Bad Introduction to Elementary Number Theory:
— *Fermat Numbers* —

revól ufiąw

0. What is number theory?

Number theory is a branch of mathematics concerning integers and their properties. Even though this might make it sound simple, that actually isn't the case. Most of the time, discrete mathematics (i.e. working with discrete values like integers) is much less intuitive than continuous mathematics (i.e. working with "smooth" values).

Example. Consider the equation

$$x^2 + y^2 = z^2$$

where $x, y, z \in \mathbb{R}^+$. Finding solutions (x, y, z) that satisfy this is rather trivial. Choose some arbitrary $x, y \in \mathbb{R}^+$ and then let z be $\sqrt{x^2 + y^2} \in \mathbb{R}^+$. These are not just infinite but *all* solutions.

Let's now consider the somewhat more difficult number-theoretic version:

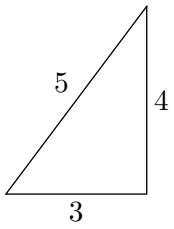
Example. Consider the equation

$$x^2 + y^2 = z^2$$

where $x, y, z \in \mathbb{Z}^+$. Such integer solutions (x, y, z) to this equation are called *Pythagorean triples*. You might know about the Pythagorean triple $(3, 4, 5)$:

$$3^2 + 4^2 = 5^2$$

It's called Pythagorean triple because of the Pythagorean formula $a^2 + b^2 = c^2$. Using Pythagorean triples, you can create triangles with integer sidelengths:



There's an easy way to generate infinite solutions: Notice that if (x, y, z) is a Pythagorean triple, that is

$$x^2 + y^2 = z^2$$

then (kx, ky, kz) is also a Pythagorean triple for $k \in \mathbb{Z}^+$ since

$$\begin{aligned} & x^2 + y^2 && = z^2 \\ \implies & k^2x^2 + k^2y^2 && = k^2z^2 \\ \implies & (kx)^2 + (ky)^2 && = (kz)^2 \end{aligned}$$

This gives us Pythagorean triples like $(6, 8, 10)$. Primitive Pythagorean triples (PPTs) are triples such that x, y, z share no common positive factors other than 1: $(3, 4, 5)$ is a PPT but not $(6, 8, 10)$ or any $(3k, 4k, 5k)$ where $k \neq 1$. Another PPT is $(5, 12, 13)$. There are an infinite number of PPTs and even a way to generate them but this box is starting to get very big.

There's also this similar looking problem, called *Fermat's Last Theorem:*

Problem. Show that for $x, y, z, n \in \mathbb{Z}^+$ and $n \geq 3$, the equation

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

has no solutions.

This problem, formulated by Pierre de Fermat, by the way, had remained unsolved for 350 years until recently proven by Andrew Wiles in 1994. It was believed to be impossible to prove using current knowledge by almost all contemporary mathematicians. The 129-page paper involving techniques from algebraic geometry and number theory is a very complex and esoteric proof.

1. Divisibility rules

We use the notation $a \mid b$ to mean that a divides b or, equivalently, that b is a multiple of a. For example $7 \mid 14$ or $2 \mid 10$. The formal definition is as follows:

Definition. For $a, b \in \mathbb{Z}$ we have

$$a \mid b \iff \text{there exists } k \in \mathbb{Z} \text{ such that } ak = b$$

By the way, the "$\iff$" means "is equivalent to", i.e. both follow from each other. For example, $a + b = a \iff b = 0$ because $b = 0 \Rightarrow a + b = a$ and $a + b = a \Rightarrow b = 0$.

Our definition tells us that all integers divide 0 since there's always a $k \in \mathbb{Z}$ such that $ak = 0$, namely $k = 0$. Also, 1 divides every number since there's a $k \in \mathbb{Z}$ such that $1 \cdot k = b$, namely $k = b$. Also $a \mid b \iff a \mid -b$. These are the most important divisibility rules:

Theorem. Let $a, b, c \in \mathbb{Z}$. Then the following rules must hold:

0. $a \mid a$
1. $a \mid b$ and $b \mid c \Rightarrow a \mid c$
2. $a \mid b \Rightarrow |a| \leq |b|$
3. $a \mid b$ and $b \mid a \Rightarrow |a| = |b|$
4. $a \mid b \iff a \mid b + ak$

