Proofs from the Book: Infinity of primes

Alex Iosevich

May 7, 2020

What are primes and why do we care about them?

- We say that a positive integer $p > 1$ is a prime if p is only divisible by 1 and itself.

What are primes and why do we care about them?

- We say that a positive integer $p > 1$ is a prime if p is only divisible by 1 and itself.

- For example, 5 is a prime, but 4 is not since $4 = 2 \cdot 2$.

What are primes and why do we care about them?

- We say that a positive integer $p > 1$ is a prime if p is only divisible by 1 and itself.
- For example, 5 is a prime, but 4 is not since $4 = 2 \cdot 2$.
- A prime factorization of the integer $n > 1$ is the expression

$$n = p_1^{a_1} \cdot p_2^{a_2} \dots p_k^{a_k},$$

where p_k's are distinct primes.

What are primes and why do we care about them?

- We say that a positive integer $p > 1$ is a prime if p is only divisible by 1 and itself.
- For example, 5 is a prime, but 4 is not since $4 = 2 \cdot 2$.
- A prime factorization of the integer $n > 1$ is the expression

$$n = p_1^{a_1} \cdot p_2^{a_2} \dots p_k^{a_k},$$

where p_k's are distinct primes.

- Moreover, the prime factorization is unique!

Uniqueness of prime factorization

- The well-ordering principle says that any non-empty subset of the positive integers contains the least element. We shall take this concept for granted since it is easily derived from the principle of mathematical induction which is an axiom.

Uniqueness of prime factorization

- The well-ordering principle says that any non-empty subset of the positive integers contains the least element. We shall take this concept for granted since it is easily derived from the principle of mathematical induction which is an axiom.

Lemma

(Bezout's identity) Let a, b be integers with the greatest common divisor d. Then there exist integers x, y such that

$$ax + by = d.$$

-

Euclid's lemma

- After proving Bezout's identity, we shall use it to prove the following result due to Euclid.

Euclid's lemma

- After proving Bezout's identity, we shall use it to prove the following result due to Euclid.

Lemma

(Euclid) If a prime p divides the product ab of two integers a and b, then p must divide at least one of those integers a and b.

Euclid's lemma

- After proving Bezout's identity, we shall use it to prove the following result due to Euclid.

Lemma

(Euclid) If a prime p divides the product ab of two integers a and b, then p must divide at least one of those integers a and b.

-
- Finally, we shall use Euclid's lemma to establish the uniqueness of the prime number factorization.

Bezout and Euclid

Bezout and Euclid

-
  - 

Bezout and Euclid

-
- 
- 

Proof of Bezout's identity

- Let
$$S_{a,b} = \{ax + by : x, y \in \mathbb{Z}; ax + by > 0\}.$$

Proof of Bezout's identity

- Let
$$S_{a,b} = \{ax + by : x, y \in \mathbb{Z}; ax + by > 0\}.$$

- Observe that if $a \geq 0$, then taking $x = 1, y = 0$ shows that $a \in S_{a.b}$. If $a \leq 0$, taking $x = -1, y = 0$ shows that $-a \in S_{a,b}$.

Proof of Bezout's identity

- Let
$$S_{a,b} = \{ax + by : x, y \in \mathbb{Z}; ax + by > 0\}.$$

- Observe that if $a \geq 0$, then taking $x = 1, y = 0$ shows that $a \in S_{a.b}$. If $a \leq 0$, taking $x = -1, y = 0$ shows that $-a \in S_{a,b}$.

- In particular, $S_{a,b}$ is not empty.

Proof of Bezout's identity

- Let
$$S_{a,b} = \{ax + by : x, y \in \mathbb{Z}; ax + by > 0\}.$$

- Observe that if $a \geq 0$, then taking $x = 1, y = 0$ shows that $a \in S_{a.b}$. If $a \leq 0$, taking $x = -1, y = 0$ shows that $-a \in S_{a,b}$.

- In particular, $S_{a,b}$ is not empty.

- By the well-ordering principle, $S_{a,b}$ has the least element
$$d = as + bt.$$

Proof of Bezout's identity (continued)

- We will show that d is the greatest common divisor of a and b.

