

## rec.1 Primes

cmp:rec:pri:  
sec

Bounded quantification and bounded minimization provide us with a good deal of machinery to show that natural functions and relations are primitive recursive. For example, consider the relation “ $x$  divides  $y$ ”, written  $x \mid y$ .  $x \mid y$  holds if division of  $x$  by  $y$  is possible without remainder, i.e., if  $y$  is an integer multiple of  $x$ . (If it doesn’t hold, i.e., the remainder when dividing  $x$  by  $y$  is  $> 0$ , we write  $x \nmid y$ .) In other words,  $x \mid y$  iff for some  $z$ ,  $x \cdot z = y$ . Obviously, any such  $z$ , if it exists, must be  $\leq y$ . So, we have that  $x \mid y$  iff for some  $z \leq y$ ,  $x \cdot z = y$ . We can define the relation  $x \mid y$  by bounded existential quantification from  $=$  and multiplication by

$$x \mid y \Leftrightarrow (\exists z \leq y) (x \cdot z) = y.$$

We’ve thus shown that  $x \mid y$  is primitive recursive.

A natural number  $x$  is *prime* if it is neither 0 nor 1 and is only divisible by 1 and itself. In other words, prime numbers are such that, whenever  $y \mid x$ , either  $y = 1$  or  $y = x$ . To test if  $x$  is prime, we only have to check if  $y \mid x$  for all  $y \leq x$ , since if  $y > x$ , then automatically  $y \nmid x$ . So, the relation  $\text{Prime}(x)$ , which holds iff  $x$  is prime, can be defined by

$$\text{Prime}(x) \Leftrightarrow x \geq 2 \wedge (\forall y \leq x) (y \mid x \rightarrow y = 1 \vee y = x)$$

and is thus primitive recursive.

The primes are 2, 3, 5, 7, 11, etc. Consider the function  $p(x)$  which returns the  $x$ th prime in that sequence, i.e.,  $p(0) = 2$ ,  $p(1) = 3$ ,  $p(2) = 5$ , etc. (For convenience we will often write  $p(x)$  as  $p_x$  ( $p_0 = 2$ ,  $p_1 = 3$ , etc.)

If we had a function  $\text{nextPrime}(x)$ , which returns the first prime number larger than  $x$ ,  $p$  can be easily defined using primitive recursion:

$$\begin{aligned} p(0) &= 2 \\ p(x+1) &= \text{nextPrime}(p(x)) \end{aligned}$$

Since  $\text{nextPrime}(x)$  is the least  $y$  such that  $y > x$  and  $y$  is prime, it can be easily computed by unbounded search. But it can also be defined by bounded minimization, thanks to a result due to Euclid: there is always a prime number between  $x$  and  $x! + 1$ .

$$\text{nextPrime}(x) = (\min y \leq x! + 1) (y > x \wedge \text{Prime}(y)).$$

This shows, that  $\text{nextPrime}(x)$  and hence  $p(x)$  are (not just computable but) primitive recursive.

(If you’re curious, here’s a quick proof of Euclid’s theorem. Suppose  $p_n$  is the largest prime  $\leq x$  and consider the product  $p = p_0 \cdot p_1 \cdot \dots \cdot p_n$  of all primes  $\leq x$ . Either  $p + 1$  is prime or there is a prime between  $x$  and  $p + 1$ . Why? Suppose  $p + 1$  is not prime. Then some prime number  $q \mid p + 1$  where  $q < p + 1$ . None of the primes  $\leq x$  divide  $p + 1$ . (By definition of  $p$ , each of the

primes  $p_i \leq x$  divides  $p$ , i.e., with remainder 0. So, each of the primes  $p_i \leq x$  divides  $p + 1$  with remainder 1, and so  $p_i \nmid p + 1$ .) Hence,  $q$  is a prime  $> x$  and  $< p + 1$ . And  $p \leq x!$ , so there is a prime  $> x$  and  $\leq x! + 1$ .)

**Problem rec.1.** Define integer division  $d(x, y)$  using bounded minimization.

## Photo Credits

## Bibliography