Quadratsummen in Restklassenringen

ELEMENTE DER MATHEMATIK
Revue de mathématiques élémentaires - Rivista di matematica elementare
Zeitschrift zur Pflege der Mathematik und zur Förderung des mathematisch-physikalischen Unterrichts
El. Math. Band 35 Heft 4 Seiten 73-104 Basel, 10. Juli 1980

Quadratsummen in Restklassenringen

Herrn Curt Schmieden zu seinem 75. Geburtstag am 22. Juni 1980.

Bekanntlich ist jede natürliche Zahl als Summe von höchstens vier Quadratzahlen darstellbar, und jede Primzahl $p \equiv 1 \pmod 4$ ist gleich der Summe von zwei Quadratzahlen. Die Theorie der quadratischen Reste hat dann geklärt, wann ein Rest k modulo m gleich einem Quadrat ist, wann es also x gibt mit $x^2 \equiv k \pmod m$.
Die Frage nach Quadratsummendarstellungen modulo m ist naheliegend, die Antwort scheint aber nicht allgemein bekannt zu sein. So ist kürzlich die Aufgabe [1] behandelt worden, wie viele Quadrate zur Darstellung von -1 modulo m erforderlich sind; da diese Aufgabe von mehreren Zahlentheoretikern bearbeitet wurde und keine Hinweise auf ältere Literatur angegeben sind, erscheint die Behandlung der folgenden ganz allgemeinen Fragestellung gerechtfertigt:

Bei gegebenem $k \in \mathbf{Z}$, $m \in \mathbf{N}$ bezeichne $s(k,m)$ das kleinste s, für welches

$$\sum_{j=1}^{s} x_j^2 \equiv k \pmod m$$

Lösungen $(x_1, \ldots, x_s)$ besitzt. Man berechne $s(k,m)$!

(Wir betrachten ohne Beschränkung der Allgemeinheit nur $k \geqq 0$.)
Offenbar gilt $s(k,m) \leqq 4$, da k ja sogar gleich einer Summe von höchstens vier Quadraten ist. Man überzeugt sich, dass $s(-1,8) = s(7,8) = 4$. Die Fälle $s(k,m) = 1$ sind durch die Theorie der quadratischen Reste geklärt. Ist $p \equiv 1 \pmod 4$ eine Primzahl, so gilt $s(p,m) \leqq 2$. In [1] ist $s(-1,m)$ für alle m berechnet: $s(-1,m) = 4$ für $8 \mid m$; $s(-1,m) = 3$ für $2^2 \| m^1)$; $s(-1,m) = 2$, falls $4 \nmid m$ und $p \mid m$ für wenigstens ein $p \equiv 3 \pmod 4$; $s(-1,m) = 1$, falls $4 \nmid m$ und aus $p \mid m$ folgt $p = 2$ oder $p \equiv 1 \pmod 4$.
Wann $s(k,m) = 1$ gilt, ergibt sich aus der Theorie der quadratischen Reste. Wir sind daher mit Aussagen wie $s(k,m) \leqq 2$ zufrieden.
Wir beweisen der Vollständigkeit halber eine einfache Hilfsbemerkung, die wir später auf die Polynome $P(x,y) = x^2 + y^2 - k$ und $P(x,y,z) = x^2 + y^2 + z^2 - k$ bei festem k anwenden werden:

Hilfssatz. *Es sei $P(x,y,\ldots,z)$ ein Polynom mit ganzen Koeffizienten in N ganzzahligen Variablen. Dann ist*

$$P(x,y,\ldots,z) \equiv 0 \pmod m$$

genau dann lösbar, wenn

$$P(x,y,\ldots,z)\equiv 0 \pmod{p_j^{a_j}}$$

für alle $j=1,\ldots,n$ *lösbar ist*[1]).

