Solving diophantine equations can be incredibly hard!

Example 28. You may have seen Pythagorean triples, which are solutions to the diophantine equation $x^2+y^2=z^2$.

A few cases. Some solutions (x,y,z) are $(3,4,5)$, $(6,8,10)$ (boring! why?!), $(5,12,13)$, $(8,15,17)$, ...

The general solution. $(m^2-n^2, 2mn, m^2+n^2)$ is a Pythagorean triple for any integers m,n.

These solutions plus scaling generate all Pythagorean triples!

For instance, $m=2, n=1$ produces $(3,4,5)$, while $m=3, n=2$ produces $(5,12,13)$.

Fermat's last theorem. For, $n>2$, the diophantine equation $x^n+y^n=z^n$ has no solutions!

Pierre de Fermat (1637) claimed in a margin of Diophantus' book *Arithmetica* that he had a proof ("I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.").

It was finally proved by Andrew Wiles in 1995 (using a connection to modular forms and elliptic curves).

This problem is often reported as the one with the largest number of unsuccessful proofs.

3 Primes

Lemma 29. (Euclid's lemma) If $d|ab$ and $\gcd(a,d)=1$, then $d|b$.

Proof. Since $(a,d)=1$, we can find x,y so that $ax+dy=1$.

We now see that $b=abx+bdy$ is divisible by d (because $d|ab$). □

Definition 30. An integer $p>1$ is a **prime** if its only positive divisors are 1 and p.

Lemma 31. If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof. If $p|a$, then we are done. Otherwise, $p\nmid a$. In that case, $\gcd(a,p)=1$ because the only positive divisors of p are 1 and p. Our claim therefore is a special case of the previous lemma. □

Corollary 32. If p is a prime and $p|a_1a_2\cdots a_r$, then $p|a_k$ for some $k\in\{1,2,\ldots,r\}$.

Example 33. This property is unique to primes. For instance, $6|8\cdot 21$ but $6\nmid 8$ and $6\nmid 21$.

Whereas, $2|8\cdot 21$ and, indeed $2|8$. Similarly, $3|8\cdot 21$ and, indeed $3|21$.

Theorem 34. (Fundamental Theorem of Arithmetic) Every integer $n>1$ can be written as a product of primes. This factorization is unique (apart from the order of the factors).

Proof. Let us first prove, by (strong) induction, that every integer $n>1$ can be written as a product of primes.

- **(base case)** $n=2$ is a prime. There is nothing to do.
- **(induction step)** Suppose that we already know that all integers less than n can be written as a product of primes. We need to show that n can be written as a product of primes, too.

  Let $d>1$ be the smallest divisor of n. Then d is necessarily a prime (because if $a>1$ divides d, then a also divides n so that $a=d$ because d is the smallest number dividing n).

  If $d=n$, then n is a prime, and we are already done.

  Otherwise, $\frac{n}{d}>1$ is an integer, which, by the induction hypothesis, can be written as the product of some primes $p_1\cdots p_r$. Then, $n=dp_1\cdots p_r$.

Finally, let us think about why this factorization is unique. Suppose we have two factorizations

$$n=p_1p_2\cdots p_r=q_1q_2\cdots q_s.$$

By the corollary, each p_i divides one of the q_j's (and vice versa), in which case $p_i=q_j$, so we can cancel common factors until we see that both factorizations are identical. □

Armin Straub
straub@southalabama.edu

Example 35. (advanced; just for fun and perspective) The following example is supposed to illustrate that the idea of factorization into primes and the uniqueness of such factorizations should not be taken entirely for granted.

- In more advanced number theory, it is common to extend the set of integers. For instance, the **Gaussian integers** are numbers of the form $a+bi$, where a and b are ordinary integers and i is the imaginary unit satisfying $i^2=-1$.

  Note that 5 is no longer a prime because we have $5=(2+i)(2-i)$. It turns out that the quantities $2\pm i$ cannot be further factored. They are primes in this setting.

  [These claims are usually proved by introducing the "norm" $N(a+bi)=a^2+b^2$. This function is multiplicative, meaning that $N(xy)=N(x)N(y)$. It follows that $2+i$ must be a prime because $N(2+i)=5$ is a prime. For contrast, $N(5)=25$ is not a prime.]

  https://en.wikipedia.org/wiki/Table_of_Gaussian_integer_factorizations

- A similar kind of integers consists of numbers of the form $a+bi\sqrt{5}$, where a and b are ordinary integers.

  [This is called the ring of integers of the field $\mathbb{Q}(\sqrt{-5})$.]

  Then we have two different factorizations of 6, namely,

  $$6=2\cdot 3,\quad 6=\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right).$$

  The numbers 2, 3, $1\pm i\sqrt{5}$ cannot be factored further.

  [They are called irreducible. However, technically speaking, they are not primes. There is a subtle distinction between these two concepts that is not visible when working with ordinary integers.]

Example 36. $140=2^2\cdot 5\cdot 7$, $2016=2^5\cdot 3^2\cdot 7$, 2017 is a prime, $2018=2\cdot 1009$, $2019=3\cdot 673$

How can we check that 2017 is indeed prime? Well, none of the small primes $2,3,5,7,11$ divide 2017. But how far do we need to check? Since $\sqrt{2017}\approx 44.91$, we only need to check up to prime 43. (Why?!)

Example 37. The **sieve of Eratosthenes** is an efficient way to find all primes up to some n.

Write down all numbers $2,3,4,\ldots,n$. We begin with 2 as our first prime. We proceed by crossing out all multiples of 2, because these are not primes. The smallest number we didn't cross out is 3, our next prime. We again proceed by crossing out all multiples of 3, because these are not primes. The smallest number we didn't cross out is 5 (note that it has to be prime because, by construction, it is not divisible by any prime less than itself).

Problem. If $n=10^6$, at which point can we stop crossing out numbers?

We can stop when our "new prime" exceeds $\sqrt{n}=1000$. All remaining numbers have to be primes. Why?!

Armin Straub
straub@southalabama.edu