Class 22: Prime Detectives

Schedule

Here's the updated (and final) schedule for the rest of the semester:

– **Problem Set 9**: due on Friday, 1 December at 6:29pm. (This will be posted on 19 November.)
– **Problem Set Omega** (this is optional, and not like the others, hence it uncountable number): due on Monday, 4 December at 11:59pm.
– **Final Exam**: Thursday, 7 December, 9am-noon (in the normal lecture room)

Number Theory

Definition: a divides b ($a \mid b$) iff there is an integer k such that $ak = b$.

Definition: A *prime* is a number greater than 1 that is divisible only by itself and 1.

Theorem: There are *infinitely* many prime numbers.

Prove by contradiction (and well ordering principle):

Fundamental theorem of arithmetic: every positive number n can be written uniquely as a product of primes: $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$ where $p_i \leq p_{i+1}$.

Groups and Rings

R is an Abelian group with respect to binary operation P if it is:

– associative: $\forall a, b, c \in R.(aPb)Pc = aP(bPc)$.
– commutative: $\forall a, b \in R.aPb = bPa$.
– has an identity: $\exists z \in R.\forall a \in R.aPz = a$.
– every element has an inverse with respect to that identity: $\forall a \in R.\exists w \in R.aPw = z$.

Which of these are Abelian groups:

– $R = \mathbb{N}, P = +$.
– $R = \mathbb{N}, P = \times$.
– $R = \mathbb{Z}, P = +$.
– $R = \mathbb{Q}, P = \times$.
– $R = \{T, F\}, P = NAND$.