Beweis: Sei $P(x_0,y_0,\ldots,z_0)\equiv 0 \pmod m$; dann gilt dieselbe Kongruenz offenbar auch nach den Moduln $p_j^{a_j}$. - Umgekehrt sei für $j=1,\ldots,n$

$$P(x_j,y_j,\ldots,z_j)\equiv 0 \pmod{p_j^{a_j}}.$$

Es ist zu zeigen, dass dann $x_0,y_0,\ldots,z_0$ existieren mit

$$P(x_0,y_0,\ldots,z_0)\equiv 0 \pmod m.$$

Dazu bestimmen wir nach dem chinesischen Restsatz die $x_0,y_0,\ldots,z_0$ als Lösungen der simultanen linearen Kongruenzen

$$\begin{aligned} x_0 &\equiv x_j \pmod{p_j^{a_j}} \\ y_0 &\equiv y_j \pmod{p_j^{a_j}} \qquad j=1,2,\ldots,n. \\ z_0 &\equiv z_j \pmod{p_j^{a_j}} \end{aligned}$$

Damit gilt $P(x_0,y_0,\ldots,z_0)\equiv 0 \pmod{p_j^{a_j}}$ für alle j und damit auch

$$P(x_0,y_0,\ldots,z_0)\equiv 0 \pmod m. \quad \square$$

Wichtig ist, dass man sich somit auf Primpotenzmoduln beschränken kann.
Für einen ersten, schon ziemlich weitreichenden Satz werden hier zwei Beweise angegeben. Der erste verallgemeinert das Verfahren von R. L. McFarland für $k=-1$ aus [1] und ist zwar kurz, aber wegen der Verwendung des Dirichletschen Primzahlsatzes für arithmetische Folgen nicht elementar. Der zweite, etwas längere Beweis ist elementar; er liefert sogar etwas mehr.

Satz 1. *Es sei* d *ungerade und* $m=2d$ *oder* $m=d$, *ferner* $(k,d)=1$. *Dann ist* $s(k,m)\leqq 2$.

Erster Beweis: Wir setzen zunächst sogar $(k,2d)=1$ voraus und machen eine Fallunterscheidung.
Sei $k\equiv 1 \pmod 4$. Wir betrachten die arithmetische Folge

$$k+4dn, \qquad n=0,1,2,3,\ldots;$$

sie enthält nach dem Satz von Dirichlet eine Primzahl q, weil $(k,4d)=1$, und wegen $q\equiv k\equiv 1 \pmod 4$ gibt es eine Darstellung von q als Summe zweier Quadrate. Also ist $s(k,m)\leqq 2$.

1) $q^a \| m$ heisst $q^a | m$ (| für «teilt»), aber $q^{a+1} \nmid m$; p bezeichnet stets eine Primzahl, $m=p_1^{a_1}\cdot\ldots\cdot p_n^{a_n}$ die kanonische Primzerlegung. Der grösste gemeinsame Teiler von m und n wird (m,n) geschrieben.

Sei $k \equiv 3 \pmod 4$. Hier nehmen wir die arithmetische Folge

$$k+2d+4dn, \qquad n=0,1,2,3,\ldots$$

Für eine in ihr enthaltene, wegen $(k+2d, 4d)=1$ sicher existierende Primzahl q gilt wegen $d \equiv \pm 1 \pmod 4$, also $2d \equiv +2 \pmod 4$, wieder $q \equiv 1 \pmod 4$, also $q \equiv x^2+y^2$. Wieder haben wir $k \equiv x^2+y^2 \pmod m$, also $s(k,m) \leqq 2$.
Es ist nun noch der Fall eines geraden k zu behandeln. (Bei ungeraden $m=d$ wäre das nicht nötig, weil dann statt k die ungerade Zahl $k'=k+m$ herangezogen werden könnte.) Wir benutzen die Identität $2(a^2+b^2)=(a+b)^2+(a-b)^2$:
Da $k=2^s \cdot u$ mit einer ungeraden Zahl $u \equiv a^2+b^2$ gilt, ist mit u auch k eine Summe zweier Quadrate. (Ist s gerade, so ist 2^s ein Quadrat, sonst kommt ein Faktor 2 dazu.) □