Try proving them yourself. *Hint: Use the definition.*

2. Prime numbers & FTA

Primes play an especially big role in number theory. I assume you most likely already know what a prime is, but here's the formal definition:

Definition. Let p, d be integers such that $1 < d < p$. Then we have

$$p \text{ is prime} \iff \text{there is no } d \text{ such that } d \mid p$$

That is, a prime has no other positive divisors than 1 and itself. If a positive integer is not prime it is called *composite*, except 1—it's neither prime nor composite. They're called "composite" because they're "composed" of primes: Any positive integer not 1 has a *prime factorization.* You get a prime factorization when you write a number in terms of powers of primes.

Example. Consider 36:

$$\begin{aligned} 36 &= 6 \cdot 6 \\ &= (3 \cdot 2) \cdot (3 \cdot 2) \\ &= 2^2 \cdot 3^2 \end{aligned}$$

Thus the prime factorization of 36 is written $2^2 \cdot 3^2$.

$$\begin{aligned} 75 &= 25 \cdot 3 \\ &= 5^2 \cdot 3^1 \\ &= 3 \cdot 5^2 \end{aligned}$$

Thus the prime factorization of 75 is written $3 \cdot 5^2$ (we can omit the exponent 1).

In fact, every prime factorization is unique. This is the *fundamental theorem of arithmetic:*

Theorem. Every integer greater than 1 has a *unique* (up to permutation) prime factorization. Thus if two integers have the same prime factorization, they are equal.

So primes can be thought of as building blocks. We know that the bigger an integer, the unlikelier it is to be prime since there are more possible factors. A natural question to then ask is:

Are there infinitely many primes?

The answer is *yes*, there are an infinite number of primes! This result had been proven by Greek mathematician Euclid of Alexandria over *2300 years ago.* The proof is very accessible and we'll present it here. It is a *proof by contradiction*, which means it assumes the opposite of what we want to show but then arrives at a contradiction even though all steps are known to be valid, thus concluding that the assumption must've been incorrect and that the desired claim is indeed true. This is also called *reductio ad absurdum* (reduction to absurdity).

Proof. Assume that there are only a finite number of primes $p_1, p_2, p_3, ..., p_n$. Now, consider the number

$$n = p_1 p_2 p_3 ... p_n + 1$$

We see that n isn't divisible by any of $p_1, ..., p_n$ because dividing n by any prime $p_1, ..., p_n$ leaves remainder 1. That means that it isn't a composite number and is itself a prime p. But this contradicts our initial assumption because p isn't one of $p_1, ..., p_n$ since $p > p_1, ..., p_n$.

Therefore, there are an infinite number of primes.

Primes seem to be distributed randomly without pattern:

2 3 5 7 11 13 17 19 23 29 31 37 41 43

47 53 59 61 67 71 73 79 83 89 97 101 103 ...

There is no known explicit formula for computing the nth prime. If you have a positive integer n then the prime-counting function $\pi(n)$[0] is defined as the number of primes less than or equal to n. For example $\pi(10) = 4$ because we have 4 primes ≤ 10: 2, 3, 5 and 7. But $\pi(11) = 5$ because 11 is a prime. In 1792, Carl Friedrich Gauss, when only 15 years old, proposed

$$\pi(n) \sim \frac{n}{\ln(n)}$$

This is a surprising result and it means that the primes less than or equal to n is roughly equal to $n/\ln(n)$.[1]

[0] Not to be confused with the other $\pi = 3.14...$

[1] You don't need to understand this but more formally: as $n \to \infty$, $n/\ln(n) \to \pi(n)$. That is, the approximation gets more accurate for larger numbers.

