Additive Kombinatorik 2.

§1. Das Waring'sche Problem.

Erinnerung: Jede natürliche Zahl ist Summe von 4 Quadratzahlen.

Satz 1.1. (Hilbert): Für jedes $k \in \mathbb{N}$ gibt's $s \in \mathbb{N}$ derart, dass jede natürliche Zahl Summe von s k-ten Potenzen ist.

Sei $g(k)$ die kleinste solche Zahl. Man weiß

k	1	2	3	4	5	6	7	...
$g(k)$	1	4	9	19	37	73	143	...

Die Zahl $2^k \lfloor (\frac{3}{2})^k \rfloor - 1 < 3^k$ erfordert $2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$ Summanden, d.h. $g(k) \geq 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$. Bis auf höchstens endlich viele Ausnahmen gilt Gleichheit.

Vielleicht interessanter ist die kleinste Zahl $G(k)$ derart, dass jede hinreichend große nat. Zahl Summe von $G(k)$ k^{ten} Potenzen ist.

k	2	3	4	5	6	7	8
$G(k)$	4	$\in \{4,7\}$	16	$\in [6,17]$	$[9,24]$	$[8,31]$	$\in [32,42]$

Wooley zeigte $G(k) \leq (1+o(1))\, k \log k$.

<u>Satz 1.2.</u> Für alle $k \in \mathbb{N}$ ist $G(k) \leq 2^k + 1$.

§ 2. Das Waring'sche Problem in Restklassenringen.

Seien $k \geq 2$ und p eine Primzahl. Wir untersuchen Summen von k^{ten} Potenzen modulo Potenzen von p. Schreibe $k = k_0 \cdot p^\tau$ mit $p \nmid k_0$, $\tau \geq 0$.

<u>Lemma 2.1.</u> Es gibt mind. $\frac{p-1}{k_0}$ Zahlen $a \in [p-1]$, für die $x^k \equiv a \pmod{p}$ lösbar ist.

<u>Beweis.</u> Da $y^p \equiv y \pmod{p}$ für alle $y \in \mathbb{Z}$ gilt (kleiner Satz des Fermat) ist $x^k \equiv x^{k_0} \pmod{p}$ für alle $x \in \mathbb{Z}$.

Setze
$$A = \{ a \in [p-1] : x^{k_0} \equiv a \pmod{p} \text{ lösbar} \}.$$

Doppeltes Abzählen
$$p-1 = \sum_{a \in A} \left| \{ x \in [p-1] : x^{k_0} \equiv a \pmod{p} \} \right|.$$

Da $\mathbb{Z}/p\mathbb{Z}$ Körper ist, kann das Polynom $X^{k_0} - a$ höchstens k_0 Nullstellen haben. Also $p-1 \leq |A| \, k_0$. $\square$

<u>Lemma 2.2.</u> Wenn p ungerade, $p \nmid n$ und $s \geq 2k-1$, dann ist
$$x_1^k + \dots + x_s^k \equiv n \pmod{p^{\tau+1}}$$
lösbar.

<u>Beweis.</u> Für $\sigma \geq 1$ setze
$$C_\sigma = \{ a \in (\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times : a = x_1^k + \dots + x_\sigma^k \text{ hat Lösung mit } x_1, \dots, x_\sigma \in \mathbb{Z}/p^{\tau+1}\mathbb{Z} \}$$

Insbesondere

$$C_1 = \{ x^k : x \in (\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times \}$$

und Lemma 2.1 verrät uns $|C_1| \geq \frac{p-1}{k_0}$.

Offenbar $C_1 \subseteq C_2 \subseteq C_3 \subseteq C_4 \subseteq \ldots$.

<u>Annahme</u> $C_1 \subsetneq C_3 \subsetneq C_5 \subsetneq \ldots \subsetneq C_{2k+1}$.

Da C_σ unter Multiplikation mit C_1 abgeschlossen ist, ist dann $|C_{2i+1} \setminus C_{2i-1}| \geq \frac{p-1}{k_0}$ für $i = 1, 2, \ldots, k$.

