Mathematical Induction

Part Two

The **principle of mathematical induction** states that if for some property P(*n*), we have that

P(0) is true

and

For any natural number *n*, P(*n*) → P(*n* + 1)

Then

For any natural number *n*, P(*n*) is true.

One Major Catch

One Major Catch

0	1	2	3	4	5	6	7	8

One Major Catch

0	1	2	3	4	5	6	7	8

One Major Catch

One Major Catch

In an inductive proof, to prove P(5), we can only assume P(4). We cannot rely on any of our earlier results!

Strong Induction

The **principle of strong induction** states that if for some property P(n), we have that

P(0) is true

and

For any natural number n,
if P(n') is true for all n' ≤ n, then P(n + 1) is true

then

For any natural number n, P(n) is true.

The **principle of strong induction** states that if for some property P(n), we have that

Assume that P(n) holds for n and all smaller n.

P(0) is true

and

For any natural number n,
if P(n') is true for all n' ≤ n, then P(n + 1) is true

then

For any natural number n, P(n) is true.

Using Strong Induction

0	1	2	3	4	5	6	7	8

Using Strong Induction

0	1	2	3	4	5	6	7	8

Using Strong Induction

0	1	2	3	4	5	6	7	8

Using Strong Induction

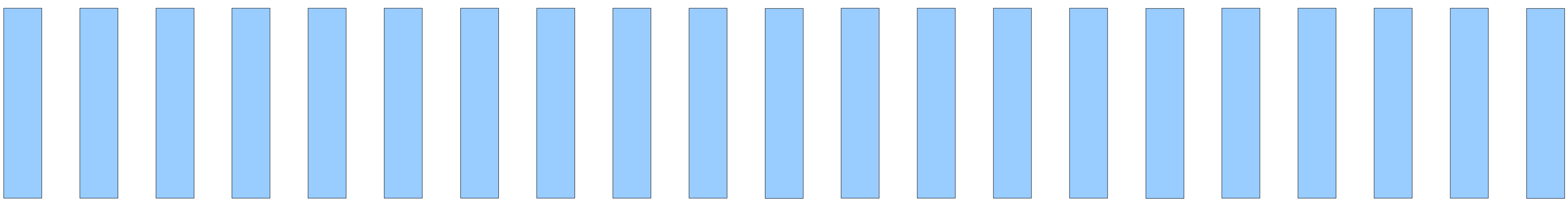
0 1 2 3 4 5 6 7 8

Using Strong Induction

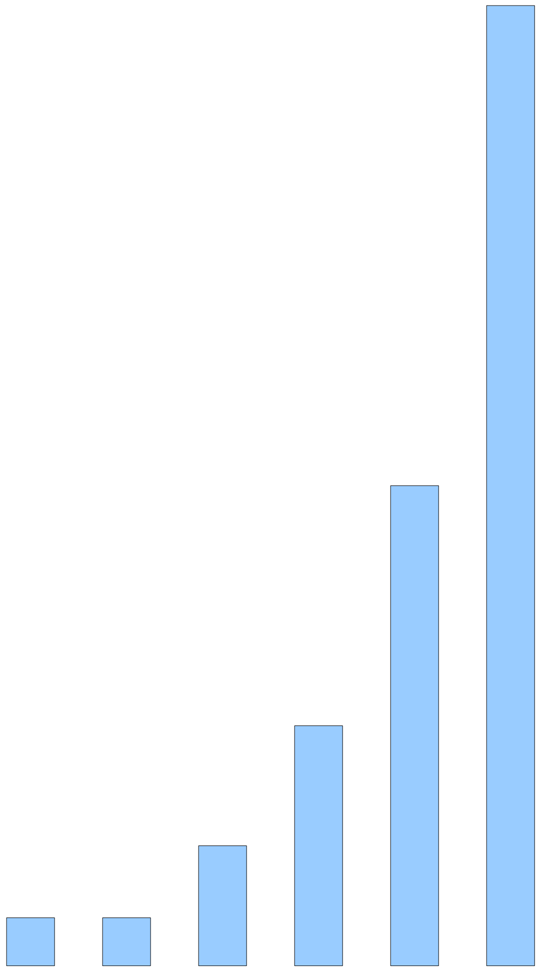
Using Strong Induction

0	1	2	3	4	5	6	7	8

Induction and Dominoes



Strong Induction and Dominoes



Weak and Strong Induction

- **Weak induction** (regular induction) is good for showing that some property holds by incrementally adding in one new piece.
- **Strong induction** is good for showing that some property holds by breaking a large structure down into multiple small pieces.

Proof by Strong Induction

- State that you are attempting to prove something by strong induction.
- State what your choice of P(n) is.
- Prove the base case:
  - State what P(0) is, then prove it.
- Prove the inductive step:
  - State that you assume for all $0 \leq n' \leq n$, that P(n') is true.
  - State what P(n + 1) is. *(this is what you're trying to prove)*
  - Go prove P(n + 1).

Application: Binary Numbers

Binary Numbers

- The **binary number system** is base 2.
- Every number is represented as 1s and 0s encoding various powers of two.
- Examples:
  - $100_2 = 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 = 4$
  - $11011_2 = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 27$
- Enormously useful in computing; almost all computers do computation on binary numbers.
- Question: How do we know that every natural number can be written in binary?

Justifying Binary Numbers

- To justify the binary representation, we will prove the following result:

Every natural number *n* can be expressed as the sum of distinct powers of two.

- This says that there's *at least* one way to write a number in binary; we'd need a separate proof to show that there's *exactly* one way to do it.
- So how do we prove this?

One Proof Idea

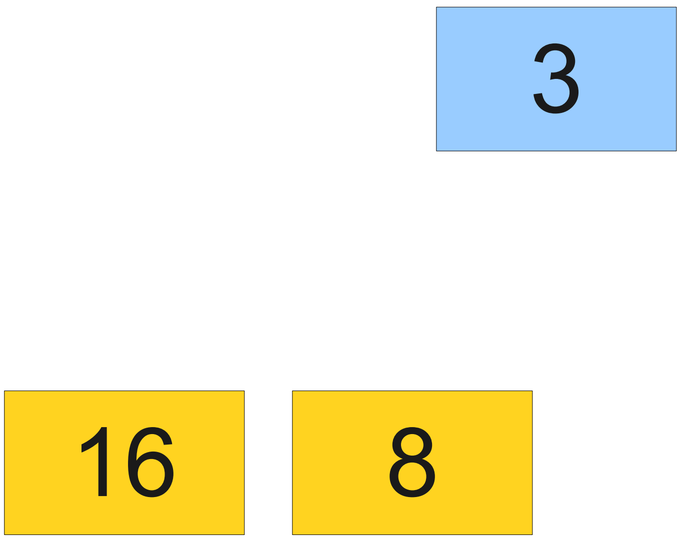
27

One Proof Idea

11

16

One Proof Idea



One Proof Idea

1

16 8 2

One Proof Idea

0

16 8 2 1

General Idea

- Repeatedly subtract out the largest power of two less than the number.
- Can't subtract 2^n twice for any *n*; otherwise, you could have subtracted 2^{n+1}.
- Eventually, we reach 0; the number is then the sum of the powers of two that we subtracted.
- How do we formalize this as a proof?

Theorem: Every natural number can be written as the sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two."

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be “n can be written as the sum of distinct powers of two.” We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be “n can be written as the sum of distinct powers of two.” We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \le n' \le n$, that P(n') holds and n' can be written as the sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two.

Notice the stronger version of the induction hypothesis. We're now showing that P(n) is true for n and all smaller natural numbers. We're going to use this fact later on.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$.

Here's the key step of the proof. If we can show that

$$n + 1 - 2^k \leq n$$

then we can use the inductive hypothesis to claim that $n + 1 - 2^k$ is a sum of distinct powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two.

This step would fail in a normal inductive proof because we're talking about some number no greater than n, not necessarily n itself. Strong induction is extremely useful in cases like this.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 – 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 – 2^k \leq n + 1 – 1 = n$. Thus, by our inductive hypothesis, $n + 1 – 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

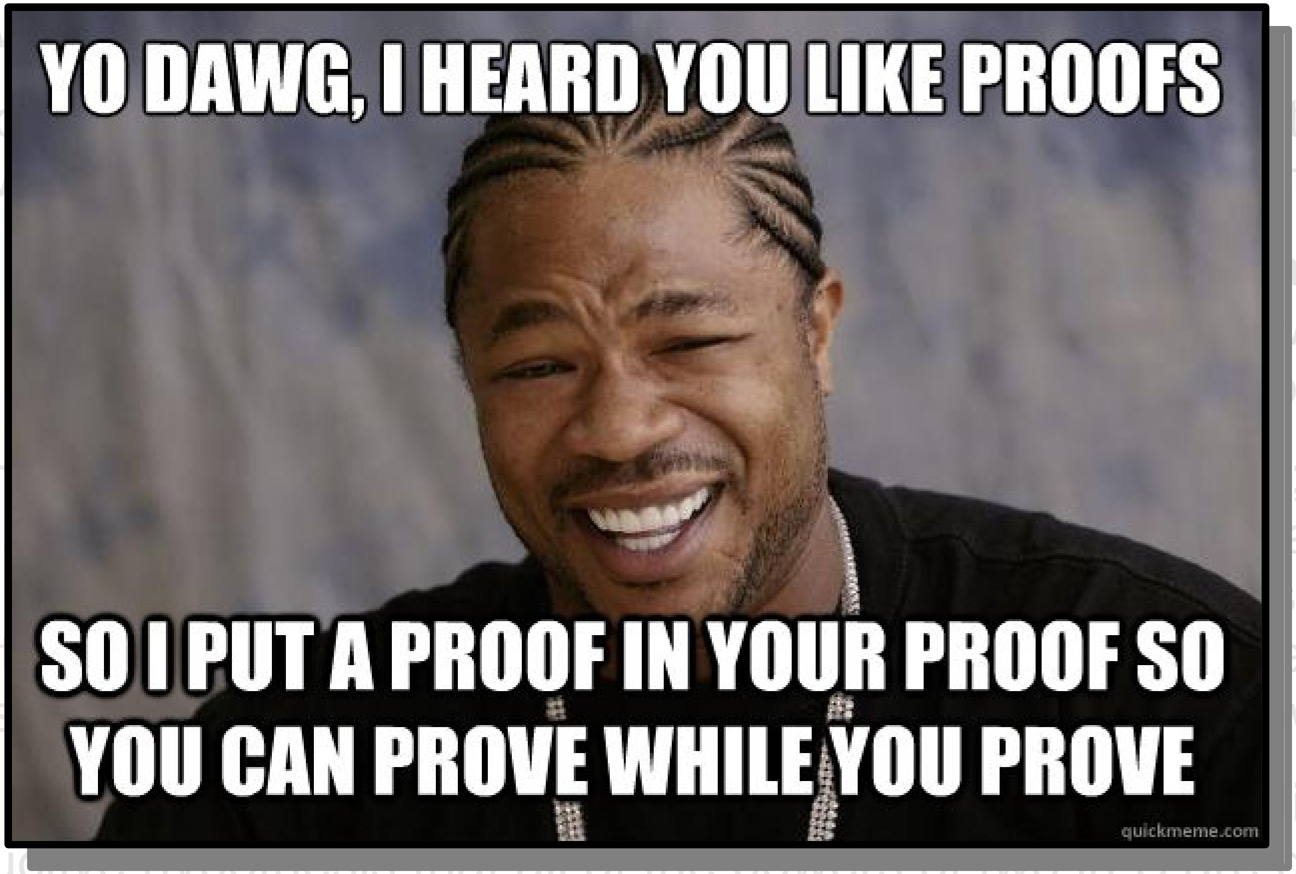
For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(*n*) be "*n* can be written as the sum of distinct
pow



As ... the sum of distinct powers
of tv ... to 0, P(0) holds.

For ... tisfying $0 \leq n' \leq n$, that
P(*n* ... vers of two. We prove
P(*n* ... owers of two.

Cor ... ; let it be 2^k. Then
con ... al number *k*, we know that
n + ... is, $n + 1 - 2^k$ can be
writ ... et of these powers of two.
This ... wers of two in *S*.

We ... inct. We know by the
indu ... distinct, so the only way
that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$. Since $2^k \in S$ and the sum of the powers of two in S is $n + 1 - 2^k$, this means that $2^k \leq n + 1 - 2^k$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 – 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 – 2^k \leq n + 1 – 1 = n$. Thus, by our inductive hypothesis, $n + 1 – 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$. Since $2^k \in S$ and the sum of the powers of two in S is $n + 1 – 2^k$, this means that $2^k \leq n + 1 – 2^k$. This means that $2(2^k) \leq n + 1$, so $2^{k+1} \leq n + 1$, contradicting the fact that 2^k is the largest power of two less than or equal to $n + 1$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$. Since $2^k \in S$ and the sum of the powers of two in S is $n + 1 - 2^k$, this means that $2^k \leq n + 1 - 2^k$. This means that $2(2^k) \leq n + 1$, so $2^{k+1} \leq n + 1$, contradicting the fact that 2^k is the largest power of two less than or equal to $n + 1$. We have reached a contradiction, so our assumption was wrong and $2^k \notin S$.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$. Since $2^k \in S$ and the sum of the powers of two in S is $n + 1 - 2^k$, this means that $2^k \leq n + 1 - 2^k$. This means that $2(2^k) \leq n + 1$, so $2^{k+1} \leq n + 1$, contradicting the fact that 2^k is the largest power of two less than or equal to $n + 1$. We have reached a contradiction, so our assumption was wrong and $2^k \notin S$. We have shown that $n + 1$ can be expressed as a sum of distinct powers of two, so P($n + 1$) holds, completing the induction.

Theorem: Every natural number can be written as the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n can be written as the sum of distinct powers of two." We prove that P(n) is true for all n.

As our base case, we prove P(0), that 0 can be written as the sum of distinct powers of two. Since the empty sum of no powers of two is equal to 0, P(0) holds.

For the inductive step, assume that for some n, for all n' satisfying $0 \leq n' \leq n$, that P(n') holds and n' can be written as the sum of distinct powers of two. We prove P($n + 1$), that $n + 1$ can be written as the sum of distinct powers of two.

Consider the largest power of 2 less than or equal to $n + 1$; let it be 2^k. Then consider the number $n + 1 - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n + 1 - 2^k \leq n + 1 - 1 = n$. Thus, by our inductive hypothesis, $n + 1 - 2^k$ can be written as the sum of distinct powers of two; let S be the set of these powers of two. This means that $n + 1$ is equal to 2^k plus the sum of the powers of two in S.

