Proseminar Lineare Algebra
Sommersemester 08
Dozent: GD Prof. O. Bogopolski

Tobias Kraushaar
Kaiserstr. 178
44143 Dortmund

Matr.- Nr.: 122964

Euklidischer Algorithmus, Restklassenring $\mathbb{Z}_m$ und seine Struktur, Chinesischer Restklassensatz

Inhaltsverzeichnis

1. EINLEITUNG

Diese Ausarbeitung soll zunächst ein Verfahren vorstellen, dass den größten gemeinsamen Teiler (ggT) von zwei ganzen Zahlen berechnet. Dieses Verfahren ist einfacher und in der Regel schneller, als die gemeinhin bekannte Primfaktorzerlegung: Der Euklidische Algorithmus. Dass dieser Algorithmus schneller ist, zeigt die daraufhin dargestellte Laufzeitanalyse von Lamé.

Im Anschluss wird der Restklassenring $\mathbb{Z}_m$und die kartesiche Summe mehrerer Ringe definiert und kurz wiederholt, worum es eigentlich geht, wenn man von Ringen spricht. Ebenfalls soll eine Aussage über die Struktur des Restklassenringes gemacht werden.

Zum Schluss wird ein Verfahren erläutert, dass ein System von Kongruenzen lösen kann, welches heute vielfach in der Kryptographie zum Einsatz kommt und schon etwa 3000 v. Chr. entdeckt wurde: Der Chinesische Restklassensatz.

2. HAUPTTEIL

2.1. Der Euklidische Algorithmus

2.1.1. Satz (Euklidischer Algorithmus)

Im Folgenden soll der Algorithmus, der bereits etwa 300 v. Chr. von Euklid veröffentlicht wurde, dargestellt werden. Dieser Algorithmus benötigt, wie anfangs erwähnt, keine Primfaktorzerlegung und ist daher ein viel schnelleres Verfahren, um den größten gemeinsamen Teiler (ggT) zweier Zahlen *a* und *b* zu bestimmen.
Setzt man die Zahl $a = a_0$ und $b = a_1$ so ergibt sich zur Berechnung des ggT das folgende Verfahren, dass erst endet, wenn man bei den dargestellten Divisionen mit Rest den Rest 0 erhält:

$$a_0 = a_1 q_1 + a_2$$
$$a_1 = a_2 q_2 + a_3$$
$$\dots$$
$$a_{n-2} = a_{n-1} q_{n-1} + a_n$$
$$a_{n-1} = a_n q_n + 0; \qquad 0 < a_n < a_{n-1} < \cdots < a_1.$$

Dann ist der ggT(*a,b)*= a_n

Der Mathematiker Bézout hat den Euklidischen Algorithmus noch erweitert, indem er in einem Lemma feststellte, dass es zwei Zahlen *u* und *v* gibt, so dass gilt:

$$\text{ggT}(a, b) = ua + vb.$$

Diese Zahlen erhält man ebenfalls durch oben vorgestelltes Verfahren.
Zudem gilt, falls der $\text{ggT}(a, b) = 1$ ist:

$$ua \equiv 1 \ (mod\ b)$$

Das bedeutet, dass ua bei Division durch *b* den gleichen Rest lässt wie 1. Dies ergibt sich direkt aus dem Lemma von Bézout, wenn man es in modulo- Schreibweise betrachtet.

2.1.2. Beispiel

Suche in diesem Beispiel den ggT(517,96):

$$a = 517, b = 96$$
$$517 = 96 \cdot 5 + 37$$
$$96 = 37 \cdot 2 + 22$$
$$37 = 22 \cdot 1 + 15$$
$$22 = 15 \cdot 1 + 7$$
$$15 = 7 \cdot 2 + 1$$
$$7 = \mathbf{1} \cdot 7 + 0$$
$$ggT(517{,}96) = 1$$

Durch die Erweiterung des Algorithmus lassen sich die Zahlen *u* und *v* ermitteln, so dass gilt: $ggT(517{,}96) = ua + vb$:

$$ggT(517{,}96) = 15 - 7 \cdot 2 = 15 - 2(22 - 15) = 3 \cdot 15 - 2 \cdot 22$$
$$= 3(37 - 22) - 2 \cdot 22 = 3 \cdot 37 - 5 \cdot 22 = 3 \cdot 37 - 5(96 - 2 \cdot 37)$$
$$= 13 \cdot 37 - 5 \cdot 96 = 13(517 - 5 \cdot 96) - 5 \cdot 96 = \mathbf{13} \cdot 517 - \mathbf{70} \cdot 96$$

Ebenfalls gibt es also die Zahl *u*, so dass $u96 = 1\ (mod\ 517)$:

$$96 \cdot u \equiv 1\ mod(517)\ \text{ mit } u = -70$$
$$\text{denn: } 96 \cdot (-70) = -6720\ \text{ und } (-6720 - 1) : 517 = -13.$$

