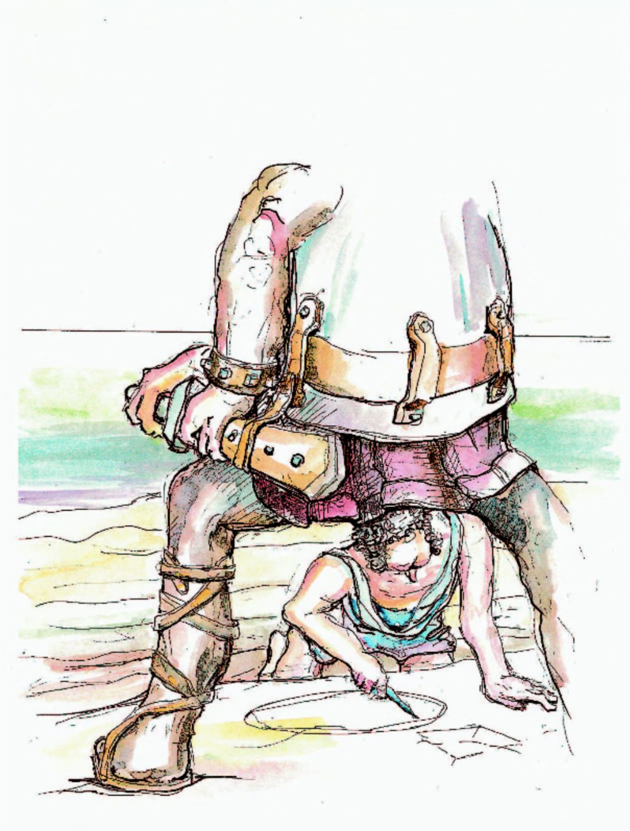
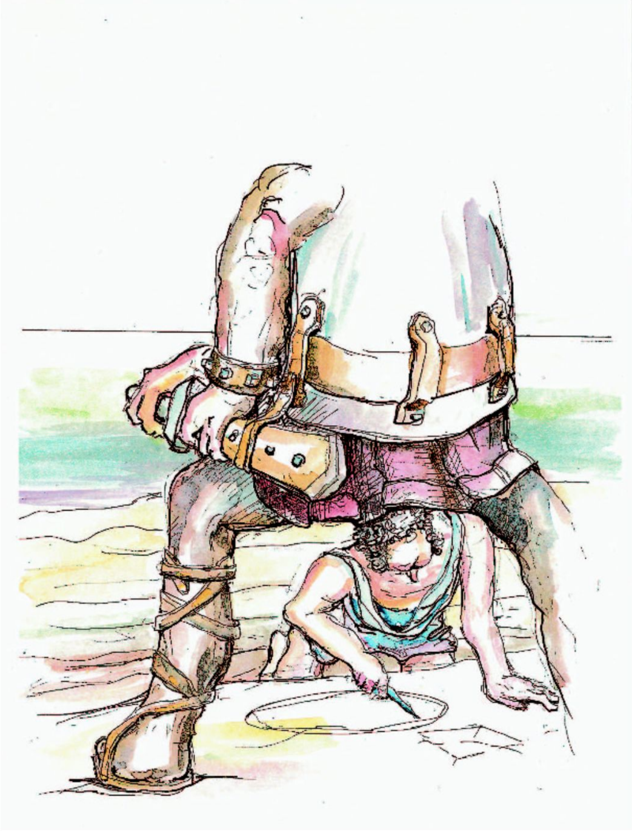
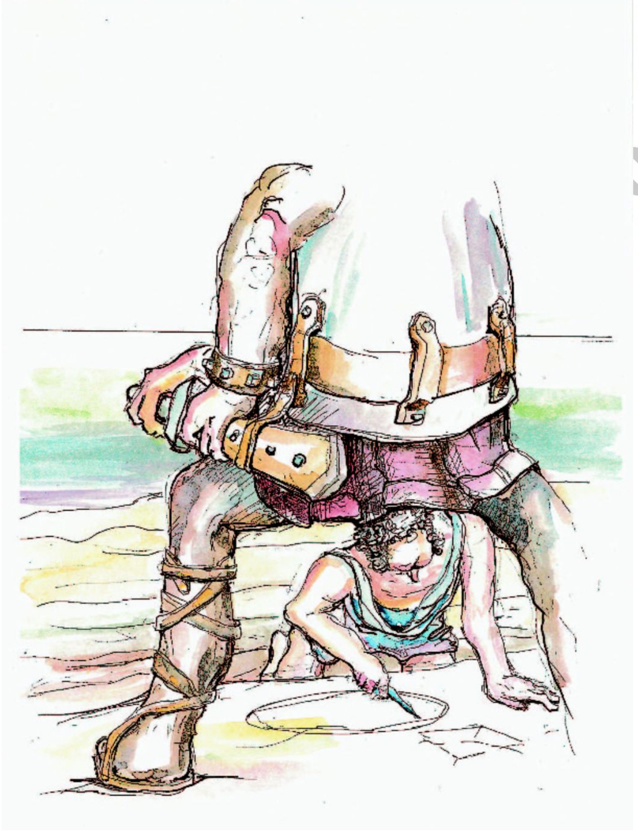




