Zahlentheorie in $\mathbb{Z}$

Def $a, b \in \mathbb{Z} \quad b \neq 0$

$b \mid a \iff \exists c \in \mathbb{Z} \Rightarrow bc = a$

P

(i) $c \mid a \quad c \mid b \Rightarrow c \mid ma + nb$

(ii) $b \mid a \quad c \neq 0 \Rightarrow bc \mid ac$

(iii) $b \mid a \quad c \mid b \Rightarrow c \mid a$

(iv) $b \mid a \quad a > 0 \; b > 0 \Rightarrow 1 \leq b \leq a$

L $a, b \in \mathbb{Z} \quad b \neq 0$

$\Rightarrow \exists! \; q, r \quad a = bq + r \quad 0 \leq r < |b|$

(i) $b > 0 \quad b = |b|$

1. Fall $\exists c \quad bc = a$

2. Fall $\exists c \quad bc < a < b(c+1)$ also $a - bc = r$

(ii) $b < 0$ nimm $|b|$

D $n > 1$ n Primzahl $\iff \nexists \; c \neq 1, n \quad c \mid n$

Viggo Brun 1910 $\sum_{p_n} \frac{1}{p_n}$ divers. (Euler)

$\sum_{\substack{p_n \\ \text{Primzwill.}}} \frac{1}{p_n}$ konverg.

S 1 Jede ganze Zahl $n > 1$ ist als Produkt v. Primzahlen darstellbar

Γ $n > 1$

1. Fall n prim

2. Fall n zus. gesetzt

$\exists d \quad 1 < d < n \quad d \mid n$

n sei d. kleinste $\Rightarrow n$ Primzahl

(denn $\exists$ Teiler kleiner n $1 < k < m \quad k \mid n$

$\Rightarrow k \mid m$ und $m \mid n$ $\lightning$ Minimal.)

Setze $n = p_1 \quad n = p_1 \cdot r$ mit $1 < r < n$

$r = p_2 \cdot s \quad 1 \leq s < r < n$ usw.

Verfahren bricht nach endl. vielen Schritten ab

$n = p_1 \cdot p_2 \cdots p_k \quad p_1 \leq p_2 \leq \ldots \leq p_k$ $\lrcorner$

B jede zusg. Zahl ist d. Prim. $p \leq \sqrt{n}$ teilbar.

denn $p_1 > \sqrt{n} \quad p_2 > \sqrt{n} \Rightarrow p_1 p_2 > n$

Das Sieb d. Eratosthenes (194 - 276 n.C.)

$\longrightarrow$ Siebtheorie (Weltressourcen)

Bsp 1. $n > 1 \quad n^4 + 4$ nicht prim

$n^4 + 4 = (n^2 + 2)^2 - 4n^2$

2. $n > 1$ $a^n - 1$ prim $\Rightarrow a = 2$ n Prim

denn $a > 2 \Rightarrow (a-1) \mid (a^n - 1)$

$a = 2$, n nicht prim $n = k \cdot l$

$\Rightarrow (2^k - 1) \mid (2^n - 1)$ $2^n - 1 : 2^k - 1 = 2^{n-k} + 2^{n-\dots}$ $-2^{n-k} - 1$

3. a zusgesetzt $2^a - 1$ keine Primzahl

4. $n \geq 1$ $2^{4n+2} + 1$ keine Primzahl

$2^{4n+2} + 1 = (2^{2n+1} + 1)^2 - 2^{2n+2}$

D

$n > 1$ $n = p_1^{a_1} \cdots p_k^{a_k}$ $p_1 < p_2 < \dots < p_k$, $a_r > 0$ $r = 1 \dots k$
heisst kanon. Zerleg. von n

S2

Die kan. Zerleg. von $n \in \mathbb{Z}^+$ $n > 1$ ist eindeutig

Bew (Lord Cherwell Wiegster. von Churchill Atomphys.)

⌈ $n > 1$ n hat zwei versch. kan. Zerleg.
N kleinste solche Zahl, mit d. Zerleg.

$N = p_1 p_2 \dots p_k = q_1 \cdot q_2 \cdots q_m$

jedes p_r ist von jedem q verschieden (Minimalit.)

o.B.d.A $p_1 \leq p_2 \dots \leq p_k$ $q_1 \leq q_2 \leq \dots \leq q_m$

$p_1 \neq q_1$ dürfen ann. $p_1 < q_1$

Bilden wir die Zahl $P = p_1 q_2 q_3 \cdots q_m$
$p_1 \mid P$ $p_1 \mid N \Rightarrow p_1 \mid N - P$ wobei
$N - P = (q_1 - p_1) q_2 \cdots q_m > 1$

1. Fall $q_1 - p_1 > 1$ ($q_1 - p_1 = 1$ für $q_1 = 3$ $p_1 = 2$)
haben Primzahlzerleg.
$q_1 - p_1 = r_1 r_2 \dots r_s$
(Diese ist eindeutig weil $q_1 - p_1 < N$ aber brauchen das nicht)

Dann ist $N - P = (q_1 - p_1) q_2 \cdots q_m > 1$
$N - P = r_1 r_2 \dots r_s q_2 \cdots q_m$
Da jedes p von jedem q verschieden ist,
Ferner ist p_1 verschieden von $r_1, r_2 \dots r_s$ weil
$p_1 \nmid (q_1 - p_1)$ da q_1 prim ist
Folglich haben wir zwei verschied. Zerleg. von $N - P$, nämlich $N - P = r_1 \dots r_s q_2 \cdots q_m$
$N - P = p_1 \cdot t_2 \dots t_m$

2. Fall $q_1 - p_1 = 1$ nur mögl. für $q_1 = 3$ $p_1 = 2$

$N - P = q_2 \cdots q_m$
$N - P = p_1 t_1 \cdots t_n$ } ⌋

D

a, b ganz $a \neq 0 \vee b \neq 0$
ggT $(a,b) = (a,b)$:= grösste posit. Zahl, welche sowohl a als auch b teilt

Ist $(a,b) = 1$ so heissen a, b teilerfremd od. rel. prim

D Ein Modul ist eine nicht leere Menge S von ganzen Zahlen mit Eigenschaft (additive Untergruppe)

$$m \in S \; n \in S \Rightarrow m-n \in S$$

Bem $m \in S, n \in S \Rightarrow 0 \in S \quad -n \in S \quad m+n \in S \quad mx+ny \in S$

D $S = \{0\}$ triviale Modul

Satz 3 Jeder nichttriviale Modul S besteht aus allen Vielfachen einer posit. ganzen Zahl

⌜ S enth. posit. ganze Zahl

d . = kleinste posit. ganze Zahl

S enth alle Vielfachen von S

zu zeigen S enthält keine anderen Zahlen

$n \in S \Rightarrow n = d \cdot k + c \qquad 0 \le c < d$

$d \in S \Rightarrow dk \in S \Rightarrow n - dk \in S \Rightarrow c \in S$

aber $c < d \Rightarrow c = 0$ ⌟

Satz 4 a, b ganze Zahlen, so besteht der Modul $S = \{ax+by \mid x, y \text{ ganz}\}$ aus allen Vielfachen von $d = (a,b)$

⌜ S ist Modul (klar)

$S \ni \Rightarrow S$ besteht aus allen Vielfachen einer posit. Zahl e

also teilt e jedes Element von S, also insbesondere $e \mid a \quad e \mid b \Rightarrow e \mid gT(a,b)$

Da $d = (a,b) \Rightarrow e \le d$

andererseits $d \mid ax+by \quad \forall x, y$

also teilt d jedes Elem. von S insbesond die 1

folgt $e = d$ ⌟

Satz 5 Die gleich. $ax+by = n$ ist genau dann in allen ganzen Zahlen x, y lösbar, wenn $(a,b) \mid n$

Beweis ⌜ (i) $(a,b) \mid n \Rightarrow n$ Vielfaches von (a,b)
$\Rightarrow n \in S \Rightarrow n = ax+by$

(ii) $(a,b) \mid a \quad (a,b) \mid b \Rightarrow (a,b) \mid ax+by$ ⌟

Kor 1 (a,b) ist ganzzahl. Linearkomb von a u. b.

Kor 2 jeder gem. Teiler v. (a,b) teilt (a,b)

denn (a,b) ist Linearkomb.

S.6 $a \mid b \cdot c \;,\; (a,b)=1 \Rightarrow a \mid c$

Euklid 300 v.C

Γ $(a,b)=1 \Rightarrow \exists x,y \quad ax+by=1$
$\rightarrow acx+bcy=c$

$a \mid bc \Rightarrow a \mid c$ $\lrcorner$

Kor 3 p, p_i Primzahlen $p \mid \prod_{i=1}^{n} p_i \Rightarrow p=p_j \;\exists j$

Bew. von Satz 2 (2. Bew.)

$N>1$ mit zwei versch. Zerlegungen

$N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = q_1^{b_1} \dots q_n^{b_n}$

$\Rightarrow p_1 \mid q_1^{b_1} \dots q_n^{b_n} \Rightarrow p_1 = q_j$

jedes p = eins } $k=n$ (1)
jedes q · einh }

$N = p_1^{a_1} \dots p_k^{a_k} = p_1^{b_1} \dots p_k^{b_k}$

mit $p_1<p_2<\dots<p_k$ nach Def. d. kan. Zerleg.

$1 \le i \le k \quad a_i > b_i \Rightarrow p_i^{b_i} \mid$ beide Teile

$p_1^{a_1} \dots p_i^{a_i - b_i} p_{i+1}^{a_{i+1}} \dots p_k^{a_k} = p_1^{b_1} \dots p_{i-1}^{b_{i-1}} \dots p_k^{b_k}$ (2)

$p_i \mid$ l.h.s. $p_i \nmid$ r.h.s. $\lightning \Rightarrow a_i \neq b_i \dots b_i \neq a_i \Rightarrow b_i = \square$

D a, b ganz $ab \neq 0$

ggV $(a,b) = \{a,b\}$ kleinste positive Zahl, welche sowohl durch a als auch durch b teilbar ist.

S.7 $ab>0 \Rightarrow (a,b) = (a,b)\{a,b\}$

Γ $\nu := \frac{a \cdot b}{(a,b)}$ $(a,b) \mid b \Rightarrow \mu$ Vielf. von a
μ Vielf. von b
$\Rightarrow \mu$ gV (a,b)

Sei ν gV (a,b) ($\nu>0$ nach Def)

Betrachte $\frac{\nu}{\mu} = \frac{\nu(a,b)}{a \cdot b}$ Da $(a,b) = ax+by$ gilt

$\frac{\nu}{\mu} = \frac{\nu(ax+by)}{a \cdot b} = \underbrace{\frac{\nu \cdot x}{b}}_{\text{ganz}} + \underbrace{\frac{\nu y}{a}}_{\text{ganz}}$ ganz

$\Rightarrow$ jedes gemeinsame Vielfache von a, b ein Vielfaches von μ $\Rightarrow \mu$ kleinstes gemeins. Vielf.

d.h. $\mu = \frac{a \cdot b}{(a,b)} = \{a,b\}$ $\lrcorner$

Kor 4 | $\forall$ ggT (a,b) ist teilbar durch kgV (a,b)

Notat. | $a \neq 0$ ganz $\quad a = \prod_{\substack{p \text{ prim} \\ p \mid a}} p^{\alpha} \quad \alpha \geq 0$

$b = \prod p^{\beta} \quad \beta \geq 0$

Bem | $(a,b) = \prod p^{\min[\alpha,\beta]} \qquad \{a,b\} = \prod p^{\max[\alpha,\beta]}$

Bsp (1) | $91x + 221y = 1053$

$221 = 91 \cdot 2 + 39$
$91 = 39 \cdot 2 + 13$
$39 = 13 \cdot 3$ $\quad \rightsquigarrow (91,221) = 13$

wiederholte Anwendung d. Algorithm.