Proof of Bezout's identity (continued)

- We will show that d is the greatest common divisor of a and b.

- We write

$$a = dq + r, \text{ where } 0 \leq r < d.$$

Proof of Bezout's identity (continued)

- We will show that d is the greatest common divisor of a and b.
- We write
$$a = dq + r, \text{ where } 0 \leq r < d.$$
- Observe that
$$r = a - dq = a - q(as + bt) = a(1 - qs) - bqt,$$
which implies that $r \in S_{a,b} \cup \{0\}$.

Proof of Bezout's identity (continued)

- We will show that d is the greatest common divisor of a and b.
- We write

$$a = dq + r, \text{ where } 0 \leq r < d.$$

- Observe that

$$r = a - dq = a - q(as + bt) = a(1 - qs) - bqt,$$

which implies that $r \in S_{a,b} \cup \{0\}$.

- But $r < d$ and d is the least element in $S_{a,b}$, so $r = 0$ and hence d is a divisor of a. In the same way, d is a divisor of b.

Proof of Bezout's identity (finale)

- It remains to show that d is the greatest common divisor.

Proof of Bezout's identity (finale)

- It remains to show that d is the greatest common divisor.
- Suppose that $a = cu, b = cv$. Then

$$d = as + bt = cus + cvt = c(us + vt),$$

Proof of Bezout's identity (finale)

- It remains to show that d is the greatest common divisor.
- Suppose that $a = cu, b = cv$. Then

$$d = as + bt = cus + cvt = c(us + vt),$$

- which implies that c is a divisor of d, so $c \leq d$.

Proof of Bezout's identity (finale)

- It remains to show that d is the greatest common divisor.
- Suppose that $a = cu, b = cv$. Then

$$d = as + bt = cus + cvt = c(us + vt),$$

- which implies that c is a divisor of d, so $c \leq d$.
- This completes the proof of Bezout's identity.

Proof of Euclid's lemma

- We shall now prove that if p is a prime and p divides ab, then p divides at least one of a, b.

Proof of Euclid's lemma

- We shall now prove that if p is a prime and p divides ab, then p divides at least one of a, b.

- Suppose that p does not divide a. Then by Bezout's identity, there exist x, y such that
$$px + ay = 1.$$

Proof of Euclid's lemma

- We shall now prove that if p is a prime and p divides ab, then p divides at least one of a, b.

- Suppose that p does not divide a. Then by Bezout's identity, there exist x, y such that
$$px + ay = 1.$$

- Multiplying both sides by b yields
$$bpx + bay = b.$$

Proof of Euclid's lemma

- We shall now prove that if p is a prime and p divides ab, then p divides at least one of a, b.
- Suppose that p does not divide a. Then by Bezout's identity, there exist x, y such that
$$px + ay = 1.$$
- Multiplying both sides by b yields
$$bpx + bay = b.$$
- Observe that $\boxed{bpx}$ is divisible by p because p is present and $\boxed{bay}$ is divisible by p because p divides ab by assumption. This implies that p divides b, and Euclid's lemma is proved.

Existence and uniqueness of prime number factorization

Theorem

Every positive integer n can be written in the form

$$p_1^{a_1} p_2^{a_2} \dots p_k^{a_k},$$

where each p_j is prime, $a_j \geq 1$, and

$$p_1 < p_2 < \cdots < p_k.$$

Moreover, this representation of n is unique.

Proof of existence

- We proceed by induction. First, 2 is prime. Now assume that every number $< n$ is either prime or a product of primes.

Proof of existence

- We proceed by induction. First, 2 is prime. Now assume that every number $< n$ is either prime or a product of primes.

- if n is prime, there is nothing to prove.

Proof of existence

- We proceed by induction. First, 2 is prime. Now assume that every number $< n$ is either prime or a product of primes.
- if n is prime, there is nothing to prove.
- If n is not prime, $n = ab$, where $a < n, b < n$.

Proof of existence

- We proceed by induction. First, 2 is prime. Now assume that every number $< n$ is either prime or a product of primes.
- if n is prime, there is nothing to prove.
- If n is not prime, $n = ab$, where $a < n, b < n$.
- By the induction hypothesis, a is a product of primes and so is b, so $n = ab$ is also a product of primes.

