16.00 Smolka: Primzahlen
17.30 Abendessen in der Jugendherberge
18.15 Diskussion über das Mathematikseminar

15.5.85 7.45 Frühstück
8.30 Smolka: Kongruenzen
10.00 Ulitzka: Erzeugung von Zufallszahlen
11.45 Gemeinsames Mittagessen im Gästekasino Mozartstraße
13.15 Stadtrundfahrt in Nürnberg mit Frau Rohloff.
16.30 Rückfahrt
18.00 Gemeinsames Abendessen bei Greding
21.00 Ankunft am Gymnasium Starnberg.

Die folgenden Manuskripte werden wiedergegeben in der Reihenfolge ihres Eingangs:

Smolka:

Z a h l e n t h e o r i e

Der folgende Artikel nimmt immer wieder Bezug auf Mathematikinformation Nr. 11 vom 31.3.1985, wo man findet

1. Einführung in die Teilbarkeitslehre.

2. Primzahlen

Definition: N sei die Menge der natürlichen Zahlen. p aus N heißt Primzahl, wenn p außer sich selbst und 1 keine weiteren natürlichen Teiler hat. Ist ein Teiler Primzahl, so heißt er Primteiler. 1 ist keine Primzahl.

2 ist die einzige gerade Primzahl; denn jede andere gerade Zahl ist per definitionem durch 2 teilbar.

2.1 Satz: Die nichtleere Menge T(a) der Teiler von a aus N enthält ein kleinstes Element, das eine Primzahl ist.

Beweis:
Jeder Teiler t von a ist eine natürliche Zahl kleiner oder gleich a; d.h. T(a) enthält höchstens a Elemente, ist also eine endliche Menge und enthält deshalb ein kleinstes Element p. Nimmt man an, p sei nicht prim, dann gibt es einen Primteiler q von p mit $1 < q < p$. Wegen der Transitivität der Teilbarkeit ist dann q auch Teiler von a. D.i. ein Widerspruch dazu, daß p der kleinste Teiler von a sei. Also ist der kleinste Teiler prim.

2.2 Fundamentalsatz der elementaren Zahlentheorie:

Jede natürliche Zahl $a > 1$ ist als Produkt von s Primzahlen darstellbar und die Darstellung ist bis auf Reihenfolge der Faktoren eindeutig.

(Dieser Satz wird auch Satz von der eindeutigen Primfaktorzerlegung genannt; er gilt nicht in allen Zahlkörpern! Man beachte: Wir arbeiten hier in N.).

Beweis:
1. Existenz einer Darstellung:
Sei $p_1$ der kleinste Primteiler von a. Ist $a = p_1$, dann ist a prim und s=1. Andernfalls besitzt a die Zerlegung $a = p_1 a'$ mit $a' < a$. Auch a' hat einen kleinsten Primteiler $p_2$ mit $a' = p_2 a''$, also $a = p_1 p_2 a''$. Setzt man dieses Verfahren fort, so gelangt man, da es höchstens a Teiler von a gibt, zu einem letzten Faktor, der selbst prim ist.
Somit ist $a = p_1 p_2 p_3 \cdot \ldots \cdot p_s$, wobei nicht alle $p_i$ verschieden sein müssen.

2. Eindeutigkeit des Satzes (Beweis nach ZERMELO [ 1 ]) durch vollständige Induktion nach a:

a) a = 2 hat als Primzahl genau eine Darstellung im Sinne des Satzes.

b) Induktionsannahme:
Die Eindeutigkeit sei bereits für Zahlen kleiner als a gezeigt und q sei der kleinste Primteiler von a.

c) Vor dem Induktionsschluß zeigen wir:

2.3 Hilfssatz: Ist q ein Primteiler von $a = m \cdot n$ und $m > 1$, so folgt q ist Teiler von m oder n.

Beweis zu 2.3:
Ohne Beschränkung der Allgemeinheit kann man annehmen, q teilt m nicht. Da q der kleinste Primteiler von a war, muß m dann einen Primteiler größer als q haben, so daß $m > q$ ist. Es gilt dann:

$0 < (m - q) \cdot n = a - q \cdot n =: a' < a.$

Nach der Induktionsannahme ist dann a' eindeutig in Primfaktoren zerlegbar und wegen q teilt $a = m \cdot n$ gilt dann auch

$q \mid a' = a - q \cdot n$ (Regel 1.V). Aus $q \nmid m$ folgt $q \nmid (m - q)$ (nach 1.VI),

so daß q als Primteiler von a' in deren eindeutiger Zerlegung als Primfaktor enthalten sein muß, also den zweiten Faktor von a', also n teilen muß. Damit ist der Hilfssatz bewiesen.