Zweiter Beweis: Nach dem Hilfssatz genügt es, Primpotenzmoduln $m=p^a$ zu betrachten.
Fall 1. $a=1$, also $m=p$. Für $p=2$ haben wir $s(k,2)=1$. Bei ungeradem p gibt es genau $(p-1)/2$ teilerfremde quadratische Restklassen (QR) und ebenso viele quadratische Nichtreste (NR). Wir betrachten für $x=0,1,2,\ldots,p-1$ und gegebenes k die Zahlen $k-x^2$. Darunter müssen $(p+1)/2$ paarweise inkongruente sein, weil aus $k-x_1^2 \equiv k-x_2^2$ folgt $x_1=x_2$ oder $x_1=p-x_2$. Unter den $(p+1)/2$ verschiedenen Restklassen muss sicher die Klasse der $0=0^2$ oder ein QR sein, da es nur $(p-1)/2$ NR gibt. Damit hat aber $k-x^2 \equiv y^2 \pmod p$ eine Lösung, es ist also $s(k,p) \leqq 2$.
Fall 2. $a=2$, p ungerade, also $m=p^2$. Es sei k_0 irgendeine Summe von zwei Quadraten, $k_0=x_0^2+y_0^2$. Für alle ganzen Zahlen g werde definiert $k_g=(x_0+gp)^2+y_0^2 \equiv k_0 + 2pgx_0 \pmod{p^2}$. Falls $(x_0,p)=1$, gibt es zu jedem $r=0,1,\ldots,p-1$ ein g, so dass $2gx_0 \equiv r \pmod p$, und damit wird $k_g=(x_0+gp)^2+y_0^2 \equiv k_0+rp \pmod{p^2}$. Also ist $s(k_0+rp,p^2) \leqq 2$, falls $(x_0,p)=1$ bei gegebenem k_0 erreicht werden kann. Da x_0, y_0 vertauschbar sind, müsste im anderen Fall $x_0 \equiv y_0 \equiv 0 \pmod p$ gelten. Aber dann folgt $k_0=x_0^2+y_0^2 \equiv 0 \pmod{p^2}$, und hier sind alle $k_g \equiv k_0 \equiv 0 \pmod{p^2}$. Alle k_0 mit $(k_0,p)=1$ sind aber als Summen von höchstens zwei Quadraten modulo p darstellbar, und k_0+rp durchlaufen alle teilerfremden Restklassen modulo p^2, also gilt $s(k,p^2) \leqq 2$ für $(k,p)=1$.

Zusatz: Wir erledigen hier gleich noch, innerhalb des Beweises, den Fall $k=g \cdot p$; ist $p \equiv 1 \pmod 4$, so gibt es eine Darstellung $p=x_0^2+y_0^2$ mit $(x_0,p)=1$, und unsere Überlegung ist wieder anwendbar, d.h. $s(gp,p^2) \leqq 2$ für $p \equiv 1 \pmod 4$. Sei nun $p \equiv 3 \pmod 4$; wäre $x^2+y^2=gp \equiv 0 \pmod p$, so folgte $-x^2 \equiv +y^2 \pmod p$. Falls $(x,p)=1$, existierte z mit $zx \equiv 1 \pmod p$, also $-1 \equiv -(zx)^2 \equiv (zy)^2 \pmod p$. Es ist aber hier -1 ein NR, also bleibt nur $(x,p)=p$, d.h. $x=ap$, $y=bp$, $g=(a^2+b^2)p$, also kann gp für $(g,p)=1$ nicht Summe von höchstens zwei Quadraten sein: $s(gp,p^2) \geqq 3$ für $p \equiv 3 \pmod 4$ und $(g,p)=1$. Damit ist der Zusatz beendet, und wir fahren mit dem Beweis von Satz 1 fort.
Fall 3. $a \geqq 3$. Wir werden vollständige Induktion nach a durchführen, um zu zeigen: $s(k,p^a) \leqq 2$ für alle k mit $(k,p)=1$ und $p \neq 2$. Für $a=1,2$ ist die Aussage bewiesen. Wir setzen sie jetzt für ein a voraus und zeigen ihre Richtigkeit für $a+1$. Sei k ge-

geben. Dann gibt es nach Induktionsvoraussetzung x_0, y_0 mit $x_0^2+y_0^2=k_0\equiv k \pmod{p^a}$. Wir erhalten jetzt für ganze g

$$\begin{aligned} k_g &= (x_0+g\cdot p^a)^2+y_0^2 \\ &\equiv k_0+2g x_0 p^a \pmod{p^{a+1}}. \end{aligned}$$

Bei $(x_0,p)=1$ [was bei $(k,p)=1$ erreichbar ist] lässt sich $2gx_0$ wieder so einrichten, dass $k_0+2g x_0 p^a\equiv k \pmod{p^{a+1}}$. □

An den Beweis zu Fall 3 können wir sogleich einen Zusatz anschliessen, für den Fall $p\equiv 1 \pmod 4$. Hier behaupten wir, dass die Voraussetzung $(x_0,p)=1$ immer erfüllbar ist. Für $a=2$ wurde das im Zusatz benutzt. Dann benutzt man für $a=3$ stattdessen $x_0+gp^2=x_0^{(3)}$, allgemein bei $a+1$ $x_0^{(a+1)}=x_0^{(a)}+gp^a$, und alle diese Zahlen sind mit x_0 teilerfremd zu p. Es ist also $x^2+y^2\equiv k\,(p^a)$ auch für $(k,p^a)>1$ stets lösbar, wenn $p\equiv 1 \pmod 4$.