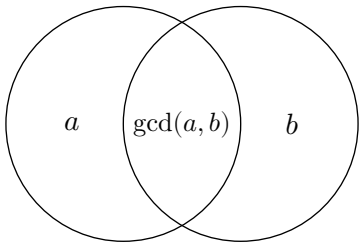
It's often useful to think of positive integers as multisets[2] of their divisors. For example the multiset for 36 would be $\{2, 3, 2, 3\}$. You get the original number by taking the product of all elements. That's why multiset of 1 is $\{\} = \varnothing$.[3]

3. GCD and LCM

Definition. The greatest common divisor (GCD) of two numbers a, b is denoted $\gcd(a, b)$.

$$\gcd(a, b) = d \iff d \text{ is the greatest (positive) integer such that } d \mid a \text{ and } d \mid b$$

We can think of this visually. If we take the multisets of a and b, then take their intersection, we get $\gcd(a, b)$. Here's the Venn diagram:

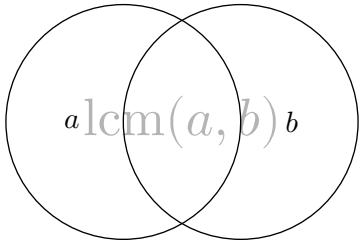


Thus if $M(n)$ is the multiset of $n \in \mathbb{Z}^+$, then we have: $M(a) \cap M(b) = M(\gcd(a, b))$.

Definition. The least common multiple (LCM) of two numbers a, b is denoted $\operatorname{lcm}(a, b)$.

$$\operatorname{lcm}(a, b) = m \iff m \text{ is the least positive integer such that } a \mid m \text{ and } b \mid m$$

In our Venn diagram, $\operatorname{lcm}(a, b)$ would just be the entire thing, i.e. $M(a) \cup M(b)$:



But: the intersection is included only once, not twice. If we'd include the intersection, we'd have $M(ab)$ instead of $M(\operatorname{lcm}(a, b))$. Try thinking about why that's the case. *Hint:*

Theorem. For $a, b \in \mathbb{Z}^+$, we have

$$\operatorname{lcm}(a, b) \gcd(a, b) = ab$$

This makes sense because $A \cap B + A \cup B = A + B$ where $A + B$ is a bit like the union of multisets, but the multiplicity of each element in the multisets is summed up. For example $\{2, 3, 4\} \cup \{3, 4, 7\} = \{2, 3, 4, 7\}$ and $\{2, 3, 4\} \cap \{3, 4, 7\} = \{3, 4\}$ but $\{2, 3, 4\} + \{3, 4, 7\} = \{2, 3, 4, 3, 4, 7\}$. Using this fact, you can convert LCM problems into GCD problems and vice versa.

Problem. For what $a, b \in \mathbb{Z}^+$ is $\gcd(a, b) = \operatorname{lcm}(a, b)$?[4]

[2] Multisets are like normal sets but they allow multiple instances of an element. For example, with multisets we can have $M = \{x, y, y\} \neq \{x, y\}$ but when working with normal sets, $S = \{x, y, y\} = \{x, y\}$.

[3] The empty product equals 1. See Wikepdia: Empty product.

[4] *Hint: Assume $a \leq b$. Then $gcd(a, b) \leq a$ and $lcm(a, b) \geq b$.*

4. Euclidean algorithm

The Euclidean algorithm is a recursive algorithm for getting the GCD of two numbers. It makes use of the fact that $\gcd(a, b) = \gcd(a, b + ak)$ for $k \in \mathbb{Z}$.

Theorem. Let $a, b, k \in \mathbb{Z}$. Then we have

$$\gcd(a, b) = \gcd(a, b + ak)$$

We'll prove that $\gcd(a, b) = \gcd(a, b + ak)$ by showing that $d \mid \gcd(a, b) \iff d \mid \gcd(a, b + ak)$, i.e. their multisets (of divisors) are equal.[5]

Proof. Let $d \mid \gcd(a, b)$. We know $\gcd(a, b) \mid a, b$ so $d \mid a, b$. This also means that $d \mid b + ak$. Thus $d \mid \gcd(a, b + ak)$. We've shown

$$d \mid \gcd(a, b) \implies d \mid \gcd(a, b + ak)$$

Now assume $d \mid \gcd(a, b + ak)$. Then $d \mid a$ and $d \mid b + ak \Rightarrow d \mid b$. So $d \mid a, b$ and therefore $d \mid \gcd(a, b)$. We've shown

$$d \mid \gcd(a, b + ak) \implies d \mid \gcd(a, b)$$

Combining both results gives us

$$d \mid \gcd(a, b) \iff d \mid \gcd(a, b + ak)$$

This is a really useful result, it gives us a way to recursively determine the GCD of two numbers. I'll give an example of the Euclidean algorithm:

Example. Imagine you need to compute $\gcd(72, 108)$. Since $\gcd(a, b) = \gcd(a, b + ak)$, we have $\gcd(72, 108) = \gcd(72, 108 - 1 \cdot 72) = \gcd(72, 36)$. We can do the same thing again but this time with $k = -2$: $\gcd(36, 72) = \gcd(36, 72 - 2 \cdot 36) = \gcd(36, 0)$. Since every integer is a divisor of 0 and the greatest divisor of 36 is 36, $\gcd(36, 0) = 36$ and thus $\gcd(72, 108) = 36$.

Let's look at another example:

Example. Say you want to find the GCD of 54 and 243.

$$\begin{aligned} & \gcd(54, 243) \\ = \ & \gcd(54, 243 - 4 \cdot 54) \\ = \ & \gcd(54, 27) \\ = \ & \gcd(54 - 2 \cdot 27, 27) \\ = \ & \gcd(0, 27) \\ = \ & 27 \end{aligned}$$

Thus $\gcd(54, 243) = 27$.

This is more efficient than finding the prime factorization of both integers and then multiplying their common factors. Finding prime factorizations of numbers is a hard task. In fact, whether integer factorization can be solved in polynomial time on a classical computer is still an open question in computer science.

Problem. Two numbers are said to be *coprime* iff they contain no common prime divisors. Show that $17n + 2$ and $9n + 1$ are coprime for all $n \in \mathbb{Z}$.[6]

[5] Make sure you understand the divisibility rules before reading the proof.

[6] *Hint: Show their GCD is 1.*

We can generalize the Euclidean algorithm as follows:

Definition. Let $a_i, b_i \in \mathbb{Z}^+$ be such that $a_i \leq b_i$ for all i. Also let $x \bmod y$ denote the remainder of x when divided by y. Then Euclidean algorithm computes the $\gcd(a, b)$ as follows:

$$\begin{aligned}
&\gcd(a, b) && = \gcd(a_0, b_0) \\
&= \gcd(a_0, b_0 \bmod a_0) && = \gcd(a_1, b_1) \text{ [7]} \\
&= \gcd(a_1, b_1 \bmod a_1) && = \gcd(a_2, b_2) \\
&= \ldots \\
&= \gcd(a_{k-1}, b_{i-1} \bmod a_{k-1}) && = \gcd(a_k, b_k = 0) \\
&= a_k
\end{aligned}$$

If you know a bit of programming, try thinking about why this Python code works:

```
def gcd(a, b):
  if a * b == 0:
    return a + b
  return gcd(min(a, b), (a + b) % min(a, b))
```

5. Fermat Numbers

The nth Fermat number is defined as $\Phi_n = 2^{2^n} + 1$ for $n \in \mathbb{N}$.[8] The first Fermat numbers are

$$\begin{aligned}
\Phi_0 &= 2^{2^0} + 1 = 2^1 + 1 &&= 3 \text{ [9]} \\
\Phi_1 &= 2^{2^1} + 1 = 2^2 + 1 &&= 5 \\
\Phi_2 &= 2^{2^2} + 1 = 2^4 + 1 &&= 17 \\
\Phi_3 &= 2^{2^3} + 1 = 2^8 + 1 &&= 257 \\
\Phi_4 &= 2^{2^4} + 1 = 2^{16} + 1 &&= 65537
\end{aligned}$$

Fermat numbers grow rapidly. The first 5 are prime numbers. Being the Fermat that he was, in 1650, he conjectured that all Φ_n are prime. This claim was disproven by Leonhard Euler in 1732. He factorized Φ_5:

$$\Phi_5 = 641 \cdot 6700417$$

But there's also an elementary proof of Φ_5's compositeness that doesn't involve any division. It was given by British mathematician G. Bennet:

Proof. First note that $5 \cdot 2^7 + 1 = 5 \cdot 128 + 1 = 641$.

$$\begin{aligned}
\Phi_5 &= 2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 \\
&= (641 - 625) \cdot 2^{28} + 1 = \left(641 - 5^4\right) \cdot 2^{28} + 1 \\
&= 641 \cdot 2^{28} - \left(5 \cdot 2^7\right)^4 + 1 \\
&= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\
&= 641 \cdot 2^{28} - \left(641^4 - 4 \cdot 641^3 + 6 \cdot 641^2 - 4 \cdot 641 + 1\right) + 1 \text{ [10]} \\
&= 641 \cdot \left(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4\right)
\end{aligned}$$

So $641 \mid \Phi_5$ and thus Φ_5 is composite.

