Einführung in die Zahlentheorie

Skizze einer Vorlesung von Nils-Peter Skoruppa
im Sommersemester 2006

Nach einem Skriptentwurf von Kristina Hanig

Version: Id: zahlentheorie.tex,v 1.36 2006/06/26 22:08:08 fenrir Exp

Inhaltsverzeichnis

0 Vorbemerkungen

7. Ap

Reflektionen zu den Fragen *„Was ist Zahlentheorie?“* und *„Wozu ist sie gut?“*

Warum studieren Sie Zahlentheorie?

„Mathematik hat mit Deutsch den Nachteil gemeinsam, sowohl universell anwendbar wie zugleich einer der Gipfel des künstlerischen Schaffens der Menschheit zu sein. Wozu braucht man Goethe, wenn man am Marktplatz seine Wünsche klar ausdrücken kann? Und wozu braucht man die Zahlentheorie, wenn man die Differentialgleichungen der Wärmeleitung numerisch lösen kann? Merkwürdig genug fahren bei diesem Spiel die Gebiete, die keine denkbare kommerzielle Anwendung haben, oft viel besser. Einer meiner Kollegen an der Durham University wurde einmal vom lokalen Fernsehen gefragt, warum er die Theorie der präzisen Datierung kretischer Vasen studiere, und antwortete, dies sei sehr nützlich beim Studium der Migration der minoischen Zivilisation. Zu meiner Überraschung wurde dies mit respektvollem Anerkennungsgemurmel akzeptiert.

Also soll unsere erste Antwort auf die Frage „Warum studieren Sie Zahlentheorie?“ vielleicht „Sie ist für das richtige Verständnis der Modulformen unentbehrlich“ sein. Nachdem wir nun die Einwände der Frivolen und Oberflächlichen erledigt haben, können wir versuchen, ernsthaft zu antworten. Die ernsthafte Antwort ist natürlich: „Warum nicht?“ Denn Biber bauen Dämme, und Kuckucks leihen Nester ohne jegliche Rückzahlungsabsicht, aber nur Menschen (soweit wir wissen) zerbrechen sich den Kopf über die Frage, welche Primzahlen Summen zweier Quadratzahlen sind. Das Verlangen nach Wissen und der Ausdruck von Schönheit sind, seitdem eine partielle Freiheit von dem niederen Überlebensbedürfnis erreicht wurde, immer das höchste Ziel der menschlichen Rasse gewesen. Der Zweck von Technologie und Erfindung ist es, unsere Zeit für das weitere Studium von Bach, Gauß und Goethe freizumachen, und nicht umgekehrt. Es ist aber eine der göttlichen Entschädigungen für unser Dasein, daß die zwanghafte Suche nach Wisssen fast immer später praktische Früchte trägt.“

A. O. L. Atkin, Chicago, anläßlich eines Besuchs im MPI für Mathematik, Juni 1985.

1 Teilbarkeit und Primzahlen

10. Ap

Definition. Sind $a, b \in \mathbb{Z}$, so sagen wir a *teilt* b, in Zeichen $a \mid b$, falls es ein $x \in \mathbb{Z}$ gibt, sodass $b = ax$.

Bemerkung. Die Teilbarkeitsrelation „$|$“ definiert eine partielle Ordnung auf $\mathbb{Z}_{\geq 0}$, d. h. die Relation „$|$“ ist es reflexiv, transitiv, und aus $a \mid b$ und $b \mid a$ folgt $a = b$.
Ist $d \mid a, b$, so folgt $d \mid ax + by$ für alle ganzen Zahlen x und y.

Definition. Ein $p \in \mathbb{Z}_{\geq 2}$ heißt *Primzahl*, falls p keine anderen positiven Teiler als 1 und p besitzt.

Satz (Fundamentalsatz (Euklid))**.** *Jede natürliche Zahl besitzt eine eindeutige Primfaktorzerlegung.*

Mit dem *Sieb des Eratosthenes* kann man alle Primzahlen ermitteln, die kleiner als eine vorgegebene natürliche Zahl n sind: Zuerst schreibt man alle natürlichen Zahlen bis zur Zahl n auf und streicht alle, von denen man weiß, da sie keine Primzahlen sind. Also zunächst die 1 und alle durch 2 teilbaren Zahlen mit Ausnahme der 2, danach alle Vielfachen der 3 mit Ausnahme der 3, dann alle Vielfachen der 5 mit Ausnahme der 5 selber. Die nächste noch nicht gestrichene Zahl ist die 7 und das ist eine Primzahl. Also streicht man alle weiteren Vielfachen von 7 usw. bis zur $\sqrt{n}$.

Satz. *Es gibt unendlich viele Primzahlen.*

Satz (Primzahlsatz, ohne Beweis)**.** *Für reelle Zahlen x bezeichne $\pi(x)$ die Anzahl der Primzahlen unterhalb x, d.h. $\pi(x) = \#\{p \text{ Primzahl } | p \leq x\}$. Dann sind $\pi(x)$ und $\frac{x}{\log(x)}$ für $x \to \infty$ aysmptotisch gleich.*

Definition (Größter gemeinsamer Teiler)**.** Für ganze Zahlen a, b, nicht beide Null, wird $\mathrm{ggT}(a,b) := \max\{d \in \mathbb{Z}_{\geq 0} : d \mid a,\ d \mid b\}$ als *größter gemeinsamer Teiler* von a und b bezeichnet.

Satz. *Für den g.g.T. von a und b gilt die Formel*

$$(a,b) := p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}},$$

wenn $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ und $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$ $(\alpha_i, \beta_i \geq 0)$ die Primfaktorzerlegungen von a und b bezeichnen.

Definition (Ideal)**.** Eine nichtleere Teilmenge I von $\mathbb{Z}$ heißt *Ideal*, falls mit $a, b \in I$ auch $a \pm b \in I$ gilt.

Beispiel. Es sind $\{0\}$ und $\mathbb{Z}$ Ideale. Ist allgemeiner d eine ganze Zahl, so ist $(d) = \mathbb{Z}d = \{dx : x \in \mathbb{Z}\}$ ein Ideal; es wird als das *von d erzeugte Hauptideal* bezeichnet. Allgemeiner ist für beliebige ganze Zahle a_i die Menge

$$(a_1, \ldots, a_r) = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_r := \{a_1x_1 + \cdots + a_rx_r : x_1, \ldots, x_r \in \mathbb{Z}\}$$

ein Ideal.

Satz. *Jedes Ideal ist Hauptideal, d. h. es gilt $I = \mathbb{Z}d$ mit geeignetem d.*

Satz (Euklidische Division)**.** *Zu jedem $m, q \in \mathbb{Z}$ und $q \neq 0$ existieren eindeutig $x, r \in \mathbb{Z}$ mit $m = qx + r$, wobei $0 \leq r < |q|$.*

Beispiel. $7 = -5 \cdot (-1) + 2$

Satz (Bézout)**.** *Zu jedem Paar $a, b \in \mathbb{Z}$, nicht beide Null, gibt es $x, y \in \mathbb{Z}$ mit $ax + by = \mathrm{ggT}(a, b)$.*

Bemerkung. Zu vorgegeben ganzen Zahlen a, b, c ist die Gleichung $ax+by = c$ genau dann in ganzen Zahlen lösbar, falls der g.g.T. von a und b die Zahl c teilt.

Satz. $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\,\mathrm{ggT}(a, b)$.

Satz (Euklid's Lemma)**.** *Sei p eine Primzahl und $a, b \in \mathbb{Z}$, so folgt aus $p \mid ab$, dass $p \mid a$ oder $p \mid b$.*

Bemerkung. Induktiv folgt aus dem Satz die etwas allgemeinere Aussage: Ist p Primzahl, $p \mid a_1 \cdots a_r$, so ist $p \mid a_j$ für mindestens ein j.

Folgerung. *Mittels Euklid's Lemma ergibt sich ein zweiter Beweis für die Eindeutigkeit der Primfaktorzerlegung.*

21. Ap

Den g.g.T. ganzer Zahlen berechnet man am kostengünstigsten mittels des *euklidischen Algorithmus*. Die einfachste Variante basiert auf folgendem Lemma.

Lemma. *Es gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, b+ax)$ für alle ganzen Zahlen a, b und x.*

Algorithmus (Berechnung des g.g.T.).

```
ggT_1( a,b) =
/*
   Input
      a,b: positive ganze Zahlen
   Output
      Der g.g.T. von a und b
*/
{
   local(c);

   while( b > 0, c = b; b = a%b; a = c);
   return(a);
}
```

Führen wir über die euklidischen Divisionen des vorstehende Algorithmus Buch, so berechnet der Euklidischer Algorithmus uns gleichzeitig auch noch Lösungen x, y wie im Satz von Bézout, d.h. Lösungen der Gleichung $ax+by = \mathrm{ggT}(a,b)$.

