Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής & Υπολογιστών
http://courses.softlab.ntua.gr/typesys/

Συστήματα Τύπων των Γλωσσών Προγραμματισμού

Σειρά Ασκήσεων #6

Προθεσμία παράδοσης: 10/3/2010

Οι ασκήσεις πρέπει να παραδοθούν μέσω e-mail στο διδάσκοντα (nickie@softlab.ntua.gr) σε ηλεκτρονική μορφή (LaTeX). Καθυστερημένες ασκήσεις θα βαθμολογούνται με μικρότερο βαθμό, αντιστρόφως ανάλογα προς το χρόνο καθυστέρησης.

1 Εξαρτώμενοι τύποι, Curry-Howard και Coq

Για τα παρακάτω, θα χρειαστεί να εγκαταστήσετε το Coq (ή να χρησιμοποιήσετε τους υπολογιστές του SoftLab). Θα βρείτε ό,τι χρειαστείτε στην ιστοσελίδα http://coq.inria.fr/ (και ο διδάσκων σας προειδοποιεί ότι θα χρειαστείτε πολλά, πολύ χρόνο και πολλή υπομονή).

Άσκηση 6.1 Άπειροι πρώτοι αριθμοί

Αποδείξτε στο Coq το παρακάτω θεώρημα, σύμφωνα με το οποίο για κάθε φυσικό αριθμό υπάρχει ένας μεγαλύτερος πρώτος αριθμός.

```
Require Export ZArith.
Require Export Znumtheory.

Theorem infinite_primes:
  forall n, exists p, n < p /\ prime p.
Proof.
  ...
Qed.
```

Είναι καλύτερα να επιχειρήσετε την απόδειξη τμηματικά, αποδεικνύοντας πρώτα ευκολότερα λήμματα και στη συνέχεια χρησιμοποιώντας αυτά.

Υπόδειξη: Τα περιεχόμενα της επόμενης σελίδας προορίζονται για διευκόλυνσή σας. Μπορείτε αν θέλετε να τα αγνοήσετε και να ακολουθήσετε το δικό σας δρόμο. Κατ' αρχήν περιγράφεται μία απόδειξη με λόγια, με λίγες περισσότερες λεπτομέρειες απ' όσες θα βρίσκατε σε ένα τυπικό βιβλίο αριθμοθεωρίας. (Ο συμβολισμός $p \mid n$ σημαίνει "ο p διαιρεί τον n".) Έπειτα περιγράφεται μία πιθανή δομή της απόδειξης στο Coq.

Απόδειξη με λόγια

Έστω τυχαίος αριθμός n. Έστω $p_1, p_2, \ldots, p_k$ όλοι οι πρώτοι αριθμοί που δεν υπερβαίνουν το n. Έστω $m = \prod_{i=1}^{k} p_i$. Εξετάζουμε τον αριθμό $m + 1$. Δύο περιπτώσεις:

1. Αν είναι πρώτος, τότε σίγουρα θα είναι $n < m + 1$, διαφορετικά θα ήταν $m + 1 = p_i$ για κάποιο i, κάτι που είναι άτοπο λόγω της κατασκευής του m. Επομένως ο αριθμός $m + 1$ είναι η απάντησή μας.
2. Αν δεν είναι πρώτος, τότε υπάρχει κάποιος πρώτος p τέτοιος ώστε $p \mid m + 1$. Συγκρίνουμε τον p με το n. Πάλι δύο περιπτώσεις:
   (α) Αν $p \leq n$, τότε θα είναι $p = p_i$ για κάποιο i, οπότε λόγω της κατασκευής του m έχουμε $p \mid m$, κάτι που είναι πάλι άτοπο γιατί έχουμε επίσης $p \mid m + 1$.
   (β) Αν $n < p$, ο αριθμός p είναι η απάντησή μας.

Δομή της απόδειξης στο Coq

Είναι αρκετά πιθανό (όχι όμως βέβαιο) ότι θα χρειαστείτε τα εξής:

- Μια συνάρτηση (ή έναν επαγωγικό ορισμό) που να υπολογίζει το γινόμενο των πρώτων αριθμών που δεν υπερβαίνουν το n.
- Ένα λήμμα που να λέει ότι αν m είναι το γινόμενο των πρώτων αριθμών που δεν υπερβαίνουν το n και $p < n$ είναι πρώτος, τότε $p \mid m$.
- Ένα λήμμα που να λέει ότι αν ο $n > 1$ δεν είναι πρώτος, τότε υπάρχει πρώτος $p < n$ τέτοιος ώστε $p \mid n$.
- Ένα λήμμα που να λέει ότι αν ο p είναι πρώτος, τότε για κάθε n δεν μπορεί να συμβαίνει συγχρόνως $p \mid n$ και $p \mid n + 1$.

Αν χρειαστείτε την κλασσική αρχή της επαγωγής των φυσικών αριθμών για τους αριθμούς του συνόλου `Z` του Coq (σε δυαδική αναπαράσταση), θα χρειαστεί να κάνετε `Require Export Wf_Z.` Έπειτα, η απλή επαγωγή δίνεται από το θεώρημα `natlike_ind` (και η πρωταρχική αναδρομή από το `natlike_rec`) ενώ μια γενικευμένη επαγωγή δίνεται από το θεώρημα `Zlt_0_ind`.