Infinity Of Primes

If $n = a\,b$ for some natural numbers then we call a and b as dividers of n.
Trivially $n = 1 \cdot n$ for all n numbers so 1 and n are trivial dividers.
The non 1 dividers of n are called factors and so the trivial n divider is allowed as factor.
This strange allowance of a number itself as factor will make sense more and more as we use this factor concept in proofs. But apart from this, if $n = a\,b$ and none of these are 1 then none of these are n either and so they are smaller numbers then n.
Then we call this a decomposition of n and n itself a composite.
There are numbers that can not be decomposed that is are not composites.
A trivial such is 1 simply because it is too small, it has only the trivial 1 as divider itself.
The ones that are bigger than 1 and yet can not be decomposed, are called primes.
The first few primes are : $2 , 3 , 5 , 7 , 11 , 13 , 17 , \ldots$
They become rarer and rarer but seem to be never stopping, so there are infinite many of them.
This fact follows immediately from a much simpler fact through a simple trick.
The simpler fact is that every n larger than 1 number has a prime factor.
So we encountered what I claimed that the factor concept is useful.
Of course, we could have avoided the concept of factors even primes by saying that:
Every n larger than 1 has a non 1 divider that has no other divider than 1 and itself.
But this doesn't sound as visual as the claim that all n has prime factor.
We can prove this claim in three ways:
The first is simply to decompose $n > 1$ deeper and deeper to encounter a prime.
Of course, already the start can be impossible if n is not a composite. But then since it is larger than 1 it is a prime and so we found a prime factor, namely itself.
If $n = a\,b$ is a decomposition then again it can be that one of these is a prime and we are finished again. Or none of them, that is both are composites and then we can decompose one of them say a. This then can continue but not infinitely because we always get smaller and smaller factors. That is non 1 dividers. So eventually the process must stop and it only stops when a decomposition factor becomes a prime. Then it is factor of the original n too.
A seemingly side issue could be to speed up the process and so not just choose one of the composites to decompose it rather decompose both of them. Indeed, we might be luckier this way meaning that we finish faster. We might even think that choosing always the smaller is a good strategy but this is not foolproof because smaller numbers can have longer way to go.
For example: $8 = 2 \cdot 2 \cdot 2$ while $9 = 3 \cdot 3$.
This side issue then has an amazing law of its own. Namely, if we relentlessly decompose n into primes only, then these final prime factors become the same regardless how we go.
This is called the Unique Prime Factorization Theorem or Fundamental Theorem Of Arithmetic.
You'll find two separate articles about this. But now lets see the second road to our claim that there is always at least one prime factor.
We can be quite specific about how to find such prime factor if we scan through all possible dividers of n. Of course we want to ignore the trivial 1 divider so we only scan factors and then amazingly we only must look for the smallest. This minfac (n) is always a prime.
Indeed, if minfac (n) were a composite then it were $a\,b$ with smaller a , b than minfac (n).
But then either of these were a smaller factor of n too, contradicting that minfac (n) was the smallest. This so called indirect argument assumed an impossibility and then refuted it.
The final third argument is even more indirect. We start with the straight out negative of our claim, that is with the claim that there are $n > 1$ numbers that have no prime factor.
This then implies that there would be an m smallest or minimal among these. Still $m > 1$.
If m is a prime then we reached a contradiction because m were a prime factor of itself.
If m is a composite then it is $a\,b$ with smaller numbers and none of these could have prime factor because it were prime factor of n too. But then these are smaller numbers without prime factor and so we contradicted that m was the first.
Now we can come to the claimed "trick" to get the infinity of primes from our claim that all n has prime factor. This is indirect too.
Suppose there were only finite many $p_1 , p_2 , \ldots , p_m$ primes among all natural numbers.

Lets multiply all these together and add 1 to it. This $p_1\ p_2\ .\ .\ .\ p_m + 1$ were a number that has 1 remainder when we divide it with any of the primes. So it is not dividable by any of the primes, contradicting that all numbers have prime factors.

An interesting task is to try to turn an indirect argument into direct.
For example, here in our last step we could have said that instead of assuming the finiteness of primes, for any p_1, p_2, . . . , p_m primes we regard $p_1\ p_2\ .\ .\ .\ p_m + 1$ and thus get a bigger one. But this is incorrect! We only created a number that must have a prime factor different from al the p-s. So this doesn't have to be bigger than all these primes. Unless these were all the primes up to a point. Then indeed, the different prime factor of $p_1\ p_2\ .\ .\ .\ p_m + 1$ must be also bigger than these. Euclid's original proof was similar to this. But he didn't use all the primes up to a p_m rather all numbers up to M. The product of these is called the factorial and is abbreviated with an exclamation sign. So M factorial = $M ! = 2 \cdot 3 \cdot 4 \cdot . . . \cdot M$.
Then $M ! + 1$ is a number not dividable by any of 2 , 3 , , . . . , M so it must have a prime factor larger than M. So for any M we found a prime above M.
To be even more specific minfac ($M ! + 1$) is always a prime bigger than M.
Amazingly, Euclid's original argument was only simplified to the bare indirectness from the prime factor existence in 1878 by Kummer.

Finally, the most interesting level of sharpening our result is not merely making the proof direct, that is giving a next prime after an n for sure but making such as close as possible to n.
Let n^* denote the next prime after n and n_* the last prime up to n so allowing n itself if it is a prime. Then $\delta(n) = n^* - n_*$ is the prime gap at n.

These gaps can be very big, in fact arbitrary big but even relative to n can vary a lot.
So to guarantee a prime for sure is pretty hard. The first serious and very hard result was by Chebishev and it merely guaranteed a prime before 2 n. This seems ridiculously weak but the sad fact is that the difficulty of his proof shows how difficult must be anything better.
He was also the first to get exact results about the already guessed limit behavior of these gaps.
$\delta(n)$ is in average $\log(n)$ around n. This denotes logarithm with base $e = 2.718 . . .$
The base 10 logarithm is simply the number of 0-s in a 10 power and so to get a feel of the prime density is very easy by multiplying this 0 number by $\log(10) \approx 2.3$. So for example, around one million $\delta(1000{,}000) \approx 6 \text{ x } 2.3 \approx 14$ so every 14-th number is a prime in average.
The meaning is clear but to tend both n and some surrounding to infinity is complicated and a simpler averaging would be to regard the δ values not around, rather up to n. This average of course feels much smaller than an around average because the gaps are increasing.
Surprisingly, the difference is only 1. So the average up to n is $\log(n) - 1$.
And if $\pi(n)$ denotes the number of primes up to n then this average is $\frac{n}{\pi(n)}$.

So the limit law is $\frac{n}{\pi(n)} \approx \log(n) - 1$. Amazingly, to prove this, it was enough to prove the consequence that the ratio of the two sides tends to 1 which is denoted by $\sim$.
This of course is true without the -1 part and so $\frac{n}{\pi(n)} \sim \log(n)$ or $\pi(n) \sim \frac{n}{\log(n)}$.
Which is called the Prime Number Theorem referring to the $\pi(n)$ number of primes as simply prime number. Now back from tendencies to actually limit the gaps:
A Conjecture of Cramer claims that: $n > 7 \rightarrow \delta(n) < (\log(n))^2$.
This also means that: $p \geq 11 \rightarrow p^* < p + (\log(p))^2$.
A consequence of this would be that: $p \geq 127 \rightarrow p^* < p + \sqrt{p}$.