Algorithmus (Lösen von $ax + by = \mathrm{ggT}(a,b)$).

```
myBezout( a, b) =
/*
   Input
      a,b: positive ganze Zahlen
   Output
      Ein Vektor [x,y] mit ax+by=ggt(a,b)
*/
{
   local(q,r,v);

   q = a\b; r = a%b;
   if( 0 == r, return( [0,1]));
   v = myBezout( b, r);
   return( [v[2], v[1]-q*v[2]]);
}
```

Definition (Kleinstes gemeinsames Vielfaches)**.** Für $a, b \in \mathbb{Z}$, nicht beide Null, wird die Zahl

$$\mathrm{kgV}(a,b) := \min\{d \in \mathbb{Z}_{>0} : a|d,\ b|d\}$$

als *kleinstes gemeinsames Vielfaches* von a und b bezeichnet.

Satz. *Für das k.g.V. zweier Zahlen a und b gilt die Formel*

$$\mathrm{kgV}(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} \cdot \cdots \cdot p_r^{\max\{\alpha_r,\beta_r\}},$$

wobei $a = p_1^{\alpha_1} \cdot \cdots \cdot p_r^{\alpha_r}$ und $b = p_1^{\beta_1} \cdot \cdots \cdot p_r^{\beta_r}$ die Primfaktorzerlegungen von a und b bezeichnen.

Als Folgerung der Formeln für den g.g.T. und k.g.V. in Termen der Primfaktorzerlegungen und der Formel $\min\{\alpha_j,\beta_j\} + \max\{\alpha_j,\beta_j\} = \alpha_j + \beta_j$ erhält man

Satz. $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = ab.$

Definition (g.g.T. und k.g.V. für mehr als zwei Zahlen)**.** Für ganze Zahlen $a_1, \ldots, a_r$, nicht alle Null, definiert man

$$\begin{aligned} \mathrm{ggT}(a_1, \ldots, a_r) &:= \max\{d \in \mathbb{Z}_{\geq 0} : d \mid a_1, \ldots, d \mid a_r\} \\ \mathrm{kgV}(a_1, \ldots, a_r) &:= \min\{d \in \mathbb{Z}_{>0} : a_1 \mid d, \ldots, a_r \mid d\} \end{aligned}$$

Satz. *Es gelten die Formeln*

$$\begin{aligned} a_1\mathbb{Z} + \cdots + a_r\mathbb{Z} &= \mathrm{ggT}(a_1, \ldots, a_r)\mathbb{Z} \\ a_1\mathbb{Z} \cap \cdots \cap a_r\mathbb{Z} &= \mathrm{kgV}(a_1, \ldots, a_r)\mathbb{Z} \end{aligned}$$

Bemerkung. Für $r \geq 3$ ist im Allgemeinen

$$\mathrm{ggT}(a_1 \cdots a_r) \cdot \mathrm{kgV}(a_1 \cdots a_r) \neq a_1 \cdots a_r.$$

Algorithmus (Simultane Berechnung des g.g.T. mehrerer Zahlen).

```
ggT_2( v) =
/*
        Input
                v: ein Vektor positiver ganzer Zahlen
        Output
                g.g.T. der Liste der Zahlen in v
*/
{
        local(b,w,r);

        while( length( v) > 1,
                v = vecsort(v);
                b = v[1]; w = [b];
                for( n= 2, length(v),
                        r = v[n]%b;
                        if( r != 0, w = concat( w, r))
                );
                v = w;
        );
        return( v[1]);
}
```

Diesen Algorithmus kann man noch leicht optimieren, indem man die Divisionen mit Rest modifiziert: statt $b = aq + r$ mit $0 \leq r < |a|$ führt man die modifizierte Restdivision $b = aq' + s$ mit $-|a|/2 < s \leq |a|/2$ durch.

2 Kongruenzrechnung

24. Ap

Definition. Seien $a, b, m \in \mathbb{Z}$. Dann nennt man a *kongruent zu* b *modulo* m (in Zeichen: $a \equiv b \bmod m$), falls $m \mid (a - b)$.

Bemerkung. Es gilt $a \equiv b \bmod 0$ genau dann wenn $a = b$.

Satz. *Für festgewähltes m ist die Relation $a \equiv b \bmod m$ eine Äquivalenzrelation.*

Definition. Die Menge der Äquivalenzklassen der Relation *kongruent modulo* m wird mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet.

Satz. *Sei $m \neq 0$ Dann ist $a \equiv b \bmod m$ genau dann, wenn a und b bei Division durch m den gleichen Rest lassen.*

Folgerung.

(i) Die Äquivalenzklassen in $\mathbb{Z}/m\mathbb{Z}$ sind von der Gestalt

$$a + m\mathbb{Z} = \{a + mx : x \in \mathbb{Z}\}.$$

(ii) Für $m \neq 0$ ist $\mathbb{Z}/m\mathbb{Z} = \{r + m\mathbb{Z} | 0 \leq r < m\}$. Insbesondere ist $\mathbb{Z}/m\mathbb{Z}$ endlich und $\#\mathbb{Z}/m\mathbb{Z} = m$.

Satz. *Sein m eine ganze Zahl. Sind $a \equiv a' \bmod m$ und $b \equiv b' \bmod m$, so ist auch $a + b \equiv a' + b' \bmod m$ und $ab \equiv a'b' \bmod m$.*

Satz. *Es ist 9 Teiler von n genau dann wenn 9 die Quersumme von n (in der Dezimalentwicklung) teilt.*

Satz. *Ist $\mathrm{ggT}(k, m) = 1$, so folgt aus $ka \equiv kb \bmod m$, dass $a \equiv b \bmod m$.*

Korollar. *Ist m Primzahl, dann folgt aus $ka = kb \bmod m$ für $k \not\equiv 0 \bmod m$ stets $a = b \bmod m$.*

Satz. *Es gibt ein k' sodass $kk' = 1 \bmod m$ genau dann, wenn $\mathrm{ggT}(k, m) = 1$.*

Algorithmus (Berechnung des Inversen zu k modulo m).

```
inv( k, m) =
/*
   Input
      k,m: ganze Zahlen, m nicht Null
   Output
```

```
      das kleinste positive k' mit kk'=1 mod m
      (falls es existiert)
*/
{
   local(v);

   if( gcd( k, m) != 1,
      error( "inv: "k" besitzt kein Inverses mod m")
   );
   v = bezout( k, m);
   return( v[1]);
}
```

Satz (Chinesischer Restsatz). *Es seine $m_1, \ldots, m_r$ paarweise teilerfremde Zahlen. Es seien $a_1, \ldots, a_r \in \mathbb{Z}$. Dann gibt es eine Lösung x der simultanen Kongruenzen*

$$x = a_j \bmod m_j \qquad (1 \leq j \leq r).$$

Diese Lösung ist modulo $m := m_1 \cdots m_r$ eindeutig bestimmt, d.h. ist x' eine weitere Lösung dieser simultanen Kongruenzen, so ist $x \equiv x' \bmod m$.

Algorithmus (Lösen simultaner Konguenzen).

```
myChinese( a_vec, m_vec) =
/*
   Input
      a_vec: ein Vektor ganzer Zahlen
      m_vec: ein Vektor teilerfremder ganzer Zahlen
      (gleiche Laenge wie a_vec)
   Output
      die kleinste psoitive Loesung x
      der simultanen Kongruenzen
         x = a_j mod m_j
      (wo a_j, m_j die Komponenten von a_vec, m_vec sind)
*/
{
   local(m, mp_vec, k_vec);

   m = prod(i=1,length(m_vec),m_vec[i]);
   mp_vec = vector(length(m_vec),i, m/m_vec[i]);
   k_vec = vector( length(m_vec), i, inv(mp_vec[i],m_vec[i]));
```

```
    return(
        sum(i=1,length(m_vec), a_vec[i]*k_vec[i]*mp_vec[i]) % m
    );
}
```

28. Ap

Folgerung. *Sei f ein Polynom mit ganzzahligen Koeffizienten in r Variablen, sei $m > 0$ eine ganze Zahl. Für jede Primzahlpotenz $p^\alpha \| m$[1] gebe es eine Lösung $\vec{x}_p \in \mathbb{Z}^r$ der Kongruenz*

$$f(\vec{x}_p) \equiv 0 \bmod p^\alpha.$$

Nach dem chinesischen Restsatz gibt es dann ein $\vec{x} \in \mathbb{Z}^r$, sodass für jede Primzahlpotenz p^α die Kongruenz $\vec{x} \equiv \vec{x}_p \bmod p^\alpha$ gilt. (Diese ist komponentenweise zu lesen.) Damit gilt dann aber auch

$$f(\vec{x}) \equiv 0 \bmod m.$$

Setzen wir

$$a(m) := \#\{(x_1, \ldots, x_r) \in \mathbb{Z} : 0 \le x_1, \ldots, x_r < m, f(x_1, \ldots, x_r) \equiv 0 \bmod m\},$$

so folgt mit vorstehender Überlegung

$$a(m) = \prod_{p^\alpha \| m} a(p^\alpha).$$

Hierbei ist das Produkt so zu verstehen, dass p^α die in m genau aufgehenden Primzahlpotenzen bedeutet.