Pacing

Topics/Style

Exercises

Cadence

■ **Euclid's Proof.** For any finite set $\{p_1, \ldots, p_r\}$ of primes, consider the number $n = p_1 p_2 \cdots p_r + 1$. This n has a prime divisor p. But p is not one of the p_i: otherwise p would be a divisor of n and of the product $p_1 p_2 \cdots p_r$, and thus also of the difference $n - p_1 p_2 \cdots p_r = 1$, which is impossible. So a finite set $\{p_1, \ldots, p_r\}$ cannot be the collection of *all* prime numbers. □

Prime p has only two factors 1 and p (ignore -1, -p)

Every integer can be expressed as a (unique) product of primes

Proof by contradiction: suppose p is one of the p_i

1) By definition of p, p divides n
2) By hypothesis, p divides $p_1 \ldots p_r$

   Therefore p divides 1, contradiction, invalidates hypothesis

■ **Second Proof.** Let us first look at the *Fermat numbers* $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, \ldots$. We will show that any two Fermat numbers are relatively prime; hence there must be infinitely many primes. To this end, we verify the recursion

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geq 1),$$

from which our assertion follows immediately. Indeed, if m is a divisor of, say, F_k and F_n $(k < n)$, then m divides 2, and hence $m = 1$ or 2. But $m = 2$ is impossible since all Fermat numbers are odd.

To prove the recursion we use induction on n. For $n = 1$ we have $F_0 = 3$ and $F_1 - 2 = 3$. With induction we now conclude

$$\prod_{k=0}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) F_n = (F_n - 2) F_n =$$

$$= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \qquad \square$$

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \\ F_5 &= 641 \cdot 6700417 \end{aligned}$$

The first few Fermat numbers

Infinite sequence of Fermat numbers

Any two Fermat numbers are coprime -> infinite number of primes (proof: F_1 has to be coprime with the rest of the sequence. Each of F_i's leftover prime wrt to F_1 has to be unique otherwise F_i and F_j would not be coprime. But the Fs are unbounded, with finite primes, contradiction)

Choose any two arbitrary Fermat numbers, show that common divisor is 1, ie they are coprime

Abstract Algebra Background

Group, G, is a set of elements with an operation (*) which is

1. Associative (brackets don't matter - a * (b * c) = (a * b) * c = a * b * c
2. Exists an identity element e, \forall x in G, x * e = x = e * x
3. For all x in G, exists an inverse x^{-1} such that x^{-1} x = e = x x^{-1}

Subgroup, S is a subset of G s.t

1. S is closed to the operation (e.g forall x, y in S, x * y in S)
2. S is closed to inverses (e.g forall x in S, x^{-1} in S)

If (1) and (2) hold, S is also a group.

Order of a: least positive integer m s.t a^m = 1 if it exists otherwise ord(a) = \infty

E.g Suppose a^m = 1, then {a, a^2, …, a^m} is a group. (i.e inverse of a is $a^{m - 1}$, identity is a^m)

Theorem: If ord(a) = n: a^t = 1 iff t is a multiple of n

Lagrange's Theorem

If G is a finite (multiplicative) group and U is a subgroup, then $|U|$ divides $|G|$.

■ **Proof.** Consider the binary relation

$$a \sim b :\iff ba^{-1} \in U.$$

It follows from the group axioms that $\sim$ is an equivalence relation. The equivalence class containing an element a is precisely the coset

$$Ua = \{xa : x \in U\}.$$

Since clearly $|Ua| = |U|$, we find that G decomposes into equivalence classes, all of size $|U|$, and hence that $|U|$ divides $|G|$. □

In the special case when U is a cyclic subgroup $\{a, a^2, \ldots, a^m\}$ we find that m (the smallest positive integer such that $a^m = 1$, called the *order* of a) divides the size $|G|$ of the group.

Relation: Set of ordered tuples

Equivalence relation: A relation that is reflexive, transitive and symmetric (i.e kind of like a generalized equals sign)

Equivalence class of a: The set of all elements such that x ~ a

Proof notes:

- Coset definition from $a \sim a^{-1}$
- |Ua| = |U|, bijection f: U -> Ua where f(u) = ua
- Equivalence classes partition a set (cosets of U, all of same size, partition G)
- |G| = number of distinct equivalence classes * |U|

■ **Third Proof.** Suppose $\mathbb{P}$ is finite and p is the largest prime. We consider the so-called *Mersenne number* $2^p - 1$ and show that any prime factor q of $2^p - 1$ is bigger than p, which will yield the desired conclusion. Let q be a prime dividing $2^p - 1$, so we have $2^p \equiv 1 \pmod{q}$. Since p is prime, this means that the element 2 has order p in the multiplicative group $\mathbb{Z}_q \backslash \{0\}$ of the field $\mathbb{Z}_q$. This group has $q - 1$ elements. By Lagrange's theorem (see the box) we know that the order of every element divides the size of the group, that is, we have $p \mid q - 1$, and hence $p < q$. □

Order of a: least positive integer m s.t $a^m = 1$ if it exists otherwise ord(a) = \infty

Theorem: If ord(a) = n: $a^t = 1$ iff t is a multiple of n

ord(2) = p. Suppose not, there exists k s.t ord(2) = k, k < p. But by above theorem, then p is a multiple of k which cannot be true as p is prime. There ord(2) = p.