2.1.3. Laufzeitanalyse

Um die Laufzeit des Euklidischen Algorithmus analysieren zu können, muss erst die Beschaffenheit der Fibonacci- Zahlen erklärt werden:
Man bezeichnet jede Fibonacci- Zahl mit einem F und als Index die Nummer der jeweiligen zahl. So ist:

$$F_1 = F_2 = 1;\ F_i = F_{i-1} + F_{i-2}$$

und es ergibt sich für die ersten neun Zahlen:

i	1	2	3	4	5	6	7	8	9
F_i	1	1	2	3	5	8	13	21	34

Ein Satz von Lamé besagt nun, dass der Euklidische Algorithmus bei zwei Zahlen *a, b* mit $a > b > 0$ maximal 5*k* Divisionen benötigt. Dabei entspricht *k* der Anzahl der Ziffern der Zahl *b*.

Beweis

Um diesen Satz zu beweisen, muss zunächst ein Hilfssatz eingeführt werden:

Lemma: $n \geq 2$: $F_{n+5} > 10F_n$ (*)

Beweis: $F_{n+5} = F_{n+4} + F_{n+3} = F_{n+3} + F_{n+2} + F_{n+2} + F_{n+1} = F_{n+2} + F_{n+1} + F_{n+1} + F_n + F_{n+1} + F_n + F_{n+1} = F_{n+1} + F_n + 4F_{n+1} + 2F_n = 5F_{n+1} + 3F_n = 5(F_n + F_{n-1}) + 3F_n = 8F_n + 5F_{n-1} > 8F_n + 4F_{n-1} \overset{1}{\geq} 8F_n + 2F_n = 10F_n$ □

[1]: $2F_{n-1} \geq F_{n-1} + F_{n-2} = F_n$

Nun kann man den Beweis von Lamé führen:

Es ist $a_n \geq 1 = F_2$, hierzu betrachte man das oben vorgestellte Verfahren von Euklid. Auch die weiteren Schlüsse sind dort ohne weiteres nachzuvollziehen.

$a_{n-1} > a_n \geq 1 = F_2$

$\Rightarrow a_{n-1} \geq 2 = F_3$

$a_{n-2} \geq a_{n-1} \cdot q_{n-1} + a_n \geq a_{n-1} + a_n \geq F_3 + F_2 = F_4$

$\Rightarrow a_{n-2} \geq F_4$

$a_{n-3} \geq a_{n-2}q_{n-2} + a_{n-1} \geq a_{n-2} + a_{n-1} \geq F_4 + F_3 = F_5$

Nimmt man diese Idee auf und führt sie analog weiter, gelangt man zu

$b = a_1 \geq F_{n+1}$

Setze nun $n > 5k$, um im weiteren Verlauf zu einem Widerspruch zu gelangen, womit gezeigt wäre, dass die Anzahl der Divisionen nur kleiner als 5*k* sein kann.

$b \geq F_{5k+2} = F_{(5(k-1)+2)+5} \overset{(*)}{\geq} 10F_{5(k-1)+2} = 10F_{(5(k-2)+2)+5}$

$\overset{(*)}{\geq} 10\left(10F_{5(k-2)+2}\right) = 10^2F_{(5(k-3)+2)+5} \overset{(*)}{\geq} 10^2\left(10F_{5(k-3)+2}\right)$

$= 10^3F_{(5(k-4)+2)+5} \overset{(*)}{\geq} 10^3(10F_{5(k-4)+2}) = \cdots \overset{(*)}{\geq} 10^kF_2 = 10^k$

Widerspruch! □

2.2. Der Restklassenring $\mathbb{Z}_m$

2.2.1. Einführung

Hier soll kurz wiederholt werden, was eine Gruppe beziehungsweise ein Ring ist.

Eine Menge G heißt **Gruppe**, falls mit innerer Verknüpfung $\cdot: GxG \to G$ gilt:

a) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$
b) $a \cdot e = e \cdot a = a \quad \forall a \in G$, e heißt neutrales Element
c) zu jedem $a \in G$ existiert ein $a^{-1} \in G$ mit $a \cdot a^{-1} = a^{-1} \cdot a = e$
d) G heißt zusätzlich abelsch, falls gilt: $a \cdot b = b \cdot a \quad \forall a, b \in G$

Eine Menge R heißt **Ring**, falls mit inneren Verknüpfungen „+“ und „· ": $RxR \to R$ gilt:

a) $(R, +)$ist abelsche Gruppe
b) Assoziativgesetz gilt bzgl. „·“
c) Distributivgesetze gelten

2.2.2. Definition Restklassenring $\mathbb{Z}_m$

Seien *x* und *m* natürliche Zahlen. Teilt man *x* durch *m* bekommt man einen Rest *r*, so dass $x = mq + r$, wobei $q, r \in \mathbb{Z}; 0 \leq r \leq m - 1$ ist.
Der Rest r wird als $\text{Rest}_m(x)$ bezeichnet. Wenn man *m* fixiert und *x* variiert, bekommt man Reste aus der Menge $\mathbb{Z}_m = \{0,1, \dots, m-1\}$.
Mit der Addition: $i +_m j = \text{Rest}_m(i + j)$ und der
Multiplikation: $i \cdot_m j = \text{Rest}_m(i \cdot j)$ ist dies ein Ring.