We now need to show that these powers of two are all distinct. We know by the inductive hypothesis that all of the powers of two in S are distinct, so the only way that a power of two would be repeated would be if $2^k \in S$. We show that this is impossible by contradiction; assume that $2^k \in S$. Since $2^k \in S$ and the sum of the powers of two in S is $n + 1 - 2^k$, this means that $2^k \leq n + 1 - 2^k$. This means that $2(2^k) \leq n + 1$, so $2^{k+1} \leq n + 1$, contradicting the fact that 2^k is the largest power of two less than or equal to $n + 1$. We have reached a contradiction, so our assumption was wrong and $2^k \notin S$. We have shown that $n + 1$ can be expressed as a sum of distinct powers of two, so P($n + 1$) holds, completing the induction. ■

Reformulating Strong Induction

The **principle of strong induction** states that if for some property P(n), we have that

P(0) is true

and

For any natural number n,
if P(n') is true for all n' ≤ n, then P(n + 1) is true

then

For any natural number n, P(n) is true.

The **principle of strong induction** states that if for some property P(n), we have that

Assume that P(n) holds for n and all smaller n.

P(0) is true

and

For any natural number n,
if P(n') is true for all n' ≤ n, then P(n + 1) is true

then

For any natural number n, P(n) is true.

The **principle of strong induction** states that if for some property P(n), we have that

P(0) is true

and

For any natural number n,
if P(n') is true for all n' < n, then P(n) is true

then

For any natural number n, P(n) is true.

Application: **Continued Fractions**

Continued Fractions

$$\cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

Continued Fractions

$$\cfrac{1}{4 + \cfrac{1}{\boxed{1 + \cfrac{1}{2}}}}$$

Continued Fractions

$$\cfrac{1}{4 + \cfrac{1}{\cfrac{3}{2}}}$$

Continued Fractions

$$\cfrac{1}{4 + \cfrac{1}{\cfrac{3}{2}}}$$

Continued Fractions

$$\frac{1}{4 + \frac{2}{3}}$$

Continued Fractions

$$\frac{1}{\boxed{4 + \frac{2}{3}}}$$

Continued Fractions

$$\frac{1}{\dfrac{14}{3}}$$

Continued Fractions

$$\cfrac{1}{\cfrac{14}{3}}$$

Continued Fractions

$$\frac{3}{14}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2}}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{\boxed{4 + \cfrac{1}{2}}}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{9}{2}}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{9}{2}}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{2}{9}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{\boxed{1 + \cfrac{2}{9}}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{\cfrac{11}{9}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{1}{\cfrac{11}{9}}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{9}{11}}$$

Continued Fractions

$$3 + \cfrac{1}{3 + \cfrac{9}{11}}$$

Continued Fractions

$$3 + \cfrac{1}{\cfrac{42}{11}}$$

Continued Fractions

$$3 + \cfrac{1}{\cfrac{42}{11}}$$

Continued Fractions

$$3 + \frac{11}{42}$$

Continued Fractions

$$3 + \frac{11}{42}$$

Continued Fractions

$$\frac{137}{42}$$

Continued Fractions

- A **continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\dots}}}}$$

- More formally, a continued fraction is either
  - An integer *n*, or
  - *n* + 1 / *F*, where *n* is an integer and *F* is a continued fraction.
- Continued fractions have numerous applications in number theory and computer science.
- (They're also really fun to write!)

Fun with Continued Fractions

- Every rational number (including negative numbers) has a continued fraction.
- Harder result: every *irrational* number has an (infinite) continued fraction.
- If we truncate an infinite continued fraction for an irrational number, we can get progressively better approximations of that number.

Pi as a Continued Fraction

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\cdots}}}}}}}}}}$$

Approximating Pi

Approximating Pi

$\pi = 3$

3 = **3**.0000...

Approximating Pi

$\pi = 3$

3 = **3**.0000...

And he made the Sea of cast bronze, ten cubits from one brim to the other; it was completely round. [... A] line of thirty cubits measured its circumference.

1 Kings 7:23, New King James Translation

Approximating Pi

$$\pi = 3 + \frac{1}{7}$$

3 = **3**.0000...

22/7 = **3.14**2857...

Approximating Pi

$$\pi = 3 + \cfrac{1}{7}$$

3 = **3**.0000...

22/7 = **3.14**2857...

Archimedes knew of this approximation, circa 250 BCE

Approximating Pi

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15}}$$

3 = **3**.0000...

22/7 = **3.14**2857...

336/106 = **3.1415**094...

Approximating Pi

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}}$$

3 = **3**.0000...

22/7 = **3.14**2857...

336/106 = **3.1415**094...

355/113 = **3.1415929**2...

Approximating Pi

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}}$$

3 = **3**.0000...

22/7 = **3.14**2857...

336/106 = **3.1415**094...

355/113 = **3.1415929**2...

Chinese mathematician Zu Chongzhi discovered this approximation in the early fifth century; this was the best approximation of pi for over a thousand years

Approximating Pi

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292}}}}$$

3 = **3**.0000...

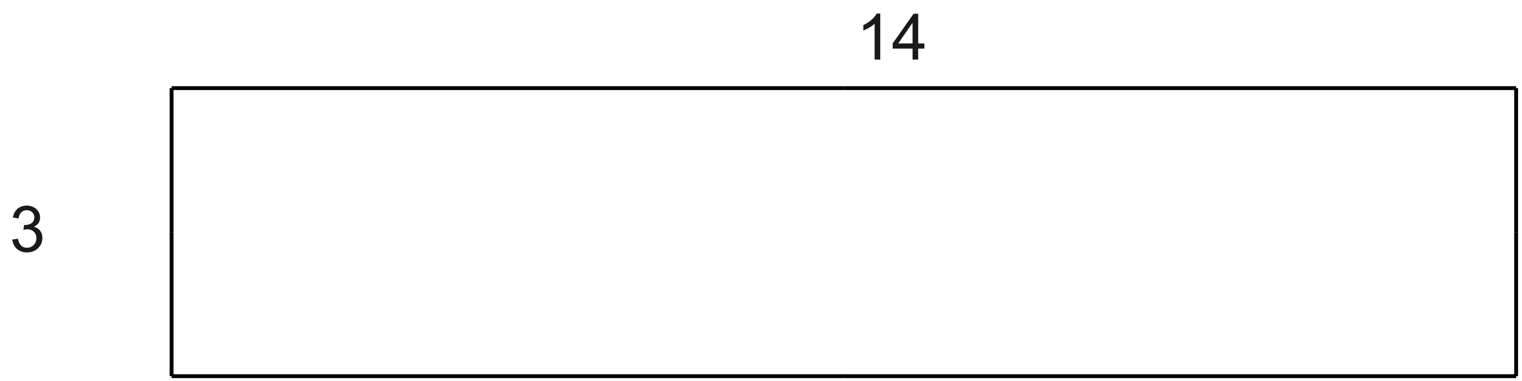
22/7 = **3.14**2857...

336/106 = **3.1415**094...

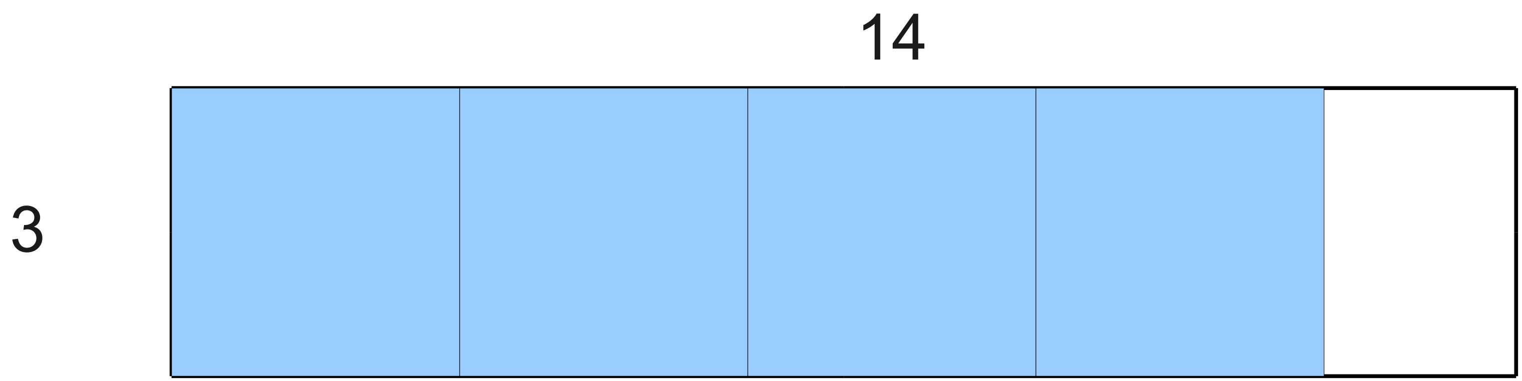
355/113 = **3.1415929**2...

103993/33102 = **3.141592653**0...

