Universität Augsburg
4. September 2013

Pizzaseminar zu konstruktiver Mathematik
3. Übungsblatt

Aufgabe 1. *Schranken für die Größe der n-ten Primzahl*

Folgender Beweis der Unendlichkeit der Primzahlen wird Euklid zugeschrieben:

> Angenommen, $p_1, \ldots, p_r$ seien alle Primzahlen. Wir setzen $N := p_1 \cdots p_r + 1$. Nach dem Fundamentalsatz der Arithmetik lässt sich N in Primfaktoren zerlegen. Das ist ein Widerspruch, denn die p_i sind keine Teiler von N, andere Primzahlen gibt es aber nach Widersprungsvoraussetzung nicht.

a) Formuliere den Beweis so um, dass er konstruktiv folgende stärkere Aussage zeigt: *Seien $p_1, \ldots, p_r$ gegebene Primzahlen. Dann gibt es eine weitere Primzahl ungleich den p_i.* (Das war auch Euklids ursprüngliche Formulierung.)

b) Sei nun $p_1, p_2, \ldots$ die aufsteigende Folge aller Primzahlen. Extrahiere aus deinem Beweis die Abschätzung
$$p_{n+1} \leq p_1 \cdots p_n + 1.$$

c) Zeige folgende Schranke für die Größe der n-ten Primzahl:
$$p_n \leq 2^{2^{n-1}}.$$

Tatsächlich ist diese Schranke sehr pessimistisch. Aus Eulers Alternativbeweis der Unendlichkeit der Primzahlen, der nicht nur die Existenz, sondern auch die Eindeutigkeit der Primfaktorzerlegung verwendet, kann man eine bessere Schranke extrahieren; siehe etwa die Analyse in U. Kohlenbach, *Applied Proof Theory*, Kapitel 2, Seite 15f.

Aufgabe 2. *Friedmans Trick*

Beweise folgende fundamentale Eigenschaften der Friedmanübersetzung:

a) Sei φ eine Aussage, in der Existenzquantoren nur über bewohnte Typen gehen. Dann gilt intuitionistisch: $F \Longrightarrow \varphi^F$.

b) Sei φ eine Aussage, in der nur $\top$, $\bot$, $\wedge$, $\vee$ und $\exists$ (über bewohnte Typen), aber nicht $\Rightarrow$ oder $\forall$ vorkommen. Dann gilt intuitionistisch: $\varphi^F \Longleftrightarrow \varphi \vee F$.

   Tipp: Induktion über den Aussageaufbau.

c) Seien φ und ψ beliebige Aussagen in einem Kontext $\vec{x}$ (mit $\exists$ nur über bewohnte Typen). Wenn $\varphi \vdash_{\vec{x}} \psi$ intuitionistisch, dann gilt auch $\varphi^F \vdash_{\vec{x}} \psi^F$ intuitionistisch.

   Tipp: Induktion über den Aufbau von Ableitungen – zu zeigen ist, dass die Friedmanübersetzungen aller Schlussregeln intuitionistisch gültig sind.

d) Die Peano-Axiome implizieren ihre Friedmanübersetzungen.

Aufgabe 3. *Formaler Nullstellensatz*

Seien $f_1, \ldots, f_n \in R[X_1, \ldots, X_m]$ Polynome in m Variablen über einem Ring R mit $1 \neq 0$.

a) Gelte $1 = p_1 f_1 + \cdots + p_n f_n$ für gewisse Polynome $p_1, \ldots, p_n$. Zeige, dass die Polynome f_i keine gemeinsame Nullstelle besitzen.

b) Zeige umgekehrt, dass man aus einem Beweis, dass die f_i keine gemeinsame Nullstelle besitzen, genauer einem Beweis der Sequenz
$$Z(f_1) \wedge \cdots \wedge Z(f_n) \vdash \bot$$
   welcher von der im Skript beschriebenen Form ist, explizit eine Darstellung des Einspolynoms wie in a) erhalten kann.