Bsp (2) $(a,b) = 1 \quad \rightsquigarrow (a+b, a-b) = \begin{cases} 1 \\ 2 \end{cases}$

(i) $a+b = a-b \Rightarrow b = 0$
$(a,b) = 1 \; b = 0 \Rightarrow a = \pm 1 \Rightarrow (a+b, a-b) = 1$

(ii) $a+b \neq a-b$
$(a+b, a-b) = d \Rightarrow d \mid a+b \quad d \mid a-b$
$\Rightarrow d \mid 2a \quad d \mid 2b$
$\Rightarrow d = 1, 2$

(vgl. Gruppentheorie)

Bsp (3) $ab' - a'b = \pm 1 \Rightarrow (a+a', b+b') = 1$ einfach? beweis

$(a,a') = 1 \; , \; (b,b') = 1 \quad (a,b) = 1, \; (a',b') = 1$

Bsp (4) $\alpha, \beta, \gamma, \delta$ ganz $\quad \alpha\delta - \beta\gamma = \pm 1$

$\Rightarrow (m,n) = (a,b)$ wobei $m = \alpha a + \beta \cdot b \quad n = \gamma a + \delta b$

S. 4. $\alpha a + \beta b = c\,(a,b)$
$\gamma a + \delta b = d\,(a,b)$

$(c,d) = 1$ denn $\alpha, \beta, \gamma, \delta$ paarw. teilerfremd

---

D | h, k ganz $\quad k > 0 \quad \frac{h}{k}$ irredu. $\Leftrightarrow (h,k) = 1$

eigentlich $\Leftrightarrow 0 \leq \frac{h}{k} \leq 1$

D | $n \geq 1$ n ganz

F_n := { alle eigentl. irredu. Brüche $\frac{h}{k}$ mit $1 \leq k \leq n$ in näml. aufsteig. Reihenfolge

heißt Farey folge von Ordnung n kan. Farey Brüche

F_1 : $\frac{0}{1}, \frac{1}{1}$

F_2 : $\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$ $\quad \frac{1}{3}, \frac{2}{3}, \frac{3}{3}$

F_3 : $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$ $\quad \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{5}{5}$

F_4 : $\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$

F_5 : $\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}$

Eulw: # Farey pnucle dn. $|F_n|$

$\sum_{k=0}^{n} e(k)$

Symmetrie

jede ration. Zahl $\frac{m}{n}$ $0 \le \frac{m}{n} \le 1$ ist gleich einem Fareybruch

S 8 (Farey-Cauchy 1816) sei $\frac{l}{m}$ unmittelbare Nachfolg von $\frac{h}{k}$ in der Fareyfolge F_N dann ist $kl - nm = 1$

$\left(\frac{h}{k} < \frac{l}{m} \right)$

Γ ist wahr für $1 \le n \le 5$

$\frac{h}{k}, \frac{l}{m}$ benachb. Brüche in F_N

sei $\frac{a}{b} \notin F_N \Rightarrow b \ge N+1$

$\frac{h}{k} < \frac{a}{b} < \frac{l}{m}$ o.B.d.A

(a) Definiere λ, μ $\quad \lambda := ka - hb$
$\mu := bl - am$

(ii) Dann gilt $\lambda \ge 0$ $\mu \ge 0$ $\lambda + \mu > 0$

(da nach Vor der Satz für F_N und $\frac{h}{k}, \frac{l}{m} \in F_N$
also:

$kl - nm = 1$ $\lambda + \mu = 0 \Rightarrow \begin{cases} \lambda = 0 \\ \mu = 0 \end{cases} \Rightarrow kl - nm =$

Sodann ist

$\lambda l + \mu h = kal - han\underline{m} = a\underbrace{(kl - nm)}_{1} = a$

analog

$\lambda m + \mu k = \ldots \ldots = b$

(iii) Ferner gilt $(\lambda, \mu) = 1$ da $(a,b) = 1$
$(h,k) = 1$
$(l,m) = 1$

also $\frac{h}{k} < \frac{a}{b} < \frac{l}{m}$ $(a,b) = 1$ $\frac{h}{k}, \frac{l}{m} \in F_N$

(iv) dann ist $\frac{a}{b} = \frac{\lambda l + \mu k}{\lambda m + \mu k}$ wobei $\lambda \ge 0$ $\mu \ge 0$
$\lambda + \mu > 0$
$(\lambda, \mu) = 1$

(v) umgekehrt: wenn λ, μ ganze Zahlen sind so dass $\lambda \ge 0$ $\mu \ge 0$ $\lambda + \mu > 0$ $(\lambda, \mu) = 1$
definiere wir

$a = \lambda l + \mu h$
$b = \lambda m + \mu k$

Dann ist eindeutig $\lambda = ka - hb$ (denn $(kl - nm = 1)$ $\mu = bl - am$.

und $(a,b) = 1$ also ist d. Bruch $\frac{a}{b}$ reduziert

und $\frac{h}{k} < \frac{a}{b} < \frac{l}{m}$ da $kl - nm = 1$ nach Vor

$\Rightarrow \frac{n}{m} < \frac{l}{m}$

Also ist $\frac{a}{b} \in F_N$ $N \geq N+1$ (d.h. $b \geq N+1$)

weiter, da $k>0$, $m>0$ $(\lambda,\mu)=1$ haben wir

$b \leq m+k \Leftrightarrow \lambda,\mu = \begin{matrix} 0,1 \\ 1,1 \\ 1,0 \end{matrix}$ sind $b = \lambda m + \mu k \leq m+k$
d.h. $(\lambda-1)m + k(\mu-1) \leq 0$

d.h. $a, b = \begin{matrix} h, k \\ \ell+h, m+k \\ \ell, m \end{matrix}$

Nun sind $\lambda \neq 0$, $\mu \neq 0$

denn $\lambda = 0 \Rightarrow \frac{a}{b} = \frac{\mu h}{\mu k}$ der reduziert ist nur wenn $\mu = 1$
und dies impliziert $h = k$ da $b = \lambda m + \mu k$
aber $h = k$ widerspricht Annahme $b \geq N+1 > k$
analog $\mu \neq 0$

(vi) Also $b \leq m+k \Rightarrow \lambda = \mu = 1$

(vii) Nun $\frac{a}{b} \in F_{N+1} \Rightarrow b = N+1$ denn $b \geq N+1$

aber $\frac{h+\ell}{k+m} \notin F_N$ denn $\frac{h}{k}, \frac{\ell}{m}$ Nachbarn in F_N

und

(viii) $\frac{h}{k} < \frac{h+\ell}{k+m} < \frac{\ell}{m}$ da $k\ell - hm = 1$ nach vor

Also $k+m \geq N+1$ $*$

(ix) $\frac{a}{b} \in F_{N+1} \Rightarrow (b = N+1) \Rightarrow b \overset{*}{\leq} m+k \overset{(vi)}{\Rightarrow} \lambda = \mu = 1$

so haben wir bewiesen dass $\frac{a}{b} \in F_{N+1} \Rightarrow a = h+\ell$

$b = k+m$ $\frac{a}{b} = \frac{h+\ell}{k+m}$

Dieser Bruch erfüllt auf keine seiner Nachbarn

$k(h+\ell) - h(m+k) = 1$ Nach vor $k\ell - nm = 1$

Also auf richtig i. F_{N+1} wenn für F_N

Bem.: Es folgt, dass jeder reduzierte Bruch eindeutig

$\frac{a}{b} = \frac{h+\ell}{k+m}$ Mediante

Die Mediante von zwei Nachbarn $\frac{h}{k}, \frac{\ell}{m} \in F_N$

ist $\frac{h+\ell}{k+m}$

Satz 9 Die Brüche von F_{N+1} die nicht zu F_N gehören sind Medianten von F_N

Satz 10 Sind $\frac{h}{k}, \frac{h''}{k''}, \frac{h'}{k'}$ aufeinanderfolg. Brüche derselben Farey folge, so ist $\frac{h''}{k''} = \frac{h+h'}{k+k'}$

Γ S.8 $\begin{matrix} kh'' - hk'' = 1 \\ k''h' - h''k' = 1 \end{matrix}$

subtr. $h''(k+k') - k''(h'+k') = 0$ ⌋

S.11 $\frac{h}{k}, \frac{l}{m}$ Nachbarn in F_N $\Rightarrow k+m \geq N+1$

S.12 $N > 1$ zwei Nachbarn in F_N haben nie denselben Nenner

$\vdash$ $k > 1$ $\frac{h'}{k}$ unmittelb. Nachfolg von $\frac{h}{k}$ in F_N

$\Rightarrow h-1 \leq h' < k$ ($h'=k$ $\frac{h'}{k} = 1 \Rightarrow k=1$)

Dann $\frac{h}{k} < \frac{h}{k-1} < \frac{h+1}{k} \leq \frac{h'}{k}$

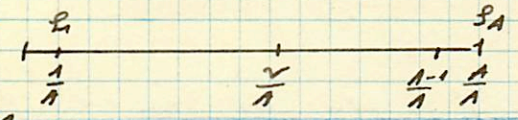
also $\frac{h}{k-1}$ in F_N zwischen $\frac{h}{k}, \frac{h'}{k}$ $\lightning$ $\dashv$

bekannt. ungel. Problem

F_N : $0 < \frac{h}{k} \leq 1$ $(h,k)=1$

A # Farey-Brüche in F_N (ohne 0)

$= \varphi(1) + \varphi(2) + \dots + \varphi(N)$



$g_\nu - \frac{\nu}{A} =: \eta_\nu = \eta_\nu(N)$

$\sum_{\nu=1}^{A} \eta_\nu^2(N) = ? \quad << N^{-1+\varepsilon} \quad \forall \varepsilon > 0$ (Cauchy)

$\Longleftarrow$ Riemannsche Vermutung $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ $\Re s > \frac{1}{2}$

Franel (1900)

andere Form d. Riem. Hypothese

$\forall \varepsilon > 0 \; \exists A \; \forall N \geq A : \left| \sum_{k=1}^{N} \mu(k) \right| < N^{1/2+\varepsilon}$

Dritter Bew v. Satz 2

genügt (Satz 6) $ax+by=1$ in $\mathbb{Z}$ x,y lösbar $(a,b)=1$

Beh. trivial, falls $a=b$ oder $a \cdot b = 0$ also

o.F.d.A. $b > a > 0$ $(a,b)=1$

Betrachte $\frac{a}{b} \in F_b$ sei $\frac{h}{k}$ unmittl. Vorg. von $\frac{a}{b}$ in F_b

$\overset{S8}{\Longrightarrow}$ $ka - hb = 1$ $x = k$, $y = -h$ ist eine Lösung

Primzahlen

S13 Euklid # Primzahlen ist unendlich

$\vdash$ Ann. p größte Primzahl

$2 \cdot 3 \cdot 5 \cdots p + 1 = q$

q nicht teilbar (kein dieser Primz.) $q > 1$

$\Rightarrow$ q Primzahl $> p$ oder q ist d. Primz. größer als p teilbar. $\lightning$ $\dashv$

Bem p_n n-te Primzahl

$\overset{S}{\Longrightarrow}$ folgt S3 $p_m \mid \left(\prod_{n=1}^{n} p_n\right) + 1$ $m > n$

$\leq p_n^n + 1$ $n \geq 1$ ($< n^{n+1}$

Kor 1 $p_{n+1} \le p_n \le p_n^n + 1 \quad n \ge 1$

$p_{n+1} \le p_1 \cdots p_n + 1 \quad n \ge 1$

Kor 2 $p_{n+1} \le p_1 \cdots p_n - 1 \quad n > 1$

Γ $Q = p_1 \cdots p_n - 1 \quad \Rightarrow Q > 1 \quad n \ge 1$
Q Primz. oder teilb. d. Primzahl $\neq p_1, \ldots p_n$
$\Rightarrow p_{n+1} \le p_1 \cdots p_n - 1 \quad n > 1$ $\lrcorner$

Kor 3 $p_n \le 2^{2^{n-1}} \quad n \ge 1 \qquad (p_n < 2^{2^{n-1}} \quad n > 1)$

Γ $p_1 \le 2 \quad p_2 \le 2^2 \quad p_3 \le 2^4 \ldots p_n \le 2^{2^{n-1}}$
$\Rightarrow p_{n+1} \le p_1 \ldots p_n + 1 \le 2^{1+2+4\ldots 2^{n-1}} + 1 =$
$= 2^{(2^n - 1)} + 1 = \frac{1}{2} 2^{2^n} + 1 < 2^{2^n}$ $\lrcorner$

D f_n ganz $\Leftrightarrow$ f_n Fermatzahl $\Leftrightarrow f_n = 2^{2^n} + 1 \quad n \ge 1$

$f_1 = 5 \quad f_2 = 17 \quad f_3 = 257 \quad f_4 = 65536$ prim
f_5 nicht prim (Euler) Heisenn: 100 895 598 169
Fermat = 8 988 423 = 112 303

Satz 14 (Polya 1925) Zwei versch. Fermatzahlen sind teilerfremd.

Γ $f_n, f_{n+k} \quad k > 0$ beliebig
$\Rightarrow$ teilerfremd $\exists m > 0$ $m \mid f_n \quad m \mid f_{n+k}$

$$\frac{f_{n+k} - 2}{f_n} = \frac{2^{2^{n+k}} + 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} \qquad x = 2^{2^n}$$
$$= x^{2^k - 1} - x^{2^k - 2} \ldots - 1 \quad \text{ganze Zahl}$$

d.h. $f_n \mid f_{n+k} - 2$ wie $m \mid f_n$ also $m \mid f_{n+k} - 2$
$\Rightarrow m \mid 2$ da $m \mid f_{n+k} \Rightarrow m = 1$ $\lrcorner$

Bem $f_1 \ldots f_{11}$ alle ungerade
$\Rightarrow$ jedes f_n teilbar durch ungerade Primzahl
die f_5 St. Lassen nicht teilen kann

Kor 1 Es existi mind n ungerade Primzahlen $\le f_n \quad n \ge 1$

$p_1 = 2 \Rightarrow p_{n+1} \le f_n \quad n \ge 1$

Definiere $f_0 \equiv 3$

$\Rightarrow p_{n+2} \le f_n = 2^{2^n} + 1 \quad n \ge 0$

(Euler: $p_{n+2} \le 2^{2^{n+1}}$!)