Nun zum Induktionsschluß von 2.2:
Da jede Zahl $a > 1$ in der Form $a = cq$ geschrieben werden kann und $c < a$ nach Annahme eindeutig zerlegbar ist, ist auch a nach dem Hilfssatz eindeutig in Primfaktoren zerlegbar.

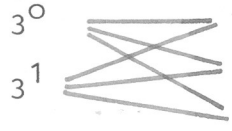
Faßt man in der Primfaktorzerlegung von a alle gleichen Faktoren zu Potenzen zusammen, so ist

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} = \prod_{i=1}^{r} p_i^{e_i} \quad \text{mit } e_i \text{ aus } N \text{ und } e_1 + \ldots + e_r = s.$$

Unmittelbar folgt:

2.4 Korollar: In $a = \prod_{i=1}^{r} p_i^{e_i}$ sind $m = \prod_{i=1}^{u} p_i^{e_i}$ ; $0 \leq a_i \leq e_i$; $u \leq r$ und nur diese Teiler von a.

z.B. $a = 12 = 3^1 \cdot 2^2$ ergibt $2 \cdot 3 = 6$ Möglichkeiten der Primfaktorkombination, wie man dem folgenden Graphen entnehmen kann:




Es gibt 6 Kombinationen.

mal

Im Beispiel ist $e_1 = 1$, $e_2 = 2$; wie man sieht, gibt es $(e_1+1)(e_2+1)=6$ verschiedene Teiler; dieser Sachverhalt gilt allgemein:

2.5 Korollar:

Mit den Bezeichnungen von oben gilt für die Kardinalität (Mächtigkeit) $\tau(a)$ der Menge T(a):
$\tau(a) = (e_1+1)(e_2+1) \cdot \ldots \cdot (e_r+1) = \prod_{i=1}^{r} (e_i+1)$. T(a) enthält also $\tau(a)$ verschiedene Teiler.

2.6 Satz: Es gibt keine größte Primzahl (d.h. es gibt mehr als endlich viele Primzahlen).

Beweis:
Seien $p_1,\ldots,p_r$ r verschiedene Primzahlen, so ist $n = p_1\cdot\ldots\cdot p_r+1$ eine weitere Primzahl und der Satz bewiesen, oder n hat, wie jede Nichtprimzahl größer 2, mindestens einen Primteiler $p < n$. Dieses p ist aber keine der betrachteten r Primzahlen; anderenfalls würde nämlich p das Produkt $p_1\cdot\ldots\cdot p_r$ aber nicht 1 teilen, wäre also kein Teiler von n (siehe 1.VI). Somit ist p neben der r Primzahlen eine weitere. Die unendliche Fortsetzbarkeit dieses Schrittes liefert die Behauptung des Satzes.

2.7 Definition: $(a_1,a_2,\ldots,a_n)$ ist der größte gemeinsame Teiler der natürlichen Zahlen $a_1,a_2,\ldots,a_n$, d.h. $(a_1,\ldots,a_n)$ ist das größte Element der Menge $T(a_1)\cap\ldots\cap T(a_n)$.

z.B. $(6,8,12) = 2$; $(6,25) = 1$.

2.8 Definition: Die natürlichen Zahlen $a_1,\ldots,a_n$ heißen teilerfremd oder relativ prim genau dann, wenn $(a_1,\ldots,a_n) = 1$.

Z.B. sind 6 und 25 relativ prim.

2.9 Rechenregeln:
2.9.1 $(ta_1,\ldots,ta_n) = t\cdot(a_1,\ldots,a_n)$
2.9.2 $(a_1,\ldots,a_{n-1},a_n) \mid (a_1,\ldots,a_{n-1})$
2.9.3 $(1,a_1,\ldots,a_n) = 1$.

2.10 Bestimmung des größten gemeinsamen Teilers:

2.10.1 durch Probieren.

2.10.2 durch Zerlegen der beteiligten Zahlen in Primfaktoren und berechnen des Produktes aus den höchsten gemeinsamen Potenzen der Primfaktoren; vergl. Lehrbücher der Jahrgangsstufe 5.

2.10.3 mit dem EUKLIDischen Divisionsalgorithmus:

Es sei zu bestimmen $g := (a,b)$; ohne Beschränkung der Allgemeinheit sei $b < a$; dann gilt mit dem EUKLIDischen Divisionsalgorithmus:

$a = q_1\cdot b + r_1$ mit passenden natürlichen Zahlen $q_1$ und $r_1$ (Rest): und $0 \leq r_1 < b$;

$b = q_2\cdot r_1 + r_2$ mit $0 \leq r_2 < r_1$;

$r_1 = q_3\cdot r_2 + r_3$ mit $0 \leq r_3 < r_2$;

usw.