Proof of uniqueness

- Suppose, to the contrary, there is an integer that has two distinct prime factorizations.

Proof of uniqueness

- Suppose, to the contrary, there is an integer that has two distinct prime factorizations.

- Let n be the least such integer and write

$$n = p_1 p_2 \dots p_j = q_1 q_2 \dots q_k,$$

where each p_i and q_i is prime, $j, k \geq 2$.

Proof of uniqueness

- Suppose, to the contrary, there is an integer that has two distinct prime factorizations.

- Let n be the least such integer and write

$$n = p_1 p_2 \ldots p_j = q_1 q_2 \ldots q_k,$$

where each p_i and q_i is prime, $j, k \geq 2$.

- We see p_1 divides $q_1 q_2 \ldots q_k$, so p_1 divides some q_i by Euclid's lemma.

Proof of uniqueness

- Suppose, to the contrary, there is an integer that has two distinct prime factorizations.
- Let n be the least such integer and write

$$n = p_1 p_2 \dots p_j = q_1 q_2 \dots q_k,$$

where each p_i and q_i is prime, $j, k \geq 2$.

- We see p_1 divides $q_1 q_2 \dots q_k$, so p_1 divides some q_i by Euclid's lemma.
- Without loss of generality, p_1 divides q_1, which implies that $p_1 = q_1$ since they are both prime.

Proof of uniqueness (concluded)

- Going back to factorization of n, we may cancel p_1 and q_1, which yields

$$p_2 p_3 \dots p_j = q_2 q_3 \dots q_k.$$

Proof of uniqueness (concluded)

- Going back to factorization of n, we may cancel p_1 and q_1, which yields

$$p_2 p_3 \dots p_j = q_2 q_3 \dots q_k.$$

- As a result, we have two distinct prime factorizations of some integer strictly smaller than n, which contradicts the minimality of n.

Proof of uniqueness (concluded)

- Going back to factorization of n, we may cancel p_1 and q_1, which yields
$$p_2 p_3 \dots p_j = q_2 q_3 \dots q_k.$$

- As a result, we have two distinct prime factorizations of some integer strictly smaller than n, which contradicts the minimality of n.

- This completes the proof of uniqueness of the prime number factorization.

Euclid's proof of the infinity of primes

- Suppose that there are finitely many primes, namely $p_1, p_2, \dots, p_n$.

Euclid's proof of the infinity of primes

- Suppose that there are finitely many primes, namely $p_1, p_2, \ldots, p_n$.
- Consider
$$m = p_1 p_2 \ldots p_n + 1.$$

Euclid's proof of the infinity of primes

- Suppose that there are finitely many primes, namely $p_1, p_2, \ldots, p_n$.

- Consider
$$m = p_1 p_2 \ldots p_n + 1.$$

- Dividing m by p_j yields the remainder of 1 for each j, so m is not divisible by any of the p_js.

Euclid's proof of the infinity of primes

- Suppose that there are finitely many primes, namely $p_1, p_2, \ldots, p_n$.

- Consider

$$m = p_1 p_2 \ldots p_n + 1.$$

- Dividing m by p_j yields the remainder of 1 for each j, so m is not divisible by any of the p_js.

- We conclude that m must be a prime number, which is a contradiction since we assumed that

$$p_1, \ldots, p_n$$

is a complete list of primes.

Sam Northshield's proof of the infinity of primes

- Suppose that the set of primes $\mathbb{P}$ is finite. Then

$$0 < \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi}{p}\right)$$

since all the angles $\frac{\pi}{p}$ are in the first quadrant.

Sam Northshield's proof of the infinity of primes

- Suppose that the set of primes $\mathbb{P}$ is finite. Then

$$0 < \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi}{p}\right)$$

since all the angles $\frac{\pi}{p}$ are in the first quadrant.