Mithin

$$|C_{2k+1}| = |C_{2k+1} \setminus C_{2k-1}| + |C_{2k-1} \setminus C_{2k-3}| + \ldots + |C_3 \setminus C_1| + |C_1|$$

$$\geq (k+1) \cdot \frac{p-1}{k_0} > k_0 p^\tau \cdot \frac{p-1}{k_0}$$

$$= p^\tau (p-1) = |(\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times| \quad \underline{\underline{\text{Wid.}}}$$

Also gibt's $i_* \leq 2k-1$ mit $C_{i_*} = C_{i_*+1} = C_{i_*+2}$.

Wenn $C_{i_*} = (\mathbb{Z}/p^{\tau+1}\mathbb{Z})^\times$ sind wir fertig.

Andernfalls wähle $j > i_*$ minimal mit $C_{i_*} \subsetneqq C_j$.

Wir wissen $j \geq i_* + 3$. Wähle $m \in \mathbb{N}$ minimal mit $m + p^{\tau+1}\mathbb{Z} \notin \cancel{C_j}\, C_{i_*}$. Da $1 \in C_{i_*}$ ist $m \geq 2$.

Wenn $m \not\equiv 1 \pmod{p}$ ist $m-1 \in C_{i_*}$, also $m \in C_{i_*+1} = C_{i_*}$, Wid. Dies zeigt $m \equiv 1 \pmod{p}$ und daher $m \geq p+1 \geq 4$.

Außerdem $m-2 \in C_{i_*}$ (da $p \nmid m-2$ und m minimal), d.h. $m = (m-2) + 1^k + 1^k \in C_{i_*+2} = C_{i_*}$, Wid. $\square$

Folgerung 2.3. Wenn p ungerade, n beliebig, $s \geq 2k$, dann hat $n \equiv x_1^k + \dots + x_s^k \pmod{p^{\tau+1}}$ eine Lösung mit $p \nmid x_1$.

Beweis. Wenn $n \not\equiv 1 \pmod{p}$ gibt's nach Lemma 2.2 eine Lösung mit $x_1 = 1$. Wenn $n \equiv 1 \pmod{p}$ ist $p \nmid n$ und Lemma 1.2 liefert eine Lösung von

$$n \equiv x_1^k + \dots + x_s^k \pmod{p^{\tau+1}}.$$

Da nicht $p \mid x_1, \dots, x_s$ sein kann ist oBdA $p \nmid x_1$. $\square$

Lemma 2.4. Wenn k, n ungerade und $t \geq 1$ beliebig, dann ist

$$x^k \equiv n \pmod{2^t}$$

lösbar.

Beweis. Zu zeigen ist, dass die 2^{t-1} Zahlen

$$1^k, 3^k, 5^k, \dots, (2^t - 1)^k$$

mod. 2^t mit

$$1, 3, 5, \dots, 2^t - 1$$

übereinstimmen.

Andernfalls gäbe es ungerade Zahlen x, y mit $1 \le x < y \le 2^t - 1$ mit $x^k \equiv y^k \pmod{2^t}$.

Nun
$$y^k - x^k = (y-x)\underbrace{(y^{k-1} + xy^{k-2} + \ldots + x^{k-1})}_{\text{ungerade viele ungerade Summanden}}$$

also doch $x \equiv y \pmod{2^t}$ Wid.

Lemma 2.5. Wenn k gerade, $s \geq 5$ wenn $k = 2$, $s \geq 4k$ wenn $k \neq 2$, $n \in \mathbb{N}$, dann hat

$$x_1^k + \ldots + x_s^k \equiv n \pmod{2^{\tau+2}}$$

eine Lösung mit ungeradem x_1.

Beweis. Wenn $k = 2$ ist $\tau = 1$ und Quadratzahlen sind $0, 1, 4 \pmod{8}$. Sei nun $k \neq 2$. Nun $s \geq 4k \geq 2^{\tau+2}$ und es gibt eine Lösung mit $x_1 = 1$ und $x_i \in \{0,1\}$ für $i \in [2, s]$. $\square$

Zusammenfassung. $k = p^{\tau} k_0$ mit $p \nmid k_0$, p prim.

Setze
$$\gamma = \begin{cases} \tau + 1 & \text{wenn } p > 2 \\ \tau + 2 & \text{wenn } p = 2 \end{cases}$$

Proposition 2.6. Wenn $s \geq 2k + 1$ und n beliebig,

dann hat
$$n \equiv x_1^k + \dots + x_s^k \pmod{p^{\gamma}}$$
eine Lösung mit $p \nmid x_1$.