2.2.3. Definition der kartesichen Summe von Ringen

Seien $K_1, \dots, K_s$ Ringe. Man bezeichnet $K_1 \oplus K_2 \oplus \dots \oplus K_s = \{(r_1, \dots, r_s);\ r_i \in K_i \forall i\}$
als die kartesische Summe der Ringe $K_1, \dots, K_s$.
Dies ist mit den Verknüpfungen
+: $(r_1, \dots, r_s) + (r_1', \dots r_s') = (r_1 + r_1', \dots, r_s + r_s')$ und
•: $(r_1, \dots, r_s) \cdot (r_1', \dots r_s') = (r_1 \cdot r_1', \dots, r_s \cdot r_s')$ ein Ring.

2.2.4. Satz über die Struktur des Restklassenringes $\mathbb{Z}_m$

Sei $m = m_1 m_2 \dots m_s$, wobei $m_1, m_2, \dots, m_s$ paarweise teilerfremde natürliche Zahlen sind. Dann ist $\mathbb{Z}_m$ isomorph zu $\mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$.
Also existiert eine bijektive, verknüpfungstreue Abbildung

$$\Phi: \mathbb{Z}_m \to \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s} \text{ mit}$$

$$\Phi: x \mapsto \left(\text{Rest}_{m_1}(x), \dots, \text{Rest}_{m_s(x)}\right).$$

Dieser Satz zeigt, dass zwei Mengen, die zunächst völlig verschieden sind, im eigentlichen Sinne doch „gleich“ sind: Eine Menge mit einzelnen Elementen ist isomorph zu einer Menge, deren Elemente aus Tupeln bestehen. Anhand eines Beispiels wird die Tragweite dieses Satzes klar:

Betrachte $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (1,1), (0,2), (1,0), (1,1), (1,2)\}$ und
$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$.
Nach Satz gilt: $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

Beweis

1. Injektivität

Annahme: $x, y \in \mathbb{Z}_m$ mit $x > y > 0$ und $\text{Rest}_{m_i}(x) = \text{Rest}_{m_i}(y)$
Es ist $x = m_i q_i + r$ und $y = m_i q_j + s$
Also muss gelten:
$r = s$
$\Leftrightarrow x - m_i q_i = y - m_i q_j$

$\Leftrightarrow x - y = m_i q_i - m_j$

$\Leftrightarrow x - y = m_i(q_i - q_j)$ (*)

$\overset{m_i teilerfremd}{\Rightarrow}$ $x - y = mq$ Widerspruch, da $m > x > y > 0$

2. Surjektivität

Die Anzahl der Elemente von $\mathbb{Z}_m$ ist gleich der Anzahl der Elemente der kartesichen Summe und Φ ist injektiv => Φ surjektiv. □

3. $\Phi(x + y) = \Phi(x) + \Phi(y)$

$\Rightarrow \text{Rest}_{m_i}(x + y) = \text{Rest}_{m_i}(\text{Rest}_{m_i}(x) + \text{Rest}_{m_i}(y))$

$\overset{(*)}{\Rightarrow} m_i \text{ teilt } (x + y) - \left(\text{Rest}_{m_i}(x) + \text{Rest}_{m_i}(y)\right)$

$\Rightarrow m_i \text{ teilt } \left(\text{x} - \text{Rest}_{m_i}(x)\right) + \left(y - \text{Rest}_{m_i}(y)\right)$

$\Rightarrow m_i \text{ teilt } \left(x - (x - m_i q_i)\right) + \left(y - \left(y - m_i q_j\right)\right)$

$\Rightarrow m_i \text{ teilt } m_i(q_i - q_j)$ □

4. $\Phi(xy) = \Phi(x)\Phi(y)$

$\Rightarrow \text{Rest}_{m_i}(xy) = \text{Rest}_{m_i}(\text{Rest}_{m_i}(x) \cdot \text{Rest}_{m_i}(y))$

$\overset{3}{\Rightarrow} m_i \text{ teilt } xy - (x - m_i q_i) \cdot \left(y - m_i q_j\right)$