$r_{n-1} = q_{n+1}\cdot r_n + r_{n+1}$ mit $0 \leq r_{n+1} < r_n$;

da die Reste immer kleiner werden, aber natürliche Zahlen sind, muß irgendwann ein Rest $r_{n+2} = 0$ übrig bleiben; u.U. ist hierbei dann $r_{n+1} = 1$:

$r_n = q_{n+2}\cdot r_{n+1} + 0$.

Nach den Teilbarkeitsregeln (siehe 1.) folgt dann:

$(a,b) = (b,r_1) = (r_1,r_2) = \ldots = (r_n,r_{n+1}) = r_{n+1}$.

z.B.
$667 = 2\cdot 299 + 69$
$229 = 4\cdot 69 + 23$
$69 = 3\cdot 23$ also $(299,667) = 23$.

Sind a,b relativ prim, so endet das Verfahren bei $(a,b) = 1$.

## 3. Restklassen

**3.1 Definition:** a,b seien aus Z, der Menge der ganzen Zahlen (die mit + und · die algebraische Struktur eines kommutativen Rings mit 1 haben), und m sei eine natürliche Zahl; dann bedeutet

$a \equiv b \bmod m$ (gelesen a kongruent b modulo m, m wird dann auch der Modul genannt),

daß a und b bei Division mit m denselben Rest haben; d.h.

$a = q_1 \cdot m + r$ mit $q_1$ und r aus Z
$b = q_2 \cdot m + r$ mit $q_2$ und demselben r aus Z.

**3.2 Satz:** $a \equiv b \bmod m$ bedeutet $a - b \equiv 0 \bmod m$, d.h. $m \mid (a - b)$.

Beweis:
Nach 3.1 ist $a = q_1 m + r$, $b = q_2 m + r$, also $a - b = (q_1 - q_2)m$ und damit $m \mid (a - b)$.

Z.B. $a \equiv 0 \bmod m$ ist gleichwertig mit $m \mid a$.

Man beachte: Der "Grenzfall" $a \equiv b \bmod 0$ darf nicht eintreten, weil in Z die Division durch 0 nicht erlaubt ist.

**3.3 Satz:** Die Kongruenz $\equiv$ ist eine Äquivalenzrelation.

Beweis:
a) Reflexivität: $a \equiv a \bmod m$; Beweis trivial.
b) Symmetrie: Aus $a \equiv b \bmod m$ folgt $b \equiv a \bmod m$, weil aus $a - b = (q_1 - q_2)m$ in Z folgt $b - a = (q_2 - q_1)m$.
c) Transitivität: Aus $a \equiv b \bmod m$ und $b \equiv c \bmod m$ folgt $a \equiv c \bmod m$; weil aus $a - b = (q_1 - q_2)m$
$b - c = (q_2 - q_3)m$ durch Addition dieser beiden Gleichungen folgt
$a - c = (q_1 - q_3)m$.

In der Algebra weiß man ganz allgemein, daß jede Äquivalenzrelation auf einer Menge zu einer besonderen Einteilung dieser Menge in Äquivalenzklassen führt, die man hier Restklassen nennt:

**3.4 Satz:** Die Kongruenz $\equiv$ modulo m zerlegt Z in elementfremde Restklassen (so etwas nennt man eine "Partition von Z") $R_m(i)$ für alle i aus Z.
Es gilt also:
a) $Z = R_m(0) \cup R_m(1) \cup \ldots \cup R_m(m-1)$, d.h. jedes Element aus Z gehört zu einer solchen Restklasse.
b) $R_m(i) \cap R_m(j) = \emptyset$ für alle $i \neq j$, d.h. jedes Element aus Z gehört zu genau einer Restklasse.