Ist hingegen $p\equiv 3 \pmod 4$, so zeigte der Zusatz, dass $x^2+y^2\equiv gp \pmod{p^2}$ für $(g,p)=1$ unlösbar ist. Dann ist $x^2+y^2\equiv gp \pmod{p^a}$ für $a>2$ erst recht unlösbar, wenn $(g,p)=1$. [Man beachte aber, dass bei $p\mid g$ durchaus Lösungen existieren können, z. B. bei $g=p$, $g=2p$, $g=5p$, nämlich etwa p^2+0^2, p^2+p^2, $p^2+(2p)^2$.] Wir fassen die Zusätze zusammen:

Satz 2. *Bei* $p\equiv 1 \pmod 4$ *gilt* $s(k,p^a)\leqq 2$ *für alle* k *und* $a\geqq 2$. *Bei* $p\equiv 3 \pmod 4$ *und* $(g,p)=1$ *gilt für alle* $a\geqq 2$: $s(g\cdot p,p^a)\geqq 3$.

Im Hinblick auf den Hilfssatz haben wir nun

Satz 3. *Aus* $p^2\mid m$ *folge* $p\equiv 1 \pmod 4$. *Dann gilt für alle* k: $s(k,m)\leqq 2$. *Ist umgekehrt* $s(k,m)\leqq 2$ *für alle* k, *so ist* m *von dieser Gestalt.*

Die ausgesagte Umkehrung ergibt sich daraus, dass $s(3,4)=3$ ist und dass $s(p,p^2)\geqq 3$ für $p\equiv 3 \pmod 4$.

Bei Moduln, welche keine dritten Potenzen enthalten, ist jetzt lediglich noch $s(gp,p^2)$ zu untersuchen, wenn $p\equiv 3 \pmod 4$. Wir behaupten sogleich etwas mehr.

Satz 4. *Bei* $(g,p)=1$ *und* $p\equiv 3$ *(mod* 4*) gilt* $s(gp,p^N)=3$, *wenn* $N\geqq 2$.

Beweis: Es geht nur noch darum, $s(gp,p^N)=4$ auszuschliessen. Dazu müssen wir bei gegebenem g irgendein a finden, so dass die natürliche Zahl $gp+a\cdot p^N$ $(N\geqq 2)$ durch weniger als vier - und dann, wie wir wissen, durch genau drei - Quadrate darstellbar ist. Dazu benutzen wir die Tatsache, dass die Zahlen, welche vier Quadrate erfordern, von der Form $4^k(8L+7)$, $k,L\geqq 0$, sein müssen, also sicher kongruent 0 modulo 4 oder (bei $k=0$) kongruent -1 modulo 4 (und sogar modulo 8). Wir betrachten $N=2M$ und unterscheiden (bei gegebenen g und $p=4j-1$):

Fall 1. gp ist nicht von der Form $4^k(8L+7)$, dann sind wir fertig.

Fall 2. $gp=4^k(8L+7)$ mit $k\geqq 1$. Wir betrachten:

$$\begin{aligned} gp+p^{2M} &= 4^k(8L+7)+(4j-1)^{2M} \\ &\equiv 1 \pmod 4, \end{aligned}$$

also nicht $\equiv 0, -1 \pmod 4$, so dass eine Summe von drei Quadraten erhalten wird.
Fall 3. $gp = 8L+7$. Wir betrachten

$$gp + 2p^{2M} = 8L+7+2(4j-1)^{2M}$$
$$\equiv -1+2 \equiv 1 \pmod 4.$$

Sei nun $N = 2M+1$, $M \geqq 1$. Wir unterscheiden wieder:
Fall 1. Wie oben.
Fall 2. $gp = 4^k(8L+7)$, $k \geqq 1$.
Dann ist

$$gp + ap^{2M+1} \equiv 0 + a \cdot p \cdot p^{2M}$$
$$\equiv a \cdot p \cdot 1 \equiv -a \pmod 4.$$

Bei $a = 2$ sind also nur drei Quadrate erforderlich.
Fall 3. $gp = 8L+7$. Hier ist $gp + ap^{2M+1} \equiv -1-a \pmod 4$, also können wir $a = 1$ wählen. □
Man beachte, dass im Beweis nicht von $(g,p) = 1$ Gebrauch gemacht wurde. Das gibt:

Satz 5. *Bei* $p \equiv 3 \pmod 4$ *gilt* $s(k, p^N) \leqq 3$ *für alle* k.