Kor 2 f_5 nicht prim (Euler)

Euklid 300 BC
Diophant 300 n.C.
Fermat 1601 - 665
Euler 1707 - 1783

Γ $f_5 = 2^{32} + 1 = (2 \cdot 2^7)^4 + 1 \quad a := 2^7 \quad b := 5$
$f_5 := (20)^4 + 1 = 2^4 a^4 + 1 \qquad 2^4 = 1 + 3 \cdot b = 1 + b(a - b^3)$
$\Rightarrow f_5 = (1 + ab - b^4) a^4 + 1 = (1 + ab) a^4 + \frac{1 - a^4 b^4}{(1+ab)(1+ab)(1+a^2b^2)}$
$= (1 + ab)[a^4 + (1 - ab)(1 + a^2 b^2)]$
$1 + ab = 641 \qquad f_5 = 641 \cdot 6700417$

Kap II Kongruenzen

1)

a, b ganz $\quad m > 0$

$a \equiv b \mod m \iff m \mid a-b$
$a \not\equiv b \mod m \iff m \nmid a-b$

$\equiv$ Äqu.-rel. also teilt "$\equiv_{(m)}$" die ganzen Zahlen in disjunkte Äquiv.klassen A, B, C ein.
$a \equiv b \ (m) \iff$ sie liegen in gl. Restklasse mod m

$0, 1, 2, \ldots m-1$ liegen in versch. Restklassen
$n = q\,m + r$ Divis. algorithm. $\Rightarrow \exists$ m Restklassen mod m
$0, \ldots m-1$ bilden Repräsent. system

$a \equiv b \ (m) \quad c \equiv d \ (m) \Rightarrow a+c \equiv b+d \ (m)$
$a-c \equiv b-d \ (m)$
$ac \equiv bd \ (m)$

$m \mid (a-b), m \mid (c-d) \Rightarrow m \mid (a-b) \pm c-d$
$m \mid (a-b) \Rightarrow m \mid (a-b)c \Rightarrow ac \equiv bc \ (m)$
$m \mid (c-d) \Rightarrow m \mid (c-d)b \Rightarrow bc \equiv bd \ (m)$ $\Big\} \Rightarrow ac \equiv bd$

$4 \equiv 12 \ (8) \not\Rightarrow 1 \equiv 3 \ (8)$

Die Regeln zeigen, dass für beliebige Elemente $a \in A$, $b \in B$ die Summe $a+b$ immer in derselben Restklasse liegt bezeichnet mit $A+B$ Analog $A-B$, AB
Folglich bilden die Restklassen mod m eine additive Abelsche Gruppe mit Nullelement $0 = \{km\} \ k \in \mathbb{Z}$ während das Inverse $A' = \{-a\}$ $a \in A$.

$ax \equiv c \ (\mathrm{mod}\, m) \iff ax - my = c$ lineare Kongruenz

nach Kap I S. 5 hat diese Gl. Lösbar $\iff (a,m) = 1$
Ferner ist diese Lösung bis auf Kongruenz eindeutig
$ax_1 \equiv c \ (m)$
$ax_2 \equiv c \ (m) \iff a(x_1 - x_2) \equiv 0 \mod m \Rightarrow m \mid (x_1 - x_2)$ da $(a,m) = 1$
ist x_0, y_0 eine spezielle Lösung d. gleich. $ax + by = n$ $(a,b) = 1$
so wird die allgem. Lösung $x = x_0 - bt$
$y = y_0 - at$

In anderen Worten: sind A, C, x Restklassen mod m, besitzt die Gleichung $Ax = C$ eine einzige Lösung x falls die Elem. von A zu m teilerfremd.
Dies: Restklassen die teilerfremd zu m sind bilden primitive Restklassen.
Sie bilden eine abelsche Gruppe bez. Multiplik. Einheit: Restkl. mit 1
jede primit. Restkl. besitzt Inverses, denn $(a,m) = 1 \Rightarrow \exists\, a'$ $aa' \equiv 1 \ (m)$.
Betrachte additive abelsche Gruppe aller Restkl. modulo Primzahl p.
Mit Ausnahme d. Nullklasse sind alles primit. Restklassen, und bilden auch eine multipl. abelsche Gruppe. Distribut. unmittelbar induziert d. Distribut. für ganze Zahlen.

Satz 1 Die Restklassen d. ganzen Zahlen modulo Primzahl p bilden einen Körper von p Elementen.

Restsysteme

Ein vollständ. Restsystem mod m (VRS) besteht aus einem Repräsentant jeder Restklasse: also hinden m ganze Zahlen jenen dann ein vollst. Restsystem modm, wenn sie paarweise inkongruent mod m sind. Hingegen besteht ein primes Restsystem mod m aus einem Repräsentant jeder primen Restklasse aus m

z.B $0, 1, 2, 3, 4, 5$ VRS zu 6
$1, 5$ primes RS $\mod 6$

D Die Eulersche Funktion $\varphi(n) := \#$ primit. Restklassen mod m

z.B. $\varphi(p) = p-1$ p Primzahl

Die Sätze von Fermat und Euler

$m \geq 1$ m ganz $a_1, a_2, \dots a_m$ VRS (m)
$(a_i, m) = 1$
$ka_1, ka_2 \dots ka_m$ VRS (m) da auch paarw. inkongruent
Allgm: k beliebig ganz. Dann bilden $ka_j + th$ $(j = 1 \dots n)$
Vollsd. Restsystem.
Bilden die Zahlen $r_1, r_2 \dots r_{\varphi(m)}$ ein primes Restsystem mod m und $(a, m) = 1$, so bilden auch die Zahlen $ar_1, ar_2, \dots ar_{\varphi(m)}$ primit. Restsystem, folglich $r_1 r_2 \dots r_{\varphi(m)} \equiv ar_1 \dots ar_{\varphi(m)} \pmod m$
d.h. $a^{\varphi(m)} - 1 \cdot r_1 r_2 \dots r_{\varphi(m)} \equiv 0 \pmod m$
$\Rightarrow a^{\varphi(m)} - 1 \equiv 0 \pmod m$ da $(r_i, m) = 1$ $\forall i \leq \varphi(m)$

Satz 2 Euler
$m \geq 1$ $(a, m) = 1$
$\Rightarrow a^{\varphi(m)} - 1 \equiv 0 \pmod m$

Satz 3 Fermat
p prim $(a, p) = 1$
$\Rightarrow a^{p-1} - 1 \equiv 0 \pmod p$

Bem (i) Es existieren zusammengesetzte Zahlen für welche $a^{n-1} \equiv 1 \pmod n$

? für wieviele Zahlen gilt die Umkehrung (Pseudoprimzahlen)

$a = 2$ $n = 341 = 11 \cdot 31$
$\Rightarrow 2^{340} \equiv 1 \pmod{341}$
$340 = 17 \cdot 20 = 34 \cdot 10$
$2^5 = 32 \equiv 1 \pmod{31}$
$(2^5)^{4 \cdot 17} \equiv 1 \pmod{31}$
$2^{10} \equiv 1 \pmod{11}$
$(2^{10})^{2 \cdot 17} \equiv 1 \pmod{11}$

Bem (ii) Jede Primzahl $\neq 2, 5$ ist ein Faktor von unendl. vielen ganz. Zahlen d. Form 9999...

$p \neq 2, 5$ p prim $(10, p) = 1$
Fermat $\Rightarrow (10^n)^{p-1} \equiv 1 \pmod p$

(iii) $n^{13} - n$ hat Faktor $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$

$n^{13-1} \equiv 1 \pmod{13}$ $13 \nmid n$
also $n(n^{12} - 1) \equiv 0 \pmod{13}$ $\forall n$
$\Rightarrow n^{13} - n \equiv 0 \pmod{13}$

Aber $n(n^{12} - 1) = n(n^6 - 1)(n^6 + 1)$
$n^6 - 1 \equiv 0 \pmod 7$ falls $7 \nmid n$
$n(n^6 - 1) \equiv 0 \pmod 7$
$\Rightarrow n^{13} - n \equiv 0 \pmod 7$

n gerade $2 \mid n$
n ungerade $\Rightarrow n^3$ ungerade $\Rightarrow n^3 + 1$ gerade
$\Rightarrow 2 \mid n^3 + 1 \Rightarrow 2 \mid n^6 - 1$
$\Rightarrow n^{13} - n \equiv 0 \pmod 2$

$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1)$
$n^4 - 1 \equiv 0 \pmod 5$
$n(n^2 - 1) = n(n-1)(n+1) \equiv 0 \pmod 3$

Satz 4 $(m,m')=1$ durchläuft a ein Vollst. Restsyst. mod m und a' ein VRS mod m' so durchläuft $am'+a'm$ ein VRS mod mm'

Beweis

Es gibt $m\cdot m'$ Zahlen $\{am'+a'm\}$ und je zwei sind inkongruent mod mm', denn

$$a_1'm + a_1m' \equiv a_2m + a_2m' \mod mm'$$

$$\Rightarrow a_1m' \equiv a_2m' \mod m$$

da $(m,m')=1$ folgt $a_1 \equiv a_2 \mod m$

Analog ist $a_1' \equiv a_2' \mod m'$ ↯ ∎

Def Eine zahlth. Funktion ist eine komplexwert. Funktion, die für jede posit. ganze Zahl def. ist. $\mathbb{N} \to \mathbb{C}$

Eine zahlth. Funktion f ist multiplikativ, falls

(1) $f \not\equiv 0$

(2) $(m,n)=1 \Rightarrow f(m\cdot n) = f(m)\cdot f(n)$

Eine zahlth. Fkt. f heißt total multiplikativ, falls

(1) $f \not\equiv 0$ (2) $f(m\cdot n) = f(m)\cdot f(n)$

S5 φ ist multiplikativ

(i) $\varphi(1)=1$

(ii) $(m,m')=1$ $a \in$ VRS (mod m), $a' \in$ VRS (mod m')

$\Rightarrow am'+a'm \in$ VRS (mod mm') (Satz 4)

zu zeigen $\varphi(m)\varphi(m') = \varphi(mm')$

suchen $(am'+a'm, mm') = 1$

$\Leftrightarrow (am'+a'm, m)=1 \wedge (am'+a'm, m')=1$

$\Leftrightarrow (am', m)=1 \wedge (a'm, m')=1$

$\Leftarrow (a,m)=1 \wedge (a',m')=1$

$\exists\, \varphi(m)$ Zahlen a, $\exists\, \varphi(m')$ Zahlen a' $\Rightarrow \exists\, \varphi(m)\varphi(m')$ Zahlen im prim VRS mod m

Frage Wie oft muss man φ iterieren um nach 1 zu gelangen?

S4' $(m,m')=1$ a, a' durchlaufen prim. RS (mod m) rsp. mod m'

$\Rightarrow am'+a'm$ durchläuft prim. Restsystem mod (mm')

Bem $n>1$ $n = \prod_{i=1}^{r} p_i^{a_i}$ kan. Zerleg.

S.5. $\Rightarrow \varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{a_i}) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i-1})$

$= \prod_{i=1}^{r} p_i^{a_i}(1-\frac{1}{p_i}) = m \prod_{p/m} (1-\frac{1}{p})$

$a=1$: $\varphi(p)=p-1$

$a>1$: $\varphi(p^a) = p^a - p^{a-1}$ $= p^a(1-\frac{1}{p})$

herauslr. V.R.S. mod p^a: $1, 2, 3, \dots p^{a-1}$

genau p^{a-1} diese Zahlen sind zu p nicht teilerfremd nämlich $p, 2p, 3p, \dots p^a$

$$\varphi(n) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Satz 6 $$n = \sum_{d \mid n} \varphi(d)$$

Γ $n = \prod_{i=1}^{r} p_i^{a_i}$

$d \mid n \Rightarrow d = \prod_{i=1}^{r} p_i^{b_i} \qquad 0 \le b_i \le a_i$

$$\sum_{d \mid n} \varphi(d) = \sum_{0 \le b_i \le a_i} \varphi\left(\prod_{i=1}^{r} p_i^{b_i}\right) = \sum_{0 \le b_i \le a_i} \prod_{i=1}^{r} \varphi(p_i^{b_i})$$

$$= \prod_{i=1}^{r} \sum_{b_i=0}^{a_i} \varphi(p_i^{b_i}) = \prod_{i=1}^{r} (\varphi(1) + \varphi(p_i) + \ldots + \varphi(p_i^{a_i}))$$

$$= \prod_{i=1}^{r} \left[1 + (p_i - 1) + p_i(p_i - 1) + \ldots + p_i^{a_i - 1}(p_i - 1)\right]$$

$$= \prod_{i=1}^{r} p_i^{a_i} = n \qquad \square$$

Bsp $\begin{cases} x^2 \equiv 2 \bmod 3 \\ x^3 \equiv 3 \bmod 13 \end{cases}$ keine Lösung

Satz 7 Lagrange

1) die Kongruenz $a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \bmod p$ (1)
$(a_0, p) = 1$ ($a_0, a_1, \ldots a_n$ ganz) $n \ge 1$ p prim
hat höchstens n Lösungen

Bem x Lösung $\Rightarrow \forall y \; y \equiv x \; (p)$ y Lösung
denn $\Rightarrow x - y = mp \Rightarrow y = x - mp$
$\rightarrow y^n = (x - mp)^n$

Deshalb berechnet man die # Lösungen # Restklassen deren Elemente die Kongr. erfüllen.
Also: die # Lösungen = # Nullstellen eines NRS mod p Kongruenz mod irgend Primzahl. Andererseits ist

$x^{p-1} \equiv 1 \bmod p$ hat die $p-1$ Lösungen $1, \ldots, p-1$
$\rightarrow x(x^{p-1} - 1) \equiv 0 \bmod p$ $\forall x$ ganz
$\rightarrow x^p = x \bmod p \quad \forall x$
$x^{p+1} \equiv x^2 \bmod p \quad \forall x$

jede Kongr. $n > p-1$ lässt sich reduzieren.
Deshalb o.B.d.A. $n \le p-1$

Ferner nennen wir $(a_0, p) = 1$ damit grad d. Kongr. n

Γ $(a_0, p) = 1 \Rightarrow$ Satz richtig für $n = 1$

Falls (1) keine Lösung $\Rightarrow$ Satz richtig
hat (1) eine Lösung $\Rightarrow a_0 x_1^n + a_1 x_1^{n-1} + \ldots + a_n \equiv 0 \; (p)$ (2)

(3) = (1) − (2): $a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + \ldots + a_{n-1}(x - x_1) \equiv 0 \bmod p$

Die Differenz durch jede Lösung von (1) reduziert wird die (3) lässt sich darstellen als

$$(x - x_1)(a_0 x^{n-1} + b_1 x^{n-2} + \ldots + b_{n-1}) \equiv 0 \bmod p$$

$b_1, \ldots, b_{n-1}$ ganze
die v. x_1 u. $a_0, a_1, \ldots a_n$
abhängen

Folglich befriedigt jede Lösung von (1) entweder die Kongr. $(x - x_1) \equiv 0 \pmod p$, welche ungl. Lösung $\pmod p$ $x = x_1$ liefert oder eine Kongruenz $a_0 x^{n-1} + \ldots + b_{n-1} \equiv 0 \; (p)$

die nach Induv. höchst. $n-1$ Lösungen hat.
Somit besitzt (1) höchst. n Lösungen ⊥

Kor 1

Falls die Kongr.

$a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \mod p$ p prim

$\Rightarrow p \mid a_0, p \mid a_1, \dots p \mid a_n$

mehrfach als n Lösungen hat

Γ a_i erste Koeff. mit $(a_i, p) = 1$ $i \geq 0$
$\Rightarrow a_i x^{n-i} + \dots + a_n \equiv 0 \ (p)$ hat mehr als n Lösungen ↯ ⊥

Kor 2

$f(x) = x^{p-1} - 1 - (x-1)(x-2)\dots(x-p-1)$

ein Polynom vom Grad $p-2$

Fermat: $x^{p-1} - 1 \equiv 0 \ (p)$ $x = 1, 2, \dots p-1$
seine verschwindet das Produkt
$(x-1)(x-2)\dots(x-p-1)$

Folglich ist $f(x) \equiv 0 \mod p$ für $x = 1, 2, \dots p-1$
Nach Kor 1 sind alle Koeff. durch p teilbar
d.h. $f(x) = p\,\varphi(x)$ wobei $\varphi(x)$ Polynom mit ganzen Koeff.

Folglich $x^{p-1} - 1 = (x-1)(x-2)\dots(x-p-1) + p\,\varphi(x)$
setze $x = p$
$\Rightarrow p^{p-1} - 1 = 1 \cdot 2 \cdot 3 \cdot \dots (p-1) + p\,\varphi(p)$
$\Rightarrow (p-1)! \equiv -1 \mod p$

Satz 8 Wilson

$(p-1)! + 1 \equiv 0 \pmod p$

die Bedingung ist auch hinreichend!

$p = qr$ $1 < q < p$ q kommt im Prod. $1 \cdot 2 \dots p-1$ vor
$(p-1)! + 1 \equiv 0 \mod q$ ist unmöglich

kap III Diophantische Approximation

ξ reell $\neq 0$

ξ rational $\Rightarrow \xi = \frac{a}{b} = \frac{h}{k}$ $(h,k)=1$ a,b,h,k ganz $k \neq 0$

ξ irrational sonst

ξ reduziert $\xi = \frac{h}{k}$ $(h,k)=1$

ξ eigentlich $\xi = \frac{h}{k}$ $0 < \frac{h}{k} < 1$

ration Zahl dicht in $\mathbb{R}$ $\forall \varepsilon \; \forall \xi \in \mathbb{R} \; \exists \frac{h}{k} \; |\xi - \frac{h}{k}| < \varepsilon < 1$

ξ reell $[\xi] = \max\{n \in \mathbb{Z} \mid n \leq \xi\}$

$\xi - [\xi] =: \{\xi\}$ gebrochen. Teil $0 \leq \{\xi\} < 1$

o.B.d.A $0 < \xi < 1$ suchen $\frac{h}{k}$ $(h,k)=1$ $0 < \frac{h}{k} < 1$ mit $|\xi - \frac{h}{k}|$ klein

Approximation mit eigentl. reduz. ration. Zahlen

S1 ξ irrat. Zahl $N > 0$ N ganz $\Rightarrow \exists \frac{h}{k}$ $k \leq N$ $|\xi - \frac{h}{k}| < \frac{1}{k \cdot N}$

Schubfachprinzip

Betrachte $\{n\xi\} \neq 0,1$ da ξ irrat. $\Rightarrow \{n\xi\} \in (0,1)$
$n = 1,2 \ldots N \rightarrow$ haben N versch. Zahlen $\{n\xi\} \in (0,1)$

Betrachte $(0, \frac{1}{N}) \; (\frac{1}{N}, \frac{2}{N}) \ldots (\frac{N-1}{N}, 1)$

In jedem solchen Intervall liegt entweder genau eine d. Zahlen $\{n\xi\}$ oder $\exists$ Teilintervall mit mind. 2 solchen Zahlen (Schubfachprinzip)

(i) $0 < m\xi - [m\xi] < \frac{1}{N}$ $\quad m \leq N$, $m \in \mathbb{N}$

$0 < \xi - \frac{[m\xi]}{m} < \frac{1}{Nm}$

$=: \frac{n}{k}$

(ii) In $(0, \frac{1}{N})$ / $\exists$ kein $\{m\xi\}$

$\Rightarrow$ sagenwir $\{n\xi\}$ und $\{m\xi\}$ im gleichen Intervall

$\Rightarrow$ haben $0 < m < n \leq N$ mit $|(n\xi - [n\xi]) - (m\xi - [m\xi])| < \frac{1}{N}$

oder $|\underbrace{(n-m)}_{:=k}\xi - (\underbrace{[n\xi] - [m\xi]}_{:=h})| < \frac{1}{N}$

$k = n - m < N$

$\Rightarrow |\xi - \frac{h}{k}| < \frac{1}{kN}$ ∎

S2 ξ irrat. Zahl $N > 0$ N ganz $\Rightarrow \exists \frac{h}{k}$ $k \leq N$ $|\xi - \frac{h}{k}| < \frac{1}{k(N+1)}$

(Farey Folgen)

F_N Fareyfolge von Ordnung N
ξ irrational $\Rightarrow \xi \notin F_N$ $\forall N \geq 1$
ξ liegt zwischen zwei Nachbarn $\frac{a}{b}, \frac{c}{d}$ in F_N
$\frac{a}{b} < \xi < \frac{c}{d}$ $\quad \frac{a+c}{b+d}$ Mediante von $\frac{a}{b}, \frac{c}{d}$

wissen $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d} \Rightarrow$ (1) $\frac{a}{b} < \xi < \frac{a+c}{b+d}$ v (2) $\frac{a+c}{b+d} < \xi < \frac{c}{d}$

$\notin F_N \Rightarrow b+d > N+1$

① $\Rightarrow 0 < \xi - \frac{a}{b} < \frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} \overset{\text{ganzzahlig}}{=} \frac{1}{b(b+d)} \leq \frac{1}{b(N+1)}$

② $0 < \frac{c}{d} - \xi < \frac{c}{d} - \frac{a+c}{b+d} = \frac{bc-ad}{d(b+d)} = \frac{1}{d(b+d)} < \frac{1}{d(N+1)}$ ✓

Bem $N \geq k$ und damit:

Satz 2' ξ irrational $\Rightarrow \exists$ unendl. viele rat. Zahlen $\frac{h}{k}$
$\left|\xi - \frac{h}{k}\right| < \frac{1}{k^2}$

Bem ξ rational $\xi = \frac{l}{m}$ $(l,m)=1$ $m > N$
$\Rightarrow \xi \notin F_N \Rightarrow \xi \notin F_m$ $1 \leq m \leq N$
Der Fall $\xi = \frac{a+c}{b+d}$ kann eintreten, daher können nicht strikte ungl. haben

Satz 3 N posit. ganze Zahl $\xi = \frac{l}{m}$ $(l,m)=1$ $m > N$
$\Rightarrow \exists$ rat. Zahl $\frac{h}{k}$ mit $k \leq N$ derart
$\left|\frac{l}{m} - \frac{h}{k}\right| \leq \frac{1}{k(N+1)}$ (wie in Satz 2)
Gleichheit: $m = N+1$

Summen v. Quadraten

Satz 4 n, A positive ganze Zahlen
$n \mid (A^2+1)$ $\Leftrightarrow \exists s, t \in \mathbb{Z}$ $n = s^2+t^2 \wedge (s,t) = 1$

Γ $1 = 1^2+0^2$ nimm $n \geq 2$

$N := [\sqrt{n}] \Rightarrow n > N$ $n \geq 2$

$n \mid A^2+1 \Rightarrow (n,A) = 1 \Rightarrow \frac{A}{n}$ reduziert mit $n > N$

S3 $\Rightarrow \exists \frac{r}{s}$ reduz. $\left|\frac{A}{n} - \frac{r}{s}\right| \leq \frac{1}{s(N+1)}$ $0 < s \leq N$

$\Rightarrow |As - nr| \leq \frac{n}{N+1} = \frac{n}{[\sqrt{n}]+1} < \sqrt{n}$

setze $t = As - rn$ $|t| < \sqrt{n}$

Dann $s^2+t^2 = s^2+(As-rn)^2 = s^2(A^2+1) - 2Asrn + r^2n^2$

(1) ⊢ Da $n \mid (A^2+1)$ $\boxed{n \mid s^2+t^2}$ (*)

Aber $0 < s \leq N < \sqrt{n}$ $|t| < \sqrt{n}$

$\Rightarrow \boxed{0 < s^2+t^2 < 2n}$ (**)

(*) (**) $\Rightarrow s^2+t^2 = n$

(2) ⊢

Zu zeigen noch $(s,t) = 1$
$(s,t) = (s, As-rn)$ $(r,s)=1$ ($\frac{r}{s}$ reduz.)
$\Rightarrow (s,t) = (s,n)$

$n = s^2+t^2 = s^2(A^2+1) = 2Asrn + r^2n^2$
$1 = \frac{s^2(A^2+1)}{n} - 2Asr + r^2n$

Nach vor $\frac{A^2+1}{n} \in \mathbb{Z} \Rightarrow gT(s,n) \mid 1$ $\Rightarrow (s,n) = 1$
$\Rightarrow (s,t) = 1$ ✓

Kor $n \mid A^2+B^2 \quad n>1 \quad (A,B)=1$
$\Rightarrow s,t \in \mathbb{Z} \quad n = s^2+t^2$

⌜ $(A^2+B^2)(C^2+D^2) = (AD+BC)^2 + (AC-BD)^2$

$(A,B)=1 \Rightarrow \exists\, C,D \quad AC-BD=1$

$\Rightarrow (A^2+B^2)(C^2+D^2) = (AD+BC)^2+1$

$\Rightarrow n \mid (AD+BC)^2+1$

$s4 \quad n = s^2+t^2$ ⌟

/ Anwend. $\exists$ ∞ viele Primzahlen d. Form $4k-1$, $4k+1$?

Satz 5 $\exists$ ∞ viele Primz. d. Form $4k-1$

⌜ $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ endl. viele Primz. d. Form $4k-1$
$N := 4 \cdot q_1 \cdot q_2 \cdots q_r - 1 = 4k-1$
Teiler von d. Form $4k-1$, $4k+1$ aber nicht alle von d. Form $4k+1$ ⌟

Satz 6 $\exists$ ∞ viele Primz. d. Form $4k+1$

⌜ $5, 13, 17, \ldots p$ größte Zahl

$4 \cdot (5 \cdot 13 \cdots p)^2 + 1$
jeder Primteiler q ungerade
$s.A. \quad q = s^2+t^2$ s,t ganz
o.B.d.A $s=0$ (4) $\quad t=1$ (4) $\rightarrow q \equiv 1$ (4)
d.h. jeder Primteiler hat Form $4k+1$
↯ denn $N>1$ und kann auch keine d. Primzahlen $5, 13 \ldots p$ teilbar, die nach Annahme die einzigen d. Form $4k+1$ sind ⌟

ohne diese Satz beweise Gaußsche reziprozitätsg.

Satz 7 $0 < \xi < 1$ ξ irrat. $\Rightarrow$ ∃ unendl. viele reduz. Brüche $\frac{h}{k}$
$\left|\xi - \frac{h}{k}\right| < \frac{1}{2k^2}$

⌜ F_N Farey-folge von Ordnung $N>1$
$\Rightarrow \xi$ liegt zwischen zwei Nachbarn in F_N, sagen wir
$\frac{a}{b} < \xi < \frac{c}{d} \quad \frac{a}{b}, \frac{c}{d} \in F_N$

Dann gilt entweder $\xi - \frac{a}{b} < \frac{1}{2b^2}$ oder $\frac{c}{d} - \xi < \frac{1}{2d^2}$

sonst: $\xi - \frac{a}{b} > \frac{1}{2b^2}$ und $\frac{c}{d} - \xi > \frac{1}{2d^2}$ damit

$\frac{c}{d} - \frac{a}{b} > \frac{1}{2d^2} + \frac{1}{2b^2}$ d.h. $\frac{bc-ad}{bd} = \frac{1}{bd} > \frac{b^2+d^2}{2(b^2d^2)}$

d.h. $(b-d)^2 < 0$ ↯

$\frac{h}{k} \in \left(\frac{a}{b}, \frac{c}{d}\right)$

ferner gilt: $\left|\xi - \frac{h}{k}\right| < \frac{c}{d} - \frac{a}{b} = \frac{1}{bd} \leq \frac{1}{b+d-1} \leq \frac{1}{N}$

denn $d(b-1) \geq b-1$ und $b+d \geq N+1$
$db \geq d+b-1$
da $b+d$ kleiner d. nächsten Nachbarn
$\frac{a+c}{b+d} \notin F_N$

⌟

Satz 8 (Hurwitz) ETH

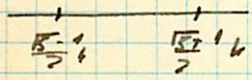
ξ irrational $\in (0,1)$
$c > 0$ $c \le \sqrt{5}$
Dann existi unendl. viele rationale reduzierte Zahlen $\frac{h}{k}$, so dass $|\xi - \frac{h}{k}| < \frac{1}{ck^2}$

Falls $c > \sqrt{5}$ $\exists$ ξ irration. für die Ungl. nur für endl. viele rationale $\frac{h}{k}$ gilt

Lemma (Khintchin) Sei $N > 1$ F_N Farey-Folge von Ordn. N
$\frac{h}{k}, \frac{h'}{k'}$ Nachbarn in F_N $\frac{h}{k} < \xi < \frac{h'}{k'}$

Wir können annehmen entweder $k' > \frac{\sqrt{5}+1}{2} k$ oder $k' < \frac{\sqrt{5}-1}{2} k$

$\Rightarrow k > \frac{2}{\sqrt{5}-1} k' = \frac{\sqrt{5}+1}{2} k'$



denn falls $\frac{\sqrt{5}-1}{2} k < k' < \frac{\sqrt{5}+1}{2} k$

$\Rightarrow k + k' > \left(\frac{\sqrt{5}+1}{2}\right) \max(k, k')$ Γ $\left(\frac{\sqrt{5}-1}{2}\right) k + k < k' + k$
$\left(\frac{\sqrt{5}+1}{2}\right) k < k' + k$
$k > \frac{2k'}{\sqrt{5}+1} = \frac{\sqrt{5}-1}{2} k'$
$k + k' > \frac{\sqrt{5}+1}{2} k'$ $\lrcorner$

wir können F_N durch F_M $M = k+k'$ ersetzen, und $\frac{h}{k}$ (oder $\frac{h'}{k'}$) durch die Mediane $\frac{h+h'}{k+k'}$ von F_N also $k + k' \ge N+1$

Setze $\frac{k'}{k} = \omega$. Dann haben wir entweder

$\omega > \frac{\sqrt{5}+1}{2}$ oder $\omega < \frac{\sqrt{5}-1}{2}$

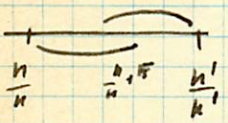
Jedenfalls haben wir $1 + \frac{1}{\omega^2} > \frac{\sqrt{5}}{\omega}$ $*$

denn $\frac{1}{\sqrt{5}}\left(1 + \frac{1}{\omega^2}\right) - \frac{1}{\omega} = \frac{1}{\sqrt{5}\omega^2}\left(\omega^2 - \sqrt{5}\omega + 1\right)$

$= \frac{1}{\sqrt{5}\omega^2}\left(\omega - \frac{\sqrt{5}+1}{2}\right)\left(\omega - \frac{\sqrt{5}-1}{2}\right) \overset{*}{>} 0$

Folglich $\frac{1}{\sqrt{5}}\left(\frac{1}{k^2} + \frac{1}{k'^2}\right) = \frac{1}{\sqrt{5}k'^2}\left(1 + \frac{1}{\omega^2}\right) \overset{*}{>} \frac{1}{\omega k^2}$

also $\frac{h'}{k'} - \frac{h}{k} = \frac{1}{k'k} = \frac{1}{k^2\omega} < \frac{1}{\sqrt{5}}\left(\frac{1}{k^2} + \frac{1}{k'^2}\right)$



Das impliziert $\frac{h'}{k'} - \frac{1}{\sqrt{5}k'^2} < \frac{h}{k} + \frac{1}{\sqrt{5}k^2}$

entweder $\left(\frac{h}{k}, \frac{h}{k} + \frac{1}{\sqrt{5}k^2}\right)$ oder $\left(\frac{h'}{k'} - \frac{1}{\sqrt{5}k'^2}, \frac{h'}{k'}\right)$ enthält ξ

d.h. $\exists \frac{a}{b} \left(= \frac{h}{k}$ oder $\frac{h'}{k'}\right)$ $\left|\xi - \frac{a}{b}\right| < \frac{1}{\sqrt{5}b^2}$

denn $\frac{h'}{k'} - \frac{h}{k} = \frac{1}{kk'}$ also $\left|\xi - \frac{a}{b}\right| < \frac{1}{kk'} < \frac{1}{k+k'-1} \le \frac{1}{N}$

Setze $\frac{a}{b} = \frac{h'}{k'}$ oder $\frac{h}{k}$ $\Rightarrow \exists$ viele $\frac{h}{k}$

Sei $c > \sqrt{5}$ $\xi = \frac{\sqrt{5}+1}{2}$

$c = \frac{\sqrt{5}}{\alpha}$ $0 < \alpha < 1$ $\left|\frac{h}{k} - \frac{\sqrt{5}+1}{2}\right| < \frac{\alpha}{\sqrt{5}k^2}$ $\Leftarrow |\theta| < \alpha$

$\theta = (\sqrt{5}k^2)\left(\frac{h}{k} - \frac{\sqrt{5}+1}{2}\right)$

$\frac{\theta}{\sqrt{5}k} = \frac{h}{k} - \frac{\sqrt{5}+1}{2}$

$h - \frac{k}{2} = \frac{\theta}{\sqrt{5}k} + \frac{\sqrt{5}k}{2}$

$\underbrace{h^2 - hk - k^2}_{\text{ganz}} = \frac{\theta^2}{5k^2} + \theta$

$= 0 \Rightarrow h = k = 0$ $\Rightarrow$ $|h^2 - hk - k^2| \ge 1$

d.h $\left|\frac{\theta^2}{5k^2} + \theta\right| \geq 1$

aber $\left|\theta + \frac{\theta^2}{5k^2}\right| \leq |\theta| + \frac{|\theta|^2}{5k^2} < \alpha + \frac{\alpha^2}{5k^2}$ $\quad |\theta| < \alpha$ nach Vor

$1 \leq \left|\theta + \frac{\theta^2}{5k^2}\right| < \alpha + \frac{\alpha^2}{5k^2}$ $\quad$ d.h $\quad 1 - \alpha < \frac{\alpha^2}{5k^2}$

$$\text{da } k^2 < \frac{\alpha^2}{5(1-\alpha)}$$

d.h. $\exists$ nur endlich viele solche k und da $\left|\xi - \frac{b}{n}\right| < \frac{1}{cn^2}$
n nur endl viele ~~gerade~~ ganze Zahlen

$\square$

(vgl. Anwend. Analysis Konvergenzkreis mit Sing auf Rand $e^{2\pi i \cdot}$)

IV Quadratische Reste

p ungerade Primzahl a ganz $(a,p)=1$

D. Ganz: a heißt q.R. mod. p geschr. $a \,R\, p$, falls $\exists$ ganze Zahl x $\quad x^2 \equiv a \ (p)$

wenn keine x exist. a ein quadr. Nichtrest genannt $a \,N\, p$

Wieviele der Zahlen $1, 2, \ldots, p-1$ sind quadr. Reste mod p ? Müssen wissen, wieviele der Kongruenzen $x^2 \equiv a \bmod p$ in x lösbar sind, wenn a die Folge $1, 2, \ldots p-1$ durchläuft

Also betrachte $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$

(i) paarweise inkongruent modulo p

$r^2 \equiv s^2 \ (p) \Rightarrow \begin{matrix} r \equiv s \ (p) \\ r \equiv -s \ (p) \end{matrix}$ ↯

(ii) $r^2 \equiv (p-r)^2 \ (p)$

d.h. quadratische Reste treten paarweise auf

(i)(ii) $\Longrightarrow$ ◻ Wenn x die Folge $1, 2, 3 \ldots p-1$ durchläuft nimmt a genau $\frac{p-1}{2}$ verschiedene an.
$\Rightarrow \exists$ genau $\frac{p-1}{2}$ quadr. Reste mod p
$\exists$ genau $\frac{p-1}{2}$ quadr. Nichtreste mod p

D Legendre:

p ungerade Prim $(m,p)=1$

$$\left(\frac{m}{p}\right) = \begin{cases} +1 & m \,R\, p \\ -1 & m \,N\, p \end{cases}$$

erweitert mit

$$\left(\frac{m}{p}\right) = 0 \quad p \mid m$$

folglich $\quad \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) = 0$

ferner $\quad m_1 \equiv m_2 \ (p) \Rightarrow \left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$

Bem $p=2$ $\exists$ zwei Restklassen $0, 1$
$0^2 \equiv 0 \pmod 2$
$1^2 \equiv 1 \pmod 2$
$\Rightarrow$ jede ganze Zahl quadr. Rest mod 2 — Triviale Fall

Das Eulersche Kriterium

Satz 1

p ungerade Prim
a teilerfrei ganz

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod p \iff a \; {}^R p$$

"$\Leftarrow$" ${}^R p \Rightarrow \exists x \; x^2 \equiv a \pmod p$
$a^{\frac{1}{2}(p-1)} \equiv x^{p-1} \equiv 1 \pmod p$
"$\Rightarrow$" $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$

"$\Leftarrow$" ${}^R p$ $\quad x^2 \equiv a \pmod p$ lösbar $(x,p)=1$ da $(a,p)=1$
$x^{p-1} \equiv a^{\frac{1}{2}(p-1)} \pmod p$ Fermat $\Rightarrow$ Beh

"$\Rightarrow$" $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$ Restgl höchstens $\frac{p-1}{2}$ Lösungen (nach Lagrange)
Es gibt genau $\frac{1}{2}(p-1)$ q.R mod, und jede erfüllt Kongruenz
$\rightarrow$ # andere Rest. $\square$

Bem p ungerade Primzahl $\quad (x,p)=1$
Nach Fermat $x^{p-1} - 1 \equiv 0 \pmod p$
$\rightarrow (x^{\frac{1}{2}(p-1)} - 1)(x^{\frac{1}{2}(p-1)} + 1) \equiv 0 \pmod p$

entweder $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$
oder $x^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$

Satz 2

p ungerade Primzahl

Beh $m^{\frac{1}{2}(p-1)} \equiv \left(\frac{m}{p}\right) \pmod p$

Kor $\left(\frac{mn}{p}\right)^{\frac{1}{2}(p-1)} \equiv (mn)^{\frac{1}{2}(p-1)} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod p$

da $\left(\frac{m}{p}\right) = \pm 1 \quad \left(\frac{n}{p}\right) = \pm 1 \quad \left(\frac{mn}{p}\right) = \pm 1$

$$\Rightarrow \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\cdot\left(\frac{n}{p}\right)$$

$m^R p \wedge n^R p \rightarrow mn^R p$
$m^R p \wedge n^N p \rightarrow mn^N p$
$m^N p \wedge n^N p \Rightarrow mn^R p$

Bsp $\left(\frac{76}{3}\right) = \left(\frac{1}{3}\right) = 1$

$n = x^2 + y^2$

p ungerade prim
$m = p-1$ in Satz 2

Da $p-1 \equiv -1 \pmod p \Rightarrow \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right)$

also $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ mod p aber $\left(\frac{-1}{p}\right) = \pm 1$
$(-1)^{\frac{1}{2}(p-1)} = \pm 1$

Satz 3 $\Rightarrow$

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

impliziert

$p \equiv 1 \pmod 4 \Rightarrow -1 \; {}^R p$
$p \equiv 3 \pmod 4 \Rightarrow -1 \; {}^N p$

Primzahl d. Gestalt $4k+3$ nicht als Summe zweier Quadrate darstellbar

Satz 4 (Euler) — Jede Primzahl der Gestalt $4k+1$ ist als Summe zweier Quadrate darstellbar

Γ p sei solche Primzahl $\Rightarrow -1 \,R\, p$

$\Rightarrow x^2 \equiv -1 \pmod p$ lösbar

$\Rightarrow \exists A \quad p \mid A^2+1 \Rightarrow p = s^2+t^2$ ⌟

Satz 5 — Zu jeder Primzahl $p \equiv 1 \pmod 4$ gibt es ganze Zahl x derart, dass

$$x^2+1 = mp \qquad 0 < m < p$$

$x^2+1 \equiv x^2 \equiv -1 \pmod p$

Γ $-1 \,R\, p$ Satz 3

$\Rightarrow \exists x$ in der Folge $1, 2, 3, \dots \frac{1}{2}(p-1)$ das die Kongruenz $x^2 \equiv -1 \pmod p$ erfüllt

$\Rightarrow x^2+1 = mp$ m ganz · Wähle $x < \frac{1}{2}p$

also $x^2+1 < \left(\frac{p}{2}\right)^2+1 < p^2$ $x^2+1 = mp$ $0 < m < p$ ⌟

Satz 6 — p ungerade Primzahl
$\Rightarrow \exists$ ganze Zahlen x und y derart, dass

$$1 + x^2 + y^2 = mp \quad \text{wobei } 0 < m < p$$

Γ Betrachte Menge d. ganzen Zahlen $\{x^2\}$ $0 \le x \le \frac{p-1}{2}$
Sie sind paarweise inkongruent mod p

ebenso die $\frac{1}{2}(p+1)$ Zahlen $\{-1-y^2;\ 0 \le y \le \frac{p-1}{2}\}$

Die beiden Mengen enth. $p+1$ Zahlen. $\exists!$ p Restklassen

$\exists x \quad x^2 \equiv -1-y^2 \pmod p \iff x^2+y^2+1 = mp$

Nun $0 \le x, y \le \frac{1}{2}(p-1) \Rightarrow x^2+y^2+1 < 2\left(\frac{p}{2}\right)^2+1 < p^2$

somit $x^2+y^2+1 = mp$ $\quad 0 < m < p$ ⌟

Satz 7 — Die posit. ganze Zahl n ist genau dann die Summe von zwei Quadraten, wenn in der kanon. Zerlegung von n alle Primzahlen der Gestalt $4k+3$ mit geradem Exponenten vorkommen

$n = x^2+y^2$ primitiv falls $(x,y) = 1$

Lemma 1 — n durch Primzahl $p \equiv 3 \pmod 4$ teilbar, so besitzt n keine primitive Darstellung

Γ $n = x^2+y^2$ primitiv $\Rightarrow (x,y) = 1$
und $p \mid x^2+y^2$ $\quad p \nmid x \Rightarrow (p,x) = 1 \Rightarrow p \nmid y$
$\Rightarrow$ Da $(p,x) = 1$ ist die gleich. $mx \equiv -1 \pmod p$
für alle c (ganz) in ganzen Zahlen m lösbar
Insbesondere für $c = y$ Es gibt also eine ganze Zahl m mit der Eigenschaft $mx \equiv y \pmod p$
folglich $x^2+y^2 \equiv x^2+m^2x^2 \equiv 0 \pmod p$
$\rightarrow p \mid m^2+1$ da $m(p,x) = 1$
d.h. $m^2 \equiv -1 \pmod p \Rightarrow m \,-1\, Rp$ ↯

Lemma 2

$p \equiv 3 \ (4)$
c positive ungerade Zahl
$p^c \mid n \quad p^{c+1} \nmid n$
$\Rightarrow$ n lässt sich nicht als Summe zweier Quadraten darstellen

Γ $\quad n = x^2 + y^2 \qquad (x,y) = d$
$\rightsquigarrow x = dx \quad y = dY \qquad (x,Y) = 1$
und $n = d^2 \underbrace{(x^2+Y^2)}_{:= N} = d^2 N$

p^m höchste Potenz von p welche d teilt
$\Rightarrow$ p^{c-2m} ist die höchste Potenz von p welche N teilt Ferner ist $c - 2m \geq 0$ da c ungerade.
somit haben N mit $N = x^2 + Y^2 \qquad (x,Y) = 1$
$p \mid N$ wobei $p \neq 3 \ (4)$

↯ zu Lemma 1 ⌟

Bew Satz 7 (i) Bedingung notwendig

$p = 4k+3$ mit $p \mid n$

L2 $\Rightarrow$ in kan. Zerl. kommt p mit gerader Exponent vor.

(ii) Bed. hinreichend

n konvergiert kanon. Zerleg.
$p \equiv 3 \ (4)$ kommt nur mit geraden Exponenten vor
$n = n_1^2 n_2$ wobei n_1 weiter Primteiler der Form $4k+3$ besitzt.
Die Primteiler von n_1 sind 2 oder ungerade Primzahlen d. Form $4k+1$
$2 = 1^2 + 1^2 \qquad 4k+1 = x^2 + y^2$

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$$

Folglich $n_1 = a^2 + b^2$

$$n = (n_1 a)^2 + (n_1 b)^2$$

⌟

3 Quadrate

$x =$			
$2m$	$x^2 \equiv 0 \ 8$		m gerade
	$x^2 \equiv 4 \ 8$		m ungerade
$2m+1$	$x^2 \equiv 1 \ 8$		m gerade
	$x^2 \equiv 1 \ 8$		m ungerade

d. h.
$x \equiv 7 \bmod 8 \Rightarrow$ nicht als Summe von 3 Quadr. darstellbar

Satz 8 Lagrange 1770

jede posit. ganze Zahl ist Summe von 4 Quadraten

Γ $\quad 1 = 0^2 + 0^2 + 0^2 + 1^2$

$n \geq 2$

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

$$\begin{aligned} z_1 &= x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \\ z_2 &= x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \\ z_3 &= x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4 \\ z_4 &= x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2 \end{aligned}$$

→ Quaternionen Lagrange

Satz 6 : Zu jeder ungeraden Primzahl p gibt es eine Zahl m $0 < m < p$ derart, dass

$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$, x_1, x_2, x_3, x_4 nicht alle durch p teilbar

$x_i < p$

Für eine fste Primzahl $p > 3$, sei m_0 die kleinste posit. ganze Zahl mit

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2 \qquad (1)$$

$m_0 = 1 \Rightarrow$ Satz ist bewiesen

$m_0 > 1 \Rightarrow$ wollen widerspruch

Zeigen
$m_0 \cdot p = x_1^2 + x_2^2 + x_3^2 + x_4^2$
$m_0 > 0$ ungerade

Annahme m_0 lässt sich als Summe von 4 Quadrat. schreiben
$\Rightarrow p$ lässt sich als Summe von 4 Quadrat. schreiben q.e.d.
$\Rightarrow m_0$

Haben Problem von p auf m_0 reduziert
$m_0 < p$

m_0 immer ungerade , denn falls m_0 gerade $\Rightarrow$ x_1, x_2, x_3, x_4 alle gerade
oder zwei gerade alle ungerade
oder zwei gerade zwei ungerade

dann wäre $\frac{1}{2} m_0 p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$

eine Summe von 4 ganzzahl. Zahlen welche nicht alle durch p teilbar sind würde minimalen, gemäß m_0 widersprechen

Man kann $x_i = b_i m_0 + y_i$ darstellen $|y_i| \leq \frac{1}{2} m_0$ (2)

Dabei ganze Zahl b_i , immer so wählbar , dass $y_i > \frac{1}{2} m_0$ — schreiben $x_i = (b_i + 1) m_0 + (y_i - m_0)$

Nicht alle x_1, x_2, x_3, x_4 durch m_0 teilbar denn daraus würde $m_0 | p$ folgen was wegen $1 < m_0 < p$ unmöglich . Folglich ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$$

(andererseits
$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{1}{2} m_0\right)^2 = m_0^2$

(1), (2) $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \mod m_0$)

haben jetzt ganze Zahlen x_i, y_i $i = 1 \dots 4$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p$$
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 \cdot m_0 \qquad 0 < m_1 < m_0$$

Also existiert (Ident. von Hurwitz) ganze Zahlen z_1, z_2, z_3, z_4

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p \qquad (3)$$

$$z_1 = \sum_{i=1}^{4} x_i y_i \overset{(2)}{=} \sum_{i=1}^{4} x_i (x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{m_0}$$

analog $z_2, z_3, z_4 \equiv 0 \pmod{m_0}$

Also $z_i = m_0 \cdot t_i$ t_i ganz $i = 1, 2, 3, 4$

also $m_1 \cdot p = t_1^2 + t_2^2 + t_3^2 + t_4^2$ $0 < m_1 < m_0$ ↯

V Das quadratische Reziprozitätsgesetz

Satz p, q ungerade Primzahlen $p \neq q$

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

legendresche Form

Bem $p \equiv q \equiv 3 \pmod 4 \iff \frac{p-1}{2}\,\frac{q-1}{2}$ ungerade

d.h. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \iff p \equiv q \equiv 3 \pmod 4$

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sonst

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

(1) $\iff$ (2)

$\vdash$ Da $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$ $\quad$ [$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \bmod p$ Euler]

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

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

also (2) $\Rightarrow$ (1) denn $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}\left(\frac{q}{p}\right)$

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

(1 $\Rightarrow$ 2)

$$\left(\frac{p}{q}\right)\underbrace{\left(\frac{q}{p}\right)^2}_{=1} = \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}\left(\frac{q}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \quad \dashv$$

p ungerade Primzahl $(a,p)=1$

Betrachte Zahlen $a, 2a, 3a \ldots \frac{(p-1)}{2}a$ (A)

sind nicht teilbar durch p, paarweise inkongruent mod p

Bsp $p=5$ $\quad 2a \equiv 4 \pmod 5$
$\quad = 9 \pmod 5$
$\quad = 14 \pmod 5$

rest mod p := kleinste positive Rest mod p

Sei ν # Zahlen aus (A) deren Rest mod p kleiner als $\frac{1}{2}p$.

Sei μ # Zahlen aus (A) mit Rest mod $p > \frac{1}{2}p$

Das Gaußsche Lemma

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

$\vdash$ ③ seien $\alpha_1 \ldots \alpha_\nu$ positiv verschieden — diejenigen Reste der Zahlen in A die kleiner als $\frac{1}{2}p$ sind

④ $(p-\beta_1)\ldots(p-\beta_\mu)$ damit $\beta_1 \ldots \beta_\mu$ negativ — diejenigen Reste die größer als $\frac{1}{2}p$ sind, alle $< \frac{1}{2}p$ sind

keine der Zahlen von ③ kann in ④ vorkommen $\beta_r \neq \alpha_s$

$\alpha_r = \beta_s \Rightarrow \exists i \quad 0 < i < \frac{1}{2}p \quad ia \equiv \alpha_r \pmod p$

$\rightsquigarrow \exists j \quad 0 < j < \frac{1}{2}p \quad ja \equiv p - \beta_s \bmod p$
$\quad \equiv p - \alpha_r \bmod p$

$(i+j)a \equiv 0 \pmod p$ aber $(a,p)=1$

$i+j < p$ damit $\lightning$ $\quad \dashv$

Es folgt, dass die Zahlen $\alpha_1, \dots \alpha_\mu, \beta_1 \dots \beta_\nu$
übereinstimmen mit d. Zahlen $1, 2, \dots \frac{p-1}{2}$
(vielleicht in anderer Reihenfolge)

Folglich $a \cdot 2a \cdot 3a \dots \frac{p-1}{2} a = \underbrace{\left(\frac{p-1}{2}\right)!}\, a^{\frac{p-1}{2}}$

$\equiv \alpha_1 \cdot \alpha_2 \dots \alpha_\mu \cdot (p-\beta_1)(p-\beta_2)\dots(p-\beta_\nu) \pmod p$

$\equiv \underbrace{(-1)^\nu \left(\frac{p-1}{2}\right)!} \pmod p$

$\Rightarrow a^{\frac{p-1}{2}} \equiv (-1)^\nu \pmod p$

Satz Gauss $\Rightarrow \left(\frac{a}{p}\right) \equiv (-1)^\nu \pmod p$ ✓

da $\left(\frac{a}{p}\right) = \pm 1$ $(-1)^\nu = \pm 1$ $p > 3$

$\rightarrow \left(\frac{a}{p}\right) = (-1)^\nu$ ✓

Satz p, q ungerade Primzahlen $(p,q) = 1$

Gauss mit 6 Lemmen

Betrachte (A) $q, 2q, 3q, \dots, \frac{p-1}{2} q$

ν # Zahlen in (A) mit Rest $\bmod p > \frac{1}{2} p$

Gauss: $\left(\frac{q}{p}\right) = (-1)^\nu$

analog (B) $p, 2p, \dots \frac{q-1}{2} p$

ν # Zahlen in (B) mit Rest $\bmod q > \frac{1}{2} q$

Dann: $\left(\frac{p}{q}\right) = (-1)^\nu$

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

genügt: $\boxed{\mu + \nu \equiv \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \pmod 2}$ *

Der kleinste positive Rest irgendeiner zu $N \bmod p$ ist 0 oder

(f) — $1, 2, \dots \frac{p-1}{2}$,

(g) — $\frac{p+1}{2}, \dots p-1$

Der kleinste positive Rest irgendeiner Zahl $\bmod q$ ist 0 oder

(F) — $0, 1, 2, 3 \dots \frac{q-1}{2}$

(F') — $\frac{q+1}{2}, \dots q-1$

Betrachte

(C) — $1, 2, 3 \dots \frac{pq-1}{2}$ keine dieser Zahlen ist durch p und durch q teilbar

$\lvert I \rvert = \alpha$	Klasse I	Reste $\bmod p$ in (f) Reste $\bmod q$ in (F)	$\lvert III \rvert + \lvert IIII \rvert + \lvert VII \rvert$ $= \beta + \delta + \nu$
$\lvert II \rvert = \beta$	Klasse II	Rest $\bmod p$ in (f') Reste $\bmod q$ in (F')	
$\lvert III \rvert = \gamma$	Klasse III	Rest $\bmod p$ in (f') Rest $\bmod q$ in (F)	
$\lvert IV \rvert = \delta$	Klasse IV	Rest $\bmod p$ in (f') Rest $\bmod q$ in (F')	
$\lvert V \rvert = \mu$	Klasse V	Rest $\bmod q = 0$ Rest $\bmod p$ in (f')	einziges Vielfache von q in (C) $q, 2q, 3q \dots \frac{p-1}{2} q$
$\lvert VI \rvert = \frac{p-1}{2} - \mu$	Klasse VI	Rest $\bmod q = 0$ Rest $\bmod p$ in (f)	
$\lvert VII \rvert = \nu$	Klasse VII	Rest $\bmod p = 0$ Rest $\bmod q$ in (F')	
$\lvert VIII \rvert = \frac{q-1}{2} - \nu$	Klasse VIII	Rest $\bmod p = 0$ Rest $\bmod q$ in (F)	

zu zeigen $\boxed{\beta + \delta + \gamma = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$ ①

dann $\gamma + \delta + \mu = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ ②

weiter zeigen $\boxed{\beta + \gamma = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$ ③

annehmen $\Longrightarrow$ $\mu + \gamma + 2\delta = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ $\rightarrow$ Beh (x)

