Prime numbers

Ben Folland

November 2021

1 Abstract

Prime numbers are numbers which have only two divisors - 1 and themselves. A number is either prime, or if not, it can be expressed as a unique factorisation of prime numbers. There is no way of predicting with certainty where primes will pop up - they just do. They have a mystical nature associated with where they can be found and the many interesting properties associated with them. In this article I am going to be investing some time exploring these properties and some proofs associated with some of them.

2 Introduction

Prime numbers and there properties were first studied extensively by the ancient Greek mathematicians. Around 300BC Euclid released his Element's which proved an important result.

Theorem 1 .1. *There are an infinite number of primes.*

Proof. Assume, for contradiction, that there only exists a finite number of primes. List these prime numbers $p_1, p_2, ...p_k$ and consider the number $N = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$. By the Fundamental Theorem of Arithmetic each number have a unique prime factorisation. Given any p_i for $1 \leq i \leq k$, $p_i \nmid N + 1$. Therefore as no prime numbers divide $N + 1$ it's either prime or it can be factored by other prime numbers not on the list. This is a contradiction and therefore there must be a infinite number of prime numbers. □

This is a pretty famous proof known by most recreational mathematicians. The simplicity of the statement combined with the elegance of the proof makes it very satisfying. Unfortunately many of the other theorems we will be discussing do not have proofs of this simplicity.

Euclid also produced a result correlating prime numbers and perfect numbers which will be discussed later on. Around a similar time as Euclid a algorithm for generating a sequence of primes was theorized by the Greek Eratosthenes.

From around 200BC to the 17th century practically no further progress was made on the properties of primes. These times were called the Dark Ages. In 17 and 18th centuries mathematicians like Fermat, Mersenne and Euler made significant steps into understanding distribution and the strange behaviour.

From then on progress in understanding them has not stopped, and will not stop as there are still many unsolved questions associated with primes.

3 Fermat and his small theorem

Pierre de Fermat was a great 17th Century French mathematician. He is well known for many profound results in areas such as; Analytic geometry, differential geometry, probability, optics, infinitesimal calculus - but what we will be looking at - number theory. He is extremely well known for his theorem named - Fermat's Last Theorem

Theorem 1 .2. *For $x, y, z, n \in \mathbf{Z}$ and $n > 2$*

$$x^n + y^n = z^n$$

has no integer solutions.

This was a massive problem in number theory but wasn't solved until the mid 1990s by Oxford mathematician Andrew Wiles. This however is not what are focus will be on, instead we will be looking at his much smaller theorem which was given the name - Fermat's Little Theorem

Theorem 1 .3. *Given p is a prime, a is an integer and $\gcd(a, p) = 1$*

$$a^p = a \mod p$$

Proof. Consider the set $G = \{1, 2, ..., p-1\}$ with operation of multiplication modulo p - where p is a prime. This forms a group, however - if your are not convinced I will give a proof that every element is invertible (the only axiom that is not trivial) at the end of this proof. Let is consider $a \in G$, and let k be the order of a. This means the set $\{1, a, ..., a^{k-1}\}$ is a subgroup of G. But Lagranges Theorem states k divdes the order of the group. This means $p - 1 = kn$ for integer n. Therefore

$$a^{p-1} \equiv a^{kn} \equiv (a^k)^n \equiv 1$$

Now those who require a proof of G being a group, suppose you have an element a of G. a will be coprime to p, therefore by Bezouts identity there exists integers x, y such that $ax + py = 1$. Consider taking this equation modulo p and you get $ax \equiv 1 \mod p$. Here x is the inverse. □

4 Bertrand and his postulate

Joseph Bertrand, not to be confused with Bertrand Russel a British mathematician, was a 19th century French mathematician specialising in number theory, differential geometry and many other fields. He conjectured in 1845 the following,

Theorem 1 .4. *for any integer $n > 3$ there always exists a prime p such that $n < p < 2n$*

Proof. This proof is not simple and requires multiple steps, first of all let us present the following inequality,

Lemma .5. $\frac{4^n}{2n} \leq \binom{2n}{n}$

Proof. Consider the binomial expansion of

$$(1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k}$$

As

$$\binom{2n}{n} \geq \binom{2n}{k}, 0 \leq k \leq 2n \implies (1+1)^{2n} \leq 2n \cdot \binom{2n}{n}$$

Therefore $4^n \leq 2n \cdot \binom{2n}{n}$ And our final result is achieved.

