Lecture 1. The sequence of prime numbers

Oleg Viro

1 Prime numbers and the set of all prime numbers

1.1 Primes and composites

Let n be a natural number. A natural number d is said to *divide* n and is called a *divisor* of d if $n = d \cdot q$ for some natural number q.

The number 1 divides any natural number n, because $n = 1 \cdot n$. For the same reason, any natural number divides itself.

A natural number $n > 1$ is called *prime* if it has no other divisors, only 1 and n divide n.

Otherwise $n > 1$ is called *composite*. Number 1 is not called prime or composite.

Lemma 1. *Any natural number $n > 1$ is divisible by some prime number.*

Proof. If n is a prime number, then it is divisible by itself. If not, then it is a composite number and is a product q_1p_1 of two numbers different from n and 1. They are smaller than n. If p_1 is prime, then we are done: we found a prime divisor p_1 of n. If not, then p_1 is a composite number, and there exist natural numbers q_2 and p_2 such that $p_1 = q_2p_2$ (and hence $n = q_1q_2p_2$) and $1 < q_2 < p_1$, $1 < p_2 < p_1$. Acting in this way, we get eventually either a prime divisor p_k of n, or a sequence of factorizations $n = q_1p_1 = q_1q_2p_2 = q_1q_2q_3p_3 = \dots$ in which $n > p_1 > p_2 > p_3 > \dots > 1$. A decreasing sequence of natural numbers cannot be infinite. The length is not greater than $n - 2$. Thus we get a prime divisor of n. □

Lemma 2. *$p \cdot q + 1$ is not divisible by p for any natural numbers p and q with $p > 1$.*

Proof. Assume the opposite, then $pq + 1 = pr$ for some natural r. Then $p(r - q) = 1$. Since $p > 1$ and $r - q$ is a natural number, $p(r - q) > 1$. Contradiction. □

1.2 The number of prime numbers

Theorem 1. *The set of prime numbers is infinite.*

Proof. Assume the opposite. Let $p_1, p_2, \ldots, p_n$ be the list of all prime numbers. Consider $N = p_1 p_2 \ldots p_n + 1$. By Lemma **??**, N is divisible by some prime number. By Lemma 2, N is not divisible by any of p_1, …, p_n. By assumption, any prime number is one of p_1,…, p_n. Contradiction. □

1.3 Digression on the history

Theorem 1 is traced back to Euclid. It is instructive to compare is statement and proof with the original Proposition 20 in Book IX of the Elements. See

`http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html`

Here is its text: "**Proposition 20.** *Prime numbers are more than any assigned multitude of prime numbers.*

Let A, B, and C be the assigned prime numbers. I say that there are more prime numbers than A, B, and C.

Take the least number DE measured by A, B, and C. (Comment: i.e., DE is the least common multiple of A, B, and C.) Add the unit DF to DE. Then EF is either prime or not.

First, let it be prime. Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C.

Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number G.

I say that G is not the same with any of the numbers A, B, and C.

If possible, let it be so. Now A, B, and C measure DE, therefore G also measures DE. But it also measures EF. Therefore G, being a number, measures the remainder, the unit DF, which is absurd.

Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C.

Therefore, prime numbers are more than any assigned multitude of prime numbers. "

Comment by David E. Joyce:

"This proposition states that there are more than any finite number of prime numbers, that is to say, there are infinitely many primes.

Outline of the proof

Suppose that there are n primes, $a_1, a_2, ..., a_n$. Euclid, as usual, takes an specific small number, $n = 3$, of primes to illustrate the general case. Let m be the least common multiple of all of them. (This least common multiple was also considered in proposition IX.14. It wasn't noted in the proof of that proposition that the least common multiple of primes is their product, and it isn't noted in this proof, either.)

Consider the number $m + 1$. If it's prime, then there are at least $n + 1$ primes.

So suppose $m + 1$ is not prime. Then according to proposition VII.31, some prime g divides it. But g cannot be any of the primes $a_1, a_2, ..., a_n$, since they all divide m and do not divide m + 1. Therefore, there are at least $n + 1$ primes. Q.E.D.

This proposition is not used in the rest of the Elements."

1.4 Gaps between subsequent primes

Theorem 2. *For any natural number N there exist subsequent prime numbers p and q such that $q - p > N$.*

Proof. Let p_1, p_2, $\dots p_n$ be all the prime numbers that are less than or equal to N. Consider numbers

$$\begin{aligned} a_2 =& p_1 p_2 \dots p_n + 2 \\ a_3 =& p_1 p_2 \dots p_n + 3 \\ & \dots \\ a_N =& p_1 p_2 \dots p_n + N \end{aligned}$$

None of them is prime. To prove that a_i is not prime, we consider separately two cases: (1) i is prime, (2) i is composite.

If i is a prime number $p_j \leq N$ the number $a_i = p_1 p_2 \dots p_n + i = p_1 p_2 \dots p_n + p_j$ is divisible by p_j. If $i \leq N$ is composite. Then i is divisible by some prime $p_j < N$, that is $i = p_j s$ for some natural number s. Hence $a_i = p_1 p_2 \dots p_n + i = p_1 p_2 \dots p_n + p_j s$ is divisible by p_j. Observe, that in either case, $p_j < a_i$ and divisiblity of a_i by p_j means that a_i is composite.

Thus we have constructed a collection of $N - 1$ subsequent composite numbers. The greatest prime number number $p < a_2$ and the least prime number $q > a_N$ have the desired properties: they are prime and $q - p > N$. □

1.5 Primes with a given remainder under division by 3

The whole set $\mathbb{N}$ of natural numbers is the union of the following three sets:

- the natural numbers divisible by 3,
- the natural numbers which gives remainder 1 under division by 3,
- the natural numbers which gives remainder 2 under division by 3.

The sets are formed by numbers belonging to three arithmetic series:

$$\begin{gathered}3, 6, 9, 12, \ldots 3n, \ldots\\ 1, 4, 7, 10, 13, \ldots 3n+1, \ldots\\ 2, 5, 8, 11, 14, \ldots 3n+2, \ldots\end{gathered}$$

The first of these sets starts with prime number 3, but it all other its elements are composite.

Theorem 3. *The set of prime numbers contained in the arithmetic series* $2, 5, 8, 11, \ldots, 3n+2, \ldots$ *is infinite.*

Lemma 3. *The product of any two natural numbers belonging to the arithmetic series* $1, 4, 7, 10, 13, \ldots 3n+1, \ldots$ *belongs to the same arithmetic series.*

Proof. Any element of this arithmetic series can be presented as $3x+1$ for some integer x. Consider the product of two such numbers. Present them as $3x+1$ and $3y+1$ for some integers x and y. Then

$$(3x+1)(3y+1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1.$$

Hence, the product gives remainder 1 under division by 3. □

Proof of Theorem 3. Assume the contrary that the set of prime numbers contained in the arithmetic series $2, 5, 8, 11, \ldots, 3n+2, \ldots$ is finite. Let p_1, p_2, $\ldots p_n$ be all the prime members of this series. (So, $p_1 = 2$, $p_2 = 5$, etc.)

Let $M = 3 \cdot p_1 \cdot p_2 \ldots p_n - 1$. First, observe that M belongs to the arithmetic series under consideration, because $M = 3 \cdot p_1 \cdot p_2 \ldots p_n - 1 = 3(p_1 \cdot p_2 \ldots p_n - 1) + 3 - 1 = 3(p_1 \cdot p_2 \ldots p_n - 1) + 2$. Second, M is not divisible by 3, or p_1, $\ldots$, p_n. Thus it may have prime divisors belonging only to the arithmetic series $4, 7, 10, \ldots, 3n+1$. But according Lemma 3 product of members of this series also belongs to this series. Contradiction. □