Definition. Ist $n|m$ so bezeichnet red_n die Abbildung

$$\mathrm{red}_n : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad a + m\mathbb{Z} \mapsto a + n\mathbb{Z}.$$

Lemma. *Die vorstehende Abbildung ist wohldefiniert (d.h. ist $a + m\mathbb{Z} = b + m\mathbb{Z}$, so gilt auch $a + n\mathbb{Z} = b + n\mathbb{Z}$).*

Den chinesischen Restsatz kann man auch folgendermassen interpretieren:

Satz. *Seien $m_1, \ldots, m_r$ paarweise teilerfremde Zahlen, $m = m_1 \cdots m_r$. Dann ist die Abbildung*

$$\begin{aligned} \mathrm{red}_{m_1} \times \cdots \times \mathrm{red}_{m_r} : \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \\ a + m\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_r\mathbb{Z}). \end{aligned}$$

bijektiv.

[1] Wir schreiben $t \| m$ und nennen t einen *exakten Teiler* von m, falls t ein Teiler von m mit $\mathrm{ggT}(t, m/t) = 1$ ist.

Definition. Eine Restklasse $a+m\mathbb{Z}$ heißt *primitiv*, falls $\mathrm{ggT}(a,m)=1$. Die Menge aller primitiven Restklassen in $\mathbb{Z}/m\mathbb{Z}$ wird mit $(\mathbb{Z}/m\mathbb{Z})^*$ bezeichnet.

Definition. Die Eulersche φ-Funktion ist erklärt durch

$$\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^* \qquad (m \geq 1).$$

Beispiel. Für die ersten Werte hat man

m	1	2	3	4	5	6	7	8	9	10	11	12	24
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	8

Satz. *Seien $m_1, \ldots, m_r$ paarweise teilerfremde Zahlen, $m = m_1 \cdots m_r$. Dann definiert die Abbildung $\mathrm{red}_{m_1} \times \cdots \times \mathrm{red}_{m_r}$ bei Einschränkung eine Bijektion*

$$(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^*.$$

Insbesondere gilt $\varphi(m) = \varphi(m_1)\cdots\varphi(m_r)$.

Lemma. *Für Primzahlpotenzen p^α gilt $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

Satz. *Es gilt*

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Hierbei durchläuft p die (paarweise verschiedenen) Primteiler von m.

Bemerkung. Für eine Primzahl p ist also $\varphi(p) = p-1$. Ist $m > 1$ keine Primzahl, so ist $\varphi(m) < m-1$.

Definition. Ist a eine zu m teilerfremde Zahl, so setzen wir

$$\mathrm{ord}(a \bmod m) = \min\{n > 0 : a^n \equiv 1 \bmod m\}.$$

Satz. *Die vorstehende Definition ist sinnvoll, d.h. zu teilerfremden a und m gibt es stets ein $n > 0$ mit $a^n \equiv 1 \bmod m$.*

Ist a zu m teilerfremd, und ist n eine ganzeZahl, so setzen wir

$$(a+m\mathbb{Z})^n = \begin{cases} a^n + m\mathbb{Z} & n > 0 \\ m\mathbb{Z} & n = 0 \\ a'^n + m\mathbb{Z} & n < o \end{cases}.$$

Hierbei bezeichnet a' die mod m eindeutig bestimmte Zahl mit $aa' \equiv 1 \bmod m$.

Satz. *Es sei a zu m teilerfremd, $n = \mathrm{ord}(a \bmod m)$. Dann gilt*

$$\{(a + m\mathbb{Z})^n : n \in \mathbb{Z}\} = \{a^k + m\mathbb{Z} : 0 \leq k < n\}.$$

Definition. Sei p^α eine Primzahlpotenz. Eine ganze Zahl w heißt Primitivwurzel modp^α, falls $\{(w + m\mathbb{Z})^n : n \in \mathbb{Z}\} = (\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

Bemerkung. Nach der vorangehenden Diskussion ist also a eine Primitivwurzel modulo p^α genau dann, wenn $\mathrm{ord}(a \bmod m) = \varphi(m)$.

Beispiel. Es ist $a = 10$ eine Primitivwurzel modulo 7: $10 \equiv_7 3$, $100 \equiv_7 2$, $1000 \equiv_7 6$, $10000 \equiv_7 4$, $100000 \equiv_7 5$, $1000000 \equiv_7 1$,

5. Mai

Satz (Kleiner Fermatscher Satz)**.** *Ist p eine Primzahl, so gilt für jede ganze Zahl $x^p \equiv x \bmod p$.*

Bemerkung. Für ganze Zahlen x, y gilt stets $(x + y)^p \equiv x^p + y^p \bmod p$.

Satz (Großer Fermatscher Satz)**.** *$a^n + b^n = c^n$ hat für $n > 2$ keine Lösung in ganzen Zahlen mit $abc \neq 0$.*

Satz (Euler)**.** *Ist x teilerfremd zu m, so gilt $x^{\varphi(m)} \equiv 1 \bmod m$.*

Bemerkung. Der kleine Fermatsche Satz impliziert einen einfachen Test einer Zahl auf Primalität: prüfe systematisch (oder zufällig) gewählte zu m teilerfremde x daraufhin, ob $x^{m-1} \equiv 1 \bmod m$ ist. Besteht ein x diesen Test nicht, so kann m keine Primzahl sein. Dieser Primalitätstest versagt allerdings für *Carmichael-Zahlen*, d.h. für Zahlen m, die keine Primzahlen sind, für die aber $x^{m-1} \equiv 1 \bmod m$ für alle zu m teilerfremden x gilt.

Satz. *Es sei a zu m teilerfremd. Dann gilt* $\mathrm{ord}(a \bmod m) | \varphi(m)$.

Lemma. *Sei p eine Primzahl, seien $a_n, \ldots, a_0$ ganze Zahlen und $a_n \not\equiv 0 \bmod p$ Dann hat die Kongruenz*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \bmod p$$

höchstens n Lösungen modulo p.

Satz. *Zu jeder Primzahl p gibt es eine Primitivwurzel modulo p.*

8. Mai

Satz. *Zu jeder ungeraden Primzahl p gibt es eine ganze Zahl w, sodass w eine Primitivwurzel modulo jeder Potenz p^α ist.*

Satz. *Zu jeder ungeraden Zahl a ud jeder Potenz 2^α gibt es eine $n \geq 0$, sodass $a \equiv \pm 5^n \bmod 2^\alpha$.*

Satz (Wilson)**.** *Ist p eine Primzahl, dann $(p-1)! \equiv -1 \bmod p$.*

Satz. *Sei p ungerade Primzahl. Dann ist $x^2 \equiv -1 \bmod p$ genau dann lösbar, wenn $p \equiv 1 \bmod 4$.*

12.Ma

Satz (Thue)**.** *Sei p eine Primzahl. Dann gibt es zu jedem zu p teilerfremdenr Zahlen $0 < a, b < \sqrt{p}$, sodass $b \equiv \pm ra \bmod p$. Allgemeiner gilt: Ist $m > 0$ und sind $0 < A, B \leq m$, $AB > m$, dann gibt es zu jedem zu m teilerfremden r Zahlen $0 < a < A$, $0 < b < B$ mit $b \equiv \pm ra \bmod m$.*

Als Folgerungen der letzten beiden Sätze erhält man:

Satz. *Eine ungerade Primzahl p ist genau dann Summe zweier Quadrate, wenn $p \equiv 1 \bmod 4$ ist.*

Algorithmus (Berechnung einer Darstellung einer Primzahl p als Summe zweier Quadrate).

```
findSquares(p) =
/*
   Input
      p: a prime = 1 mod 4
   Output
      a vector of integers [a,b] such that p=a^2+b^2
*/
{
   local( x, a, b, r);

   if(
      \\ 0 == isprime(p) ||  /* this could be time consuming */
      1 != p%4,
      error( "findSquares( "p
      "): argument must be a prime congruent to  1 mod 4")
   );
   x=2; while( Mod( -1, p) != Mod( x, p)^((p-1)/2), x++);
   x = lift( Mod( x, p)^((p-1)/4));
   if( x < p/2, x = p - x); print(x);
   a=p; b=x; while( b > sqrt(p), r=a%b; a=b; b=r);print(b);
   return( vecsort( [ b, sqrtint(p-b*b)]));
}
```

Die Gültigkeit des Algorithmus beruht auf folgendem Satz, den wir in einem späteren Kapitel beweisen werden:

Satz. *Sei p eine Primzahl und x eine Lösung von $x^2 \equiv -1 \bmod p$ mit $p/2 < x < p$. Es bezeichne r_n die durch $r_0 = p$, $r_1 = x$ und $r_n = r_{n-2} \% r_{n-1}$ $(n \geq 2)$ definierte Folge. Sei l der kleinste Index, sodass $r_l < \sqrt{p}$. Dann ist $p - r_l^2$ eine Quadratzahl.*

2.1 Anhang: Diskurs über Gruppen, Körper und über Ringe

Ein *Körper* ist eine Menge K zusammen mit zwei Operationen, die die aus der linearen Algebra bekannten Axiome erfüllen. Unter einer Operation auf einer Menge M versteht man eine Abbildung $M \times M \to M$.
Ein *Ring* ist eine Menge R, versehen mit zwei Operationen, für die die gleichen Axiome wie für einen Körper gelten mit Ausnahme des Axioms, welches die Existenz der multiplikativen Inversen postuliert. Genauer definiert man also:

Definition (Ring)**.** Eine Menge R mit zwei Operationen $\oplus, \odot : R \times R \to R$ heit *Ring*, wenn gilt:

(i) $\forall a, b, c \in R : (a \oplus b) \oplus c = a \oplus (b \oplus c)$.