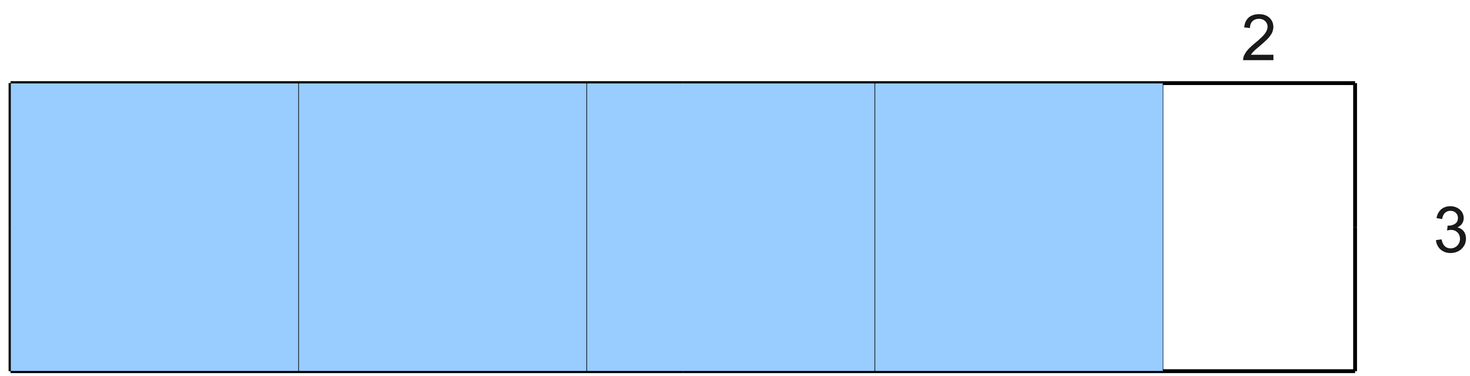
More Continued Fractions



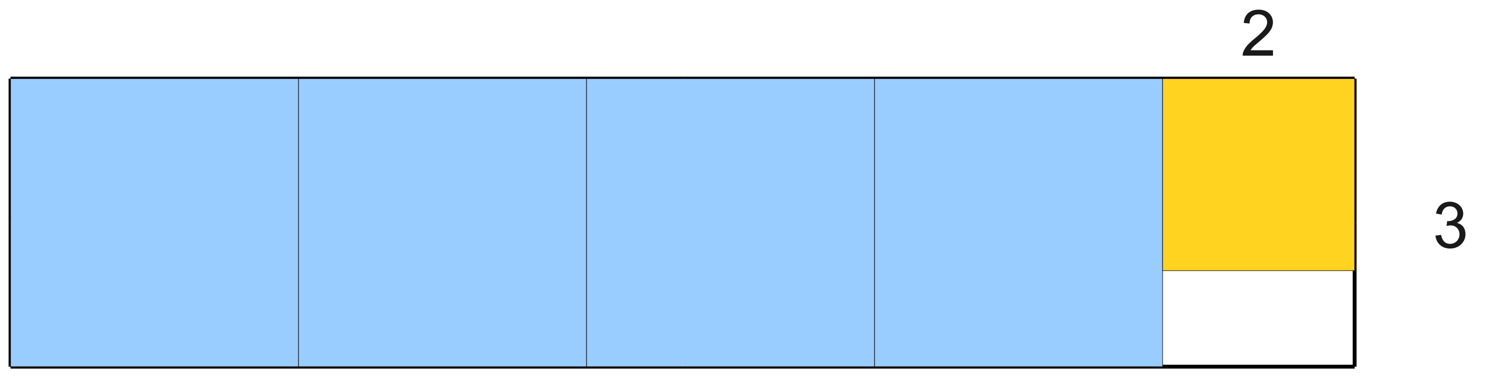
More Continued Fractions



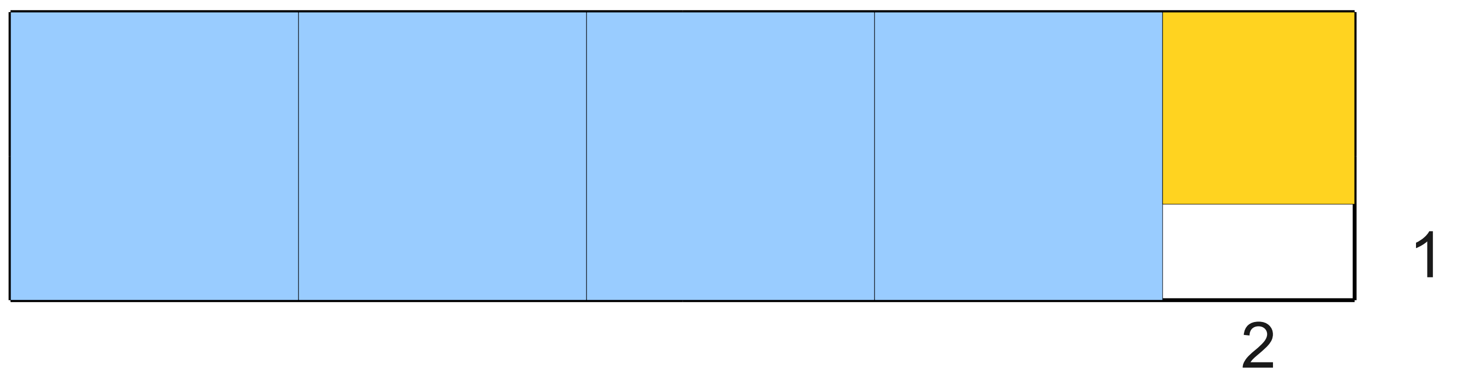
More Continued Fractions



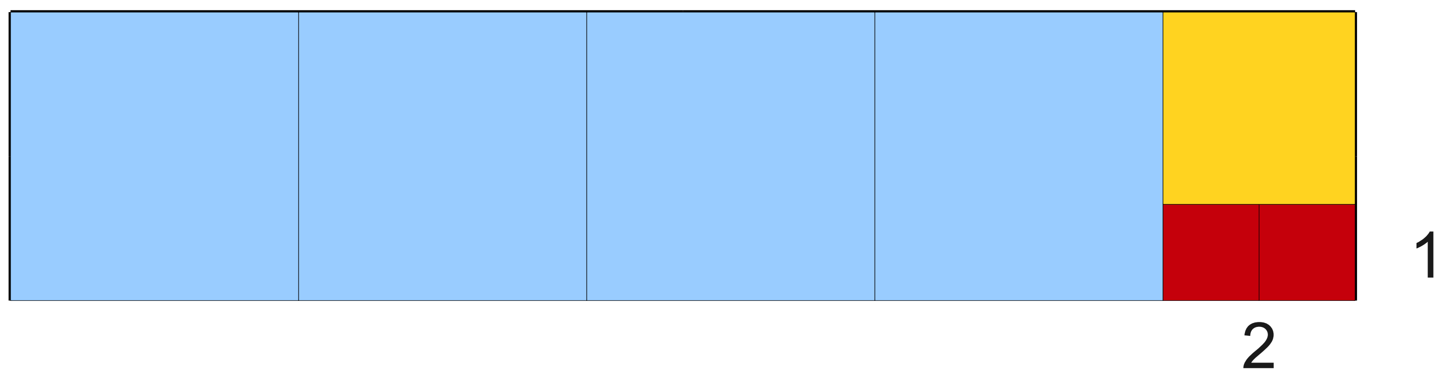
More Continued Fractions



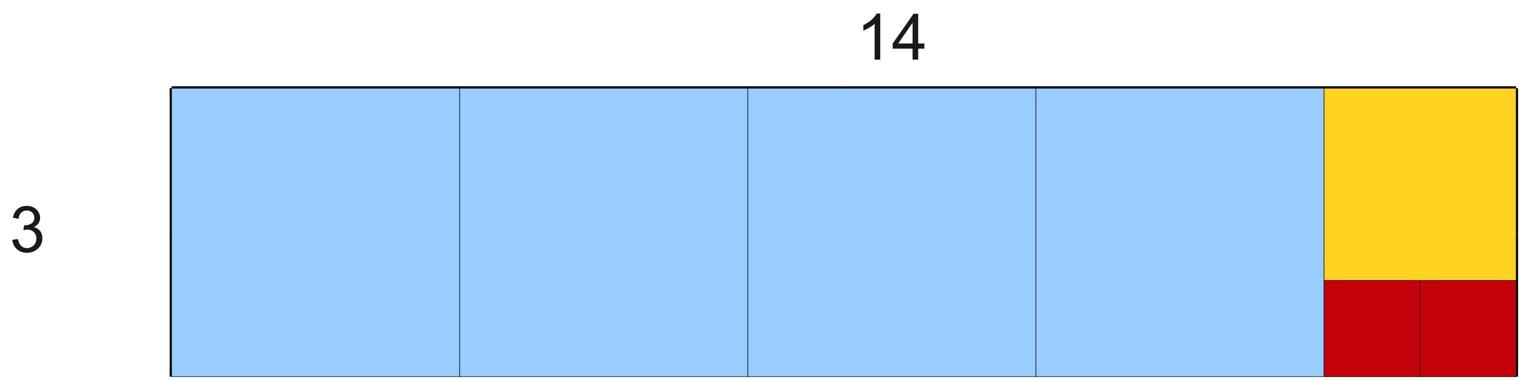
More Continued Fractions



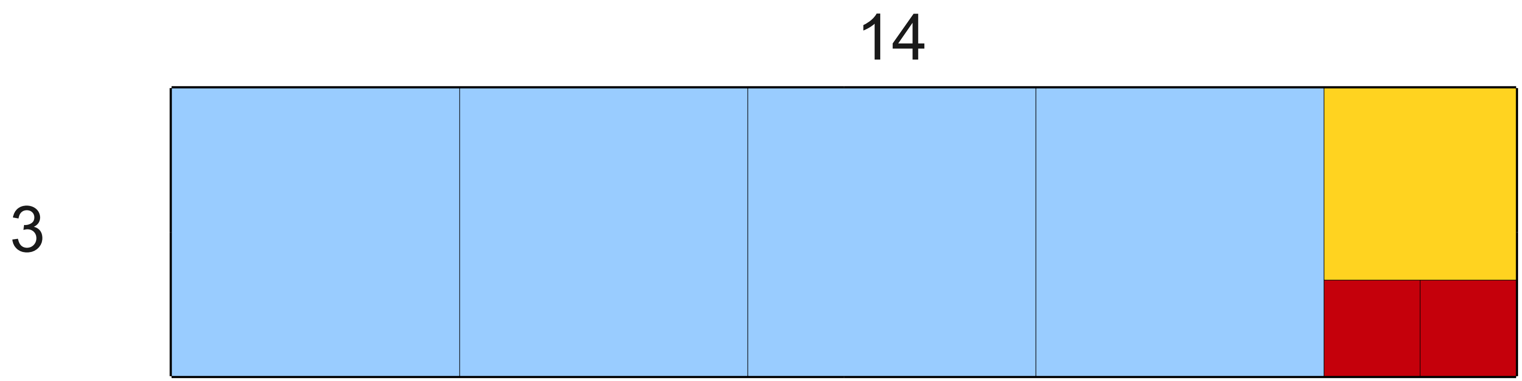
More Continued Fractions



More Continued Fractions

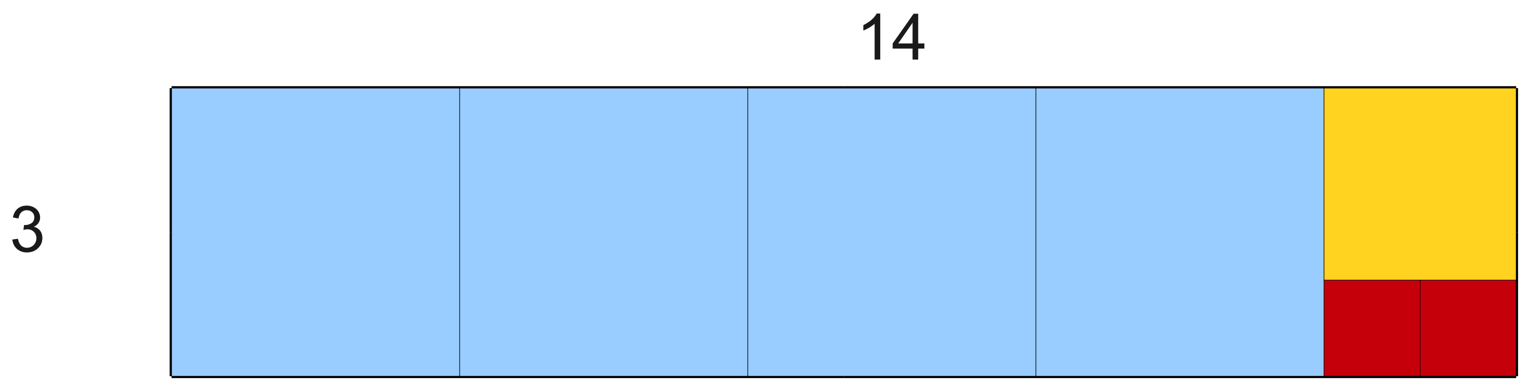


More Continued Fractions



$$\frac{3}{14} = \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

More Continued Fractions



$$\frac{3}{14} = \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}}}}}}}}$$

An Interesting Continued Fraction

$x = 1$

1 / 1

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 \cdot}$$

1 / 1

2 / 1

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1}}$$

1 / 1

2 / 1

3 / 2

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}$$

1 / 1

2 / 1

3 / 2

5 / 3

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}$$

1 / 1

2 / 1

3 / 2

5 / 3

8 / 5

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}$$

1 / 1

2 / 1

3 / 2

5 / 3

8 / 5

13 / 8

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}$$

1 / 1

2 / 1

3 / 2

5 / 3

8 / 5

13 / 8

21 / 13

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}}$$

1 / 1

2 / 1

3 / 2

5 / 3

8 / 5

13 / 8

21 / 13

34 / 21

An Interesting Continued Fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}}}$$

1 / 1

2 / 1

3 / 2

5 / 3

8 / 5

13 / 8

21 / 13

34 / 21

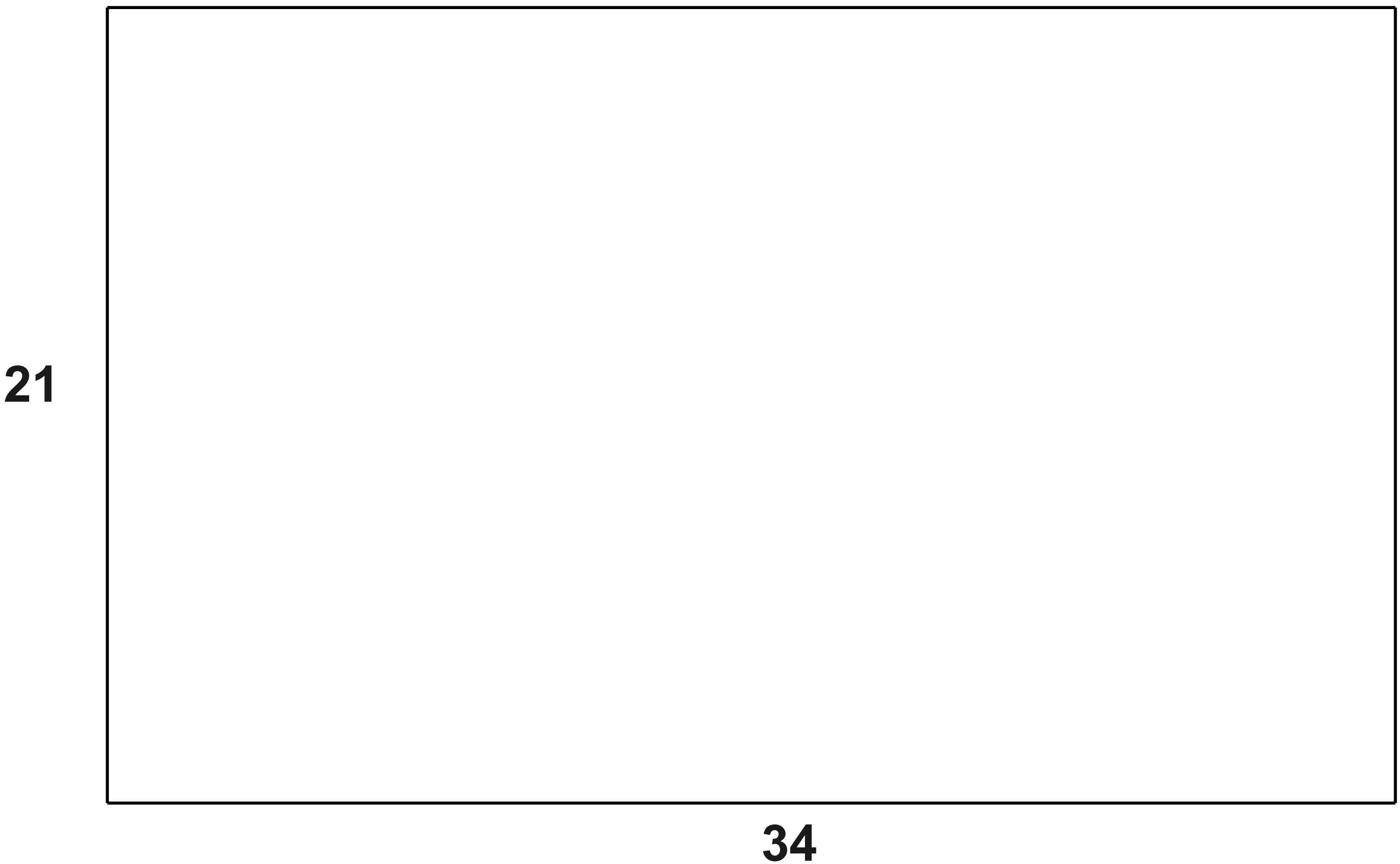
Each fraction is the ratio of consecutive Fibonacci numbers!

