<u>Summe von 2 Quadraten</u>: Wie in §5 definiere für $n \in \mathbb{N}$:

$$R(n) = \# \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid n = a^2 + b^2 \text{ mit } (a,b) = 1 \}.$$

Eigentlich interessiert uns aber

$$r(n) = \# \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid n = a^2 + b^2 \}$$

$n = a^2 + b^2$, $d = (a,b)$ $\qquad n = (da')^2 + (db')^2 = d^2(a'^2 + b'^2)$

$\mathbb{N} \ni \frac{n}{d^2} = a'^2 + b'^2$ mit $(a', b') = 1$. Also

(1) $$r(n) = \sum_{d^2 \mid n} R\left(\frac{n}{d^2}\right)$$

(2) $$r(n) = \sum_{x \mid n} q(x) R\left(\frac{n}{x}\right) \quad \text{mit} \quad q(n) = \begin{cases} 1 & \text{wenn } n \text{ Quadrat} \\ 0 & \text{sonst} \end{cases}$$

(2') $$r = q * R$$

In §5 gezeigt: Hat n keine Primteiler $p \equiv 3 \bmod 4$ und ist $4 \nmid n$, so gilt

$$R(n) = 2^{s+2} \text{ mit } s = \text{Anzahl der ungeraden Primteiler von } n.$$
$\ulcorner R(1) = 4, \quad R(2) = 4 \lrcorner$

$$R(n) = 0 \text{ für alle anderen } n.$$

$\rho(n) := \# \{ x \bmod n \mid x^2 + 1 \equiv 0 \bmod n \}$. Dann

(3) $$R(n) = 4\rho(n) \quad \text{, denn:}$$

$\rho(n) \neq 0 \implies n$ wie oben und $\rho(n) = 2^s$ $\quad \ulcorner$vgl. §6, F2$\lrcorner$
$\rho(n) = 0 \implies R(n) = 0$ $\quad \ulcorner$klar bzw. ÜA$\lrcorner$

(3) und (2'):

$$(3') \qquad r = 4(q * \varrho)$$

q, ϱ multiplikativ! Also $q * \varrho$ multiplikativ.
(aber r nicht)

<u>F7:</u> Sei $n = 2^{\mu} m$ mit $2 \nmid m$ (μ bel.); und m habe nur Primteiler $p \equiv 1 \bmod 4$. Dann ist

$$r(n) = 4\,\tau(m) \qquad \ulcorner \tau(m) = \text{Anzahl der Teiler von } m \lrcorner$$

2.2. $(q*\varrho)(n) = \tau(m)$

<u>Bew.</u> Da $q * \varrho$ und τ multipl. ist, genügt es folgende Fälle zu betrachten:

① n 2-Potenz >1 ② n p-Potenz >1 mit $p \equiv 1 \bmod 4$

①: $\varrho(2^j) = 0$ für $j > 1$, $\varrho(1) = \varrho(2) = 1$; also

$$(4) \quad (q * \varrho)(2^{\mu}) = q(2^{\mu}) + q(2^{\mu-1}) = 1 = \tau(1) = 1$$

② $$(q*\varrho)(p^{2k}) = \overset{1}{\overset{\parallel}{q(1)}}\,\underset{\underset{2}{\parallel}}{\varrho(p^{2k})} + \overset{0}{\overset{\parallel}{q(p)}}\,\varrho(p^{2k-1}) + \overset{1}{\overset{\parallel}{q(p^2)}}\,\underset{\underset{2}{\parallel}}{\varrho(p^{2k-2})} + \ldots + \underline{q(p^{2k})\underset{\underset{1}{\parallel}}{\varrho(1)}}$$

$\ulcorner$vgl. §6$\lrcorner$

$$= 2k + 1 = \tau(p^{2k})$$

$$(q*\varrho)(p^{2k+1}) = q(p^0)\varrho(p^{2k+1}) + q(p^2)\varrho(p^{2k-1}) + \ldots + q(p^{2k})\varrho(p)$$

$$= (k+1)2 = 2k+2 = \tau(p^{2k+1})$$

Satz 2: Es sei $\chi = \chi_4$ definiert durch

$$\chi(n) = \begin{cases} (-1)^{\frac{n-1}{2}} & \text{für } n \text{ ungerade} \\ 0 & \text{für } n \text{ gerade} \end{cases}$$

(χ ist vollständig multipl.!, und zwar auch auf $\mathbb{Z}$)

Dann gilt für die Anzahl $r(n)$ der Darstellungen von $n \in \mathbb{N}$ als Summe von 2 Quadraten die Formel

$$r(n) = 4 \sum_{d|n} \chi(d).$$

Bew. Nach (3') ist zu zeigen:

$$q * \rho = \chi * i_0$$

Alle Funktionen multiplikativ. Also genügt es folg. Fälle zu betrachten:

1) $(\chi * i_0)(2^k) = \chi(1) = 1$ (denn $\chi(d) = 0$ für $2|d$)

$(q * \rho)(2^k) = 1$, vgl. (4)

2) $p \equiv 1 \bmod 4$: $\chi(p^i) = \chi(p)^i = 1^i = 1$ für alle i

$$(\chi * i_0)(p^k) = k+1 = \tau(p^k) \overset{F7}{=} (q * \rho)(p^k)$$

3) $p \equiv 3 \bmod 4$: $\chi(p^i) = \chi(p)^i = (-1)^i$

$$(\chi * i_0)(p^k) = 1 - 1 + 1 - \ldots + (-1)^k = \begin{cases} 1 & k \text{ gerade} \\ 0 & k \text{ ungerade} \end{cases}$$

$$(q * \rho)(p^k) = \rho(1)q(p^k) + \underset{0}{\rho(p)}\, q(p^{k-1}) + \underset{0}{\rho(p^2)}\, q(p^{k-2}) + \ldots$$

$$= q(p^k) = \begin{cases} 1 & k \text{ gerade} \\ 0 & k \text{ ungerade} \end{cases} \qquad \square$$

Nachtrag zu §1:

Wie oft kommt p in $n!$ vor? $\quad (n \in \mathbb{N}, p \in \mathbb{P})$

Fg: $\boxed{w_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots = \sum_{j \geq 1} \left[\frac{n}{p^j}\right]}$

Bew. klar.

Kor. Hat n die p-adische Entw. $n = a_r p^r + \dots + a_1 p + a_0$ $\ulcorner a_i \in \mathbb{Z},\ 0 \leq a_i \leq p-1,\ a_r \neq 0 \lrcorner$, so gilt

$$w_p(n!) = \frac{n - s_n}{p-1} \quad \text{mit } s_n = a_0 + a_1 + \dots + a_r$$

Bew. üA.

$1 \leq j \leq r$ $\quad \ulcorner \frac{n}{p^j} = a_r p^{r-j} + \dots + a_j + \underbrace{\frac{a_j}{p} + \dots + \frac{a_j}{p^j}}_{\leq p-1\left(\frac{1}{p} + \dots + \frac{1}{p^j}\right) < \frac{p-1}{p} \frac{1}{1-\frac{1}{p}} = 1}$

also $\left[\frac{n}{p^j}\right] = a_r p^{r-j} + \dots + a_{j+1} p + a_j$, $\implies$

$$\sum_{j=1}^{r} \left[\frac{n}{p^j}\right] = \sum_{j=1}^{r} \left(a_r p^{r-j} + \dots + a_{j+1} p + a_j\right) = \sum_{m=1}^{r} a_m \left(1 + p + \dots + p^{m-1}\right)$$

$$= \sum_{m=1}^{r} a_m \frac{p^m - 1}{p-1} = \frac{1}{p-1} \sum_{m=1}^{r} a_m (p^m - 1) =$$

$$\frac{1}{p-1} \left(\sum_{m=1}^{r} a_m p^m - \sum_{m=1}^{r} a_m\right) = \frac{1}{p-1} (n - s_n) \quad \lrcorner$$

Lemma: Für $x, y \in \mathbb{R}$ gilt
$$[x+y] - [x] - [y] \in \{0, 1\}$$

Bew. $x = [x] + \langle x\rangle$, $y = [y] + \langle y\rangle$ mit $0 \le \langle x\rangle, \langle y\rangle < 1$