$\Rightarrow m_i \text{ teilt } m_i(-xq_j - yq_i + m_i q_i q_j)$ □

2.3. Der Chinesische Restklassensatz

2.3.1. Der Satz

Seien $m_1, m_2, \ldots, m_s$ paarweise teilerfremde ganze Zahlen. Dann existiert für jedes Tupel ganzer Zahlen $x_1, x_2 \ldots, x_s$ eine ganze Zahl x, so dass die folgenden Kongruenzen erfüllt sind:

$$x \equiv x_1 \ (mod\ m_1)$$
$$x \equiv x_2 \ (mod\ m_2)$$
...
$$x \equiv x_s \ (mod\ m_s)$$

Setzt man $m = m_1 m_2 \ldots m_s$, dann findet man x mit

$$x_0 = \sum_{i=1}^{s} c_i \left(\frac{m}{m_i}\right) x_i$$

dabei ist c_i Inverses zu $\frac{m}{m_i}$ in $\mathbb{Z}_{\boldsymbol{m}}$.

Also ist $c_i \left(\frac{m}{m_i}\right) \equiv 1 (mod\ m_i)$. Dies zeigt, dass zur Berechnung der c_i der Euklidische Algorithmus, insbesondere seine Erweiterung genutzt werden kann.

Alle anderen x sind zu diesem kongruent *(mod m)*.

Dieser Satz wurde bereits etwa 3000 v. Chr. entdeckt und ist heute noch elementar in vielen Anwendungen, beispielsweise der Kryptographie.

Beweis

1. Existenz:

Es gilt, dass $m_j \ \frac{m}{m_i}$ für $i \neq j$ teilt.

Betrachte dazu: $\frac{m}{m_i} = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_s$. Wenn nun $i \neq j$ ist lässt sich die rechte Seite durch m_j teilen. Somit gilt:

$$c_i \left(\frac{m}{m_i}\right) x_i \equiv 0 \ \left(mod\ m_j\right) \text{ für } i \neq j$$

$$\text{und } c_i \left(\frac{m}{m_i}\right) x_i \equiv x_i \left(mod\ m_j\right) \text{ für } i = j$$

Also gilt für die Reihe

$$\underbrace{\sum_{i=1}^{s} c_i \left(\frac{m}{m_i}\right) x_i}_{x_0} = x_i \ \ (mod \ \ m_j)$$

Daher gilt $x_0 \equiv x_i \ \ \left(mod\ m_j\right) \ \forall\, j = 1, \dots, s$, wie gewünscht.

2. Eindeutigkeit:

Annahme: $x = x_0$ mit $x \equiv x_j \ (mod\ m_j)$

$$\Rightarrow \text{Rest}_{m_i}(x) = \text{Rest}_{m_i}(x_o)$$

$$\Rightarrow m_i \text{ teilt } (x - x_0) \ \forall i$$

$$\overset{m_i \ teilerfremd}{\Rightarrow} \quad x - x_0 = mq$$

$$\Rightarrow \ x - x_0 = 0$$

$$\Rightarrow x = x_0 \qquad \square$$

2.3.2. Beispiel

Man bestimme ein *x* so, dass folgende Kongruenzen erfüllt sind:

$$x \equiv 2 \ (mod\ 3)$$

$$x \equiv 3 \ (mod\ 4)$$

$$x \equiv 2 \ (mod\ 5)$$

Es gilt:

$$x_0 = \sum_{i=1}^{s} c_i \left(\frac{m}{m_i}\right) x_i$$

$$= c_1 \left(\frac{60}{3}\right) \cdot 2 + c_2 \left(\frac{60}{4}\right) \cdot 3 + c_3 \left(\frac{60}{5}\right) \cdot 2$$

$$= 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 2$$

$$= 287$$

$$\Rightarrow x \equiv 47 \ (mod 60)$$

3. SCHLUSS

Es wurde in dieser Ausarbeitung also klar, dass der Euklidische Algorithmus eine Bedeutung hat, die noch heute relevant ist. Zum einen lässt sich dadurch nach wie vor, der ggT zweier Zahlen auf einfache Weise berechnen und zum anderen fließt er in den Chinesischen Restklassensatz, der heutzutage sehr aktuell ist, indirekt mit ein.
Ebenfalls ist ersichtlich geworden, welche Struktur der Restklassenring aufweist und dass es auch Isomorphismen zwischen Mengen gibt, die zunächst völlig konträr erscheinen.
Ein interessanter Aspekt wäre sicherlich noch die Frage, wozu der Chinesische Restklassensatz zur Zeit seiner Entdeckung gedient hat, doch die Quellenlage hierzu ist eher dürftig.

4. QUELLENANGABE

Prof. Bogopolski, Oleg: Algorithmische Zahlentheorie mit Anwendungen in der Kryptographie.

Beutelspacher, Albrecht: Lineare Algebra. Eine Einführung in die Wissenschaft der Vektoren, Abbildungen und Matrizen

Fischer, Gerd: Lineare Algebra.