Aufgabenzettel 3.

3.1. Die Aufgabe 2.4 legt folgende Vermutung nahe: *Sei p Primzahl, seien t, n natürliche Zahlen mit $1 \leq n \leq p^t$. Ist s maximal, sodass p^s Teiler von n ist, so gilt*

$$\binom{p^t}{n}_p = p^{t-s}.$$

Man beweise diese Vermutung. Hilfestellung. Zeige zuerst: Seien x, x', y positive reele Zahlen mit $\frac{x+x'}{y} \in \mathbb{N}$. *Ist auch* $\frac{x}{y} \in \mathbb{N}$, *so ist*

$$\lfloor \frac{x+x'}{y} \rfloor = \lfloor \frac{x}{y} \rfloor + \lfloor \frac{x'}{y} \rfloor.$$

Ist dagegen $\frac{x}{y}$ *keine natürliche Zahl, so ist*

$$\lfloor \frac{x+x'}{y} \rfloor = \lfloor \frac{x}{y} \rfloor + \lfloor \frac{x'}{y} \rfloor + 1.$$

Folgere: $\lfloor \frac{p^t}{p^i} \rfloor = \lfloor \frac{n}{p^i} \rfloor + \lfloor \frac{p^t-n}{p^i} \rfloor$ genau dann, wenn p^i ein Teiler von n ist. Folgere daraus die Behauptung.

3.2. Wir betrachten wieder den Binomialkoeffizienten $\binom{2n}{n}$. Wir wissen: Ist p eine Primzahl, die diesen Binomialkoeffizienten teilt, so ist $p \leq 2n$.

Betrachte alle Primzahlen p mit $\sqrt{2n} < p \leq 2n$. Ist p eine solche Primzahl, wähle t maximal mit $p \leq \frac{2n}{t}$. Zeige:

(a) Ist t gerade, so ist $\binom{2n}{n}_p = 1$,

(b) Ist t ungerade, so ist $\binom{2n}{n}_p = p$.

(Dies verallgemeinert die Aussagen (1), (2) im Abschnitt 1.3.; als Beispiel sollen die Primteiler $p > \sqrt{2n}$ von $\binom{400}{200}$ angegeben werden.)

3.3. (Erdös). Zeige mit Hilfe der folgenden Überlegungen:

$$\pi(n) \geq \frac{1}{2 \ln 2} \ln n.$$

(wieder ein Beweis, dass es unendlich viele Primzahlen gibt...)

(a) Zeige: Die Anzahl der Quadratzahlen m mit $m \leq n$ ist höchstens $\sqrt{n}$.

(b) Die Anzahl der quadratfreien Zahlen m mit $m \leq n$ ist höchstens $2^{\pi(n)}$.

(c) Folgere aus der eindeutigen Primfaktorzerlegung, dass demnach gilt:

$$n \leq \sqrt{n}\, 2^{\pi(n)},$$

und zeige damit die Behauptung.

(d) Vergleiche diese Abschätzung mit der Abschätzung $\pi(n) \geq \frac{\ln 2}{4} \cdot \frac{n}{\ln n}$, die in der Vorlesung gezeigt wurde.

3.4. Fermat-Zahlen. Die Zahlen der Form $F_n = 2^{2^n} + 1$ mit $n \in \mathbb{N}_0$ nennt man *Fermat-Zahlen.*

(a) Setze $G_n = F_n - 2 = 2^{2^n} - 1$. Zeige: $F_n G_n = G_{n+1}$ für $n \in \mathbb{N}_0$.

(b) Folgerung: $\prod_{t=0}^{n} F_t = G_{n+1}$.

(c) Folgerung: Die Fermat-Zahlen sind paarweise teilerfremd.

(d) Folgere daraus: Es gibt unendliche viele Primzahlen.

Präsenz-Aufgaben.

1. Das Sieb des Eratosthenes (276-194 v.u.Z.). Man verwende Aufgabe 1.4 um alle Primzahlen $p \leq 200$ explizit anzugeben: Man bestimmt zuerst die Primzahlen $p_1 < \cdots < p_6$ mit $p_i \leq \sqrt{200}$. Dann notiert man die Zahlen n mit $1 \leq n \leq 200$. Man streicht als erstes die Zahl 1, dann alle Vielfachen der Zahlen p_i, für $1 \leq i \leq 6$ (also alle geraden Zahlen, alle durch 3 teilbaren Zahlen, alle durch 5 teilbaren Zahlen, usw.). Übrig bleiben die Primzahlen p mit $\sqrt{200} < p \leq 200$. Warum?

2. Zyklische Gruppen.

(a) Bestimme alle Elemente $\overline{z}$ in der Gruppe $G = (\mathbb{Z}/22, +)$ mit $G = \langle \overline{z} \rangle$.

(b) Man suche ein Element $\overline{z}$ in der Gruppe $G = ((\mathbb{Z}/23)^*, \cdot)$ mit $G = \langle \overline{z} \rangle$.

(c) Wie findet man in $G = ((\mathbb{Z}/23)^*, \cdot)$ weitere Elemente $\overline{z}$ mit $G = \langle \overline{z} \rangle$?

(d) Statt $p = 23$ betrachte man in (b) und (c) die Primzahlen $p = 17$ und $p = 11$.

English translation: see

`http://www.math.uni-bielefeld.de/birep/ez/Welcome.html`

Link: Aufgaben.