The Golden Ratio

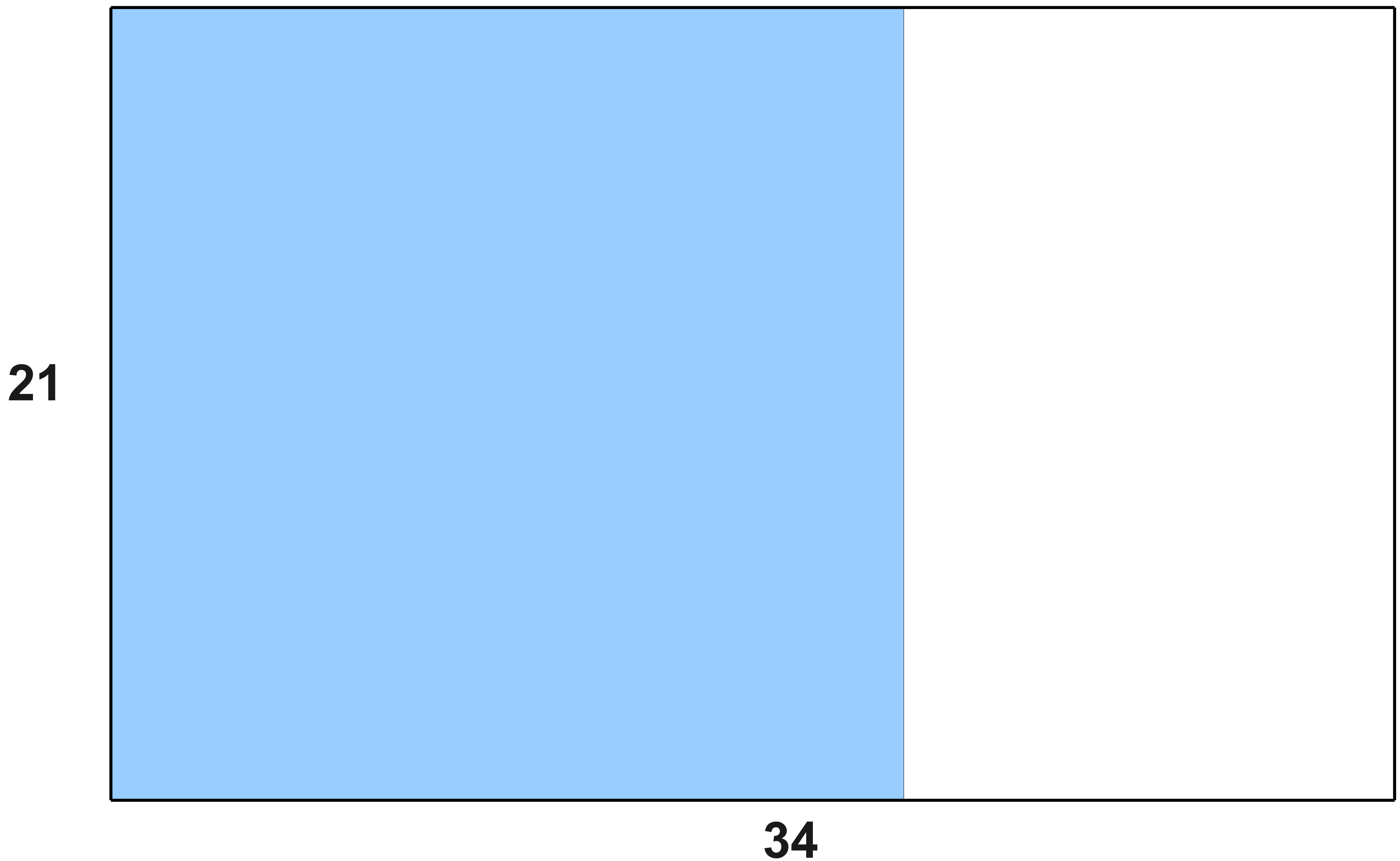
$$\phi = \frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}}$$