[7] It's not necessary that $(a_1, b_1) = (a_0, b_0 \bmod a_0)$. a_1, b_1 are chosen such that $a_1 \leq b_1$.

[8] Also, $\mathbb{N} = \{0, 1, 2, \ldots\}$.

[9] Such towers are calculated from top to bottom, that is $a^{b^c} = a^{(b^c)}$. It doesn't make sense to define a^{b^c} as $\left(a^b\right)^c$ because $\left(a^b\right)^c$ can also just be written as a^{bc}. E.g. $3^{2^1} = 3^2 = 9$.

[10] $(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$. This is the binomial theorem. See Wikepdia: Binomial theorem.

There are a lot of open questions regarding Fermat numbers, like:

– Is Φ_n composite for all $n > 4$?

– Or are there even infinitely many composite Φ_n?

– Are there infinitely many Fermat primes?

By the way, the largest known composite Fermat number is $\Phi_{18233954}$ that was discovered to have the prime factor $7 \cdot 2^{18233956} + 1$. If you're interested, definitely check out Wikipedia: Fermat number and Wolfram Mathworld: Fermat Number.

But there is one interesting result that we can prove here, namely:

Theorem. Fermat numbers are coprime. That is,

$$\gcd\left(2^{2^a} + 1, 2^{2^b} + 1\right) = 1$$

for $a, b \in \mathbb{N}$ and $a \neq b$.

We'll present a this really neat proof:

Proof. How do we go from some Fermat number to the next one? Like this:

$$\Phi_n = (\Phi_{n-1} - 1)^2 + 1$$

This is because

$$\begin{aligned}
&(\Phi_{n-1} - 1)^2 + 1 \\
&= \left(2^{2^{n-1}}\right)^2 + 1 = 2^{2^{n-1} \cdot 2} + 1 \\
&= 2^{2^n} + 1 = \Phi_n
\end{aligned}$$

Expanding the binomial gives

$$\begin{aligned}
\Phi_n &= \Phi_{n-1}^2 - 2\Phi_{n-1} + 2 \\
&= \Phi_{n-1}(\Phi_{n-1} - 2) + 2
\end{aligned}$$

But then $\Phi_{n-1} = \Phi_{n-2}(\Phi_{n-2} - 2) + 2$. Substituting gives

$$\Phi_n = \Phi_{n-1}(\Phi_{n-2}(\Phi_{n-2} - 2)) + 2$$

We can repeat this up until Φ_0 to get

$$\Phi_n = \Phi_0\Phi_1...\Phi_{n-1} + 2$$

Now, for some $a, b \in \mathbb{N}$ with $a < b$, assume that $\gcd(\Phi_a, \Phi_b) = d > 1$. We can write

$$\Phi_b = \Phi_0\Phi_1...\Phi_{b-1} + 2$$

We have

$$d \mid \Phi_b \Rightarrow d \mid \Phi_0\Phi_1...\Phi_{b-1} + 2$$

We know that $\Phi_a \in \{\Phi_0, ..., \Phi_{b-1}\}$ and $d \mid \Phi_a$, so

$$d \mid \Phi_0\Phi_1...\Phi_{b-1}$$

But this also means $d \mid (\Phi_0...\Phi_{b-1} + 2) - \Phi_0...\Phi_{b-1} = 2$. Since $d > 1$, we must have $d = 2$. But Fermat numbers are all odd: $\Phi_n = 2^{2^n} + 1 = 2k + 1$, meaning that the GCD of two Fermat numbers can't be 2. Therefore we must conclude that $\gcd(\Phi_a, \Phi_b) = 1$ and the Fermat numbers are indeed coprime.

6. Important notice

This is version alpha. If you find any errors or have suggestions for cool facts about Fermat numbers, contact me on Discord (revol_ufiaw). Also: