MATH453 Elementary Number Theory

Lecture 3: Primes

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

3.1 Elementary Properties of Primes

Recall that a natural number **greater than 1** is ***prime*** if it has no factors other than 1 and itself. A natrual number greater than 1 is ***composite*** if it is not prime.

We begin by introducing some elementary facts about prime numbers.

Lemma 3.1. Every integer greater than 1 has a prime divisor.

Proof. By (strong) induction on n.

Base case: $n = 2$. The lemma clearly holds because 2 is a prime.

Inductive step: Let $n \geq 2$ be an arbitrary integer. Suppose that the lemma is true for all integers $2 \leq n' < n$. If n is prime, we are done. So assume n is not prime. Then, by definition, n is composite and can be expressed as $n = ab$ for some $a, b < n$. By induction hypothesis, a and b both have at least one prime divisors. Hence, n also have a prime divisors. ■

Theorem 3.2 (Infinitude of Primes)**.** There exists infinitely many primes.

Proof. By contradiction. Suppose there exist only finitely many primes $p_1, \ldots, p_n$.

Let $N = p_1 p_2 \ldots p_n + 1$. By Lemma 3.1, N has at least one prime divisor and since $\{p_1, \ldots, p_n\}$ are all the primes by assumption, there must exists some i such that $p_i \mid N$. Since $p_i \in \{p_1, \ldots, p_n\}$, we have that $p_i \mid p_1 \ldots p_n$ trivially. Further, $p_i \mid N$, so $p_i \mid N - p_1 \ldots p_n$. This implies that $p_i \mid 1$. But no prime can divide 1. This is a contradiction. ■

Proposition 3.1. If n is composite, then there exists at least one prime $p \leq \sqrt{n}$ dividing n.

Proof. By contradiction. Let n be an arbitrary composite number. By Lemma 3.1, we know that has at least one prime divisor p_j. Suppose for contradiction that all such p_j are $p_j > \sqrt{n}$.

n is composite, so we assume that it has m divisors of n where $m \geq 2$. Then,

$$n > \underbrace{\sqrt{n}\sqrt{n} \cdots \sqrt{n}}_{m} = n^{m/2} \geq n$$

This implies $n > n$, which is a contradiction. ■

3.2 Finding Primes

Algorithm known as the Sieve[1] of Eratosthenes.

To find all primes $\leq x$, we list all integers up to x. Strike out every integer $\leq \sqrt{x}$ that is a multiple of primes $\leq \sqrt{x}$. In the end, whatever remains are primes.

Example (Finding primes ≤ 28). List all numbers:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

2 is prime, so we circle it. Then, we strike out all numbers that is a multiple of 2.

$\boxed{2}$ 3 $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ 9 $\cancel{10}$ 11 $\cancel{12}$ 13 $\cancel{14}$ 15 $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ 21 $\cancel{22}$ 23 $\cancel{24}$ 25 $\cancel{26}$ 27 $\cancel{28}$

The next number, 3, is not struck out, so 3 is prime. We circle 3 and cross out all multiples of 3.

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ 25 $\cancel{26}$ $\cancel{27}$ $\cancel{28}$

The next number, 5, is not struck out, so 5 is prime. We circle 5 and cross out all multiples of 5 that are not yet struck out.

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$

Since $4 < \sqrt{28} < 5$, we can stop here and box all the remaining numbers. They are primes because they are not struck out.

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ $\boxed{11}$ $\cancel{12}$ $\boxed{13}$ $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ $\boxed{17}$ $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$ $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$

To test if a number n is prime, we test all primes $p \leq \sqrt{n}$. If none divides n, then n is prime. There are more efficient algorithms for primality testing. More recently, the AKS primality testing algorithm was shown to be able to run in polynomial time.

3.3 Consecutive Composites

Proposition 3.2. For every $n \in \mathbb{Z}^+$, there exists n consecutive composite numbers.

Proof. By construction.

$(n+1)!+2$, $(n+1)!+3$, ..., $(n+1)!+(n+1)$ are all composite. ■

Note that this construction may not give the smallest n consecutive composite numbers.

[1]strainer, colanders, used for filtering; this name is likely due to the fact that the algorithm "filters out" the non-primes.