(ii) $\exists n \in R \, \forall a \in R : a \oplus n = n \oplus a = a$. (Es gibt höchstens solch ein n, wie man sich leicht überlegt.)

(iii) Mit dem n wie aus (ii) gilt: $\forall a \in R \, \exists \, a' \in R : a \oplus a' = n$.

(iv) $\forall a, b \in R : a \oplus b = b \oplus a$.

(v) $\forall a, b, c \in R : (a \odot b) \odot c = a \odot (b \odot c)$.

(vi) $\exists e \in R \, \forall a \in R : a \odot e = e \odot a = a$. (Es gibt höchstens solch ein e, wie man sich leicht überlegt.)

(vii) $\forall a, b \in R : a \odot b = b \odot a$.

(viii) $\forall a, b, c \in R : (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

Bemerkung. Wegen (vi) und (vii) nennt man $(R, \oplus, \odot)$ genauer auch kommutativen Ring mit Eins. Die ducrh die Axiome (ii) und (vi) eindeutig bestimmten Elemente n und e bezeichnet man meist einfach mit 0 und 1 (was dann nicht mit den *Zahlen* 0 und 1 verwechselt werden darf.

Beispiel. Bespiele für Ringe sind $\mathbb{Z}$, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $\mathbb{Z}[X]$, und natürlich jeder Körper.
Bespiele für Körper sind $\mathbb{Q}$, $\mathbb{R}$, $\overline{Q}$ (d.h. die Menge der algebraischen Zahlen, also der komplexen Zahlen, die als Nullstellen von Polynomen postiven Grads

mit rationalen Koeffizenten auftreten), $Q(X)$ (d.h. der Körper der rationalen Funktionen mit Koeffizienten in $\mathbb{Q}$).
Die Operationen in den voangehenden Beispielen sind die natrlichen Additionen und Multiplikationen.

Sei jetzt $m > 1$ eine ganze Zahl. Für $a + m\mathbb{Z}, b + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ setzt man

(i) $(a + m\mathbb{Z}) \oplus (b + m\mathbb{Z}) := (a + b) + m\mathbb{Z}$

(ii) $(a + m\mathbb{Z}) \odot (b + m\mathbb{Z}) := (a \cdot b) + m\mathbb{Z}$.

Satz. *Die in der obigen Definition erklärten Operationen*

$$\oplus, \odot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

sind wohldefiniert, d. h. hängen nicht von der Wahl der Repräsentanten ab.

Satz. *Die Menge der Restklassen $\mathbb{Z}/m\mathbb{Z}$, versehen mit der Addition $\oplus$ und der Multiplikation $\odot$, ist ein Ring.*

Satz. *Für eine Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$, versehen mit $\oplus$ und $\odot$, ein Körper.*

Bemerkung. Eine übliche Bezeichnung für den Körper $\mathbb{Z}/p\mathbb{Z}$ ist auch $\mathbb{F}_p$.

Definition. Ist R ein Ring, so nennt man

$$R^* = \{r \in R : \exists\, r' \in R : rr' = 1\}$$

die *Gruppe der Einheiten des Ringes R.*

Satz. *Die Menge R^*, versehen mit der Multiplikation des Ringes R, ist eine abelsche Gruppe.*

Satz. *Die früher eingefürte Gruppe der primen Restklassen $(Z/mZ)^*$ stimmt mit der Gruppe der Einheiten des Ringes $\mathbb{Z}/m\mathbb{Z}$ überein.*

Die Sätze von Fermat bzw. Euler sind Spezialfälle des für allgemeine allgemeine Gruppen gültigen

Satz. *Ist G eine endliche Gruppe und $g \in G$, so gilt $g^{\#G} = 1$.*

Definition (Zyklische Gruppe)**.** Eine Gruppe G heisst zyklisch, falls ein Element $g \in G$ existiert, sodass $G = \{g^n : n \in \mathbb{Z}\}$.

Unsere Sätze über die Existenz Primitivwurzeln kann man dann auch folgendermassen formulieren:

Satz. *Für ungerade Primzahlpotenzen p^α ist die Gruppe $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ zyklisch.*

15.Ma

2.2 p-adische Zahlen und Nullstellen von Polynomen

Satz. *Sei $f(x)$ ein Polynom mit ganzahligen Koeffizienten, p^n eine Primzahlpotenz und für eine ganze Zahl x_1 gelte $f(x_1) \equiv 0 \bmod p$, $f'(x_1) \not\equiv 0 \bmod p$. Dann gibt es genau ein $0 \leq x_n < p^n$ mit $f(x_n) \equiv 0 \bmod p^n$, $x_n \equiv x_1 \bmod p$.*

Korollar. *Unter den gleichen Voraussetzungen wie im Satz gibt es genau eine Folge $(x_\alpha)_{\alpha \geq 1}$ von Zahlen $0 \leq x_\alpha < p^\alpha$, sodass $f(x_\alpha) \equiv 0 \bmod p^\alpha$ und $x_\alpha \equiv x_{\alpha-1} \bmod p^{\alpha-1}$ für alle $\alpha \geq 2$.*

Definition. Der Ring der p-adischen Zahlen $\mathbb{Z}_p$ ist definiert als

$$\mathbb{Z}_p = \{(z_\alpha)_{\alpha \geq 1} : \forall \alpha \geq 1 \ (z_\alpha \in \mathbb{Z}/p^\alpha\mathbb{Z}, \ r_\alpha(z_{\alpha+1}) = z_\alpha)\},$$

versehen mit der komponenterweisen Addition und Multiplikation. (r_α ist die natürliche Abbildung $r_\alpha : \mathbb{Z}/p^{\alpha+1}\mathbb{Z} \to \mathbb{Z}/p^\alpha\mathbb{Z}$.)

Man identifieziert $\mathbb{Z}$ mit seinem Bild in $\mathbb{Z}_p$ unter der Injektion

$$x \mapsto (x + p^\alpha\mathbb{Z})_{\alpha \geq 1}.$$

Das vorangehende Korollar kann nun folgendermassen formuliert werden:

Satz. *Sei p eine Primzahl, f ein Polynom mit ganzzahligen Koeffizienten, und x_1 eine ganze Zahl mit $f(x_1) \equiv 0 \bmod p$, $f'(x_1) \not\equiv 0 \bmod p$. Dann gibt es genau ein $z \in \mathbb{Z}_p$ mit $f(z) = 0$ und $z_1 = x_1 + p\mathbb{Z}$.*

3 Quadratische Reziprozität

Definition. Eine Zahl a heisst *quadratischer Rest modulo m*, falls die Kongruenz $x^2 \equiv a \bmod m$ lösbar ist.

Satz. *Sei p^n eine ungerade Primzahl und a eine nicht durch p teilbare Zahl. Dann ist die Zahl a quadratischer Rest modulo p^n genau dann, wenn sie quadratischer Rest modulo p ist.*

Bemerkung. Sei a ungerade. Dann ist a stets quadratischer Rest modulo 2, es ist a quadratischer Rest modulo 4 genaus dann, wenn $a \equiv 1 \bmod 4$, und für $\alpha \geq 3$ st a quadratischer Rest modulo 2^α genau dann, wenn $a \equiv 1 \bmod 8$.

Definition (Legendre-Symbol)**.** Für ungerade Primzahlen p und ganze Zahlen a setzen wir

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } x^2 \equiv a \bmod p \text{ lösbar ist und } \mathrm{ggT}(a,p) = 1 \\ 0 & \text{falls } p \mid a \\ -1 & \text{sonst} \end{cases}$$

Satz. *Es sei p eine ungerade Primzahl.*

1. *Gilt $a \equiv a' \bmod p$, so ist $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$.*
2. *Es gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*
3. *$\left(\frac{1}{p}\right) = 1$ und für alle zu p teilerfremden a ist $\left(\frac{a^2}{p}\right) = 1$.*
4. *$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.*
5. *Ist w eine Primitivwurzel modulo p, so ist $\left(\frac{w^\nu}{p}\right) = (-1)^\nu$ für alle ν.*

19.Ma

Definition. Ein Dirichletcharakter modulo m ist ein Gruppenhomomorphismus[2] $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ (d.h. eine Abbildung, die $\chi(ab) = \chi(a)\chi(b)$ für alle $a, b \in (\mathbb{Z}/m\mathbb{Z})^*$ erfüllt).