$$\phi \approx 1.61803399$$

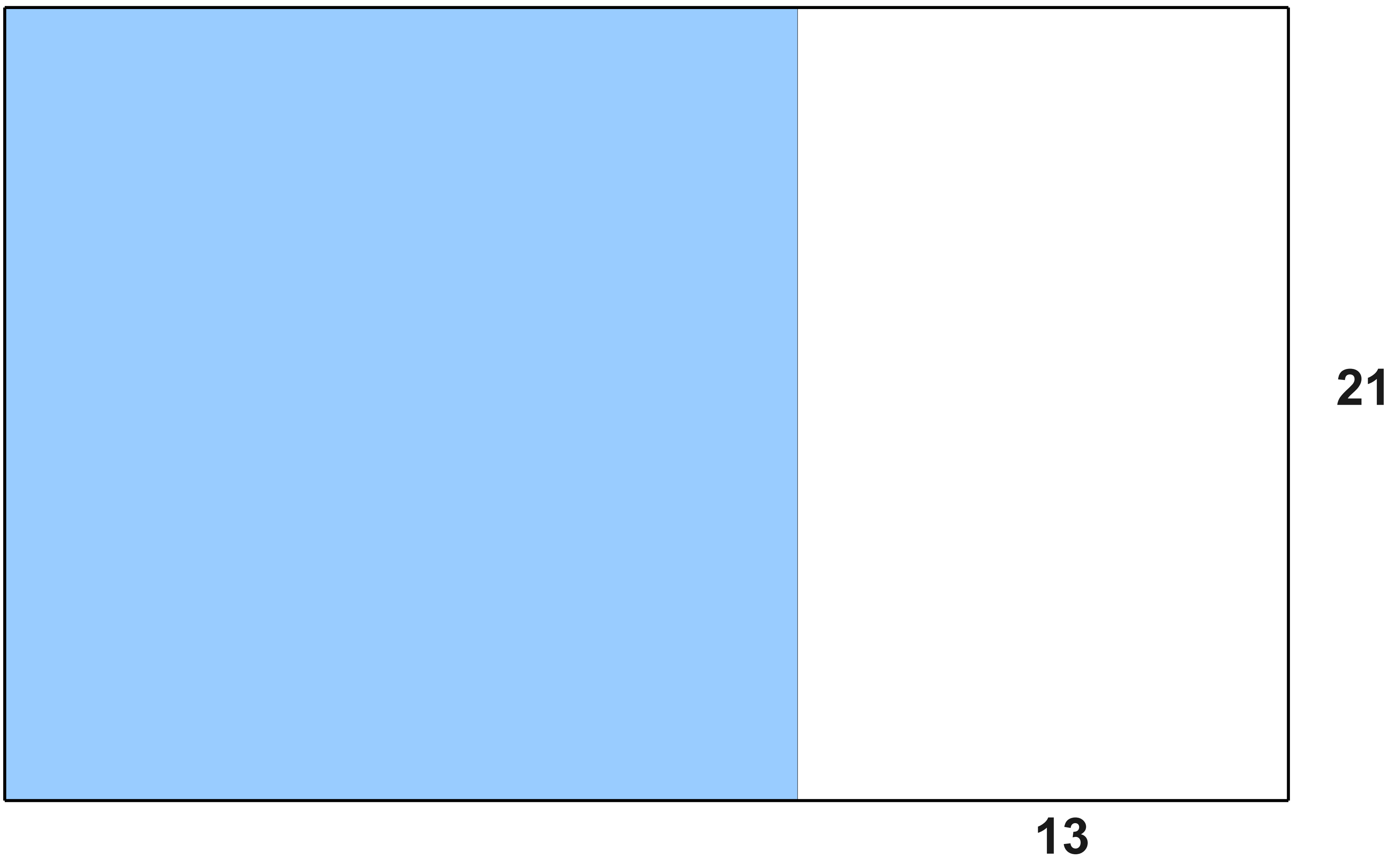
The Golden Ratio



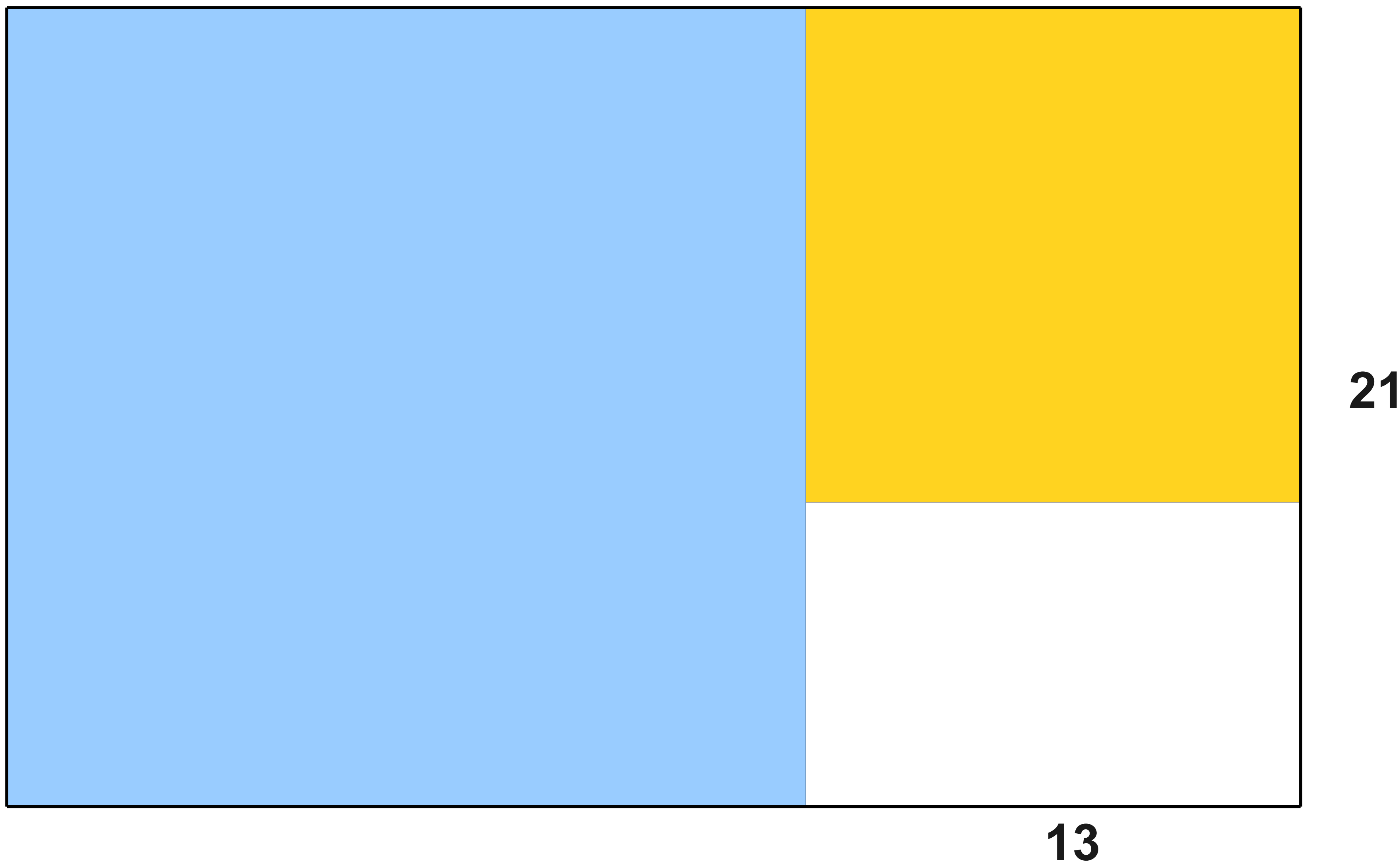
The Golden Ratio



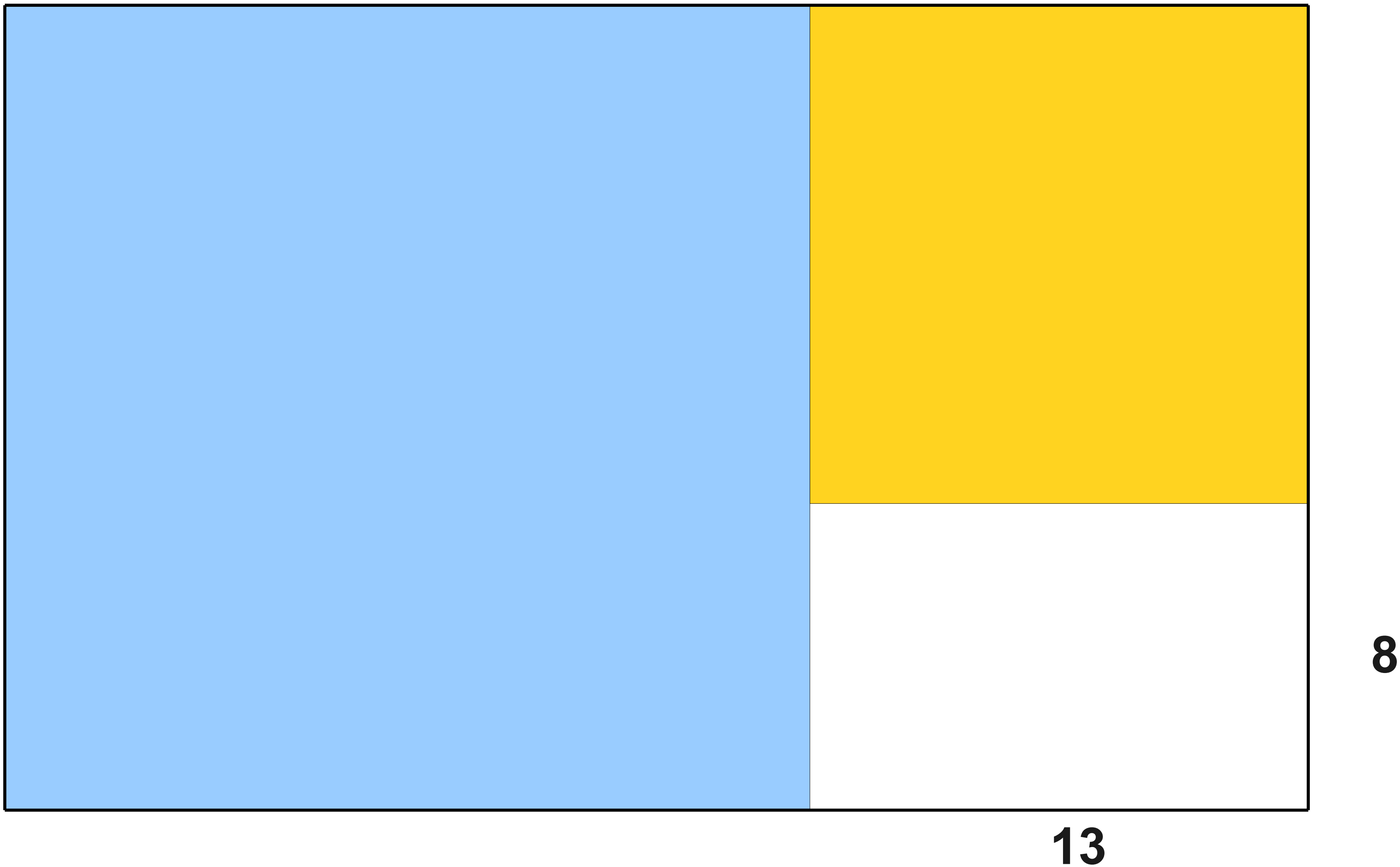
The Golden Ratio



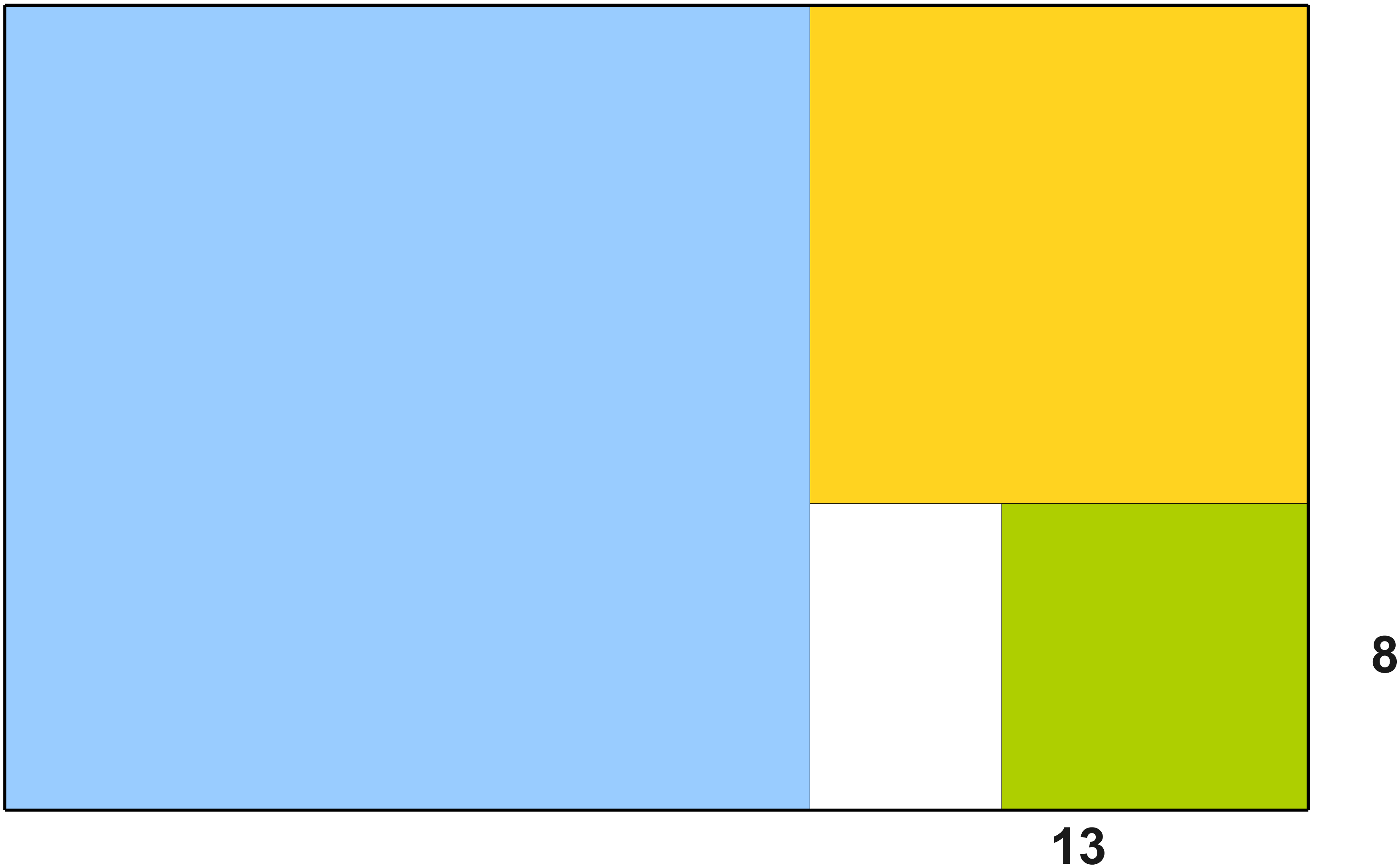
The Golden Ratio



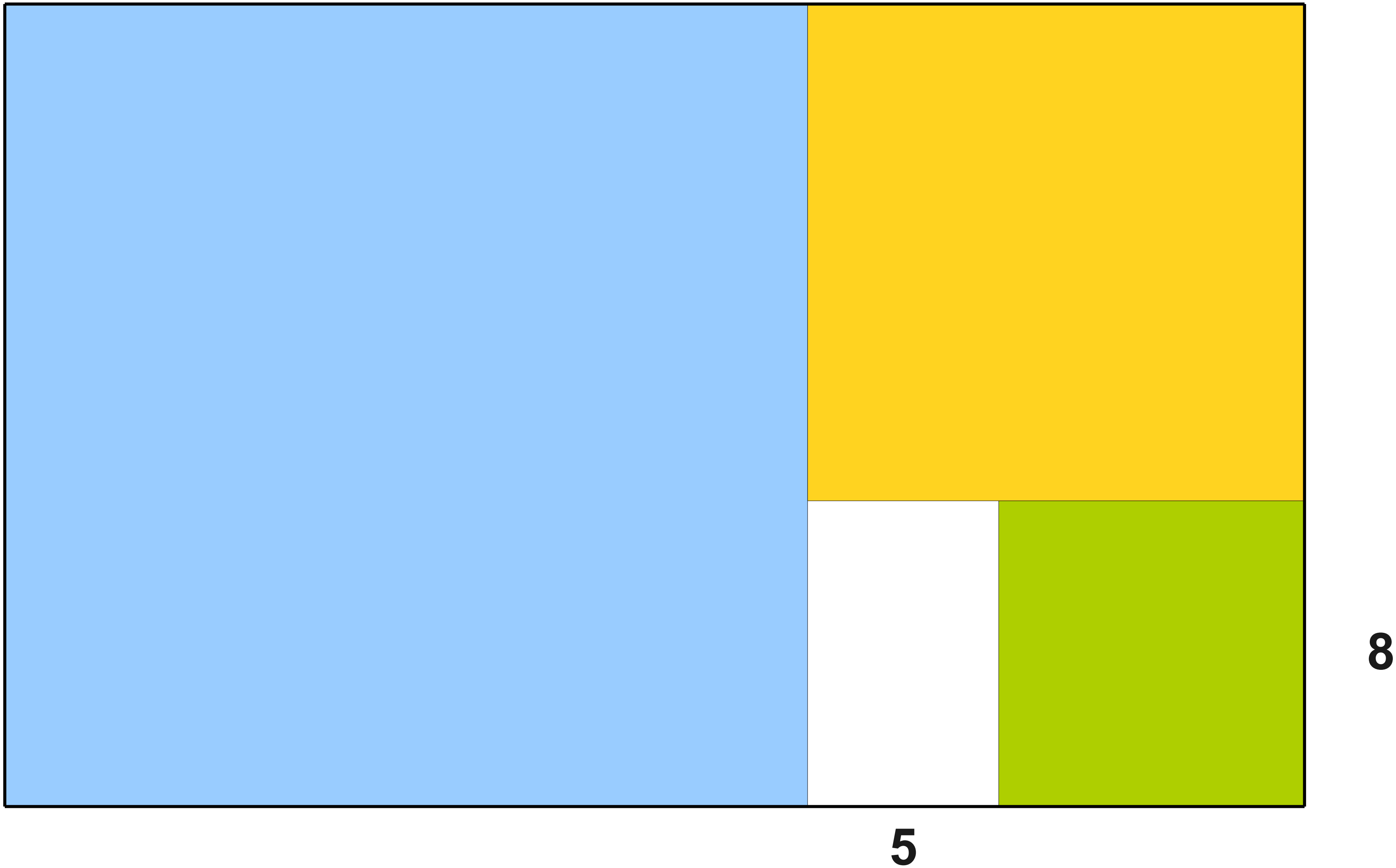
The Golden Ratio



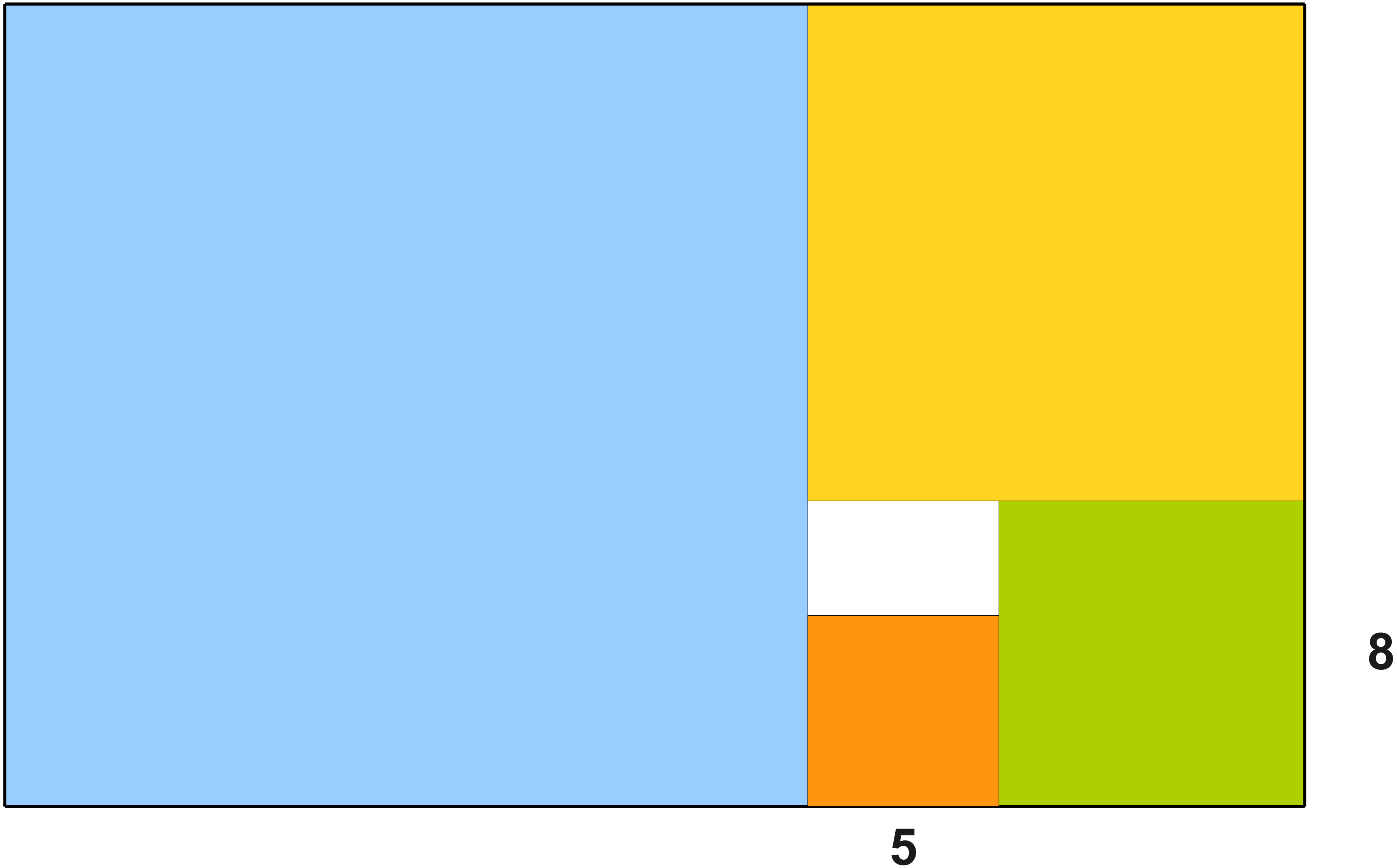
The Golden Ratio



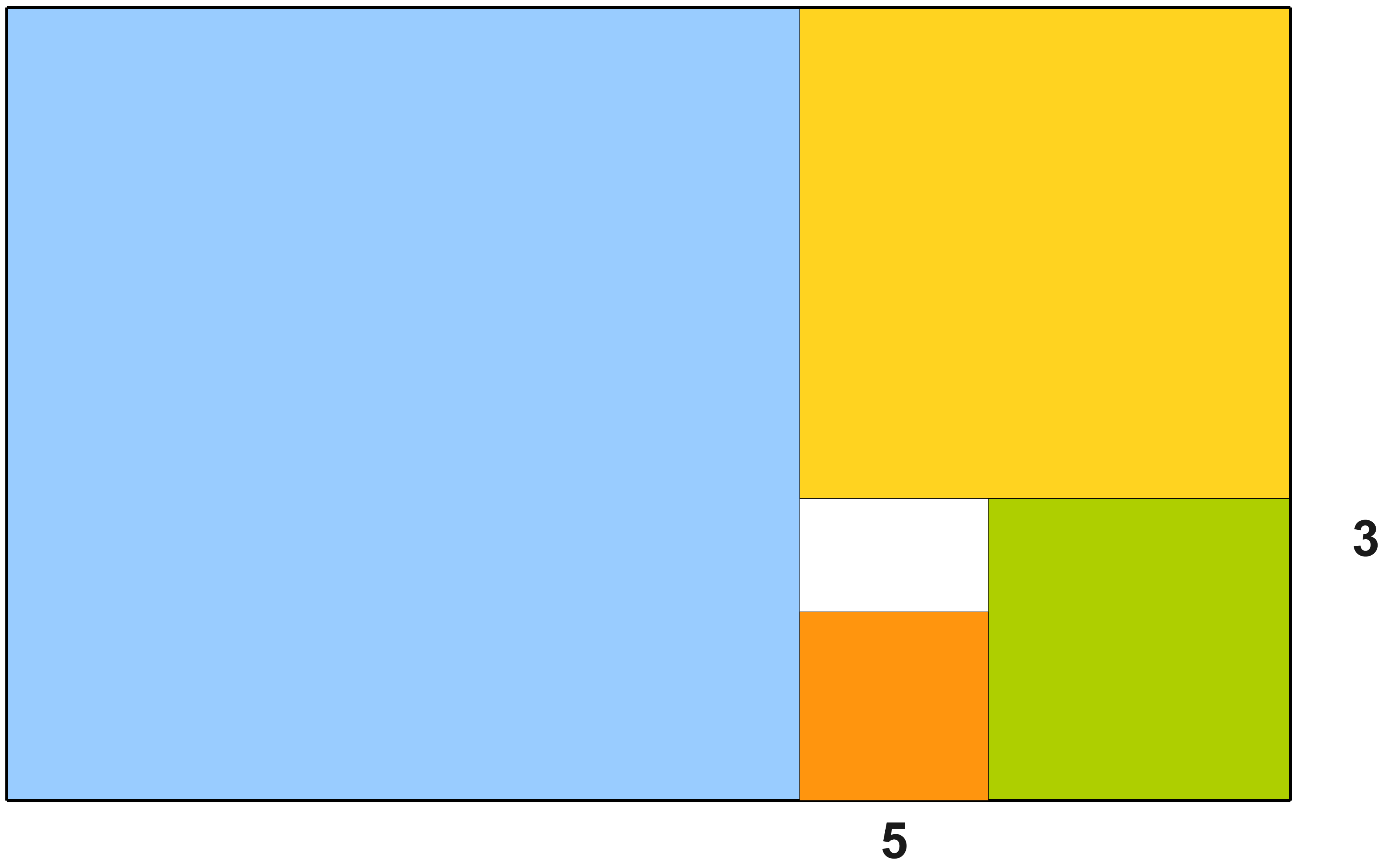
The Golden Ratio



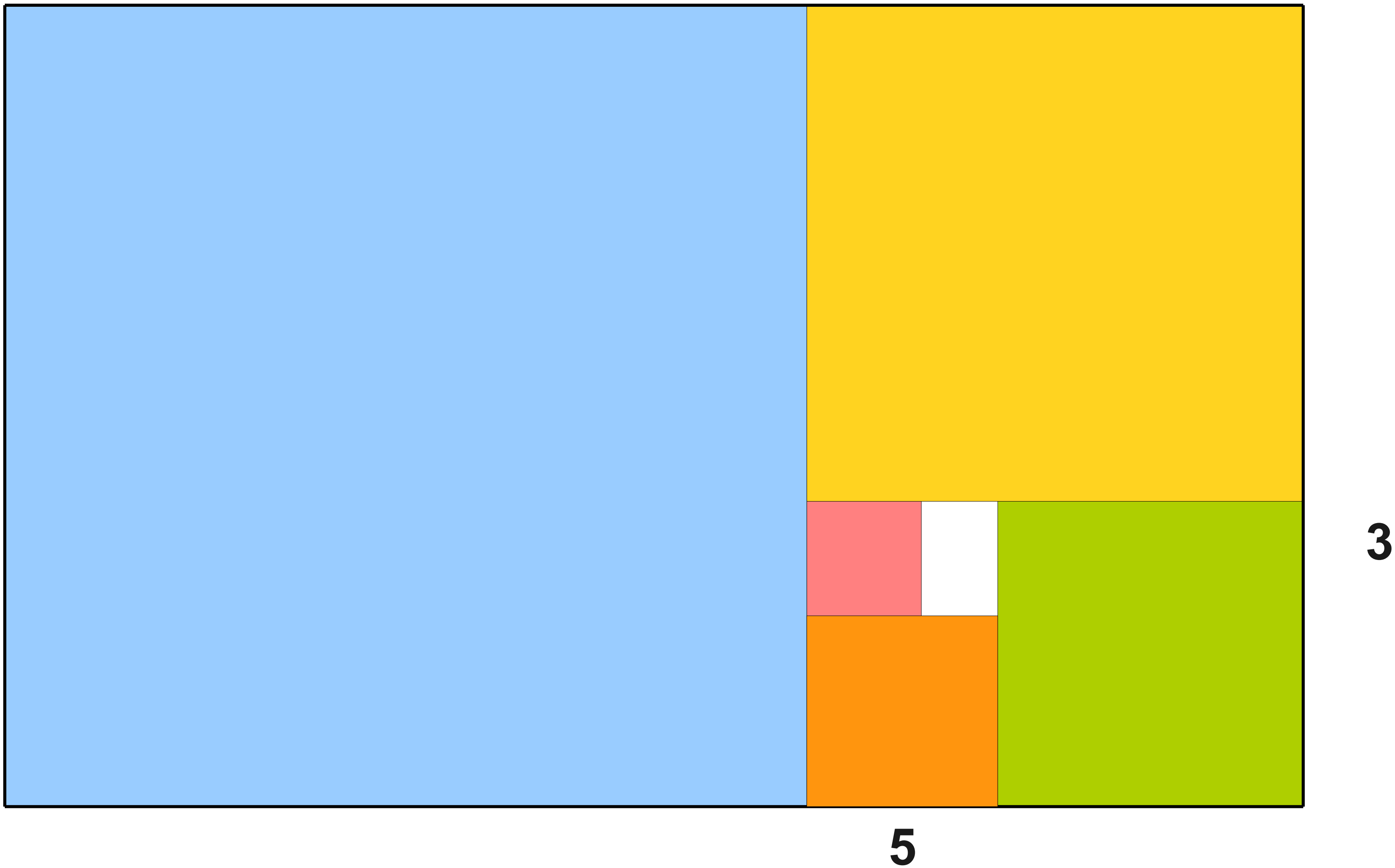
The Golden Ratio



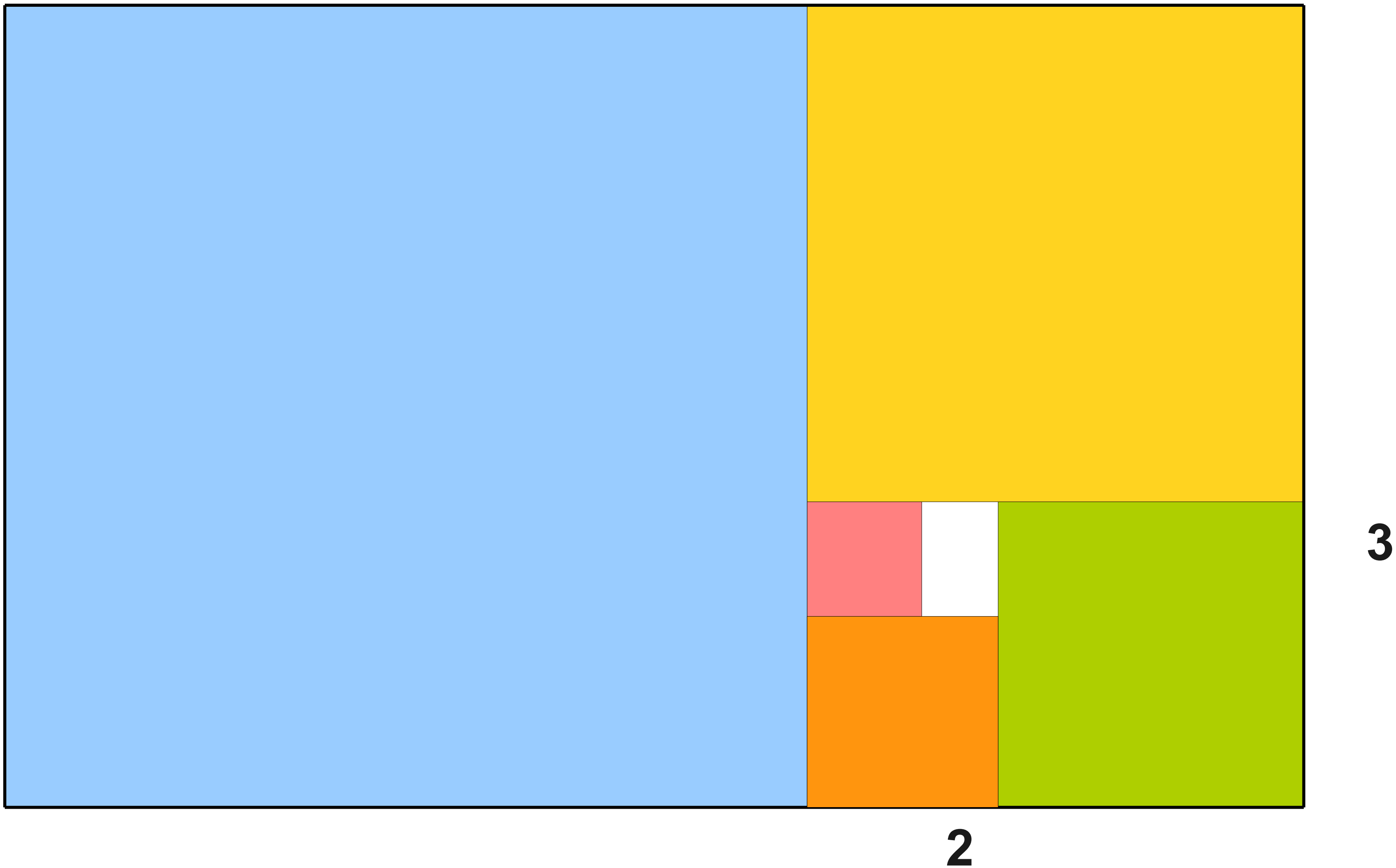
The Golden Ratio



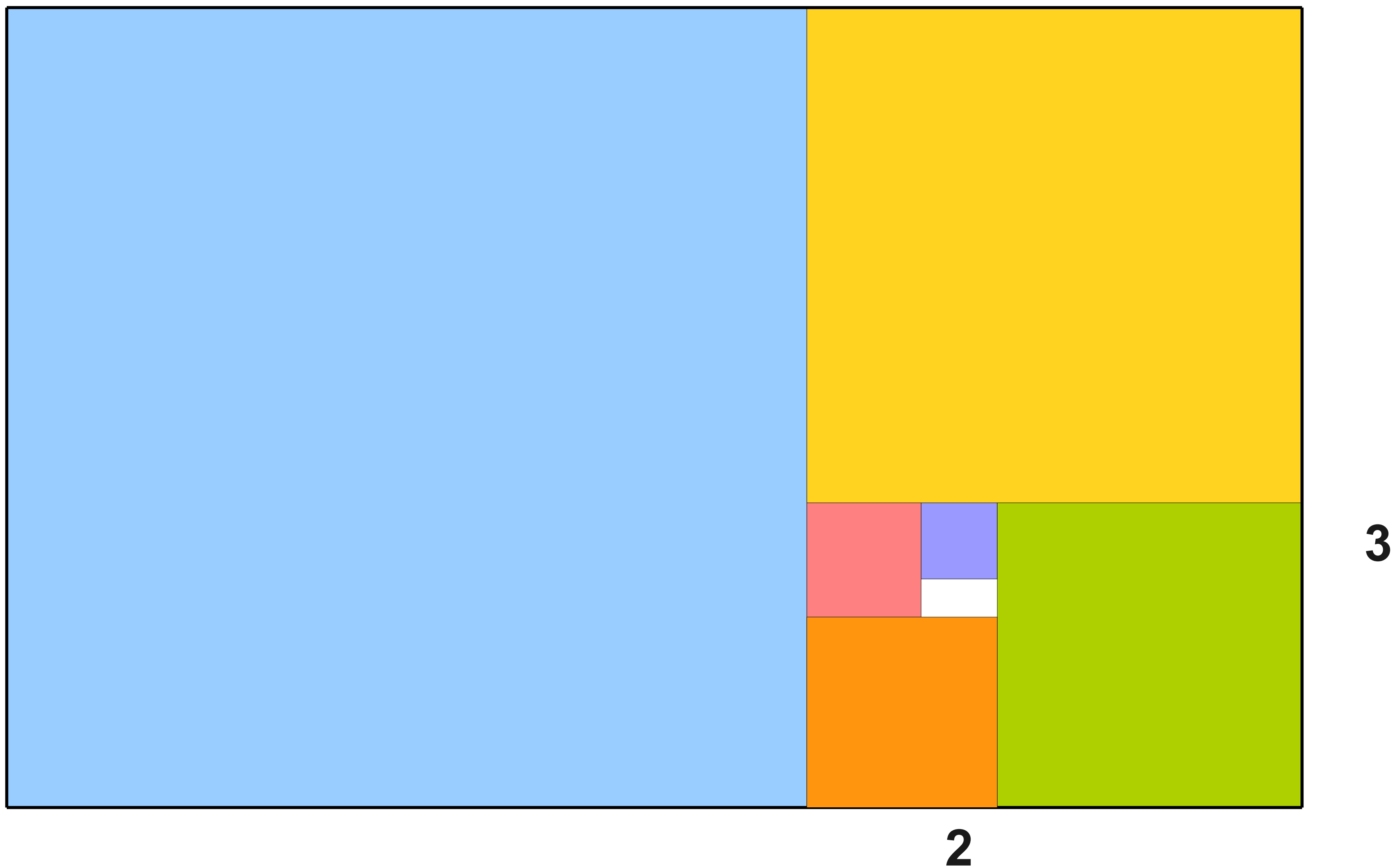
The Golden Ratio



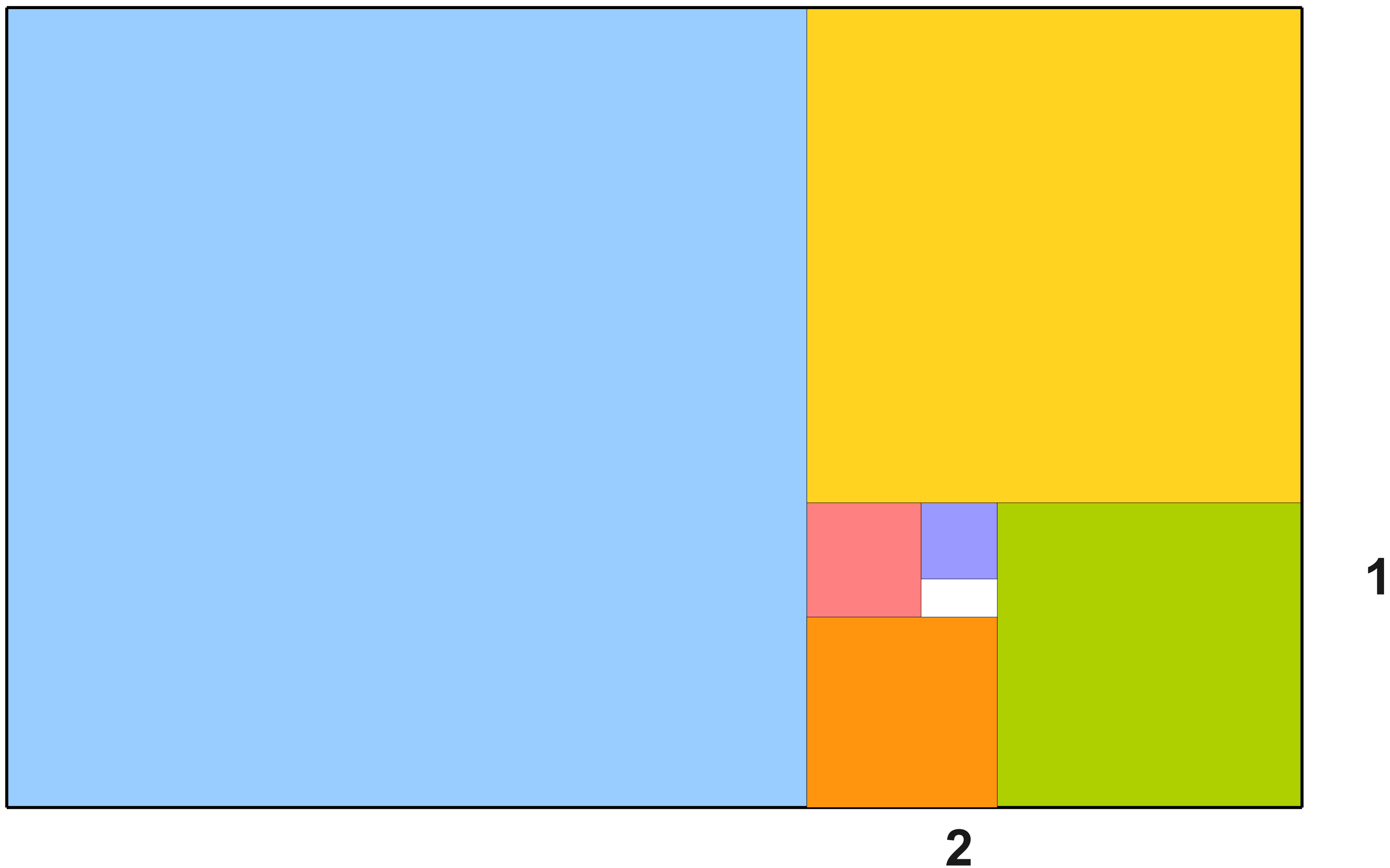
The Golden Ratio



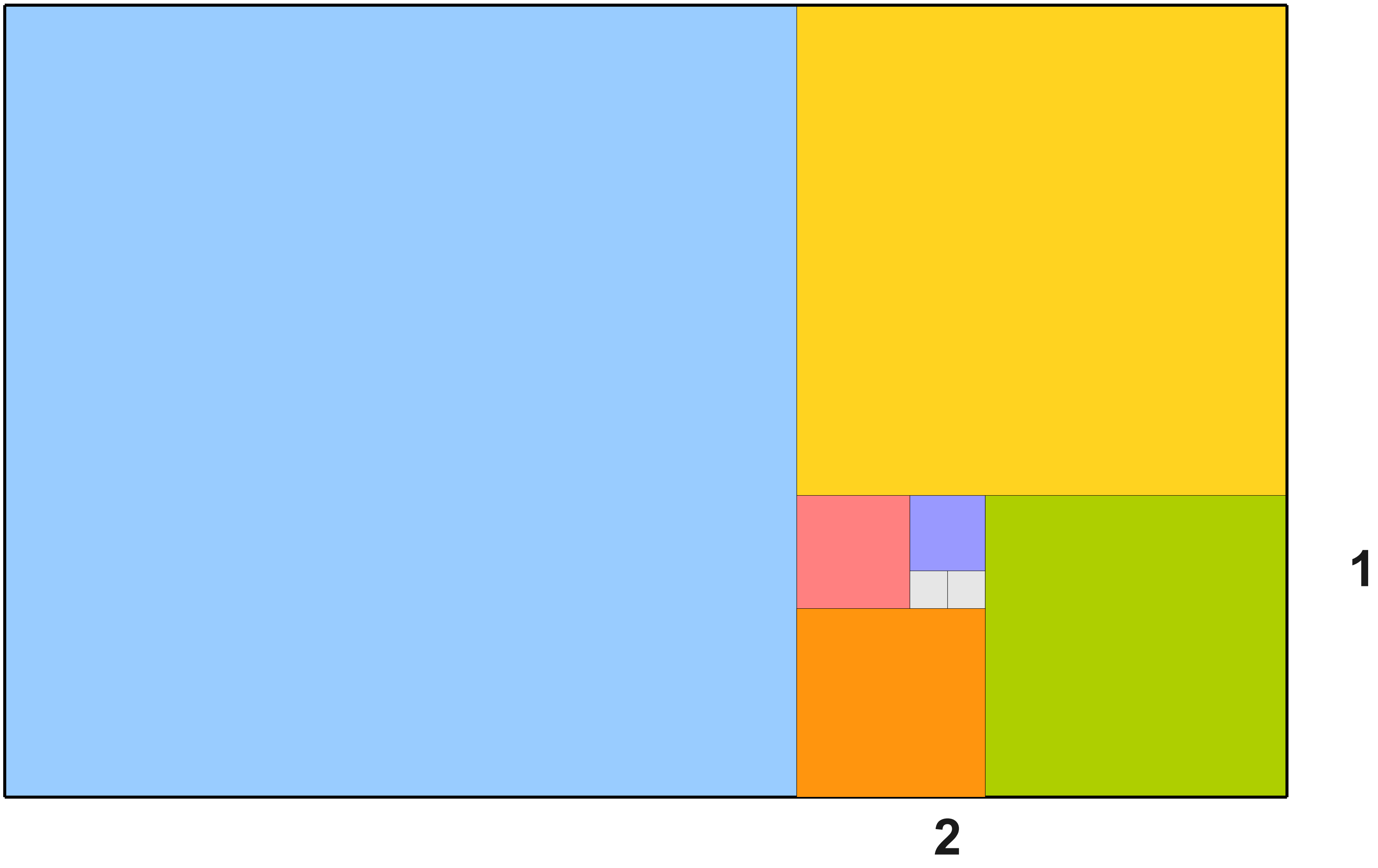
The Golden Ratio



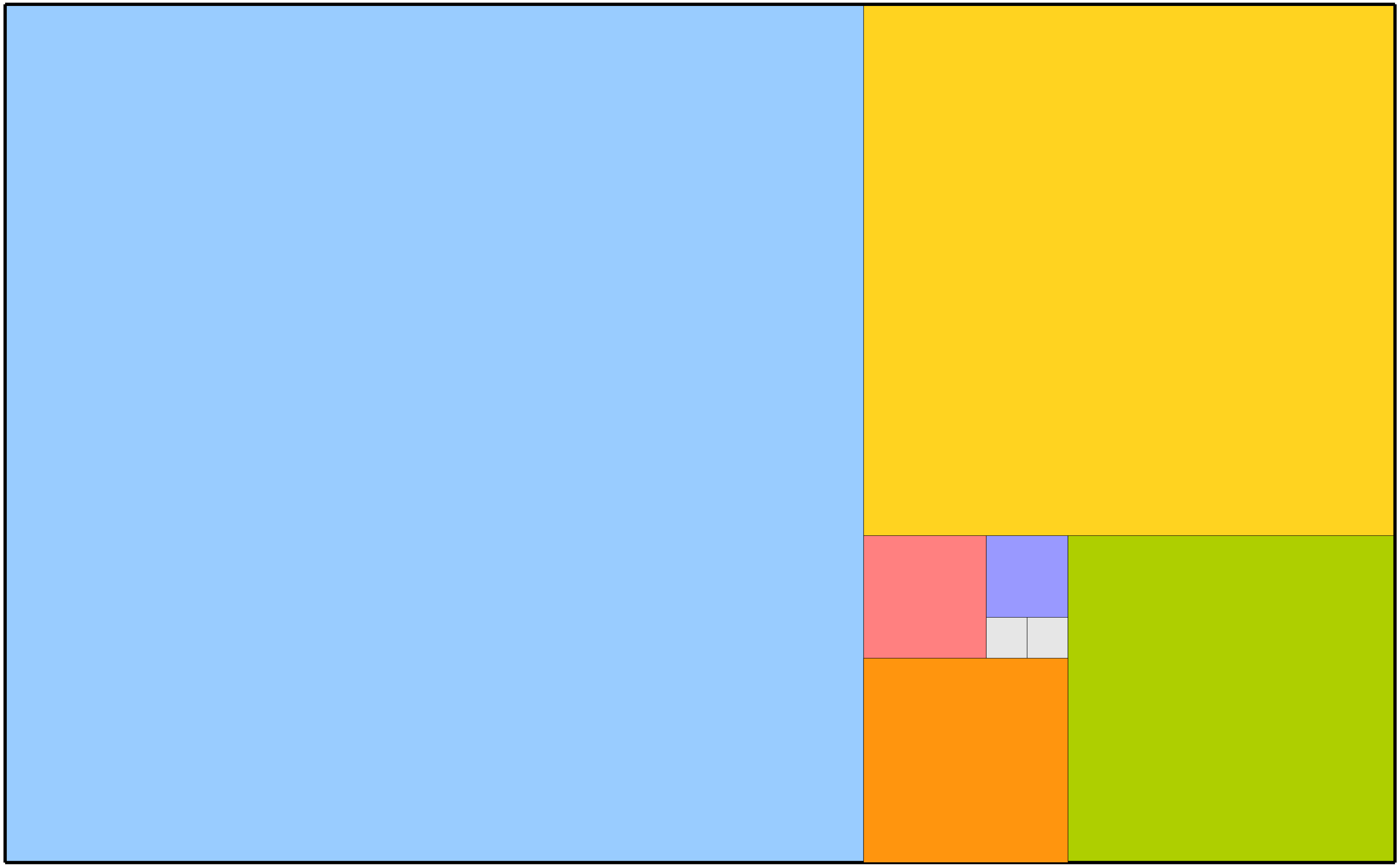
The Golden Ratio



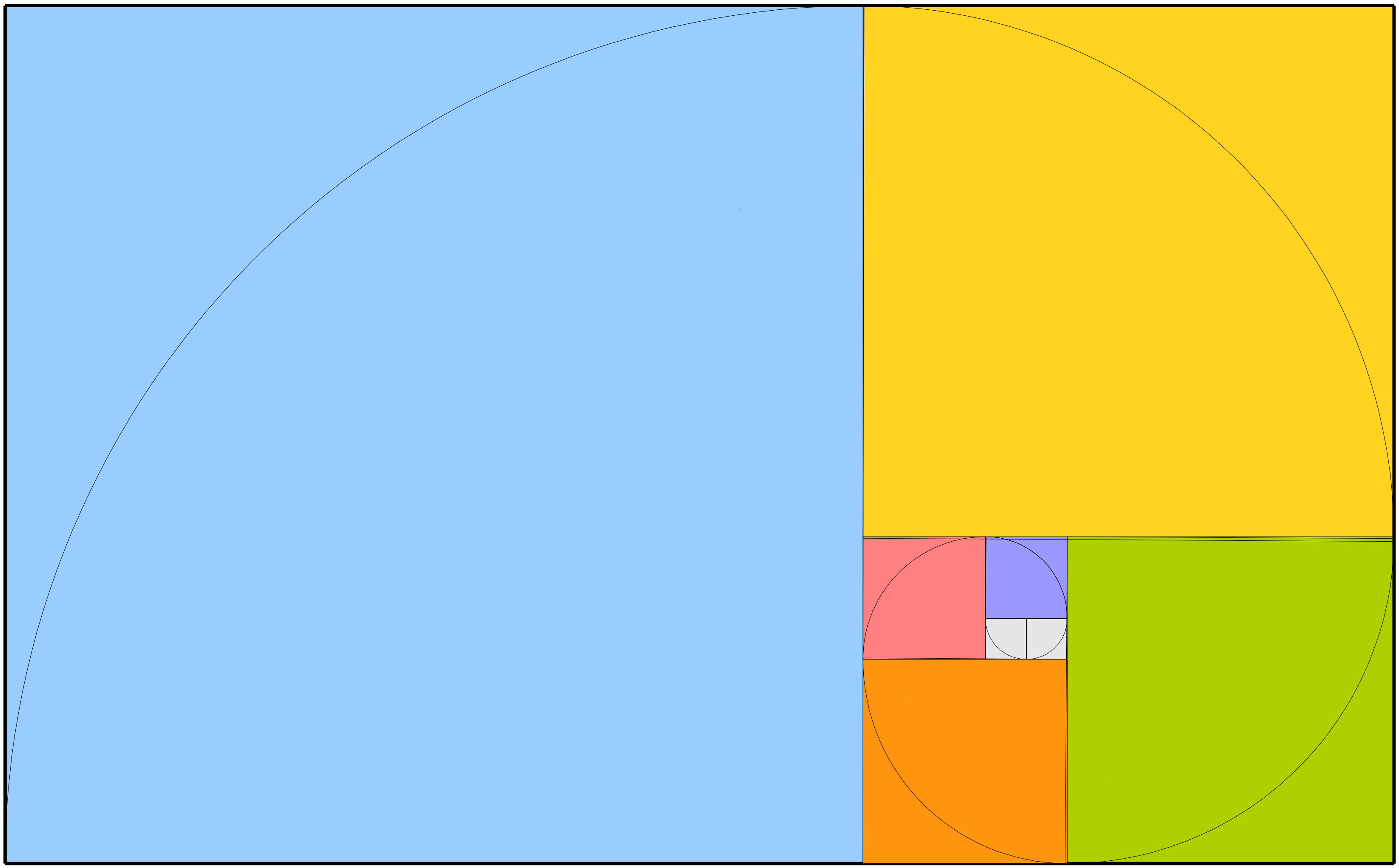