Wann ist nun eigentlich mit $s(k,m) = 4$ zu rechnen? Wendet man die Vorüberlegung auf das Polynom $x^2+y^2+z^2-k$ an, so lässt sich dieses genau dann nicht zu Null machen, wenn für eine Primpotenz $p_j^{a_j} \mid m$ gilt $s(k, p_j^{a_j}) = 4$. Bei ungeraden p_j kann das aber nach unseren Sätzen nicht eintreten. Daher ist nur noch übrig $p = 2$. Da $s(k, 2^2) \leqq 3$ und $s(k, 2^3) = 4$ genau für $k \equiv -1 \pmod 8$, brauchen wir nur $m = 2^a$ bei $a \geqq 3$ zu betrachten. Sei etwas allgemeiner $m = 8L$, dann untersuchen wir auf Lösbarkeit

$$x^2+y^2+z^2 \equiv -1+8j \pmod{8L};$$

falls eine Lösung existiert, gälte

$$x^2+y^2+z^2 = -1+8j+8Lq,$$

also $x^2+y^2+z^2 \equiv -1 \pmod 8$, aber das ist unlösbar. Also ist $s(-1, 8L) = 4$.
Von jetzt an sei k beliebig und $m = 2^N$, $N \geqq 3$; dann wird $s(k,m) = 4$ genau dann eintreten, wenn k und alle $k+qm$ von der Form (F) $4^K(8L+7)$ sind. Ist $k = 8L+7$, so folgt

$$k + q \cdot 2^N = 8(L + q \cdot 2^{N-3}) + 7,$$

und das ist wieder von der Form (F), also

$$s(8L+7, 2^N) = 4 \quad \text{für} \quad N \geqq 3. \tag{1}$$

Ist aber $k=4^K(8L+7)$ mit $K\geqq 1$, so kann s alle Werte von 1 bis 4 annehmen. Wir erörtern das genauer. Dazu setzen wir $N=2K+J$, wobei $J>0$ vorausgesetzt werden soll, weil sonst $k\equiv 0 \pmod{2^N}$ wäre. Dann ist

$$\begin{aligned} k+q\cdot 2^N &= 4^K(8L+7)+q\cdot 2^{2K+J} \\ &= 4^K(8L+q\cdot 2^J+7). \end{aligned}$$

Falls $J\geqq 3$, ist das wieder von der Form (F), also

$$s\left(4^K(8L+7),2^N\right)=4 \quad \text{für} \quad N\geqq 2K+3. \tag{2}$$

Es bleiben noch die Fälle $J=1, J=2$, mit

$$k+q\cdot 2^N=4^K[8L+2q+7] \quad \text{bei} \quad J=1 \tag{3}$$

und

$$k+q\cdot 2^N=4^K[8L+4q+7] \quad \text{bei} \quad J=2 \tag{4}$$

mit $q=0,1,2,3,\ldots$
Im Falle (3) betrachten wir $q=2r+1$ und haben

$$k+(2r+1)2^N=4^K[8(L+1)+4r+1].$$

Der Ausdruck in eckigen Klammern stellt eine arithmetische Folge dar, auf die der Satz von Dirichlet anwendbar ist. Für geeignetes r wird der Ausdruck zu einer Primzahl $p\equiv 1 \pmod 4$, also $p=x^2+y^2$, so dass also gilt

$$k\equiv (2^K)^2(x^2+y^2)\equiv (2^Kx)^2+(2^Ky)^2 \pmod{2^N},$$

es ist also im Falle $J=1$

$$s(k,2^N)\leqq 2.$$

Im Falle (4) liegt für $q=1$ nicht die Form (F) vor, also ist $s(k,2^N)\leqq 3$.
Wir fassen die Ergebnisse zu (1), (2), (3), (4) zusammen und haben insbesondere eine Kennzeichnung der Fälle $s(k,m)=4$:

Satz 6. *Es gilt $s(k,m)=4$ genau dann, wenn $8\mid m$ und bei $2^N\| m$, $k>0$ gilt: $k=4^K(8L+7)$, wobei $K\leqq (N-3)/2$.*
Ist $k=4^K(8L+7)$ bei $m=2^N>8$ und $N=2K+1$, so gilt $s(k,m)\leqq 2$; bei $N=2K+2$ gilt $s(k,m)\leqq 3$.

