Zahlentheorie: Übungsblatt 2
(für die Übungen am 1./2. November 2012)

Aufgabe 1 (mündlich)**.** Wir betrachten die abelsche Gruppe $F = \mathbb{Z}/5\mathbb{Z}$.

(a) Beschreiben Sie die Elemente von F (als Mengen) und geben Sie Repräsentanten für die Elemente an. Was ist der Repräsentant von $5\mathbb{Z}$?

(b) Seien $a = \overline{1}$ und $b = \overline{2}$. Beschreiben Sie $a + b$ als Menge.

(c) Wir definieren $\overline{2} \cdot \overline{3} = \{ab \mid a \in \overline{2}, b \in \overline{3}\}$. Ist dies wieder ein Element von F und wenn ja, welches?

(d) Gibt es ein Element $x \in F$, so dass $x \cdot \overline{4} = \overline{1}$? Ist es eindeutig?

(e) Sei jetzt $F' = \mathbb{Z}/6\mathbb{Z}$. Ändert sich Ihre Antwort auf die Fragen aus (a), (c) und (d)? Wie verhält es sich im Falle $\mathbb{Z}/n\mathbb{Z}$ für $n \in \mathbb{Z}$?

Aufgabe 2 (schriftlich)**.** (a) Die Fermatzahlen sind gegeben durch die Folge $F_n = 2^{2^n} + 1$ für $n \in \mathbb{N}$. Zeigen Sie, dass die Fermatzahlen F_m und F_n für $m \neq n$ teilerfremd sind und folgern Sie, dass es unendlich viele Primzahlen gibt.

(b) Sei $f(x)$ ein (nichtkonstantes) Polynom mit ganzzahligen Koeffizienten. Zeigen Sie, dass dann die Anzahl der Primteiler der Menge $\{f(k) \mid k \in \mathbb{N}_0\}$ unendlich ist. Folgern Sie, dass es unendlich viele Primzahlen geben muss.

Aufgabe 3 (schriftlich)**.** Eine ungerade Zahl $N \in \mathbb{N}$ soll faktorisiert werden mit Hilfe des folgenden Algorithmus: Setze $M_1 = N_1 = N$ und definiere q_k, N_k und M_k rekursiv wie folgt:

- $q_k \in \mathbb{N}$ ist gegeben durch $N_k = (2k+1) \cdot q_k + r_k$, wobei r_k der Rest nach Division von N_k durch $2k+1$ ist.
- $N_k = kN_1 - (2k+1)(q_1 + \ldots + q_{k-1})$.
- $M_k = N_1 - 2(q_1 + \ldots + q_{k-1})$.

Ist N_k teilbar durch $2k+1$ dann stoppt der Algorithmus und man erhält die Faktorisierung $N = (2k+1) \cdot M_{k+1}$.

(a) Benutzen Sie den Algorithmus, um $N = 4511$ zu faktorisieren.

(b) Zeigen Sie, dass der Algorithmus funktioniert.

Aufgabe 4 (mündlich)**.** Wir betrachten Kettenbrüche der Form

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \dots}}},$$

die wir der Einfachheit halber als $a_1 + \frac{1}{a_2+}\frac{1}{a_3+}\frac{1}{a_4+}\dots\frac{1}{a_n}$ schreiben. Der Kettenbruch $a_1 + \frac{1}{a_2+}\dots\frac{1}{a_k}$ heißt der $k$te Näherungsbruch. Kettenbrüche können als gewöhnlicher Bruch der Form $\frac{a}{b}$ geschrieben werden und man bezeichnet dann mit $[a_1, a_2, \dots, a_n]$ den Zähler des entsprechenden Bruches für $a_1 + \frac{1}{a_2+}\dots\frac{1}{a_n}$.

(a) Berechnen Sie $[a_1], [a_1, a_2], [a_1, a_2, a_3]$ und $[a_1, a_2, a_3, a_4]$.

(b) Zeigen Sie, dass

$$a_1 + \frac{1}{a_2+}\frac{1}{a_3+}\frac{1}{a_4+}\dots\frac{1}{a_n} = \frac{[a_1, a_2, \dots, a_n]}{[a_2, a_3, \dots, a_n]}$$

und

$$[a_1, a_2, \dots, a_n] = a_1[a_2, a_3, \dots, a_n] + [a_3, a_4, \dots, a_n].$$

Aufgabe 5 (mündlich)**.** Besitzt die Gleichung $x^4 + y^4 = z^4$ Lösungen in $\mathbb{N}$? [Benutzen Sie Aufgabe 5 aus Blatt 1 zweimal.]

http://www.mathematik.uni-stuttgart.de/studium/infomat/ZahlTheo-Koenig/