The Golden Ratio



The Golden Ratio



The Golden Spiral



How do we prove all rational numbers have continued fractions?

Constructing a Continued Fraction

$$\frac{25}{9}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \frac{7}{9}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

$$\frac{9}{7}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

$$\frac{9}{7} = 1 + \frac{2}{7}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

$$\frac{9}{7} = 1 + \cfrac{1}{\cfrac{7}{2}}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \frac{1}{\frac{9}{7}}$$

$$\frac{9}{7} = 1 + \frac{1}{\frac{7}{2}}$$

$$\frac{7}{2}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

$$\frac{9}{7} = 1 + \cfrac{1}{\cfrac{7}{2}}$$

$$\frac{7}{2} = 3 + \frac{1}{2}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

$$\frac{9}{7} = 1 + \cfrac{1}{\boxed{\cfrac{7}{2}}}$$

$$\boxed{\frac{7}{2} = 3 + \frac{1}{2}}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{\cfrac{9}{7}}$$

$$\frac{9}{7} = 1 + \cfrac{1}{3 + \cfrac{1}{2}}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \frac{1}{\boxed{\frac{9}{7}}}$$

$$\boxed{\frac{9}{7} = 1 + \frac{1}{3 + \frac{1}{2}}}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

Constructing a Continued Fraction

$$\frac{25}{9} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

$$\frac{9}{7}$$

$$\frac{7}{2}$$

$$\frac{2}{1}$$

Constructing a Continued Fraction

$$\frac{25}{\mathbf{9}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

$$\frac{9}{\mathbf{7}}$$

$$\frac{7}{\mathbf{2}}$$

$$\frac{2}{\mathbf{1}}$$

Constructing a Continued Fraction

$$\frac{25}{\color{red}{\mathbf{9}}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

