Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix

Elementare Zahlentheorie

Sommersemester 2017

Übungsblatt 4 16. Mai 2017

Aufgabe 17. (IMO 1967, Aufgabe 3)

Seien k, m, n natürliche Zahlen, so daß $p = m + k + 1$ eine Primzahl größer als $n + 1$ ist.

Wir setzen $c_x = x(x + 1)$ für alle $x \in \mathbb{N}$ und betrachten das Produkt

$$N = (c_{m+1} - c_k)(c_{m+2} - c_k) \cdot \ldots \cdot (c_{m+n} - c_k).$$

Zeigen Sie, daß N durch $\prod_{i=1}^{n} c_i$ teilbar ist.

Tipp: (1) Faktorisieren Sie für allgemeine $x, y \in \mathbb{Z}$ den Ausdruck $c_x - x_y$ in zwei Faktoren, die linear in x und y sind. (2) Wozu ist es nützlich/nötig, daß p eine Primzahl ist?

Aufgabe 18. (IMO 1972, Aufgabe 3)

(a) Zeigen Sie, daß für alle $x, y \in \mathbb{R}$ gilt:

$$\lfloor 2x \rfloor + \lfloor 2y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor.$$

(b) Zeigen Sie, daß für alle natürlichen Zahlen $n, m \in \mathbb{N}$ der Bruch

$$\alpha = \frac{(2n)!(2m)!}{n!m!(n + m)!}$$

eine natürliche Zahl ist.

Tipp: Was haben die beiden Aufgabenteile miteinander zu tun?

Aufgabe 19. (Umkehrung des Satzes von Wilson)

(a) Sei $n \in \mathbb{Z}$ eine ganze Zahl, $n > 1$. Zeigen Sie:

$$(n - 1)! \equiv -1 \pmod{n} \iff n \text{ ist Primzahl.}$$

(b) Zeigen Sie, daß es eine endliche Menge $S \subseteq \mathbb{Z}$ gibt, so daß für alle $n \in \mathbb{Z}$, $n > 0$ es ein $a \in S$ gibt mit $(n - 1)! \equiv a \pmod{n}$.

(c) Kann man $S \subseteq \mathbb{N}$ wählen?

(d) Finden Sie ein S wie in (b) mit der kleinsten möglichen Anzahl von Elementen.
Tipp: Zeigen Sie $0, -1 \in S$.

Aufgabe 20.

(a) Sei ℓ ein Primfaktor von $2^p - 1$. Zeigen Sie, daß $\ell > p$.

(b) Beweisen Sie mittels (a), daß es unendlich viele Primzahlen gibt.

Aufgabe 21. (Summe zweier Quadrate)

Zeigen Sie:

(a) Ist eine natürliche Zahl n als Summe zweier Quadrate *rationaler* Zahlen darstellbar (Beispiel: $13 = (\frac{17}{5})^2+(\frac{6}{5})^2$), so läßt sie sich auch als Summe zweier Quadrate *ganzer* Zahlen darstellen.

(b) Sind $l, m \in \mathbb{N}$, so gilt:

$$\exists\, x, y \in \mathbb{Q} : \frac{l}{m} = x^2 + y^2 \quad \Longleftrightarrow \quad \exists\, u, v \in \mathbb{Z} : lm = u^2 + v^2.$$

(c) Sind $l, m \in \mathbb{N}$ teilerfremd, so läßt sich l/m genau dann als Summe zweier Quadrate rationaler Zahlen darstellen, wenn l und m Summen zweier Quadrate ganzer Zahlen sind.

Abgabe: Am kommenden Montag, den **22. Mai 2017**, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

`http://www.uni-frankfurt.de/65113368/17_SS_Elementare-Zahlentheorie`