Lemma .6. $\prod\limits_{p\leq x} p \leq 4^{x-1}$ *Note the left hand side of the inequality represent the product of primes upto* x

Proof. Consider when $x = 2$, this is trivially true as $2 \leq 4$. Please also notice that if the statement is true for an odd integer $x = 2k + 1$ for example

$$\prod_{p\leq 2k+1} p \leq 4^{2k}$$

Then the proposition is also true for $x = 2k + 2$ as it is will be even therefore

$$\prod_{p\leq 2k+1} p = \prod_{p\leq 2k+2} p \leq 4^{2k} \leq 4^{2k+1}$$

So all we need to do is prove true for odd integers and we get the even ones as a result of this. Now assume true for $x = k + 1$, this implies

$$\prod_{p\leq k+1} p \leq 4^{k}$$

Considering $x = 2k + 1$ gives the result

$$\prod_{p\leq 2k+1} p = \left(\prod_{p\leq k+1} p\right)\left(\prod_{k+1\leq p\leq 2k+1} p\right) \leq (4^k)\left(\prod_{k+2\leq p\leq 2k+1} p\right) \leq \binom{2k+1}{k+1}$$

It is a fact that

$$\binom{2k+1}{k+1} \text{ is divisible by } \prod_{k+1\leq p\leq 2k+1} p$$

as $p|(2k+1)!$ and $p \nmid (k+1)!$ and $p \nmid k!$ therefore

$$\prod_{k+2\leq p\leq 2k+1} p \leq \binom{2k+1}{k+1}$$

We can achieve an inequality on $\binom{2k+1}{k+1}$ by considering the expansion

$$(1{+}1)^{2k+1} = \binom{2k+1}{0}+\binom{2k+1}{1}+\cdots+\binom{2k+1}{k}+\binom{2k+1}{k+1}+\cdots+\binom{2k+1}{2k}+\binom{2k+1}{2k+1}$$

It follows that

$$(1+1)^{2k+1} \geq \binom{2k+1}{k} + \binom{2k+1}{k+1} = 2\binom{2k+1}{k+1}$$

Boom! We now have

$$\binom{2k+1}{k+1} \leq 2^{2k} = 4^k$$

This gives us

$$\prod_{k+2 \leq p \leq 2k+1} p \leq 4^k$$

Finishing it all off we have

$$\prod_{p \leq 2k+1} p \leq (4^k)(4^k) = 4^{2k}$$

□

□

Lemma .7. *If* $p|\binom{2n}{n}$ *then* α *is the the power of* p *where* p *is a prime in the prime factorisation of* $\binom{2n}{n}$ *then,*

$$p^{\alpha} \leq 2n$$

Proof. Let $r(p)$ be such that,

$$p^{r(p)} \leq 2n < p^{r(p)+1}$$

Also consider that if k is the power of p in $n!$ then

$$k = \sum_{i \geq 1}^{\infty} \lfloor \frac{n}{p^i} \rfloor$$

Therefore α can be defined as follows,

$$\alpha = \sum_{i \geq 1}^{r(p)} (\lfloor \frac{2n}{p^i} \rfloor \; - 2\lfloor \frac{n}{p^i} \rfloor)$$

Considering the part inside the sum,

$$0 \leq \lfloor\frac{2n}{p^i}\rfloor \; - 2\lfloor\frac{n}{p^i}\rfloor < \frac{2n}{p^i} - 2(\frac{n}{p^i} - 1) = 2$$

