Twitter a Proof

Prime numbers are used, e.g., in some hashing schemes and cryptographic methods. We like the fact that there exist infinitely many of them. Here is a raw write-up of a proof of the infinitude of primes, based on Euclid'd famous idea.

"First collect the list of all primes. We assume that this list is finite. Then we can multiply all primes and add 1 to the product. This number is larger than any of the primes. If this number itself is prime, then we have found a prime larger than all primes in our set, thus a new prime. This contradicts the assumption that all primes were already in our set. If our number is not prime, then it must be composite. That is, we can write it as a product of at least two primes. But these primes cannot come from our original set. The argument is that our number is not divisible by any of the primes in the original set, since we added 1 to their product. In both cases we can conclude that our original set did not yet contain all primes. We can insert at least one new prime. Now we can repeat the procedure with our larger set of primes, and so on, until infinity."

Let us get rid of some bubbles in this text. The last argument is superfluous. Once we have a contradiction to our first assumption, the proof is finished.

"First collect the list of all primes. We assume that this list is finite. Then we can multiply all primes and add 1 to the product. This number is larger than any of the primes. If this number itself is prime, then we have found a prime larger than all primes in our set, thus a new prime. This contradicts the assumption that all primes were already in our set. If our number is not prime, then it must be composite. That is, we can write it as a product of at least two primes. But these primes cannot come from our original set. The argument is that our number is not divisible by any of the primes in the original set, since we added 1 to their product. In both cases we can conclude that our original set did not yet contain all primes, a contradiction."

Next, the text refers several times to "the original set" and "our number". Why not give them names instead? It also changed the term "list" into "set". (One may wonder: Does it refer to the same object?)

"First collect the set L of all primes. We assume that L is finite. Then we can build the product p of all primes and add 1 to it. Note that $p + 1$ is larger than any of the primes. If $p + 1$ itself is prime, then we have found a prime larger than all primes in L, thus a new prime. This contradicts the assumption that all primes were already in L. If $p + 1$ is not prime, then it must be composite. That is, $p + 1$ is a product of at least two primes. But these primes cannot come from L. The argument is that $p+1$ is not divisible by any of the primes in L, since we added 1 to their product. In both cases we can conclude that L did not yet contain all primes, a contradiction."

The phrase "Note that ..." is inserted only because a sentence should not begin with a mathematical symbol or expression. Anyway, some "contractions" yields smoother formulations without making the steps harder to follow. For instance, everybody knows that $p+1$ is obtained by adding 1 to p; there is no need to say that. And instead of saying "we can do" this and that, just do it. Furthermore, it is obvious what the contradiction is.

"Assume that L is the finite set of all primes, and let p be their product. Note that $p + 1$ is larger than any of the primes. If $p + 1$ itself is prime, then we have found a prime larger than all primes in L, thus a new prime, a contradiction. If $p + 1$ is not prime, then it must be composite. That is, $p + 1$ is a product of at least two primes. But these primes cannot come from L. The argument is that $p + 1$ is not divisible by any of the primes in L. In both cases we can conclude that L did not yet contain all primes, a contradiction."

The last changes were estethical changes concerning the language, naming, referencing, and ways to express things. But also the logical structure is bulky. Actually we do not need this case distinction. Moreover, the argument that $p + 1$ is larger than anything in L is (although not being wrong) not really needed. The divisibility argument applies to the first case, too, therefore we can drastically simplify the proof.

"Assume that L is the finite set of all primes, and let p be their product. Note that $p + 1$ is either a prime or a product of at least two primes. But these primes cannot come from L. The argument is that $p+1$ is not divisible by any of the primes in L. We can conclude that L did not yet contain all primes, a contradiction."

Now that our text describes the essence of the proof, it becomes apparent that we can further contract the formulations without sacrificing the contents. Note that the "Note that"- sentence still makes the useless case distinction.

"Assume that L is the finite set of all primes, and let p be their product. The prime factors of $p+1$ are not in L, since $p+1$ is not divisible by any of the primes in L. Hence L did not yet contain all primes, a contradiction."

Assuming that our readers are bright enough to recognize that adding 1 to a number cannot preserve any factor, we can finally shorten the text to this minimalistic one, which still retains the complete argument:

"Let L be the finite set of all primes. Let p be their product. The prime factors of $p + 1$ are obviously not in L, a contradiction."

Voluntary Exercise

You don't have to submit it – only if you like.

The proof of infinitude of primes relies on the following elementary fact: "Every integer has a factorization into primes." Write a proof of this fact, again as concise as possible, yet readable and with a complete argument.

This was all about compression of texts, so to speak. Imagine that somebody wants to sell you a program that can do lossless compression of every *file*: He claims that his program can strictly shorten every input file and later reconstruct the original file. Write to him a proof that such a method is impossible; again as concise as possible, yet readable and with a complete argument.