Bemerkung. (1) Es gilt stets $\chi(1) = 1$. (2) Ist χ ein Dirichletcharakter modulo m, so sind die Werte von χ stets $\phi(m)$-te Einheitswurzeln. Insbesondere nimmt ein reeller (d.h. reelwertiger) Dirichletcharakter nur die Werte $\{\pm 1\}$ an. (3) Man fasst, *by abuse of language*, einen Dirichletcharakter modulo m oft auch als Abbildung $\chi : \mathbb{Z} \to \mathbb{C}^*$ auf, indem man definiert:

$$\chi(x) = \begin{cases} \chi(x + m\mathbb{Z}) & \text{falls } \gcd(x, m) = 1, \\ 0 & \text{sonst.} \end{cases}$$

Korollar. *Die Abbildung*

$$(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}, \quad a + p\mathbb{Z} \to \left(\frac{a}{p}\right)$$

ist wohldefiniert und definiert einen Dirichletcharacter modulo p.

Korollar. *Sei g eine Primitivwurzel modulo der ungeraden Primzahl p. Dann durchläuft $\{1 = g^0, g^2, g^4, ..., g^{p-1}\}$ ein vollständiges Repräsentantensystem für die Restklassen der quadratischen Reste modulo p. Insbesondere gibt es genau so viele quadratische Reste modulo p wie quadratische Nichtreste.*

Satz (Eulersches Kriterium)**.** *Für zu p prime a gilt $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.*

[2] Ein Gruppenhomomorphismus ist eine Abbildung $f : G \to H$ zwischen Gruppen G und H, so da $f(ab) = f(a)f(b)$ für alle $a, b \in G$ gilt.

Satz (Gaussches Kriterium)**.** *Es sei a teilerfremd zu p. Es bezeichne n die Anzahl der aj mit $0 < j < \frac{p}{2}$, so daß $aj \equiv -j' \bmod p$ mit einem $0 < j' < \frac{p}{2}$ gilt. Dann ist $\left(\frac{a}{p}\right) = (-1)^n$.*

Bemerkung. Man kann das Gaussche Kriterium für postive a auch anwenden, indem man man zählt wieviele der Zahlen aj $(0 < j < \frac{p}{2})$ in der Vereinigung der Intervalle $(\frac{(2k-1)p}{2a}, \frac{2kp}{2a})$ $(1 \le k \le \lfloor \frac{a}{2} \rfloor)$ liegen. Danach ergibt sich die Formel

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\lfloor \frac{a}{2} \rfloor} \#(\frac{(2k-1)p}{2a}, \frac{2kp}{2a}) \cap \mathbb{Z}}.$$

Für $a = 3$ ergibt sich damit zum Beispiel

$$\left(\frac{3}{p}\right) = (-1)^{\#(\frac{p}{6}, \frac{p}{3}) \cap \mathbb{Z}}.$$

Beispiel. Eine einfache Fallunterscheidung nach der Restklasse von p modulo 3 in der letzten Formel ergibt

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

Satz. *Es gilt* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Satz. *Es sei a ungerade und teilerfremd zu p. Dann gilt*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{aj}{p} \rfloor}.$$

Bemerkung. Die Formel des Satzes kann man auch in der folgenden Form formulieren: Es gilt $\left(\frac{a}{p}\right) = (-1)^{\Delta}$, wobei

$$\Delta = \#\{(x, y) \in \mathbb{Z}^2 : 0 < x < \frac{p}{2},\ 0 < y < \frac{a}{p}x\}.$$

22.Ma

Satz (Quadratisches Reziprozitätsgesetz)**.** *Für ungerade Primzahlen p, q gilt*

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

Definition (Verallgemeinertes Legendre-Symbol)**.** Für ungerades positives b und ganze Zahlen a setzen wir

$$\left(\frac{a}{b}\right) = \prod_{p^\alpha || b} \left(\frac{a}{p}\right)^\alpha.$$

Lemma. *Die Abbildung*

$$(\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* \to \{\pm 1\}, \quad (a+4\mathbb{Z}, b+4\mathbb{Z}) \mapsto \langle a|b\rangle := (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

ist bilinear.

Satz (Verallgemeinerte quadratische Reziprozität)**.** *Seien a, b ungerade, positive und zueinander teilerfremd. Dann gilt*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

Algorithmus (Verallgemeinertes Legendre-Symbols).

Pending Exercise

3.1 Quadratische Gleichungen und Kubikwurzeln

Satz. *Seien a, b, c ganze Zahlen und sei p eine ungerade Primzahlen, $p \nmid a$. Dann gilt*

$$\#\{0 \le x < p : ax^2 + bx + c \equiv 0 \bmod p\} = 1 + \left(\frac{\Delta}{p}\right),$$

wobei $\Delta = b^2 - 4ac$.

Satz. *Die Abbildung $\mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^3$ ist bijektiv, falls $p \equiv 0, -1 \bmod 3$, und sie ist 3 zu 1 andernfalls.*

26.Ma

4 Mersennesche und Fermatsche Primzahlen

Definition. Eine Primzahl der Gestalt $p = 2^n + 1$ mit einer ganzen Zahl $n \ge 0$ heißt *Fermatsche Primzahl.*

Beispiel. Die ersten Fermatschen Primzahlen sind

$$3 = 2 + 1,\ 5 = 2^2 + 1,\ 17 = 2^4 + 1,\ 257 = 2^8 + 1,\ 65537 = 2^{16} + 1.$$

Satz. *Ist $p = 2^n + 1$ eine Primzahl, so ist n eine Zweierpotenz.*

Definition. Als *n-te Fermatsche Zahl* bezeichnet man die Zahl

$$F_n := 2^{2^n} + 1.$$

Bemerkung. Die Zahlen F_0, F_1, F_2, F_3, F_4 sind die einzigen bekannten Fermatschen Primzahlen. Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt

Satz (Gauss)**.** *Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist.*

Satz. *Es ist $\varphi(n)$ eine Zweierpotenz genau dann, wenn $n = 2^t p_1 p_2 \cdots p_r$ mit paarweise verschiedene Fermatsche Primzahlen p_i.*

Satz. *Sei $k \geq 2$. Dann ist die k-te Fermatsche Zahl $p := F_k$ genau dann eine Primzahl, wenn $3^{\frac{p-1}{2}} \equiv -1 \bmod p$.*

Satz. *Sei $k \geq 2$. Ist p ein Primteiler von F_k, so ist $p \equiv 1 \bmod 2^{k+2}$.*

Definition (Mersennesche Primzahlen)**.** Eine Primzahl der Gestalt $p = 2^n - 1$ mit einer ganzen Zahl $n \geq 0$ heißt *Mersennesche Primzahl.*

Bemerkung. Ist $2^n - 1$ eine Primzahl, so ist n Primzahl

Definition (Mersennesche Zahlen)**.** Die Zahl $M_n = 2^n - 1$ heißt n-te Mersennesche Zahl.

Bemerkung. Die einzigen Mersenneschen Primzahlen M_n mit $n \leq 258$ sind sien die M_n mit $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$.
Es sind im Augenblick 43 Mersennesche Primzahlen bekannt.

Satz (Lucal-Lehmer-Test)**.** *Sei p eine ungerade Primzahl. Dann ist die Mersennesche Zahl M_p genau dann prim, falls sie Teiler des Gliedes C_{p-1} der durch $C_1 = 4$ und $C_n = C_{n-1}^2 - 2$ $(n \geq 2)$ definierten Folge[3] ist.*

Algorithmus (Lucas-Lehmer Test).

```
lucasLehmerTest(p) =
/*
   Input
      p: an odd prime
   Output
      1 (true) if M_p=2^p-1 is a prime,
      0 otherwise.
*/
{
   local(m,s);
```

[3] siehe http://www.research.att.com/~ njas/sequences/A003010

```
    m = 2^p-1;
    s = 4;
    for( n = 2, p-1, s = (s*s - 2)%m);
    return( 0 == s);
}
```

Definition. Eine positive ganze Zahl n heißt *vollkommen*, wenn sie gleich der Summe aller ihrer von n verschiedenen positiven Teiler ist.

Beispiel. Die ersten vollkommenen Zahlen sind 6, 28, 496, 8128.

Satz (Euler)**.** *Eine gerade Zahl n ist genau dann eine vollkommene Zahl, wenn sie von der Gestalt $2^{p-1}M_p$ ist, wo M_p eine Mersennesche Primzahl ist.*

Bemerkung. Es ist nicht bekannt, ob es eine ungerade vollkommene Zahl gibt. Ebenso ist offen, ob es unendlich viele Mersennesche Primzahlen bzw. unendlich viele gerade vollkommene Zahlen gibt. Schliesslich ist auch unbekannt, on es unendlich viele zusammengesetzte Mersennesche Zahlen gibt.