① $\beta + \delta + \gamma = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$

Γ II + III + VII = Zahlen in © mit Rest mod q in F'

Falls ξ gegeben Rest mod q in (F') dann sind $\xi,\ q+\xi,\ 2q+\xi,\ \dots \frac{p-3}{2}q + \xi$ auch in II + III + VII

Γ sie sind alle $\equiv \xi \bmod q$;
$t q + \xi \leq \frac{pq-1}{2} = \frac{p-1}{2}q + \frac{q-1}{2}$

$\Leftrightarrow t q \leq \frac{p-3}{2}q + (q + \frac{q-1}{2} - \xi)$ (⊗)

Da $\xi \in (F') \Rightarrow \frac{q+1}{2} \leq q + \frac{q-1}{2} - \xi \leq q-1$

Γ - $\xi \notin (F') \Rightarrow \frac{q+1}{2} \leq \xi \leq q-1$

$\Rightarrow q + \frac{q-1}{2} - \xi \leq q + \frac{q-1}{2} - \frac{q+1}{2} = q-1$
$\Rightarrow q + \frac{q-1}{2} - \xi \geq q + \frac{q-1}{2} - (q-1) = \frac{q+1}{2}$ ✓

Analog gilt (⊗) für $t \leq \frac{p-3}{2}$ (und nicht für $t = \frac{p-1}{2}$), denn $\frac{p-1}{2}q \leq \frac{p-3}{2}q + (q + \frac{q-1}{2} - \xi)$

$\Rightarrow q \leq q + \frac{q-1}{2} - \xi$

$\rightarrow \xi \leq \frac{q-1}{2}$ ↯ da ξ hat Rest mod q in (F') ✓

Für ein geg. ξ haben wir $\frac{p-1}{2}$ solche Zahlen für $t = 0, 1, 2, \dots \frac{p-3}{2}$

Andererseits kann ξ $\frac{q-1}{2}$ Werte annehmen $\rightarrow$ Beh ✓

② $\gamma + \delta + \mu = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ analoger Beweis

③ $\beta + \gamma = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$

Γ

Betrachte die Folge $(pq - ©)$: $\frac{pq+1}{2}, \frac{pq+3}{2}, \dots pq-1$ Ⓓ

$a \in © \Longleftrightarrow pq - a \in Ⓓ$

$\Rightarrow$ Falls d. Rest von a (mod p) $\in (I')$ (d.h Rest $> \frac{p}{2}$)
$\rightarrow$ Rest von $pq-a$ (mod p) in (I) und umgekehrt

Γ $pq \equiv 0 \pmod p$ $\quad a \equiv b \pmod p$
$b \in I'$ d.h $\frac{p+1}{2} \leq b \leq p-1$

$\rightarrow pq - a \equiv \begin{cases} -b \\ p-b \end{cases} \bmod p$ $\quad (-p-1) \leq -b \leq -\left(\frac{p+1}{2}\right)$ also $p-b \in (I)$
$1 \leq p-b \leq \frac{p-1}{2}$

Analog Falls Rest von a mod p $\in$ (F)
$\Rightarrow$ Rest von $pq-a$ mod p $\in (F')$ u. umgekehrt

Also enthält die Klasse III genau soviele Zahlen, wie es Zahlen in ② mit "Rest mod p" in ① und "Rest mod q" in ③ gibt

Also f = # Zahlen in ② mit "Rest mod p" in ① und "Rest mod q" in ③

Sei ④ := ① ∪ ② = $\{1, 2, 3, \dots pq-1\}$

Diese Zahlen sind alle positiv, verschieden, paarweise inkongruent (mod pq) Also entspricht zu jedem solchen Paar eindeutig eine Zahl in ④
solche Paare = $(\frac{p-1}{2})(\frac{q-1}{2}) = pr$

Schlussfolgerung : ① + ② + ③ : $pr + r + 2f = (\frac{p-1}{2})(\frac{q-1}{2})$ → Beh ✱

Satz 2 — Ergänzung u. Lagrange

p ungerade Primzahl, dann gilt
$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$

Euler Krit. $m^{\frac{p-1}{2}} = \left(\frac{m}{p}\right) \bmod p$

$m=2$ $\quad 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \bmod p$

Idee von Siegel : $\quad 2 = \frac{(1+i)^2}{i}$

$$\rightarrow \left(\frac{2}{p}\right) = \frac{(1+i)^{p-1}}{i^{\left(\frac{p-1}{2}\right)}} \equiv \frac{(1+i)^p}{(1+i)\, i^{\frac{p-1}{2}}} \equiv \frac{1+i^p}{(1+i)\, i^{\frac{p-1}{2}}} \quad \text{(binom. Zerlegg.)}$$

$$\equiv \frac{i^{Pp}\left(i^{Pk} + i^{-Pk}\right)}{i^{Pk}\left(i^{Pk} + i^{-Pk}\right)} \equiv \frac{\cos\frac{\pi}{4}p}{\cos\frac{\pi}{4}}$$

$\left|\left(\frac{2}{p}\right)\right| = 1 \qquad \left|\frac{\cos\frac{\pi}{4}p}{\cos\frac{\pi}{4}}\right| = \left|\frac{\pm\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}}\right| = 1$ (3. Gl. p prim)

$$\rightarrow \left(\frac{2}{p}\right) = \frac{\cos\frac{\pi}{4}p}{\cos\frac{\pi}{4}} = \begin{cases} +1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

$p = 8m+1$, $p = 8m-1$ $\rightarrow$ $p+1 = 8m+2$, $p+1 = 8m$ $\rightarrow$ $\left[\frac{p+1}{4}\right] = 2m$

$\rightarrow (-1)^{\left[\frac{p+1}{4}\right]} = (-1)^{2m} = 1$

$p = 8m+3$, $p = 8m-3$ $\rightarrow$ $p+1 = 8m+4$, $p+1 = 8m-2$ $\rightarrow$ $\left[\frac{p+1}{4}\right] = 2m+1$, $2m-1$

$\rightarrow (-1)^{\left[\frac{p+1}{4}\right]} = (-1)^{2m+1} = -1$ ∎

Rem $\quad p = 8m \pm 1 \rightarrow \frac{p^2-1}{8}$ gerade

$p = 8m \pm 3 \rightarrow \frac{p^2-1}{8}$ ungerade

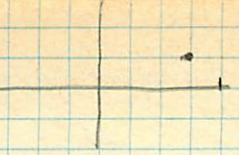
Satz 2' — $3 \le p$ Primzahl $\rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

d.h. $2^R p$, $p = 8n \pm 1$; $2^N p$, $p = 8n \pm 3$

BSp $\quad \left(\frac{24}{31}\right)\left(\frac{18}{59}\right) = \left(\frac{2^3}{31}\right)\left(\frac{3}{31}\right)\left(\frac{2}{59}\right)\left(\frac{3^2}{59}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right)\left(\frac{2}{59}\right) = (+1)\left(\frac{3}{31}\right)(-1)$

$= (-1)\left(-\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1$

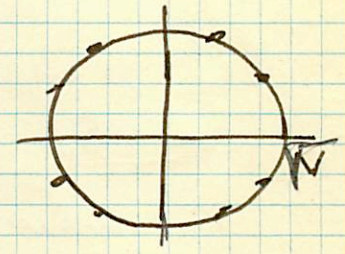
VI Gitterpunktproblem



$r(n) :=$ # Darstellungen von n als Summe zweier Quadrate, wobei Darstellungen, die sich nur durch Vorzeichen und Vertauschen als verschieden notiert werden.

Bsp $r(1) = 4 \qquad 1 = 1^2+0^2 = 0^2+1^2 = (-1)^2+0^2 = 0^2+(-1)^2$

Bem
- $n_i^2 \equiv 0,1 \pmod 4 \Rightarrow r(n) = 0$ falls $n = 4k+3$
- $\lim_{n\to\infty} r(n) = 0$
- $r(n) = O(n^\varepsilon) \quad \forall \varepsilon > 0$



$R(N) := \sum_{n=0}^{N} r(n) \qquad r(0) = 1$

= # Gitterpunkte, die innerhalb oder auf dem Kreis $x^2+y^2 = N$ liegen

Satz 1 (Gauß)
$$R(N) = \pi N + O(\sqrt{n})$$
Vermut. $R(N) = \pi N + O(N^{\frac{1}{4}+\varepsilon})$

⌜ $\pi(\sqrt{N}-\sqrt{2})^2 \le R(N) \le \pi(\sqrt{N}+\sqrt{2})^2$

$\pi N - 2\sqrt{2}\pi\sqrt{N} + 2\pi \le R(N) \le \pi N + 2\pi\sqrt{2}\sqrt{N} + 2\pi$

$-c\sqrt{N} \le R(N) - \pi N \le c\sqrt{N}$ ⌟

Vermutung $O(N^{\frac{1}{4}+\varepsilon})$ ungelöst

Sierpinsky	1906	$O(N^{\frac{1}{3}+\varepsilon})$
Huxley		$O(N^{\frac{15}{46}+\varepsilon})$
Hardy Landau	1915	$\neq O(N^{\frac{1}{4}})$

$d(n) :=$ # posit. Teiler von n

Satz 2 $d(n)$ ist multiplikativ

⌜ (i) $d(1) = 1$
(ii) $(m,n) = 1 \Rightarrow d(m\cdot n) = d(m)\cdot d(n)$ ⌟

Satz 3
$$n = \prod_{k=1}^{r} p_k^{\alpha_k} \Rightarrow d(n) = \prod_{k=1}^{r} (\alpha_k + 1)$$

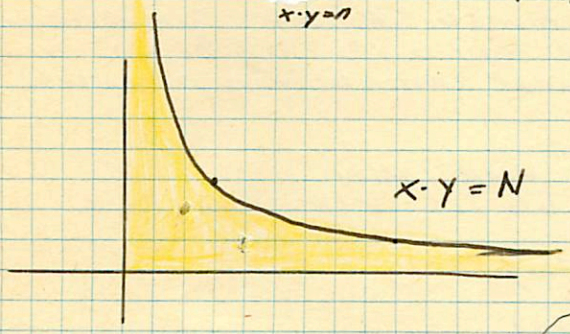
⌜ multiplikativ ⌟

Bem $\overline{\lim}\, d(n) = \infty$

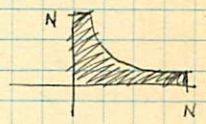
$\underline{\lim}\, d(n) = 2$

$$D(N) := \sum_{n=1}^{N} d(n) \qquad d(n) = \sum_{t \mid n} 1 = \sum_{x \cdot y = n} 1 = \sum_{1 \le x \cdot y \le N} 1$$

$$D(N) = \sum_{n=1}^{N} \sum_{x \cdot y = n} 1 = \sum_{1 \le x \cdot y \le N} 1 = \#\text{ Gitterpunkte d. ersten Quadranten unter d. Hyperbel } x \cdot y = N \text{ aber nicht auf d. Achse}$$



$$N \cdot \log N - N = 2 \cdot \int_{\sqrt{N}}^{N} \frac{N}{x}\, dx - N = \text{Fläche}$$

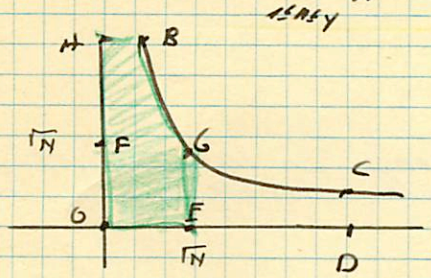


Satz 4 $\qquad D(N) = N \cdot \log N + (2\gamma - 1) N + O(\sqrt{N})$

Dirichlet 1849

$$(*) \qquad \sum_{1 \le n \le y} \frac{1}{n} = \log y + \gamma + O\left(\frac{1}{y}\right) \qquad y \to \infty$$

(Restglied ohne Beweis)



Symmetrie bez. $x = y$

$\Rightarrow$ ABGEO hat gleichviele Gitterpunkte wie CDOEG

$$\Rightarrow D(N) = 2 \sum_{\substack{1 \le x \le \sqrt{N} \\ 1 \le x \cdot y \le N}} 1 - [\sqrt{N}]^2$$

$$[\sqrt{N} - \theta]^2 = N + \theta^2 - 2\sqrt{N}\,\theta$$

$$\frac{N}{x} = \left[\frac{N}{x}\right] + \theta_x \qquad 0 \le \theta_x < 1$$

$$= 2 \sum_{1 \le x \le \sqrt{N}} \left[\frac{N}{x}\right] - [\sqrt{N}]^2 = 2N \cdot \sum_{1 \le x \le \sqrt{N}} \frac{1}{x} - \overbrace{2 \sum_{1 \le x \le \sqrt{N}} \theta_x}^{< c\sqrt{N}} - N + 2\theta\sqrt{N} - \theta^2$$

also $\quad D(N) = 2N \sum_{1 \le x \le \sqrt{N}} \frac{1}{x} - N + O(\sqrt{N})$

$(y = \sqrt{N}$ in $*)$ $\quad D(N) = N \cdot \log N + 2\gamma(2\gamma - 1) N + O(\sqrt{N})$ qed

Weiteres $\quad D(N) = \ldots + O(N^{\frac{1}{4} + \varepsilon})$

$D(N) = \ldots + O(N^{\frac{1}{4}})$ falsch

Voronoy $\quad D(N) = \ldots O(N^{\frac{1}{3} + \varepsilon})$

$D(N) = \ldots O(N^{\frac{13}{46} + \varepsilon})$

Verallgemeinerungen: $\quad - d_k(n)$ mit k Faktoren

- mehrdimensional
- # Gitterpunkte eines Kreises $\le$ konst.