Z_q / {0} = {1, 2, …, q}

Cyclic subgroup of <2> = {2^1, 2^2, …, 2^p} (why not 2^{p+1}? $2^{p+1} = 2^p\, 2^1 = 1\, 2^1 = 2$ is already in the group)

By Lagrange, since <2> is a subgroup of Z_q / {0}, …

Also, p | q - 1 -> p < q? Exists k >= 1 s.t p k = q - 1, k = (q - 1) / p >= 1, q - 1 >= p -> q > p

■ **Fourth Proof.** Let $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ be the number of primes that are less than or equal to the real number x. We number the primes $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ in increasing order. Consider the natural logarithm $\log x$, defined as $\log x = \int_1^x \frac{1}{t} dt$.

Now we compare the area below the graph of $f(t) = \frac{1}{t}$ with an upper step function. (See also the appendix on page 10 for this method.) Thus for $n \le x < n+1$ we have

$$\begin{aligned}\log x &\le 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n} \\ &\le \sum \frac{1}{m}, \text{ where the sum extends over all } m \in \mathbb{N} \text{ which have only prime divisors } p \le x.\end{aligned}$$

Since every such m can be written in a *unique* way as a product of the form $\prod_{p \le x} p^{k_p}$, we see that the last sum is equal to

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \Big(\sum_{k \ge 0} \frac{1}{p^k} \Big).$$

The inner sum is a geometric series with ratio $\frac{1}{p}$, hence

$$\log x \le \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

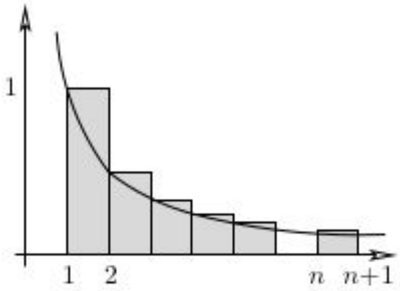
Now clearly $p_k \ge k+1$, and thus

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \le 1 + \frac{1}{k} = \frac{k+1}{k},$$

and therefore

$$\log x \le \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Everybody knows that $\log x$ is not bounded, so we conclude that $\pi(x)$ is unbounded as well, and so there are infinitely many primes. □



Steps above the function $f(t) = \frac{1}{t}$

Sum 1 / m contains all the previous terms and some more

Swapping sum/product isn't obvious to me but examples work

■ **Sixth Proof.** Our final proof goes a considerable step further and demonstrates not only that there are infinitely many primes, but also that the series $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverges. The first proof of this important result was given by Euler (and is interesting in its own right), but our proof, devised by Erdős, is of compelling beauty.

Let $p_1, p_2, p_3, \ldots$ be the sequence of primes in increasing order, and assume that $\sum_{p \in \mathbb{P}} \frac{1}{p}$ converges. Then there must be a natural number k such that $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Let us call $p_1, \ldots, p_k$ the *small* primes, and $p_{k+1}, p_{k+2}, \ldots$ the *big* primes. For an arbitrary natural number N we therefore find

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}. \qquad (1)$$

Finite series -> convergent so series diverging -> infinite series

Definition of convergent series:

$$\exists l, \forall \epsilon > 0 \exists N, \forall n > N : |S_n - l| < \epsilon$$

Let N_b be the number of positive integers $n \leq N$ which are divisible by at least one big prime, and N_s the number of positive integers $n \leq N$ which have only small prime divisors. We are going to show that for a suitable N

$$N_b + N_s < N,$$

which will be our desired contradiction, since by definition $N_b + N_s$ would have to be equal to N.

To estimate N_b note that $\lfloor \frac{N}{p_i} \rfloor$ counts the positive integers $n \leq N$ which are multiples of p_i. Hence by (1) we obtain

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \qquad (2)$$

Let us now look at N_s. We write every $n \leq N$ which has only small prime divisors in the form $n = a_n b_n^2$, where a_n is the square-free part. Every a_n is thus a product of *different* small primes, and we conclude that there are precisely 2^k different square-free parts. Furthermore, as $b_n \leq \sqrt{n} \leq \sqrt{N}$, we find that there are at most $\sqrt{N}$ different square parts, and so

$$N_s \leq 2^k \sqrt{N}.$$

Since (2) holds for *any* N, it remains to find a number N with $2^k \sqrt{N} \leq \frac{N}{2}$ or $2^{k+1} \leq \sqrt{N}$, and for this $N = 2^{2k+2}$ will do. □