- On the other hand,

$$\prod_{p \in \mathbb{P}} \sin\left(\frac{\pi}{p}\right) = \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi}{p} + \frac{2\pi \prod_{p' \in \mathbb{P}} p'}{p}\right)$$

Sam Northshield's proof (concluded)

- $$= \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi \left(1 + 2 \prod_{p' \in \mathbb{P}} p'\right)}{p} \right) = 0.$$

Sam Northshield's proof (concluded)

- $$= \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi\left(1 + 2\prod_{p' \in \mathbb{P}} p'\right)}{p}\right) = 0.$$

- Why is it 0?

Sam Northshield's proof (concluded)

- $$= \prod_{p \in \mathbb{P}} \sin\left(\frac{\pi \left(1 + 2\prod_{p' \in \mathbb{P}} p'\right)}{p} \right) = 0.$$

- Why is it 0?

- Because
$$1 + 2 \prod_{p' \in \mathbb{P}} p'$$
must be divisible by some $p \in \mathbb{P}$ by the virtue of the fact that every number is a product of primes.

Fermat numbers proof

- Let

$$F_n = 2^{2^n} + 1, \;\; n \geq 0.$$

Fermat numbers proof

- Let
$$F_n = 2^{2^n} + 1, \;\; n \geq 0.$$

- If we can show that all the Fermat numbers are relatively prime (no divisors in common), then there must be infinitely many primes.

Fermat numbers proof

- Let

$$F_n = 2^{2^n} + 1, \ \ n \geq 0.$$

- If we can show that all the Fermat numbers are relatively prime (no divisors in common), then there must be infinitely many primes.

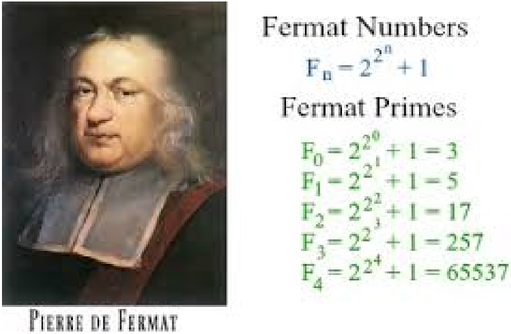
- To this end, we are going to prove that

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

Fermat and friends

Fermat and friends

-



Fermat numbers proof (continued)

- Suppose that we can prove this recurrence. Then if some F_k has a divisor m in common with F_n, $k < n$, then m divides 2.

Fermat numbers proof (continued)

- Suppose that we can prove this recurrence. Then if some F_k has a divisor m in common with F_n, $k < n$, then m divides 2.
- This implies that $m = 1$ or $m = 2$. The latter is impossible since all Fermat numbers are odd.

Fermat numbers proof (continued)

- Suppose that we can prove this recurrence. Then if some F_k has a divisor m in common with F_n, $k < n$, then m divides 2.
- This implies that $m = 1$ or $m = 2$. The latter is impossible since all Fermat numbers are odd.
- This proves that F_n's are relatively prime provided that the recurrence above holds.

Fermat numbers proof (continued)

- Suppose that we can prove this recurrence. Then if some F_k has a divisor m in common with F_n, $k < n$, then m divides 2.
- This implies that $m = 1$ or $m = 2$. The latter is impossible since all Fermat numbers are odd.
- This proves that F_n's are relatively prime provided that the recurrence above holds.
- We now turn our attention to the proof of the recurrence.

Proof of the Fermat recurrence

- We proceed by induction. If $n = 1$, we have

$$3 = F_0 = F_1 - 2 = 2^{2^1} + 1 - 2.$$

Proof of the Fermat recurrence

- We proceed by induction. If $n = 1$, we have

$$3 = F_0 = F_1 - 2 = 2^{2^1} + 1 - 2.$$

- Assuming the formula for n, we have

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

Proof of the Fermat recurrence

- We proceed by induction. If $n = 1$, we have

$$3 = F_0 = F_1 - 2 = 2^{2^1} + 1 - 2.$$

- Assuming the formula for n, we have

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

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

Proof via mysterious definitions

- For $a, b \in \mathbb{Z}$, $b > 0$, define

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Proof via mysterious definitions

- For $a, b \in \mathbb{Z}$, $b > 0$, define

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

- This is a two-way infinite arithmetic progression in $\mathbb{Z}$.