Unsere Resultate sind für $s(k,m)=4$ optimal, und für $s(k,m)=1$ kann man, wie eingangs erwähnt, die Theorie der quadratischen Reste heranziehen. Damit sind Aussagen $s(k,m)\leqq 2$ entscheidbar. In einigen Fällen haben wir lediglich $s(k,m)\leqq 3$ erhalten, so dass dann noch zwischen 2 und 3 zu unterscheiden ist.

Immerhin lassen sich unsere Ergebnisse zu Algorithmen zur effektiven Abschätzung von $s(k,m)$ verwenden. Dabei zeigt sich, dass Satz 1 bereits sehr oft hilfreich sein kann.

Detlef Laugwitz, TH Darmstadt

LITERATURVERZEICHNIS

1 Am. Math. Monthly: Advanced Problem 6148. Proposed by Charles Small: *84*, 300 (1977); solution by R.L. McFarland: *86*, 61 (1979).
2 G.H. Hardy und E.M. Wright: Einführung in die Zahlentheorie. München 1958.

Kleine Mitteilungen

Eine Bemerkung über Stammfunktion und Zwischenwerteigenschaft

Es bezeichnen im folgenden R die Menge der reellen Zahlen und I ein beschränktes oder nichtbeschränktes Intervall von R. Den Begriff der Stammfunktion verstehen wir hier im engeren Sinne (für eine erweiterte Fassung vgl. [1], S. 159): $g: I \to R$ heisst eine *Stammfunktion der Funktion* $f: I \to R$ *auf* I, wenn für *jede* Stelle x von I gilt: g bei x differenzierbar und $g'(x) = f(x)$. Wir sagen, $f: I \to R$ habe die *Zwischenwerteigenschaft auf* I, wenn gilt: Sind $a, b \in I$ mit $f(a) \neq f(b)$ und d zwischen $f(a)$ und $f(b)$, so gibt es ein c zwischen a und b mit $f(c) = d$.
Die Eigenschaft von f, auf I eine Stammfunktion zu besitzen, steht bekanntlich in keiner einfachen Implikationsbeziehung zur Riemann-Integrierbarkeit auf den kompakten Teilintervallen von I (vgl. [4], S. 146–147). Die leider viel zu wenig bekannte Tatsache (*) $g: I \to R$, g auf I differenzierbar $\Rightarrow g'$ hat die Zwischenwerteigenschaft auf I (vgl. z.B. [3], S. 25) ist nun mitbeteiligt an der Begründung der folgenden Aussage.

Satz. *Für* $f: I \to R$ *und die Bedingungen*
(i) f *ist auf* I *stetig,*
(ii) f *besitzt eine Stammfunktion auf* I,
(iii) f *hat die Zwischenwerteigenschaft auf* I
gilt (i) $\not\Leftrightarrow$ *(ii)* $\not\Leftrightarrow$ *(iii).*

[Man beachte, dass (i) $\Rightarrow$ (iii) die Aussage des Bolzanoschen Zwischenwertsatzes ist.]

Beweis: (i) $\Rightarrow$ (ii) lässt sich in bekannter Weise mit Hilfe des Riemannschen Integrals begründen, und (ii) $\Rightarrow$ (iii) folgt aus (*). Für (ii) $\not\Rightarrow$ (i) wähle man $I = R, f(x) = \sin(1/x)\,(x \neq 0), f(0) = 0$ (vgl. [1], S. 164, Problem 6a, oder [2]). Schliesslich sei $h(x) = \sin(1/x)\,(x \neq 0), h(0) = 1$. h hat die Zwischenwerteigenschaft auf R. Es sei nun g_1 eine Stammfunktion der vorhin erwähnten Funktion f auf R. Besässe auch h eine Stammfunktion g_2 auf R, so wäre $g_2 - g_1$ auf R differenzierbar und $[g_2(x) - g_1(x)]'$