Satz (Euler)**.** *Sei p eine Primzahl, $p \equiv 3 \bmod 4$. Dann ist $2p+1$ genau dann Primzahl wenn $2^p = 1 \bmod (2p+1)$.*

Vermutung. *Es gibt unendlich viele Primzahlpaare Sophie Germain Primzahlen p, d.h. Primzahlen p, sodass auch $2p+1$ eine Primzahl ist.*

Bemerkung. Als scheinbar verblüffende Eigenschaft liest man oft, dass iteriertes Bilden der Quersumme, beginnend mit einer von 6 verschiedenen vollkommenen Zahl, schliesslich auf die Zahl 1 führt. Wir lassen es als Übungsaufgabe, den Grund dafür zu finden.

29.Ma

5 Arithmetische Funktionen

Definition. Unter einer *arithmetische Funktion* versteht man eine Abbildung $\alpha : \mathbb{Z}_{\geq 1} \to \mathbb{C}$.

Beispiel.

1. Die *Eulersche φ-Funktion* $\varphi(n)$ =Anzahl der primitiven Restklassen mod n.
2. $d(n)$ =Anzahl Teiler von n.

3. $\sigma(n) =$ Summe der Teiler von n.
4. $\sigma_k(n) =$ Summe der k-ten Potenzen der Teiler von n.
5. Die Liouville-Funktion $\lambda(n) = (-1)^{(\text{Anzahl der Primteiler von } n)}$.

Definition. Unter der *summatorischen Funktion einer arithmetischen Funktion* g versteht man die arithmetische Funktion G mit

$$G(n) = \sum_{d|n} g(d).$$

Hier und im Folgenden bedeutet $\sum_{d|n}$, dass die Summe über alle positiven Teiler von n zu erstrecken ist.

Beispiel. Fr die Funktonen G und g der folgenden Tabelle gilt jeweils die Beziehung $G(n) = \sum = d|ng(d)$:

$g(n)$	1	n	n^k	$\varphi(n)$
$G(n)$	$d(n)$	$\sigma(n)$	$\sigma_k(n)$	n

Definition. Unter dem *Dirichlet-Produkt zweier arithmetischer Funktionen* f *und* g versteht man die arithmetische Funktion

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{de=n} f(d)g(e).$$

Bemerkung. Bezeichnet C die konstante Funktion $C(n) = 1\ \forall n$, so ist $C * f$ die summatorische Funktion der arithmetischen Funktion f.

Satz. *Die Menge* $\mathbb{A}$ *der arithmetischen Funktionen (d. h. die Menge aller Abbildungen* $f : \mathbb{Z}_{>0} \to \mathbb{C}$*) wird durch die gewöhnliche Addition von Funktionen und dem Dirichlet-Produkt zu einem Ring (genauer, zu einem kommutativen Ring mit Einselement).*

Bemerkung. Das Einselement des Ringes $\mathbb{A}$ ist die Funktion

$$\mathbb{E}(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{sonst} \end{cases}.$$

Satz. *Sei* $f \in \mathbb{A}$*. Dann ist* $f \in \mathbb{A}^*$*, d.h. eine Einheit des Ringes* $\mathbb{A}$*, genau dann wenn* $f(1) \neq 0$*.*

Definition. Eine arithmetische Funktion $f : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ heißt *multiplikativ*, falls

(i) $f(mn) = f(m) \cdot f(n)$ für alle m, n mit $\mathrm{ggT}(m,n) = 1$, und

(ii) $f \not\equiv 0$.

Eine arithmetische Funktion f heit *stark multiplikativ*, falls $f(mn) = f(m) \cdot f(n)$ für alle m, n gilt.

Bemerkung. Ist f multiplikativ, so gilt:

$$f(1) = 1, \quad f(n) = \prod_{p^\alpha \| n} f(p^\alpha).$$

Satz. *Die Menge $\mathbb{M}$ der multiplikativen arithmetischen Funktionen ist eine Untergruppe von $\mathbb{A}^*$. d. h.*

(i) ist f multiplikativ, dann ist $f \in \mathbb{A}^*$,

(ii) sind f, g multiplikativ, dann auch $f * g$,

(iii) ist f multiplikativ, dann auch f^{-1}.

Beispiel. Es ist $\sigma = C * \mathrm{Id}$ multiplikativ, da die konstante Funktion $C \equiv 1$ und die Identität Id multiplikativ sind.

9.Jun

Definition (Möbius'sche Funktion)**.**

$$\mu(n) = \begin{cases} 0 & \text{falls } n \text{ nicht quadratfrei ist} \\ (-1)^r & \text{falls } n = p_1 \cdot \cdots \cdot p_r, p_1 < \cdots < p_r \text{ Primzahlen} \end{cases}$$

Beispiel.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Satz. *Es gilt*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases},$$

d.h. die μ ist die bzgl. der Dirichletmultplikation inverse Funktion der konstanten Funktion $C \equiv 1$.

Satz (Möbius'sche Umkehrformel)**.** *Seien f, g arithmetische Funktionen. Dann gilt*

$$\forall n : g(n) = \sum_{d|n} f(d) \quad \textit{genau dann, wenn} \quad \forall n : f(n) = \sum_{d|n} \mu(n/d)\, g(d).$$

Beispiel. Es ist $\sum_{d|n} \varphi(d) = n$. Mittels Möbius-Inversion folgt hieraus $\varphi(d) = \sum_{d|n} \mu(n/d)\, d$.

5.1 Größenabschätzungen

Offenbar gelten die Abschätzungen

$$\varphi(n) \leq n-1, \quad \sigma(n) \geq n+1$$

(für $n > 1$). Diese lassen sich nicht verbessern, wie man leicht sieht, indem man für n eine Primzahl wählt. Schwere zu beweisen ist

Satz. *Für $n > 1$ gelten die Ungleichungen*

$$\frac{n}{2\log\log n} < \varphi(n),$$
$$\sigma(n) < 2n\log\log n.$$

Dagegen kann man leicht die folgende Abschätzung erhalten:

Satz. *Für $n > 1$ ist*

$$\frac{6}{\pi^2} < \frac{\sigma(n)\varphi(n)}{n^2} < 1.$$

12.Jun

Satz.

$$\max_{k\leq n} d(k) \sim n\frac{\log 2}{\log\log n}$$

Satz. *Es gilt:*

$$\frac{1}{n}\sum_{k=0}^{n}\sigma(k) \sim \frac{\pi^2}{12}\cdot n$$

Bemerkung. Ganz analog kann man beweisen

$$\frac{1}{n}\sum_{k=0}^{n}\sigma_r(k) \sim \frac{\zeta(r+1)}{2}\,n,$$

wo $\zeta(s)$ die im nächsten Abschnitt besprochene Riemannsche Zeta-Funktion bedeutet.

5.2 Die Riemannsche Zeta-Funktion

Definition. Die durch die Formel

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$$

für $s > 1$ erklärte Funktion wird *Riemannsche Zeta-Funktion* genannt.

Bemerkung. Die folgenden Eigenschaften für die Riemannsche Zera-Funktion sind bekannt:

(1) $\zeta(s)$ kann man zu einer in $\mathbb{C} \setminus \{1\}$ holomorphen Funktion fortsetzen. (Nach grundlegenden Sätzen der Funktionentheorie ist solch eine Fortsetzung eindeutig.)

(2) $\zeta(s)$ hat bei $s = 1$ einen Pol; dieser ist von erster Ordnung und mit Residuum gleich 1.

(3) Für $\mathrm{Re}(s) > 1$ gilt
$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$
Hierbei ist das Produkt über alle Primzahlen p zu nehmen.

(4) Für alle komplexen s gilt
$$\zeta^*(s) := \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \zeta^*(1 - s),$$
wobei $\Gamma(s)$ die Gamma-Funktion bedeutet.

(4) Es ist $\zeta(s) \neq 0$ für $\mathrm{Re}(s) > 1$ und

(5) $\zeta(s) \neq 0$ für $Re(s) = 1, 0$

(6) Für $\mathrm{Re}(s) < 1$ ist $\zeta(s) = 0$ genau dann, wenn $s = -2, -4, -6, \ldots$.

(7) Im Streifen $0 < \mathrm{Re}(s) < 1$ besitzt $\zeta(s)$ unendlich viele Nullstellen.

Vermutung (Riemannsche Vermutung)**.** *Alle Nulllstllen von $\zeta(s)$ im Streifen $0 < Re(s) < 1$ liegen auf der Geraden $Re(s) = \frac{1}{2}$.*

Satz. *Für positive ganze Zahlen k gilt*
$$\zeta(2k) = \pi^{2k} \frac{2^{2k-1}}{(2k)!} B_{2k}.$$

Hierbei bezeichnet B_k die k-te Bernoullis-Zahl.