Proof via mysterious definitions

- For $a, b \in \mathbb{Z}$, $b > 0$, define

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

- This is a two-way infinite arithmetic progression in $\mathbb{Z}$.

- Define a subset O of $\mathbb{Z}$ to be **open** if either O is empty, or for every $a \in O$, there exists $b > 0$ such that

$$N_{a,b} \subset O.$$

Properties of open and closed sets

- We say that $O \subset \mathbb{Z}$ is **closed** if $\mathbb{Z} \backslash O$ is open.

Properties of open and closed sets

- We say that $O \subset \mathbb{Z}$ is **closed** if $\mathbb{Z} \backslash O$ is open.
- Every set $N_{a,b}$ is **open** since given any $a' \in N_{a,b}$, i.e $a' = a + kb$ for some k,
$$N_{a,b} = N_{a+kb,b}.$$

Properties of open and closed sets

- We say that $O \subset \mathbb{Z}$ is **closed** if $\mathbb{Z} \backslash O$ is open.

- Every set $N_{a,b}$ is **open** since given any $a' \in N_{a,b}$, i.e $a' = a + kb$ for some k,

$$N_{a,b} = N_{a+kb,b}.$$

- By the same argument, the union of any number (finite or infinite) of $N_{a,b}$'s is **open**.

Properties of open sets (continued)

- We claim that the intersection of two **open** sets is **open**.

Properties of open sets (continued)

- We claim that the intersection of two **open** sets is **open**.

- Suppose that O_1 and O_2 are both **open** and consider $a \in O_1 \cap O_2$.

Properties of open sets (continued)

- We claim that the intersection of two **open** sets is **open**.
- Suppose that O_1 and O_2 are both **open** and consider $a \in O_1 \cap O_2$.
- Then $N_{a,b_1} \subset O_1$ and $N_{a,b_2} \subset O_2$ for some $b_1, b_2 > 0$.

Properties of open sets (continued)

- We claim that the intersection of two **open** sets is **open**.
- Suppose that O_1 and O_2 are both **open** and consider $a \in O_1 \cap O_2$.
- Then $N_{a,b_1} \subset O_1$ and $N_{a,b_2} \subset O_2$ for some $b_1, b_2 > 0$.
- But then

$$N_{a,b_1 b_2} \subset O_1 \cap O_2,$$

so $O_1 \cap O_2$ is **open**.

Properties of closed sets

- We claim that $N_{a,b}$ is also **closed**.

Properties of closed sets

- We claim that $N_{a,b}$ is also **closed**.
- To see this, observe that

$$N_{a,b} = \mathbb{Z} \setminus \cup_{k=1}^{b-1} N_{a+i,b}$$

Properties of closed sets

- We claim that $N_{a,b}$ is also **closed**.
- To see this, observe that

$$N_{a,b} = \mathbb{Z} \setminus \cup_{k=1}^{b-1} N_{a+i,b}$$

- since

$$\mathbb{Z} = \cup_{k=0}^{b-1} N_{a+i,b},$$

Properties of closed sets

- We claim that $N_{a,b}$ is also **closed**.
- To see this, observe that

$$N_{a,b} = \mathbb{Z} \setminus \cup_{k=1}^{b-1} N_{a+i,b}$$

- since

$$\mathbb{Z} = \cup_{k=0}^{b-1} N_{a+i,b},$$

- hence $N_{a,b}$ is a complement of an **open** set, so it is **closed**!

Primes enter the picture

- What does it mean to say that every integer is a product of primes in terms of our current setup? It means that

$$\mathbb{Z} \backslash \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Primes enter the picture

- What does it mean to say that every integer is a product of primes in terms of our current setup? It means that

$$\mathbb{Z} \backslash \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

- Suppose that the set of primes $\mathbb{P}$ is finite. Then the right hand side is a union of finitely many **closed sets**.

Primes enter the picture

- What does it mean to say that every integer is a product of primes in terms of our current setup? It means that

$$\mathbb{Z} \backslash \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

- Suppose that the set of primes $\mathbb{P}$ is finite. Then the right hand side is a union of finitely many **closed sets**.
- If $\bigcup_{p \in \mathbb{P}} N_{0,p}$ is **closed**, we are done because then $\{-1, 1\}$ is **open**, which is impossible since by definition, **open** sets contain an infinite two-sided arithmetic progression.

