Dr. Z.'s Number Theory Lecture 5 Handout: Prime Numbers, the sieve of Eratosthenes

By Doron Zeilberger

Definition: A *prime number* is a positive integer (larger than 1) that is **only** divisible by 1 and itself.

How to decide whether a positive integer n is prime? (The VERY STUPID WAY).

Starting with 2, try to divide it by any integer smaller than n, and see whether you ever get remainder 0. If you do, then the candidate integer n is **composite**, otherwise it is **prime**.

Problem 5.1: Decide whether 17 is prime using the **very stupid way**.

Solution to 5.1: $17/2 = 8(1), 17/3 = 5(2), 17/4 = 4(1), 17/5 = 3(2), 17/6 = 2(5), 17/7 = 2(3), 17/8 = 2(1),\ 17/9 = 1(8), 17/10 = 1(7), 17/11 = 1(6), 17/12 = 1(5),\ 17/13 = 1(4), 17/14 = 1(3), 17/15 = 1(2), 17/16 = 1(1)$.

So if you divide 17 by all integers from 2 to 16 you never get 0 remainder. Hence 17 is prime.

How to decide whether a positive integer n is prime? (The STUPID WAY).

Since if $n = ab$, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (why?), it is enough to check every integer $\leq \sqrt{n}$.

Problem 5.1': Decide whether 17 is prime using the **stupid way**.

Solution to 5.1': $4 < \sqrt{17} < 5$, so we only have to check $17/2 = 8(1), 17/3 = 5(2), 17/4 = 4(1)$.

So if you divide 17 by all integers from 2 to $[\sqrt{17}] = 4$ you never get 0 remainder. Hence 17 is prime.

How to decide whether a positive integer n is prime? (The OK WAY).

If n is divisible by some integer $< \sqrt{n}$, it must be divisible by some *prime* $< \sqrt{n}$ So it is enough to check every **prime** $\leq \sqrt{n}$.

Problem 5.1": Decide whether 17 is prime using the **OK way**.

Solution to 5.1": $4 < \sqrt{17} < 5$, so we only have to check $17/2 = 8(1), 17/3 = 5(2)$.

So if you divide 17 by all primes from 2 to $[\sqrt{17}] = 4$ you never get 0 remainder. Hence 17 is prime.

There is only one catch, how do we find out all the primes $\leq n$. Using the OK way, we do it *recursively*, one-by-one, by using the *sieve* of Eratosthenes.

Input: A positive integer n

Output: The list of all prime numbers $\leq n$, written in increasing order.

Step 1: Write down *all* the integers from 2 to n

Step 2.0: Cross out the (proper) multiples of 2. Look at the smallest new survivor (it happens to be 3).

Step 2.1: Cross out the proper multiples of 3. Look at the smallest new survivor (it happens to be 5).

Step 2.: Until you reach $\sqrt{n}$, keep crossing-out the multiples of the new smallest survivor (that has not been used before).

The list of *survivors* (those that have not been crossed out), is the list of primes $\leq n$.

Problem 5.2: Find all the prime numbers ≤ 20.

Solution to 5.2:

Step 1:

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20$$

Step 2.1: Cross-out, all multiples of 2 (except 2)

$$2, 3, \mathbf{4}, 5, \mathbf{6}, 7, \mathbf{8}, 9, \mathbf{10}, 11, \mathbf{12}, 13, \mathbf{14}, 15, \mathbf{16}, 17, \mathbf{18}, 19, \mathbf{20}$$

Step 2.2: Cross-out, all multiples of 3 (except 3)

$$2, 3, \mathbf{4}, 5, \mathbf{6}, 7, \mathbf{8}, \mathbf{9}, \mathbf{10}, 11, \mathbf{12}, 13, \mathbf{14}, \mathbf{15}, \mathbf{16}, 17, \mathbf{18}, 19, \mathbf{20}$$

The smallest survivor 5 is larger than $\sqrt{20}$, so we are done!

Ans. to 5.2: The list of prime numbers ≤ 20 are

$$2, 3, 7, 11, 13, , 17, 19 \quad .$$

Euclid's Proof that there are "infinitely" many primes

Suppose that there are only finitely many primes, n of them, let's call them, in order

$$p_1, p_2, \ldots, p_n \quad .$$

Consider

$$P = p_1 p_2 \cdots p_n + 1 \quad .$$

This number leaves remainder 1 when divided by each of $p_1, \ldots, p_n$, hence is either prime (larger than p_n), or is divisible by a prime larger than p_n, contradiction. Hence there is always an infinite supply of prime numbers.

This can be used to construct, an *infinite* sequence of prime numbers.

Let $p_1 = 2$, and let p_n be the smallest prime-divisor of $p_1 p_2 \cdots p_{n-1} + 1$.

It starts like this: $2, 3, 7, 43, 13, \ldots$, and it is called the **Euclid-Mullin** sequence.