x-1)}{2} + x$ für $x = 1, 2, 3, \ldots$; die Quadratzahlen $1, 4, 9, 16, \ldots$ sind die Werte von $f_4(x) = x^2 = 2\frac{x(x-1)}{2} + x$; die pentagonalen Zahlen $1, 5, 12, 22, \ldots$ sind die Werte von $f_5(x) = 3\frac{x(x-1)}{2} + x$; schließlich die r-gonalen Zahlen die Werte von $f_r(x) = (r-2)\frac{x(x-1)}{2} + x$.

   Lagrange (1770) bewies die Vermtung für $r = 4$ (dies wurde bereits gesagt), Gauß (1796) für $r = 3$ und Cauchy (1815) für beliebiges r.

4. Waring-Goldbach: *Ist $k \in \mathbb{N}$ gegegeben und $n \in \mathbb{N}$ hinreichend groß, ist dann n Summe von k-ten Potenzen von Primzahlen?*

   Vinogradov (1938) hat gezeigt, daß es eine Zahl $V(k)$ gibt, so daß diese Frage die Antwort *ja* hat und die Anzahl der Summanden $\leq V(k)$ ist.

   Beispiel: $V(5) \leq 23$, $V(6) \leq 33$, $V(7) \leq 47$.