Bemerkung. Die Bernoullizahlen sind durch die Gleichung
$$\frac{x}{e^x - 1} = \sum_{k \geq 0} \frac{B_k}{k!} x^k$$
definiert.

Satz (Apéry)**.** *Der Wert $\zeta(3)$ ist irrational.*

5.3 Reinterpretation des Dirichletprodukts

Definition (Dirichletreihen)**.** Für eine arithmetische Funktion a erklären wir die *zugeordnete Dirichletreihe* durch

$$D_a(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

Bemerkung. Wir fassen $D_a(s)$ als formale Reihe auf, d.h. wir untersuchen im Folgende nicht die Frage, für welche a und s die Reihe $D_a(s)$ konvergiert.

Satz. *Es gilt* $D_{a*b}(s) = D_a(s)\, D_b(s)$.

Satz. *Es ist a gaenau dann multiplikativ, wenn*

$$D_a(s) = \prod_p \sum_{r=0}^{\infty} \frac{a(p^r)}{p^{rs}}.$$

Satz. *Es bezeichne C die konstante Funktion $C \equiv 1$. Dann gilt:*

$$\begin{aligned} \zeta(s) &= D_C(s) \\ D_{\sigma_k}(s) &= \zeta(s-k)\zeta(s) \\ D_\mu(s) &= 1/\zeta(s) \\ D_\varphi(s) &= \zeta(s-1)/\zeta(s) \\ D_\lambda(s) &= \zeta(2s)/\zeta(s). \end{aligned}$$

16.Jun

6 Diophantische Gleichungen

6.1 Vorbemerkungen

Unter einer *diophantischen Gleichung* versteht man eine Gleichung der Gestalt

$$f(x_1, \ldots, x_n) = 0,$$

wobei f ein Polynom in n Unbestimmten mit rationalen Koeffizienten ist. Gesucht werden ganzzahlige oder rationale Lösungen $x_1, \ldots, x_n$.

Beispiel. Viele klassische Probleme führen auf diophantische Gleichungen.

(1) Es sind alle rechtwinkligen Dreiecke mit rationalen Seitenlängen zu bestimmen. Nach dem Satz von Pythagoras bedeutet dies die Bestimmung aller positiven rationalen Lösungen der diophantischen Gleichung

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

Die Lösungen dieser Gleichung heissen *Pythagoräisches Zahlentripel*.

(2) Es sind alle natürlichen Zahl $n \in \mathbb{Z}_{>0}$ zu bestimmen, die Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen sind. Solche natürlichen Zahlen heißen *Kongruenzzahlen*. Nach bekannten Sätzen der Elementargeometrie ist also n genau dann eine Kongruenzzahl, wenn die diophantischen Gleichungen

$$n = \frac{1}{2}ab, \quad a^2 + b^2 = c^2$$

eine gemeinsame Lösung besitzen.

6.2 Das zehnte Hilbertsches Problem

In einem gewissen Sinne ist jedes mathematische Problem äquivalent zur Untersuchung einer diophantischen Gleichung. Diese Aussage ist die eher philosophischer Interpretation des nachstehenden Satzes von Matiyasevich Dieser Satz beantwortetet letztendlich das zehnte der 23 von Hilbert auf dem zweiten internationalen Mathematikerkongress 1900 in Paris vorgetragenen Probleme[4]:

10. Hilbertsches Problem (Entscheidung der Lösbarkeit einer Diophantischen Gleichung)**.** *Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Der Begriff des *Verfahrens* oder besser Algorithmus ist mittlerweile nach Vorarbeiten in der mathematischen Grundlagenforschung in der ersten Hälfte des 19ten Jahrhunderts, die sich mit Namen wie Gödel, Turing, Church und vielen anderen verbindet, hinreichend gut geklärt[5].

[4] vgl. http://www.mathematik.uni-bielefeld.de/ kersten/hilbert/rede.html

[5] Diese mathematisch-philosophischen Untersuchungen sind in einem gewissen Sinne der Ausgangspunkt der gesellschaftlichen Veränderungen, die durch die zunehmende Digitalisierung von Informationen und Abläufen verursacht werden. Natürlich ist im Gegenzug die Grundlagenforschung auch nicht unabhängig von gesellschaftlichen Veränderungen.

Insbesondere hat man den mathematisch präzisen Begriff der *rekursiven Menge*. Dies sind Teilmengen B der natürlichen Zahlen $\mathbb{Z}_{\geq 0}$, zu denen ein Algorithmus esistiert, der entscheidet, ob eine gegebene natürliche Zahl zu B gehört oder nicht. Verwandt ist der Begriff der *rekursiv aufzählbaren Mengen*. Dies sind Teilmengen A der natürlichen Zahlen, zu denen ein Algorithmus existiert, der die Elemente von A aufzählt. Es ist eine Teilmenge B der natürlichen Zahlen genau dann rekursiv, wenn sie und ihr Komplement rekursiv aufzählbar sind.
Hat man einen Computer, so kann man in geeigneter Maschinensprache Programme schreiben, die Mengen von natürlichen Zahlen berechnet oder zumindest aufzählen. Es it genau festgelegt, was ein gültiges Programm ist und damit auch, welche Mengen auf einem gegebenen Computer berechenbar oder aufzählbar sind. Bis jetzt konnte noch in jedem Fall bewiesen werde, dass die auf dem gegebenen Computer berechenbaren oder aufählbaren Mengen rekursiv bzw. rekursiv aufzählbar sind.

Definition (Diophantische Menge)**.** Eine Teilmenge $T \subset \mathbb{Z}_{\geq 0}^n$ heißt *diophantisch*, falls es ein Polynom $P(x_1, \ldots, x_n, y) \in \mathbb{Z}[x_1, \ldots, x_n, y]$ gibt, sodaß

$$T = \left\{ y \in \mathbb{Z}_{\geq 0} : \exists x_1, \ldots, x_n \in \mathbb{Z}_{\geq 0}^n : P(x_1, \ldots, x_k, y) = 0 \right\}.$$

Man überlegt sich leicht, dass jede diophantische Menge mit einem Computer aufzählbar ist.

Satz (Yuri Matiyasevich, 1970)**.** *Jede rekursiv aufzählbare Menge ist diophantisch.*

Korollar (Lösung des zehnten Hilbertschen Problems)**.** *Es gibt keinen Algorothmus, der entscheidet, ob eine vorgelegte diophantsiche Gleichung lösbar ist oder nicht.*

6.3 Diophantische Gleichungen in einer Variablen

Gegeben sei ein Polynom mit rationalen Koeffizienten

$$P(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Gesucht werden alle ganzen Zahlen $\frac{r}{s}$, $s \neq 0$, sodass $P(r/s) = 0$. Offenbar kann man sich auf den Fall beschränken, dass die Koeffizienten a_j alle ganzzahlig sind (anderfalls multipliziere man das Polynom P mit dem Hauptnenner seiner Koeffizienten). Ferner kann man natürlich annehmen, dass r und s teilerfremd sind. Sckilesslich kann man sich offenbar auch noch auf den Fall beschränken, dass a_n und a_0 von Null verschieden sind.

Satz. *Die Koefizienten des Polynoms $P(x)$ seien ganzzahlig, und es gelte $a_n a_0 \neq 0$. Dann gilt*

$$\left\{\frac{r}{s} \in \mathbb{Q} : r, s \in \mathbb{Z},\ \mathrm{ggT}(r,s) = 1,\ P\left(\frac{r}{s}\right) = 0\right\} \subseteq \left\{\frac{r}{s} \in \mathbb{Q} : r \mid a_0, s \mid a_n\right\}.$$

Korollar. *Ist $P(x)$ normiert (d. h. $a_n = 1$), dann ist jede rationale Nullstelle von $P(x)$ ganzzahlig.*

Korollar. *Sei n eine positive ganze Zahl. Dann ist $\sqrt{n}$ ganua dann irrational, falls n kein perfektes Quadrat ist.*

Korollar. *$\sqrt{2}$ ist irrational.*

16.Jun

6.4 Lineare diophantische Gleichungen

Satz. *Seien $a_1, \ldots, a_n$ und b ganze Zahlen. Dann hat die diophantische Gleichung*

$$a_1 x_1 + \cdots + a_n x_n = b$$

genau dann eine Lösung, wenn der $\mathrm{ggT}(a_1, \ldots, a_n)$ die Zahl b teilt.

Beispiel.

Algorithmus (Berechnung einer partikulären Lösung).

Satz. *Seien x_0, y_0 ganzzahlige Lösungen der Gleichung $ax + by = c$. Dann ist*

$$\{(x,y) \in \mathbb{Z}^2 : ax + by = c\} = \{\left(x_0 - \frac{b}{g}t, y_0 + \frac{a}{g}t\right) : t \in \mathbb{Z})\},$$

wobei $g = \mathrm{ggT}(a,b)$.

