

Taster lecture: Counting primes

The natural numbers are those basic abstraction of quantity we first learn about as children; in particular they are the positive whole numbers:

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

We also consider the *integers*

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Although simple in some sense, the patterns and relationships that appear among these sets of numbers have intrigued and challenged generations of the mathematicians. Despite hundreds of years of progress, there is still many areas we know very little about.

The focus of our lecture today will be on prime numbers, which can be viewed as the elementary building blocks of the integers. Recall that a natural number $p \in \mathbb{N}$ is said to be *prime* if its only divisors are 1 and p .

One of the most fundamental results in mathematics is the following theorem, which makes rigorous our claim that the primes are the building blocks of the integers.

Theorem 1 (The Fundamental Theorem of Arithmetic). Let $n \in \mathbb{N}$. Then n can be written uniquely in the form $n = p_1^{k_1} \dots p_t^{k_t}$, where $p_1 < \dots < p_t$ are primes, and $k_1, \dots, k_t \in \mathbb{N}$.

In our courses in the Warwick Mathematics Institute, we prove almost every theorem we state. We will not do that here, just so that we have time to see some interesting applications of the The Fundamental Theorem of Arithmetic (FTA).

To facilitate the rest of our lecture, we will need

Definition 2. For positive integers m and n , we will say that m *divides* n , and write $m \mid n$, if there exists $t \in \mathbb{Z}$ such that $n = mt$.

Remark. A couple of very useful facts we will use are as follows:

1. Let $n \in \mathbb{Z}$. If p is prime, then we can write $n = p^a m$ for some integer $a \geq 0$ and some $m \in \mathbb{Z}$ with $p \nmid m$. Indeed, the if p does not divide n , we just take $a = 0$ and $m = n$. If $p \mid n$, then we write $n = p_1^{k_1} \dots p_t^{k_t}$ as in the FTA, so that $p = p_i^{k_i}$ for some $1 \leq i \leq t$. Now take $m := \prod_{j \neq i} p_j^{k_j}$.
2. Let $n_1, n_2, m \in \mathbb{Z}$, and suppose that m divides both n_1 and n_2 . Then m divides $n_1 - n_2$. Indeed, writing $n_i = t_i m$, we have $n_1 - n_2 = m(t_1 - t_2)$.

Theorem 3. (Euclid) There are infinitely many prime numbers.

Proof. Suppose that the theorem is false; that is, that there are only finitely many primes. Write these primes as p_1, \dots, p_k . Set $n_1 := p_1 \dots p_k + 1$ and $n_2 := p_1 \dots p_k$. Let p be a prime divisor of n_1 . Then p lies in the set $\{p_1, \dots, p_k\}$, since this is the set of all primes! Thus, p divides $p_1 \dots p_k = n_2$. It follows that p divides $n_1 - n_2 = 1$, a contradiction. \square

Having shown that there are infinitely many primes, can we be a bit more precise about how the primes behave? To do so, we are naturally lead to the following definition.

Definition 4. Fix a positive integer n , and write $\pi(n)$ for the number of primes at most n . The function $\pi : \mathbb{N} \rightarrow \mathbb{N}$ is called the *prime counting function*

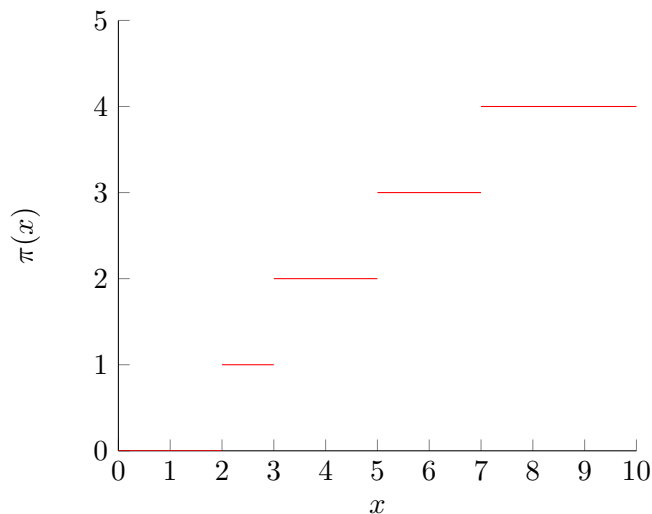
So for example, 2, 3, 5 are the only primes at most 5, so $\pi(5) = 3 = \pi(6)$. Similarly, $\pi(7) = 4 = \pi(10)$.

The fact that there are infinitely many primes, is equivalent to the statement that the function $\pi : \mathbb{N} \rightarrow \mathbb{N}$ is unbounded.

We are then lead towards two typical types of questions in mathematics: an analytic type question, and an algebraic type question (respectively).

In Analysis, one tends to “zoom out” and study a function $f(n)$ on \mathbb{N} (or \mathbb{Z} or \mathbb{Q} or \mathbb{R}) by looking at its behaviour as $n \rightarrow \infty$. Our natural analytic question is then

Analytic type question The function $\pi(n)$ is very mysterious (see its graph, plotted below!), which makes it difficult to study as n approaches infinity. Can we find “nice” upper and lower bounds on $\pi(n)$, so that we can study the function analytically?



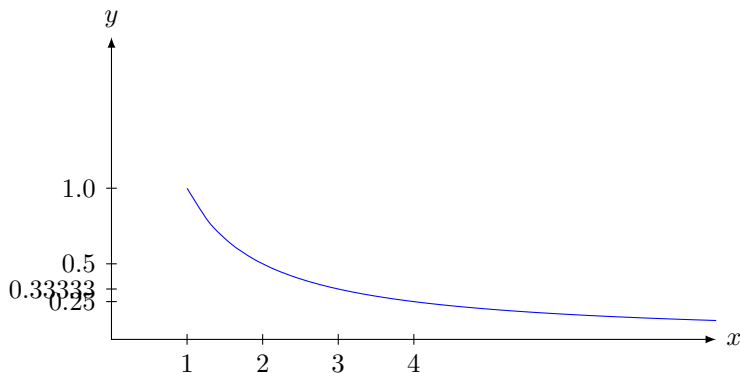
In Algebra, one tends to “zoom in” and study detailed properties of a function at certain specific points.

Algebraic type question We know that all primes bigger than 2 are odd, but what else can we say about their structure? Are there infinitely many primes of the form $4n + 1$, for example? What about $4n + 3$?

In the exercises after our lecture, you will study some algebraic type questions. Below, we examine the analytic question mentioned above.

1 Counting primes

Consider the function $\pi(n)$ as defined above. We also define $\log n$ to be the area underneath the graph of the function $f(x) = 1/x$ (i.e. the function in blue below), for $1 \leq x \leq n$.



Theorem 5. $\pi(n) \geq \log(n+1) - 1$.

Proof. First, we compare the area below the graph of $f(x) = 1/x$ with the area below the graph of the upper step function $g : [1, \infty) \rightarrow \mathbb{R}$ given by

$$g(x) := 1/n \text{ for } n \leq x \leq n+1.$$

The areas under the graph of g between 1 and $n+1$ is of course $1 + 1/2 + \dots + 1/n$. We can see from the figure that this is larger than the area under the graph of f between 1 and $n+1$. Thus, we have

$$\begin{aligned} \log(n+1) &\leq 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} \\ &\leq \sum_{m \in P(n)} \frac{1}{m} \end{aligned}$$

where $P(n) = \{m \in \mathbb{N} : \text{all prime divisors of } m \text{ are less than or equal to } n\}$. Write $p_1 < \dots < p_t \leq n$ for the primes less than or equal to n . By the FTA, all $m \in P(n)$ can be written uniquely in the form $m = \prod_{i=1}^t p_i^{k_i(m)}$, for some non-negative integers $k_i(m)$. We deduce that

$$\sum_{m \in P(n)} \frac{1}{m} = \prod_{i=1}^t \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right).$$

The inner sum is a geometric series with common ration $1/p_i$, so we get

$$\log(n+1) \leq \prod_{i=1}^t \left(\frac{p_i}{p_i - 1} \right).$$

Now, $p_i \geq i+1$, so $p_i/(p_i - 1) = 1 + 1/(p_i - 1) \leq 1 + 1/i = (i+1)/i$. Thus,

$$\log(n+1) \leq \prod_{i=1}^t \left(\frac{p_i}{p_i - 1} \right) \leq \prod_{i=1}^t \left(\frac{i+1}{i} \right) = \pi(n) + 1.$$

□

2 Properties of primes

In Section 1 above, the set

$$P(n) = \{m \in \mathbb{N} : \text{all prime divisors of } m \text{ are less than or equal to } n\}$$

was incredibly useful. It turns out that this set has pretty remarkable properties. We will actually prove the following amazing result.

Theorem 6. Fix $n \in \mathbb{N}$, let $P(n)$ be as above, and write $t := \pi(n)$. Let X be any subset of $P(n)$ of size $2^t + 1$. Then there exists distinct elements x and y in X with xy a perfect square.

To prove this theorem, we will use ideas from both combinatorics and geometry. We begin with the former. The following is arguably one of the most important results in all of mathematics.

Proposition 7. (The pigeonhole principle) Let $k < n$ be positive integers. If n objects are each placed into k boxes, then at least one box must contain more than one object.

The pigeonhole principle is incredibly useful! For example, suppose that $n \in \mathbb{N}$ is fixed, and A is a subset of $\{1, \dots, 2n\}$ of size $n + 1$. Then of course, at least two of elements of A must be consecutive. Thus, at least two of the elements of A are coprime (i. e. have no prime divisor in common).

Incredibly, a (sort of) converse to this holds! We claim that there exists two distinct elements a and b of A with $a \mid b$. To see this, for each element a of A , write $a = 2^{n_a} m_a$, where n_a is a non-negative integer, and m_a is an odd natural number. Since $1 \leq a \leq 2n$, we have $1 \leq m_a \leq 2n - 1$, for all $a \in A$. Thus, there are at most n possibilities for the integers m_a . We deduce from the pigeonhole principle that $m_a = m_b$ for some distinct $a, b \in A$. Thus, either a divides b or b divides a , as needed.

We can now prove our theorem.

Proof of Theorem 6. Recall that $t = \pi(n)$. Write p_1, \dots, p_t for the primes less than or equal to n . By the FTA, for $x \in X$, we may write $x = p_1^{k_1} \dots p_t^{k_t}$, where the k_i are non-negative integers. Define $f(x) := (\alpha_1, \dots, \alpha_t)$, where $\alpha_i := 0$ if k_i is odd, and $\alpha_i := 1$ if k_i is even. The set of t -tuples of 0s and 1s has precisely 2^t elements. So there exists distinct x and y in X with $f(x) = f(y)$ by the pigeonhole principle. Then $x = p_1^{k_1} \dots p_t^{k_t}$ and $y = p_1^{n_1} \dots p_k^{n_k}$ with each $n_i + m_i$ even. Thus, $xy = p_1^{m_1+n_1} \dots p_k^{m_k+n_k}$ is a perfect square. □