Beweis:
a) Der EUKLIDische Divisionsalgorithmus zeigt, daß der Divisionsrest höchstens m-1 sein kann; also gibt es die genannten i Restklassen. Da jedes Element aus N durch m mit einem solchen Rest dividiert werden kann, bleibt zu zeigen, wie sich dies mit den negativen Zahlen -n mit n aus N verhält: Ohne Beschränkung der Allgemeinheit sei $n = q_1 m + i$ mit $0 \leq i < m$. Dann ist $-n = -q_1 m - i$
$= -(q_1 - 1)m + (m - i)$, wobei $0 \leq m - i \leq m - 1$. D.h. aus $n \equiv i \bmod m$ folgt $-n \equiv (m - i) \bmod m$; dies ist später eine allgemeinere Rechenregel.

b) Angenommen es gäbe $a \in R_m(i) \cap R_m(j)$, dann gäbe es $q_1, q_2$ in Z und $i \neq j$ aus N mit $i \leq m-1$ und $j \leq m-1$ und es würde gelten:

$a = q_1 m + i = q_2 m + j$; das wäre zur Eindeutigkeit der Division ein Widerspruch.

Die in 3.1 beschriebene Struktur von Z zieht sich nun in die Menge $R_m(Z)$ der Restklassen $R_m(i)$ $i \leq m-1$ durch:

3.5 Satz: $R_m(Z) := \{R_m(0), R_m(1), \ldots, R_m(m-1)\}$ wird durch die folgenden Definitionen zu einem kommutativen Ring mit 1.

$R_m(i) + R_m(j) := R_m(t)$ mit $i + j \equiv t \bmod m$.

$R_m(i) \cdot R_m(j) := R_m(s)$ mit $i \cdot j \equiv s \bmod m$.

Man kann also in $R_m(Z)$ rechnen, wie wir dies in Z gewohnt sind.

Beweis:
1. Zunächst ist einmal zu zeigen, daß die im Satz definierten Restklassen $R_m(t)$ und $R_m(s)$ wohldefiniert sind, d.h. t und s unabhängig von den gewählten Repräsentanten i und j immer dieselben Zahlen sind:

Deshalb wählen wir $a \in R_m(i)$ und $b \in R_m(j)$ beliebig, d.h.

$a = q_1 m + i$ mit irgendeinem $q_1 \in Z$ und
$b = q_2 m + j$ mit irgendeinem $q_2 \in Z$.

Dann gilt: $a + b = (q_1 + q_2)m + (i + j)$ und $i + j \equiv t \bmod m$ mit einem eindeutig bestimmten t: $0 \leq t \leq m-1$ nach dem Vorherigen.
Also ist
$a + b = (q_1 + q_2 + q_3)m + t$ usw.
Außerdem gilt: $a \cdot b = (q_1 m + i)(q_2 m + j) = q_1 q_2 m^2 + i q_2 m + j q_1 m + ij =$

$= (q_1 q_2 m + i q_2 + j q_1 + q_3)m + s$, wenn $ij = q_3 m + s$.
s ist aber wieder durch Division eindeutig festgelegt.

D.h. für beliebige Repräsentanten a und b ergeben sich stets dieselben Zahlen s und t, d.h. Summe und Produkt sind wohldefiniert.

2. Man kann jetzt nachrechnen, daß für + das Kommutativgesetz, Assoziativgesetz gilt, $R_m(0)$ das neutrale Element ist und stets die Gleichung $R_m(i) + R_m(x) = R_m(j)$ eindeutig lösbar ist; für die Lösung schreibt man

3.6 Definition: Die Lösung von $R_m(i) + R_m(x) = R_m(j)$ ist

$$R_m(x) =: R_m(j) - R_m(i).$$

Fortsetzung des Beweises zu 3.5:
Genauso kann man nun für · zeigen die Gültigkeit des Kommutativgesetzes, des Assoziativgesetzes; $R_m(1)$ ist die Eins in $R_m(Z)$, d.h. es gilt

$$R_m(i) \cdot R_m(1) = R_m(i) \text{ für alle } i.$$

Schließlich gilt auch noch das Distributivgesetz. Also ist $R_m(Z)$ ein Ring der beschriebenen Art.

Bemerkung: Anschließende Beispiele werden zeigen, daß die Multiplikation in $R_m(Z)$ i.a. keine Umkehrung":"hat.

3.7 Vereinbarung: Bei Rechnungen, bei denen der Modul m nicht gewechselt wird, ist es oft zweckmäßig für $R_m(i) = \overline{i}$ zu schreiben.
Es gilt dann nach 3.5:

$$\overline{i} + \overline{j} := \overline{i + j}$$

$$\overline{i} \cdot \overline{j} := \overline{i \cdot j}$$

mit den Rechenregeln eines kommutativen Rings mit 1.

z.B. modulo 3 gilt: $\overline{3}.\overline{4} = \overline{12} = \overline{0}$, $\overline{2} \cdot \overline{7} = \overline{14} = \overline{2}$, $\overline{3} + \overline{4} = \overline{0} + \overline{1} = \overline{1}$.