Lemma. *Sei $a \in \mathbb{Z}^n$ ein ganzahliger primitiver Vektor (d.h. die Komponenten von a seien teilerfremd). Dann existiert eine Matrix $U \in \mathrm{GL}(n, \mathbb{Z})$, deren erste Zeile gleich a ist.*

Satz. *Seien $a_1, \ldots, a_n$ und b ganze Zahlen, sodass der g.g.T. g der a_j die Zahl b teilt. Sei U ene Matrix mit $(a_1/g, \ldots, a_n/g)$ als erster Zeile. Dann gilt*

$$\{x \in \mathbb{Z}^n : a_1 x_1 + \cdots + a_n x_n = b\} = U^{-1} \begin{pmatrix} b/g \\ \mathbb{Z} \\ \vdots \\ \mathbb{Z} \end{pmatrix}.$$

Algorithmus (Berechnung der Matrix U).

Pending Exercise

Beispiel.

6.5 Quadratische diophantische Gleichungen

Gesucht sind alle rationalen Lösungen der Gleichung

$$x^2 + y^2 = 1.$$

Die Idee zue Auffindung aller Lösungen geht auf Diophant zurück: Die Geraden des Geradenbüschels durch die patikuläre Lösung $(1, 0)$ parametrisieren alle (nicht notwendig rationalen) Punkte des Kreises $x^2 + y^2 = 1$, da ja jede von Ihnen genau zwei Punkte des Kreises enthält und durch diese auch eindeutig bestimmt ist. Diese Geraden eines Geradenbüschels durch einen Punkt werden wiederum durch ihre Steigungen parametrisiert. Eine genauere Analyse zeigt, dass eine Steigung genau dann rational ist, wenn der von $(0, 1)$ verschiedene Schnittpunkt des Kreises mit der durch die gegebene Steigung festgelegten Geraden rational ist. Dies führt zu dem nachfolgenden Satz.

Satz. *Es gilt*

$$\{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1, (x, y) \neq (1, 0)\} = \{\left(\frac{\lambda^2 - 1}{\lambda^2 + 1}, \frac{-2\lambda}{\lambda^2 + 1}\right) : \lambda \in \mathbb{Q}\}$$

23.Jun

Satz (Pythagoräische Zahlentripel)**.** *Die Gleichung $x^2 + y^2 = z^2$ besitzt als allgemeine Lösung mit $\mathrm{ggT}(x, y, z) = 1$, $x, y, z > 0$, $2|y$, gerade die Zahlentripel $x = p^2 - q^2$, $y = 2pq$, $z = p^2 + q^2$, wobei $p, q \in \mathbb{Z}$, $p > q > 0$, $\mathrm{ggT}(p, q) = 1$, und $p + q$ ungerade ist.*

Bemerkung. Die oben geschilderte Methode zur Parametrisierung aller rationalen Lösungen von $x^2 + y^2 = 1$ kann man allgemein auf *Kegelschnitte über* $\mathbb{Q}$, d.h. diophantische Gleichungen der Gestalt

$$Q(x, y) = aX^2 + bXY + cY^2 + dX + eY + f = 0 \quad (a, b, c, d, e, f \in \mathbb{Q}),$$

anwenden (wenn man etwa $b^2 - 4ab \neq 0$ voraussetzt.). Allerdings benötigt man als Startwert noch eine Lösung $(x_1, y_1) \in \mathbb{Q}^2$.
Zur Untersuchung, ob eine solche Lösung existiert oder nicht, ist es vorteilhaft, das Problem zunächst zu *normalisieren*: Es gibt eine affine Transformation

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \quad (A \in GL(2, \mathbb{Q})),$$

sodaß $Q(xA + b) = a'x^2 + b'y^2 + c'$ mit geeigneten $a', b', c' \in \mathbb{Q}$. Die Frage ist dann, ob die zugeordnete *homogene* Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

eine nicht-triviale[6] ganzzahlige Lösung $(x, y, z) \neq 0$ besitzt. Man überlegt sich leicht, dass man sich auf den Fall beschränken kann, dass a', b', c' paarweise teilerfremd und quadratfrei sind.

Satz (Legendre)**.** *Seien a, b, c paarweise teilerfremde und quadratfreie ganze Zahlen. Dann besitzt die Gleichung $ax^2 + by^2 + cz^2 = 0$ genau dann eine nicht-triviale Lösung in $\mathbb{Z}$, wenn sie eine nicht-triviale reelle Lösung besitzt und die Kongruenzen*

$$t_1^2 \equiv -bc \bmod a$$
$$t_2^2 \equiv -ac \bmod b$$
$$t_3^2 \equiv -ab \bmod c$$

lösbar sind.

Bemerkung. Die Gleichung $ax^2 + by^2 + cz^2 = 0$ besitzt offenbar genau dann eine nicht-triviale reelle Lösung, falls die Koeefizienten a, b, c nicht alle das gleiche Vorzeichen haben.

Algorithmus (Berechnung einer nicht-trivialen rationalen Lösung von $ax^2 + by^2 + cz^2 = 0$).

Pending Exercise

26.Jun

6.6 Diophantische Gleichungen höheren Grades in 2 Variablen

Die diophantischen Gleichungen $F(x, y) = 0$ mit Polynomen F vom Grad 3 bzw. mit Polynomen vom Grad gröesser oder gleich 4 verhalten sich sehr verschieden und auch unterschiedlich zum Fall eines Polynoms vom Grad 1 oder 2. Im Jahr 1983 wurde nämlich von Faltings die Mordellsche Vermutung bewiesen:

Satz (Mordell, Faltings)**.** *Sei C eine über $\mathbb{Q}$ definierte nicht-singuläre Kurve vom Geschlecht $g \geq 2$. Dann ist die Menge der rationalen Punkte von C endlich.*

[6] Eine Lösung heisst *nicht-trivial*, falls sie von $(0, 0, 0)$ verschieden ist.

Auf ebene Kurven $F(x,y) = 0$ angewandt, besagt der Satz von Faltings, dass es nur endlich viele Lösungen $(x,y) \in \mathbb{Q}^2$ gibt, wenn F ein Polynom mit rationalen Koefizienten vom Grad grösser oder gleich 4 ist und es keine komplexen Lösungen (x_0, y_0) der Gleichung $F(x,y) = 0$ mit $\partial F/\partial x(x_0,y_0) = \partial F/\partial y(x_0,y_0) = 0$ gibt.
Insbesondere impliziert der Satz von Faltings, dass die Fermatsche Kurve $x^n + y^n = 1$ für $n \geq 4$ nur endlich viele Lösungen besitzt. In det Tat ist aber die schärfere *Fermatsche Vermutung*, nämlich dass diese Gleichung für $n \geq 3$ keine Lösungen mit $xy \neq 0$ besitzt, 1996 von Andrew Wiles bewiesen worden.
Die Theorie der diophantischen Gleichungen vom Geschlecht $g \geq 2$ dreht sich naheliegenderweise im Wesentlichen darum, gute Abschätzungen für die Grösse und die Anzahl der rationalen Lösungen zu erhalten.

6.7 Elliptische Kurven

Definition. Eine diophantische Gleichung der Gestalt

$$y^2 = x^3 + Ax + B$$

mit ganzen Zahlen A, B und sodass das Polynom $x^3 + Ax + B$ keine mehrfachen Nullstellen enthält, heisst *elliptische Kurve über* $\mathbb{Q}$.

Bemerkung. Man kann zeigen, dass jede Kurve vom Geschlecht 1 (mit mindestens einer *projektiven* rationalen Lösung), insbesondere jede ebene nichtsinguläre Kurve $F(x,y) = 0$ vom Grad 3, durch *algebraische Transformationen* in eine Gleichung wie in der Definition überführt werden kann.

Beispiel. Wir erinnern, dass eine positive ganze Zahl n Kongruenzzahl heisst, falls die diphantischen Gleichungen

$$a^2 + b^2 = c^2, \quad n = \frac{1}{2}ab$$

eine simultane rationale Lösung $a, b, c > 0$ besitzt.
Durch die beiden Gleichungen wird eine Kurve vom Geschlecht 1 beschrieben. Wir können sie demnach in eine elliptische Kurve transformieren transformieren
Nach den Ergebnissen des ersten Abschnitts wissen wir, dass jede rationale Lösung der ersten Gleichung mit $a, b, c \neq 0$ von der Gestalt

$$a = (\lambda^2 - 1)t, \quad b = 2\lambda t$$

mit rationalen Zahlen $\lambda, t \neq 0$ ist. Danach ist n also Kongruenzzahl genau dann, wenn die Gleichung

$$n = t^2\lambda(\lambda^2 - 1)$$

in rationalen Zahlen $\lambda, t \neq 0$ lösbar ist.
Setzen wir

$$x = -\frac{n}{\lambda}, \quad y = \frac{n^2}{t\lambda^2},$$

so wird die Lösbarkeit der letzten Gleichung äquivalent zur Lösbarkeit der Gleichung

$$y^2 = x^3 - n^2x$$

mit rationalen Zahlen $x, y \neq 0$.