Therefore,

$$0 \leq \lfloor\frac{2n}{p^i}\rfloor - 2\lfloor\frac{n}{p^i}\rfloor < 2$$

This means

$$\max(\lfloor\frac{2n}{p^i}\rfloor - 2\lfloor\frac{n}{p^i}\rfloor) = 1$$

Finishing this of we achieve,

$$\alpha \leq r(p)$$

Exponentiating,

$$p^{\alpha} \leq p^{r(p)} \leq 2n$$

□

Corollary .7.1. *Let α be the exponent of p in $\binom{2n}{n}$, if $\alpha > 1$ then $p \leq \lfloor\sqrt{2n}\rfloor$*

Proof. Suppose p is a prime factor of $\binom{2n}{n}$ for $\alpha > 1$, by Lemma .6.

$$p^{a} \leq 2n$$

Directly implying that

$$p \leq p^{\frac{a}{2}} \leq \lfloor\sqrt{2n}\rfloor$$

□

Don't stop now we are nearly here - just one more lemma to go before we can complete the proof!

Lemma .8. *For any prime number p, if $\frac{2n}{3} < p \leq 2n$ then p is not a factor of $\binom{2n}{n}$ when $n \geq 3$*

Proof. Assume

$$\frac{2n}{3} < p \leq n \implies 2n < 3p \leq 3n$$
$$\frac{2n}{3} < p \leq n \implies \frac{4n}{3} < 2p \leq 2n$$

Combining these two we achieve,

$$p \leq n < 2p \leq 2n < 3p \leq 3n$$

As $p \leq n$, $2p \leq 2n$ and $3p > 2n$ we see that $p^2|(2n)!$ but $p^3 \nmid (2n)!$ Also notice $p|n!$ but $(2p)|n!$ therefore $p^2 \nmid n!$ This means p appears exactly once in the prime factorisation of $n!$ and exactly twice in $(2n)!$. Therefore $\binom{2n}{n}$ contains no factors of p □

We are finally here - we have all the tools to complete Bertrand by contradiction - lets get to it!

Consider the following product representing all the primes with exponents greater than 1 in the prime factorisation of $\binom{2n}{n}$ (Corollary .6.1.)

$$\prod_{p \leq \sqrt{2n}} p^{\alpha} \leq \prod_{p \leq \sqrt{2n}} 2n < (2n)^{\lfloor \sqrt{2n} \rfloor}$$

Therefore

$$\binom{2n}{n} < (2n)^{\sqrt{2n}} \left(\prod_{p \leq \frac{2n}{3}} p \right)$$

Using Lemma .4. and .5. we achieve

$$\frac{4^n}{2n} < \binom{2n}{n} < (2n)^{\sqrt{2n}} \left(\prod_{p \leq \frac{2n}{3}} p \right) < (2n)^{\sqrt{2n}} \cdot 4^{\lfloor \frac{2n}{3} \rfloor - 1}$$

Simplyfying we get,

$$4^{n - \lfloor \frac{2n}{3} \rfloor + 1} < (2n)^{1 + \sqrt{2n}}$$

Considering the fact that

$$n - \lfloor \frac{2n}{3} \rfloor + 1 \geq \frac{n+3}{3}$$

We can substutite that in and take logarithms of both sides giving us,

$$\frac{1}{3}(n+3)\ln 4 < (1 + \sqrt{2n}) \ln 2n$$

Wow, we have come so far. Now all we need to do is find a positive integer N such that for all $n \geq N$ the inequality is wrong meaning a contradiction is held. This is left as an excercise for a keen reader. The answer you are looking for is $N = 460$, it is sufficient to check the postulate for $N < 460$ which it indeed comes out true. □

The postulate has been proved! So - why is it still named 'Bertrand's Postulate' not 'Bertrand's Theorem'? I have no clue...