Mit Restklassen auf Z kann man neue Strukturen gewinnen, die wir im folgenden durch ihre Additions- und Multiplikationstafeln darstellen:

Vereinbarung: Wir kennzeichnen die Restklassen mit jeweils ihren kleinsten Repräsentanten aus Z:

$R_5(Z) =: Z_5$

| + | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |

| · | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{4}$ | $\overline{1}$ | $\overline{3}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{1}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

In der Additions- wie in der Multiplikationstafel kommt in jeder Zeile jedes Element genau einmal vor; deshalb sind Addition und Multiplikation in $Z_5$ umkehrbar.

Wie das nächste Beispiel zeigt, muß das in $R_m(Z)$ nicht immer so sein:

$R_6(Z) =: Z_6$

| + | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{5}$ | $\overline{5}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |

| · | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
|---|---|---|---|---|---|
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{4}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{0}$ | $\overline{3}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{2}$ | $\overline{0}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{5}$ | $\overline{5}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Auch hier zeigt die Additionstafel in jeder Zeile verschiedene Elemente; deshalb ist, wie in 3.5 bewiesen, die Addition umkehrbar. Mit der Multiplikation ist dies nicht mehr:
Die Gleichung $\overline{2}\cdot x = \overline{1}$ ist z.B. unlösbar. Andererseits gilt $\overline{2}\cdot\overline{3} = \overline{0}$; deshalb definiert man:

3.8 Definition: Gilt in einer algebraischen Struktur $a\cdot b = 0$, ohne daß a oder b Null sind, so sagt man, die Struktur habe die Nullteiler a und b.

$Z_6$ hat die Nullteiler $\overline{2}$, $\overline{3}$, $\overline{4}$.

3.9 Satz: Die Gleichung $\overline{a}\cdot\overline{x} = \overline{c}$ ist in $Z_m$ genau dann lösbar, wenn $(a,m) \mid c$. In diesem Fall besitzt die Gleichung $(a,m)$ zueinander modulo m inkongruente Lösungen. Für den Spezialfall $(a,m) = 1$ gehört zu jedem c aus Z genau eine (modulo m) eindeutige Lösung.

Beweis:
$\overline{a}\cdot\overline{x} - \overline{c} = \overline{0}$ ist in $Z_m$ genau dann lösbar, wenn $m \mid ax - c$. Dies ist wiederum genau dann der Fall, wenn $ax - mz = c$ mit einem z aus Z lösbar ist. Nun gibt es a' und m' mit $(a',m') = 1$ und $a = a'\cdot(a,m)$ und $b = b'\cdot(a,m)$. Die Gleichung $ax - mz = c$ erhält dann die Gestalt $(a'x - m'z)d = c$. $a'x - m'z = c:d$ ist daher mit ganzzahligen x,z dann und nur dann lösbar, wenn $d \mid c$.

weil $(a',a') = 1 \Rightarrow a'x' - m'y' = 1$

$\Rightarrow a'x'\frac{c}{d} - m'y'\frac{c}{d} = \frac{c}{d}$

Für den Fall $d \mid c$, also $c = c'd$ mit einem $c'$ aus Z ist $ax - mz = c$ gleichbedeutend mit $a'dx - m'dz = c'd$ oder $a'x - m'z = c'$. Daher stimmen die Lösungen von $ax \equiv c \bmod m$ mit den Lösungen von $a'x = c' \bmod m'$ überein.
Sei $x_1$ eine Lösung und $x_i$ eine weitere, so gilt $a'(x_1 - x_i) \equiv 0 \bmod m'$, d.h. $m' \equiv a'(x_1 - x_i)$. Da $(a',m') = 1$ ist, folgt $m' \mid (x_1 - x_i)$. Alle weiteren Lösungen haben deshalb die Gestalt $x_i = x_1 + m'y$, von denen $x_i = x_1 + (i - 1)m'$ mit $1 \leq i \leq d$ inkongruent modulo m sind.
Für den Fall $d = (a,m) = 1$ existiert folglich nur eine einzige modulo m eindeutige Lösung.

3.10 Korollar: Ist p prim, so ist $Z_p$ ein Körper.

Schlußbemerkung: Im Mathematikseminar in Erlangen wurden die hier nochmals vorgestellten Sätze stets anhand von Beispielen eingeführt. Insbesondere wurde hierbei das in Mathematikinformation Nr. 11 abgedruckte Aufgabenblatt stark eingesetzt.

Literatur:

[1] Scholz, Schoeneberg: Einführung in die Zahlentheorie, Sammlung Göschen, 5.Auflage 1973, de Gruyter.