Minkowski : konvexe Körper in $\mathbb{R}^3$
$0 \in K \quad x \in K \Rightarrow -x \in K$
Lebesgue messbar

Beziehung: Mass $\sim \exists$ mind. Gitterpunkt $\neq 0$

neues Gebiet: Geometrie d. Zahlen

Satz Minkowski : Ist S eine beschränkte konvexe symmetrische Menge in $\mathbb{R}^n$ mit Mass $> 2^n$ so gibt es in S einen vom Nullpunkt verschiedenen Gitterpunkt.

Bem ① S konv. symm. $x \in S \Rightarrow \lambda x \in S \quad \forall \lambda \in \mathbb{R} \quad |\lambda| \leq 1$
② S konv. symm. $x \in S \; y \in S \Rightarrow \lambda x + \mu y \in S \quad \forall \lambda, \mu \quad |\lambda| + |\mu| \leq 1$

① $\lambda x = \left(\frac{1}{2} + \frac{\lambda}{2}\right) x + \left(\frac{1}{2} - \frac{\lambda}{2}\right)(-x) \in S$

② $\lambda = 0 \vee \mu = 0 \rightarrow$ ①
$\lambda \neq 0 \quad \mu \neq 0$ $\varepsilon_1 = \operatorname{sgn} \lambda$
$\varepsilon_2 = \operatorname{sgn} \mu$
aus ① und $|\lambda| + |\mu| \leq 1$ folgt

$x' := \varepsilon_1 (|\lambda| + |\mu|) x \in S$
$y' := \varepsilon_2 (|\lambda| + |\mu|) y \in S$

Definiere $\rho = \frac{|\lambda|}{|\lambda| + |\mu|} \quad \sigma = \frac{|\mu|}{|\lambda| + |\mu|} \quad \rho \geq 0 \quad \sigma \geq 0$
$\rho + \sigma = 1$

$\underbrace{\rho x' + \sigma y'}_{\in S} = \lambda x + \mu y \in S$

Lemma Blichfeldt Ist S eine messbare Menge in $\mathbb{R}^n$ mit Mass > 1 dann gibt es zwei versch. Punkte $x, y \in S$ so dass $x - y$ ein Gitterpunkt

Idee: Verschiebe die gebrochenen Teile d. Einheitswürfels und zeige: $\exists$ Überlappungen)

Sei $g = (g_1, \ldots, g_n)$ Gitterpunkt
Betrachte Würfel $\{x_i \mid g_i \leq x_i \leq g_i + 1\}$ $i = 1, \ldots, n$

$S^g = S \cap \{x_i \mid g_i \leq x_i \leq g_i + 1\}$

S^g disj. Vereinigung welche S^g in Einh.würfel $0 \leq x_i \leq 1$ hängt

$S^g_{-g} \subset \{x_i \mid 0 \leq x_i \leq 1\}$

V^g Mass von $S^g \qquad \sum_g V^g = m(S) > 1$

$\Rightarrow \exists \; S^g_{-g}, S^{g'}_{-g'} \quad (\exists x \in S^g \; y \in S^{g'} \quad x - g = y - g')$

haben also $x \in S \quad y \in S \quad x - y = g - g'$

und $x - y \neq 0$ da $g \neq g'$ ∎

Beh S konvex $\Rightarrow \frac{1}{2}S$ konvex $m\frac{1}{2}S = \left(\frac{1}{2}\right)^n m(S) > 1$

Nach Lemma v. Birkhoff $\exists$ 2. verschl. Punkte $x, y \in \frac{1}{2}S$
$x - y = g$ Gitterpunkt. $g \neq 0$ da $x \neq y$

$\frac{1}{2}x - \frac{1}{2}y \in \frac{1}{2}S$ d.h. $\frac{1}{2}g \in \frac{1}{2}S \Rightarrow g \in S$ ⌟

analog Beh. mit Koordinaten ...

Bem Bei Satz ist essentiell:

$|x_i| < 1 \quad 1 \le i \le n$

d.h. können nicht $m(S) \ge 2^n$ annehmen

Satz 2 Eine abgeschl. konvexe, beschränkte, ~~konvexe~~ symmetrische Menge S in $\mathbb{R}^n$ mit Mass $\ge 2^n$ enthält einen von Null verschiedenen Gitterpunkt

Beweis ⌜ sei $\varepsilon \quad 0 < \varepsilon < 1$

Behaupte $S' =: (1+\varepsilon)S$
S messbar $\Rightarrow S'$ messbar $m(S') = (1+\varepsilon)^n m(S)$
$> (1+\varepsilon)^n 2^n > 2^n$

$\exists$ g Gitterpunkt $l_\varepsilon \neq 0$ $l_\varepsilon \in (1+\varepsilon)S$
Es gibt nur endlich viele Möglichkeiten für l_ε

Folglich gibt es einen von Null versch. Gitterpunkt l_0 derart dass $l_0 \in (1+\varepsilon)S \quad \forall \varepsilon$ mit $0 < \varepsilon < 1$

d.h. $\frac{l_0}{1+\varepsilon} \in S$

lassen $\varepsilon \to 0 \Rightarrow l_0 \in S$ da S abgeschlossen

(S konvex, messbar $0 < m(S) < \infty \Rightarrow S$ beschränkt) ⌟

Satz 2' S beschr. messbare konv. symm. Menge in $\mathbb{R}^n$ mit $m(S) \ge 2^n$ so gibt es in S einen von Null versch. Gitterpunkt

Voraus. $\bar{S}$ ist konvex

⌜ $\bar{S}$ ist konvex, abgeschl. beschr. und $m(\bar{S}) \ge m(S) \Rightarrow$ S. 2.

ohne Beweis

Anwend.: $\ln = \ln x \cdot Bd x$
$\ln \ln x = \ln x$
$\ln x = x^c$
$Bd x = \sqrt[c]{a-1}\, c\, x$
$Bd x \cdot Bd x^c = i\, Fl A$
$Fl x = \ln H$
Zsl. $\ln x, Bd x, Bd x^c \ln x^c$

Gg $\lambda_n \mu_n \to \lambda\mu$
$x, y \in \bar{S}$ $x_n \to x$, $y_n \to y$

$\lim_{n\to\infty} \frac{\lambda x_n + \mu y_n}{2n} \in S$

⌟

Minkowski 1864–1909
ETH 1896–1902

Anwendungen:

$\xi_i = a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n \qquad (i = 1,2,\dots n)$
$(x_i, a_{ij}$ reell$)$

$\Delta = \det[a_{ij}]$ voraus. $\Delta \neq 0$

$L : \mathbb{R}^n \to \mathbb{R}^n$
$S \to T$
$x \mapsto \xi$

L (konvex) konvex
L (symm) symm.

$\int_T d\xi_1 d\xi_2 \dots d\xi_n = |\Delta| \int_S dx_1 \dots dx_n$

Das Bild im ξ Raum d. Menge d. Gitterpunkte Λ im x Raum heißt ein Gitter zu Λ assoziert mit L.

Nach Satz 1 angewendet auf dem ξ Raum einmalen

Satz 3 Ist Λ ein Gitter mit Determ. $\Delta \neq 0$
B messbare konvexe symm. Menge von Maß $m(B) > 2^n \cdot |\Delta|$
dann enthält B außer d. Nullpunkt noch einen weiteren Punkt von Λ.

Satz 4 Ist Λ Gitter mit $|\Delta| \neq 0$
B abg. beschr. symm. konv. Menge von Maß $m(B) \geq 2^n |\Delta|$
dann enthält B außer d. Nullpunkt noch einen weiteren Punkt von Λ.

Bsp I: $|\xi_i| \leq c_i \qquad i = 1,2,\dots,n$

definiere in x Raum abgeschl. Menge
$S \ni x \iff -x \in S$ symmetrisch, konvex $z = \lambda x + \mu y$

denn $|a_{i1}z_1 + \dots + a_{in}z_n| \leq \lambda |a_{i1}x_1 + \dots a_{in}x_n|$
$+ \mu |a_{i1}y_1 + \dots a_{in}y_n|$
$\leq \max(|a_{i1}x_1 + \dots a_{in}x_n|, |a_{i1}y_1 + \dots a_{in}y_n|)$
$\leq c_i$

S beschränkt.

Sei d_{ij} die inverse Matrix von (a_{ij})

$\xi_i = \sum_{j=1}^n a_{ij}x_j \to x_i = \sum_{j=1}^n d_{ij}\xi_j$

$\Rightarrow |x_i| \leq \sum |d_{ij}| c_j$

$\Rightarrow S$ beschränkt

$m(T) = 2^n c_1 c_2 \dots c_n$

Satz 4 liefert

Satz 5 Sind $\xi_1, \xi_2 \dots \xi_n$ homogene lineare Formen in den Variablen $x_1, x_2 \dots x_n$ mit reellen koeff. und mit $\det A \neq 0$ und sind $c_1, c_2, \dots c_n$ positive reelle Zahlen derart, dass $c_1 \cdot c_2 \cdot \dots \cdot c_n \geq |\Delta|$

dann gibt es ganze Zahlen $x_1 \dots x_n$ nicht alle Null derart mit d. Eigenschaft dass $|\xi_1| \le c_1 \quad |\xi_2| \le c_2$ $\dots \quad |\xi_n| \le c_n$

Bem Gi) Nimm $c_i = |\Delta|^{1/n}$ → Bedingung erfüllt
Gii) $\Delta = 0 \quad c_i > 0$ → Masse ist unendlich
Satz 5 bleibt gültig

Satz

$|\xi_i| \le c_i \quad i = 1 \dots m \quad m < n$

Es wird dadurch eine in im + Raum unbeschränkte Menge definiert denn gewisse Variablen sind frei.
trotzdem gilt Satz 5 (n-m+1 mal die n-m te Gleichung wiederholen) mit $\Delta = 0$

(II) ξ Raum $T \quad |\xi_1| + |\xi_2| + \dots + |\xi_n| \le c$
T konvex, dann $\xi = (\xi_1, \dots, \xi_n) \in T$
$\xi' = (\xi_1', \dots, \xi_n') \in T$

und $\lambda \ge 0 \; \mu \ge 0 \quad \lambda + \mu = 1$

$$\Rightarrow \sum_{k=1}^{n} |\lambda \xi_k + \mu \xi_k'| \le \lambda \sum_{k=1}^{n} |\xi_k| + \mu \sum_{k=1}^{n} |\xi_k'|$$
$$\le \max\left(\sum_{k=1}^{n} \xi_k, \sum_{k}^{n} \xi_k'\right) \le c$$

($n = 2$ T ist Oktaeder)

T besteht aus 2^n kongr. Teilen.
derjenige Teil im 'Oktaeder' $\xi_1 \ge 0, \xi_2 \ge 0, \dots, \xi_n \ge 0$
hat das Mass $c^n \int_0^1 d\xi_1 \int_0^{1-\xi_1} d\xi_2 \dots \int^{1-\xi_1 - \dots - \xi_{n-1}} d\xi_n$

$$= \frac{c^n}{n!}$$

also $m(T) = \frac{(2c)^n}{n!}$

Ist $c^n \ge n! |\Delta|$, dann $m(T) \ge 2^n |\Delta|$

Also m. Satz 4 — Satz 6

Es gibt ganze Zahlen $x_1, x_2, \dots, x_n$ nicht alle 0 für welche $|\xi_1| + |\xi_2| + \dots + |\xi_n| \le (n! |\Delta|)^{1/n}$
$|\xi_1 \dots \xi_n|^{1/n} \le$

Satz 6' ∃ ganze Zahlen $x_1 \dots x_n$ nicht alle Null für welche $|\xi_1 \xi_2 \dots \xi_n| \le \frac{n! |\Delta|}{n^n}$

(III) Bereiche $\Phi \subseteq \mathbb{R}^n$ def. durch $\xi_1^2 + \dots + \xi_n^2 \le c^2$

P symmetrisch, auch konvex, denn

$$\sum_{k=1}^{n} (\lambda \xi_k + \mu \xi_k')^2 = \lambda^2 \sum \xi_k^2 + \mu^2 \sum \xi_k'^2 + 2\lambda\mu \sum_{k=1}^{n} \xi_k \xi_k'$$
$$\le \left(\lambda \sqrt{\sum_{k=1}^{n} \xi_k^2} + \mu \sqrt{\sum_{k=1}^{n} \xi_k'^2}\right)^2$$

Schwarzsche Ungleichung

$$\le \lambda^2 c^2 + \mu^2 c^2 + 2\lambda\mu c^2$$
$$= (\lambda + \mu) c^2 = c^2$$

$$c^n \int_{\xi_1^2+\dots+\xi_n^2 \le 1} \dots \int d\xi_1 \dots d\xi_n = c^n \cdot \beta_n = c^n \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}$$

Satz $\exists$ ganze Zahlen $x_1, \dots, x_n$ nicht alle gleich Null, mit welche

$$x_1^2 + x_2^2 + \dots + x_n^2 \le 4 \left(\frac{|A|}{\beta_n}\right)^{2/n}$$

Verallgm. $\#$ Gitt. $N = n_1' + \dots + n_n'$
mit posit. quadr. Form.
Konst. von besonder Wichtigkeit ...