Beweis: Wenn p ung. benutze Folgerung 2.3 und $s \geq 2k$.
Wenn $p = 2$ benutze Lemma 2.4, 2.5. $\square$

Lemma 2.7. Für alle $t \geq \gamma$ und $i \geq 2$, dann $p^{t+1} \mid \binom{k}{i} p^{i(t-\tau)}$.

Beweis. Sei $\eta \geq 0$ maximal mit $p^{\eta} \mid i$.

Für $p > 2$ ist $3^{\eta} \leq p^{\eta} \leq i < 3^{i-1}$, also $\eta \leq i - 2$.

Für $p = 2$ ist $2^{\eta} \leq i < 2^{2i-2}$, also $\eta \leq 2i - 3$.

Lemma 2.8. Wenn $p \nmid a$, $t \geq \gamma$ und $x^k \equiv a \pmod{p^t}$ lösbar ist, dann ist $x^k \equiv a \pmod{p^{t+1}}$ auch lösbar.

Beweis. Sei $x^k \equiv a \pmod{p^t}$. Für $\frac{x^k - a}{p^t} = b$ ist also

$$x^k \equiv a + b \cdot p^t \pmod{p^{t+1}}.$$

Für alle $h \in \mathbb{Z}$ ist

$$(x + h \cdot p^{t-\tau})^k \equiv x^k + k \cdot x^{k-1} \cdot h p^{t-\tau} + \sum_{i \geq 2} \underbrace{\binom{k}{i} p^{(t-\tau)i}}_{\text{durch } p^{t+1} \text{ teilbar}} h^i x^{k-i}$$

$$\equiv x^k + k_0 x^{k-1} h p^t$$

$$\equiv a + (b + \underbrace{k_0 x^{k-1}}_{\text{nicht durch } p \text{ teilbar}} h) p^t \pmod{p^{t+1}}.$$

In beiden Fällen $\eta \leq (i-1)(g-\tau)-1 \leq (i-1)(t-\tau)-1$,

also $t+1+\eta \leq (t-\tau)\cdot i + \tau$.

Folglich $p^{t+1+\eta} \mid p^{(t-\tau)\cdot i} \cdot p^{\tau} \cdot k_0 \cdot \binom{k-1}{i-1}$.

Da $p^{\tau} \cdot k_0 \cdot \binom{k-1}{i-1} = k \cdot \binom{k-1}{i-1} = i \cdot \binom{k}{i}$

zeigt dies $p^{t+1} \mid p^{(t-\tau)\cdot i} \cdot \frac{i}{p^\eta} \cdot \binom{k}{i}$.

nicht durch p teilbar, da η maximal

Also $p^{t+1} \mid p^{(t-\tau)\cdot i} \cdot \binom{k}{i}$. $\square$

Wählt man h so, dass $p \mid b + k_0 x^{k-1} h$, dann

$$(x + h x^{t-\tau})^k \equiv a \pmod{p^{t+1}}.$$

Für $n, q, s \in \mathbb{N}$ setze

$$M_q(n,s) = \left| \{ (x_1, \dots, x_s) \in (\mathbb{Z}/q\mathbb{Z})^s : n = x_1^k + \dots + x_s^k \} \right|$$

<u>Lemma 2.9.</u> Wenn $s \geq 2^k + 1$, $t \geq 8$, $n \in \mathbb{N}$,

dann $|M_{p^t}(n,s)| \geq p^{(t-8)(s-1)}$.

<u>Beweis.</u> Nimm $(x_1, \dots, x_s) \in (\mathbb{Z}/p^8\mathbb{Z})^s$ mit

$x_1^k + \dots + x_s^k = n$, $p \nmid x_1$ (Prop 2.6)

Man kann $x_2, \dots, x_s$ jeweils auf p^{t-8} Arten nach

$\mathbb{Z}/p^t\mathbb{Z}$ heben. Für jede der $p^{(t-8)(s-1)}$ Kombinationen

gibt's geeignetes x_1 nach Lemma 2.8. $\square$

Satz 2.10. Wenn $s \geq 2^k + 1$, dann gilt

$$\liminf_{t \to \infty} \frac{M_{p^t}(n, s)}{p^{t(s-1)}} > 0$$

Beweis. Nach Lemma 2.9 ist die linke Seite sogar

$$p^{-\gamma(s-1)}.$$

$\square$