Unions of **closed** sets

- Since each $N_{0,p}$ is **closed**, it is a complement of a **open** set O_p.

Unions of **closed** sets

- Since each $N_{0,p}$ is **closed**, it is a complement of a **open** set O_p.

- By DeMorgan Laws (which we shall prove in a moment),

$$\bigcup_{p\in\mathbb{P}} N_{0,p} = \bigcup_{p\in\mathbb{P}} \mathbb{Z}\setminus O_p = \mathbb{Z}\setminus \bigcap_{p\in\mathbb{P}} O_p.$$

Unions of **closed** sets

- Since each $N_{0,p}$ is **closed**, it is a complement of a **open** set O_p.

- By DeMorgan Laws (which we shall prove in a moment),

$$\bigcup_{p\in\mathbb{P}} N_{0,p} = \bigcup_{p\in\mathbb{P}} \mathbb{Z}\backslash O_p = \mathbb{Z}\backslash \bigcap_{p\in\mathbb{P}} O_p.$$

- Since the intersection of finitely many **open** sets is open, as we showed above, we conclude that

$$\bigcup_{p\in\mathbb{P}} N_{0,p} \text{ is } \textbf{closed} \text{ and we are done!}$$

DeMorgan Laws

- We shall state these for subsets of the integers, but these laws are really universal. Let $A_1, A_2, \dots, A_n \subset \mathbb{Z}$. Then

$$\bigcup_{i=1}^{n} \mathbb{Z} \backslash A_i = \mathbb{Z} \backslash \bigcap_{i=1}^{n} A_i.$$

DeMorgan Laws

- We shall state these for subsets of the integers, but these laws are really universal. Let $A_1, A_2, \ldots, A_n \subset \mathbb{Z}$. Then

$$\bigcup_{i=1}^{n} \mathbb{Z} \backslash A_i = \mathbb{Z} \backslash \bigcap_{i=1}^{n} A_i.$$

- To prove this, suppose that $m \in \mathbb{Z} \backslash \bigcap_{i=1}^{n} A_i$. Then $m \notin \bigcap_{i=1}^{n} A_i$.

DeMorgan Laws

- We shall state these for subsets of the integers, but these laws are really universal. Let $A_1, A_2, \ldots, A_n \subset \mathbb{Z}$. Then

$$\bigcup_{i=1}^{n} \mathbb{Z} \backslash A_i = \mathbb{Z} \backslash \bigcap_{i=1}^{n} A_i.$$

- To prove this, suppose that $m \in \mathbb{Z} \backslash \bigcap_{i=1}^{n} A_i$. Then $m \notin \bigcap_{i=1}^{n} A_i$.

- It follows that $m \in \mathbb{Z} \backslash A_i$ for some i, which means that

$$m \in \bigcup_{i=1}^{n} \mathbb{Z} \backslash A_i.$$

DeMorgan Laws (continued)

- Now suppose that $m \in \bigcup_{i=1}^{n} \mathbb{Z} \backslash A_i$. Then $m \in \mathbb{Z} \backslash A_i$ for some i.

DeMorgan Laws (continued)

- Now suppose that $m \in \bigcup_{i=1}^{n} \mathbb{Z} \backslash A_i$. Then $m \in \mathbb{Z} \backslash A_i$ for some i.

- This implies that $m \notin \bigcap_{i=1}^{n} A_i$, so we conclude that

$$m \in \mathbb{Z} \backslash \bigcap_{i=1}^{n} A_i.$$

DeMorgan Laws (continued)

- Now suppose that $m \in \bigcup_{i=1}^{n} \mathbb{Z} \setminus A_i$. Then $m \in \mathbb{Z} \setminus A_i$ for some i.
- This implies that $m \notin \bigcap_{i=1}^{n} A_i$, so we conclude that

$$m \in \mathbb{Z} \setminus \bigcap_{i=1}^{n} A_i.$$

- We have shown that the left hand side is a subset of the right hand side, and vice-versa, so the proof is complete.

DeMorgan Laws in pictures

-

DeMorgan Laws in pictures