$x+y = [x] + [y] + \langle x\rangle + \langle y\rangle$, $\Rightarrow$ $[x+y] = [x] + [y] + \underbrace{[\langle x\rangle + \langle y\rangle]}_{= 0 \text{ oder } 1}$

$n \in \mathbb{N}, p \in \mathbb{P}$
$k \in \mathbb{N}_0$ mit $k \le n$

F10: $$\boxed{w_p\left(\binom{n}{k}\right) \le \frac{\log n}{\log p}}$$

Bew. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, $\Rightarrow$ $w_p\left(\binom{n}{k}\right) = w_p(n!) - w_p(k!) - w_p((n-k)!)$

$\overset{F9}{=} \sum_{j \ge 1} \underbrace{\left(\left[\frac{n}{p^j}\right] - \left[\frac{k}{p^j}\right] - \left[\frac{n-k}{p^j}\right]\right)}_{\in \{0,1\} \text{ nach Lemma}} \le r$ mit dem maximalen $r \in \mathbb{N}_0$, so daß $p^r \le n$,

d.h. $r \log p \le \log n$

$r \le \frac{\log n}{\log p}$

$\Rightarrow$ Beh.

F11: $$\boxed{\binom{n}{k} \le n^{\pi(n)}}$$ (mit n, k wie oben; $\pi(n)$ die Anzahl der $p \in \mathbb{P}$ mit $p \le n$)

Bew. Habe $\binom{n}{k}$ die PFZ $\binom{n}{k} = \prod_{i=1}^{s} p_i^{\nu_i}$. o.E. $s \ge 1$.

Nach F10: $\nu_i \le \frac{\log n}{\log p_i}$, $\Rightarrow$ $(\log p_i)\nu_i \le \log n$, $\Rightarrow$ $e^{(\log p_i)\nu_i} \le e^{\log(n)}$,

$\Rightarrow$ $p_i^{\nu_i} \le n$; insbesondere $p_i \le n$ (da $\nu_i \ge 1$)

Es folgt
$$\binom{n}{k} = \prod_{i=1}^{s} p_i^{\nu_i} \le \prod_{i=1}^{s} n = n^s \le n^{\pi(n)}$$

F11 liefert schon wichtige Teilinformation über $\pi(n)$:

F12: $$\boxed{\pi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}}$$ für alle $n \geq 2$. $\ulcorner \frac{\log 2}{2} = 0{,}346\ldots \lrcorner$

Bew. Beh. richtig für $n = 2, 3, 4, 5$. Sei also $n \geq 6$

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \overset{F11}{\leq} \sum_{k=0}^{n} n^{\pi(n)} \leq (n+1)\, n^{\pi(n)}, \Rightarrow$$

$$n \log 2 \leq \log(n+1) + \pi(n) \log n, \Longrightarrow$$

$$\pi(n) \geq \log 2 \frac{n}{\log n} - \frac{\log(n+1)}{\log n}, \text{ d.h.}$$

(1) $$\pi(n) \geq \frac{n}{\log n}\left(\log 2 - \frac{\log(n+1)}{n}\right) \text{ für alle } n \geq 2.$$

$$\frac{\log(n+1)}{n} \leq \frac{\log 2}{2} \text{ für } n \geq 6$$ $\ulcorner$da $(n+1)^2 \leq 2^n$ für $n \geq 6$; ÜA: Induktion

Es folgt die Beh.

F12': Für alle reellen $x \geq 2$ gilt

(2) $$\boxed{\pi(x) \geq \frac{\log 2}{2} \frac{x}{\log x}}$$

Bew. ÜA.

$\ulcorner f(x) = \frac{x}{\log x}$ ist monoton wachsend für $x \geq e$, monoton fallend für $x \leq e$,
denn $f'(x) = \frac{\log x - 1}{(\log x)^2}$. Für $2 \leq x \leq e$ ist also $\frac{x}{\log x} \leq \frac{2}{\log 2}$,
also $\frac{\log 2}{2} \frac{x}{\log x} \leq 1 = \pi(x)$. Für $e \leq x < 3$ ist
$$\frac{\log 2}{2} \frac{x}{\log x} \leq \frac{\log 2}{2} \frac{3}{\log 3} < 1 = \pi(x).$$ Also