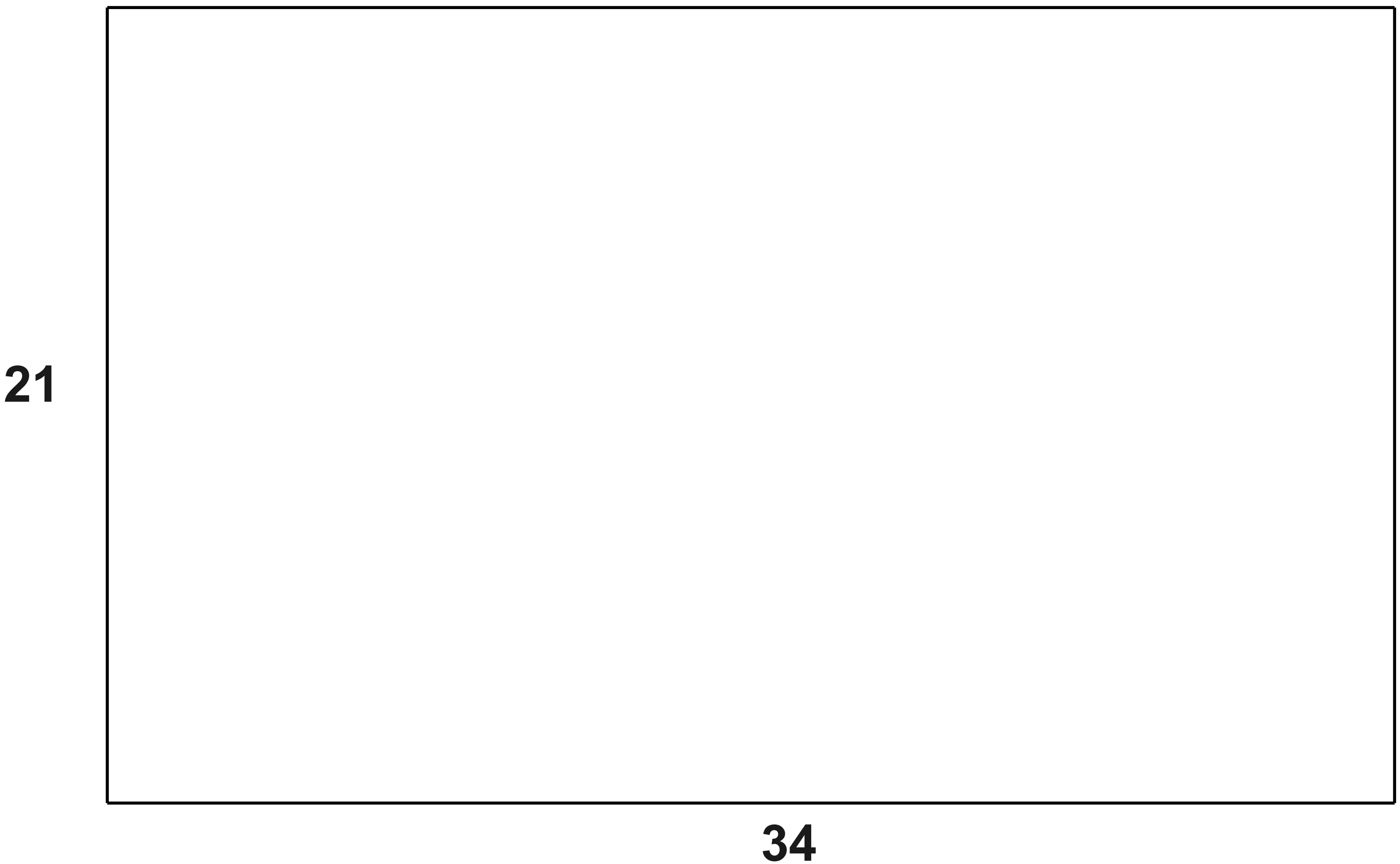
$$\frac{9}{\color{red}{\mathbf{7}}}$$

$$\frac{7}{\color{red}{\mathbf{2}}}$$

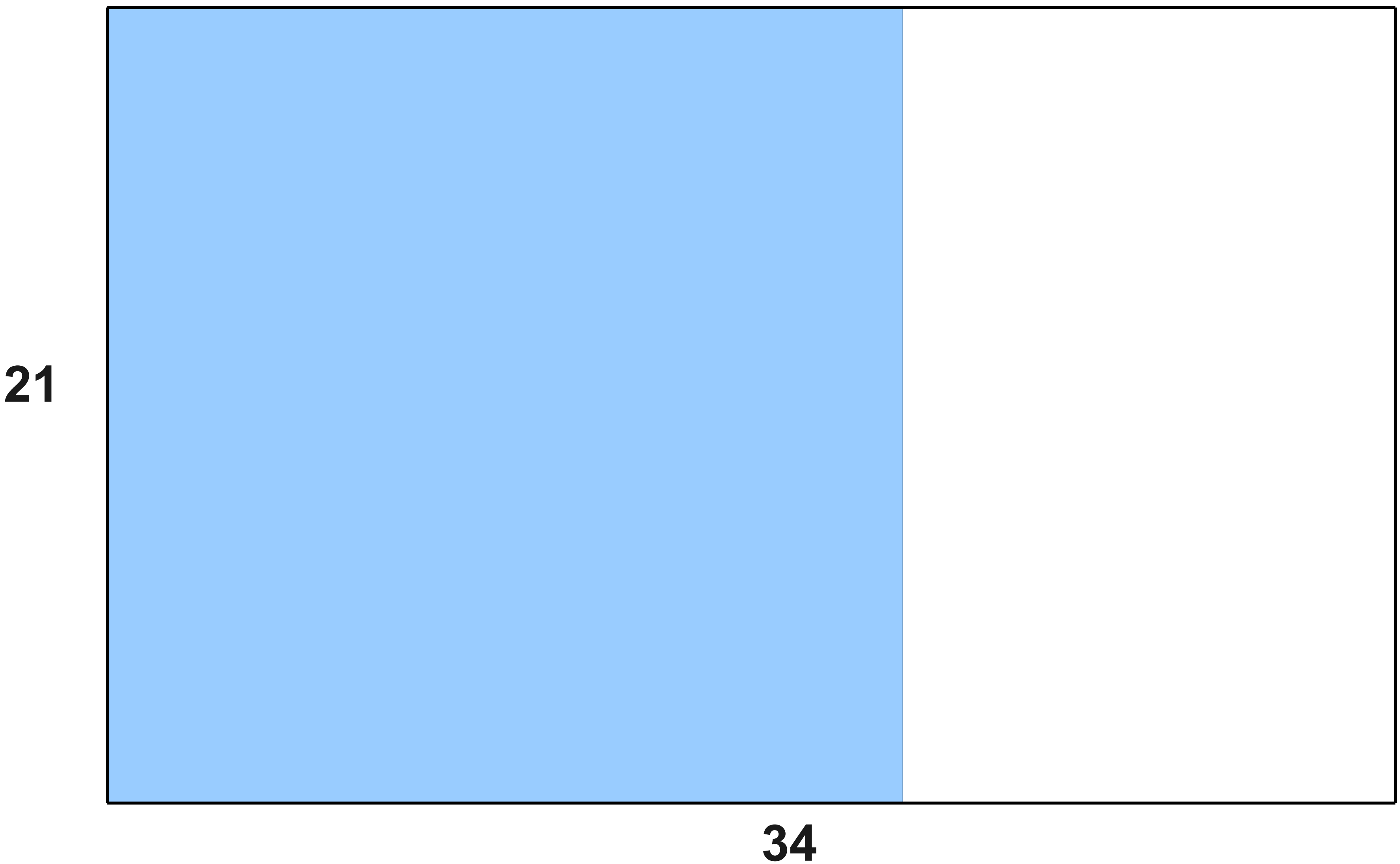
$$\frac{2}{\color{red}{\mathbf{1}}}$$

$$\color{red}{\mathbf{9 > 7 > 2 > 1}}$$

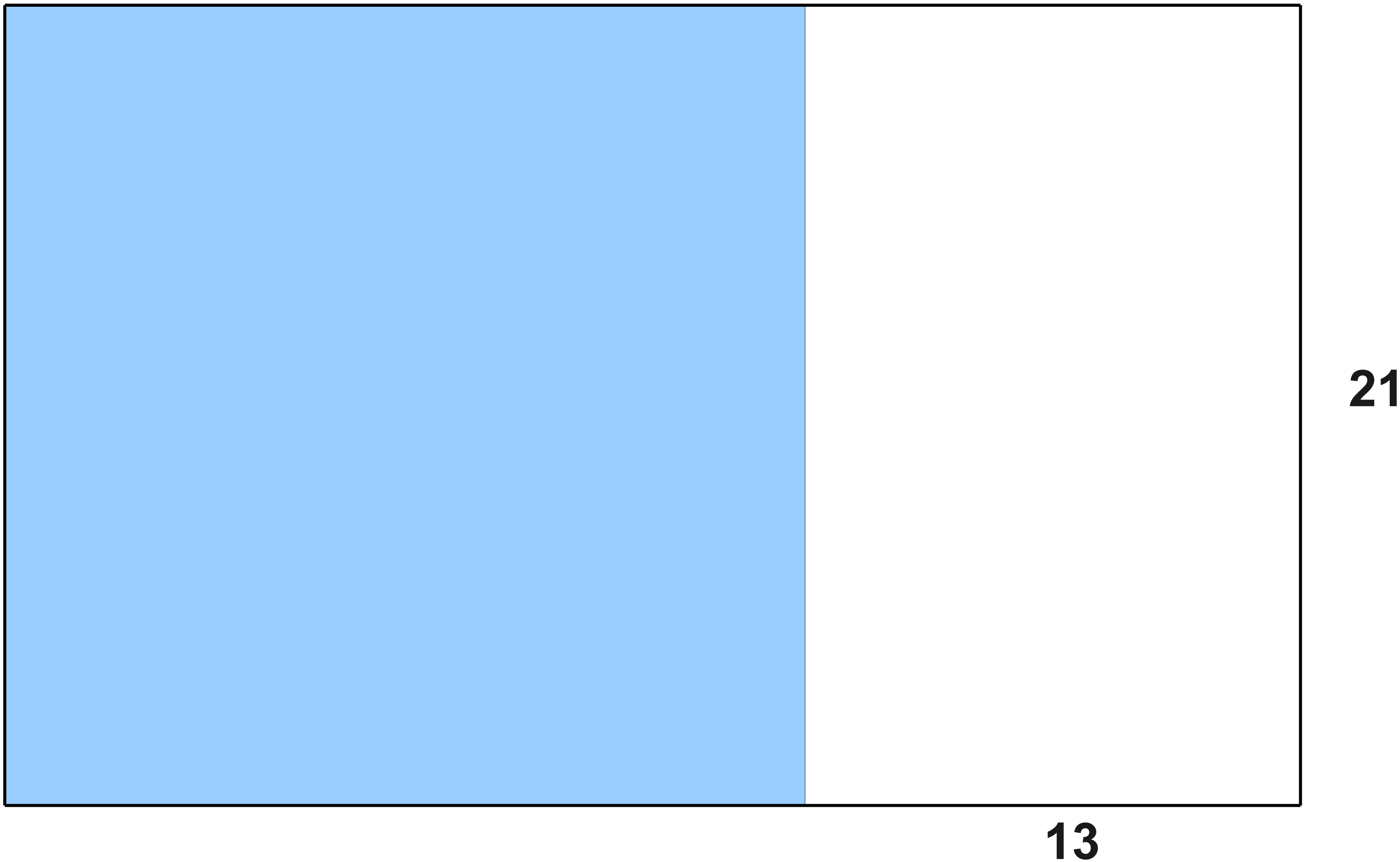
The Golden Ratio



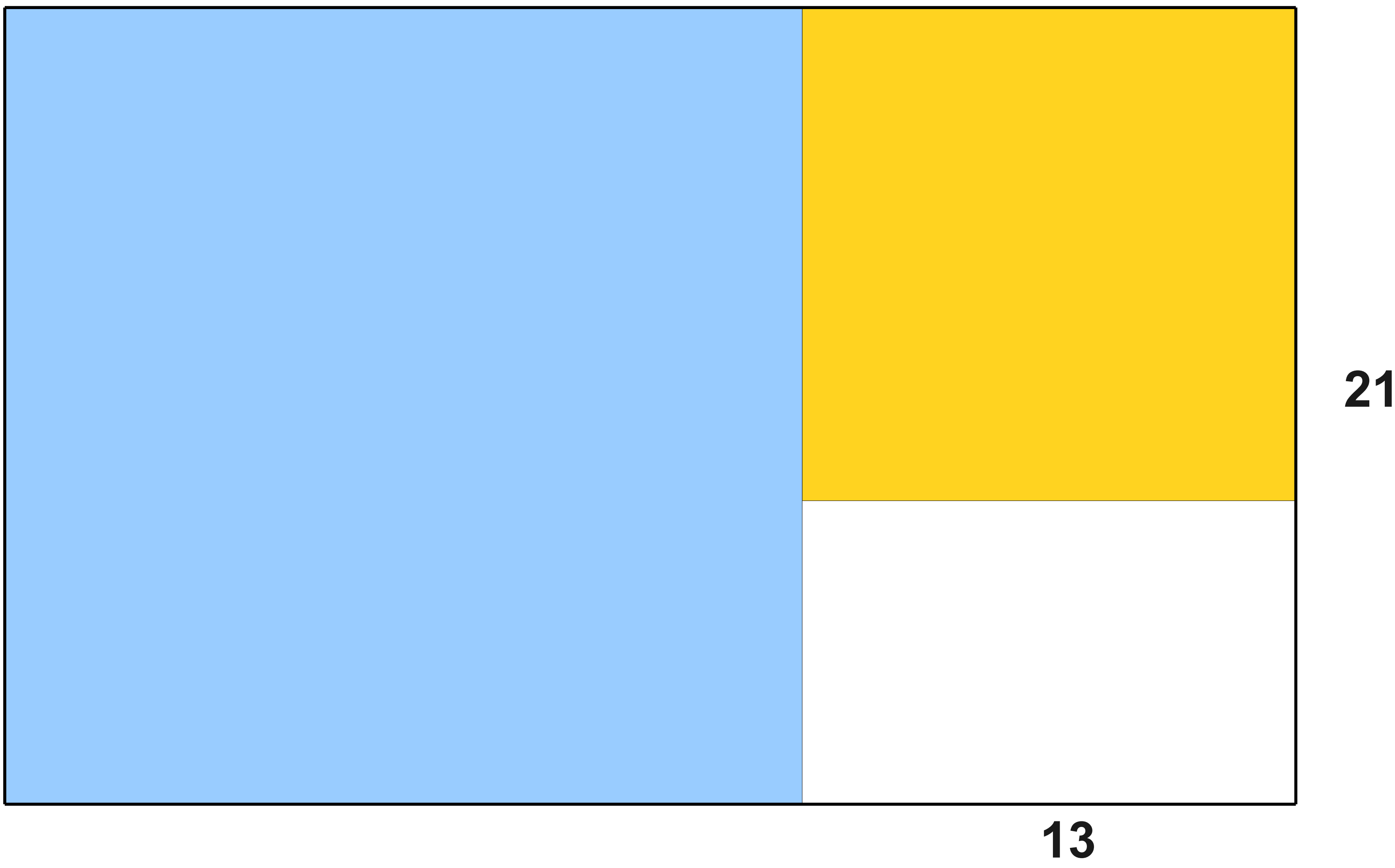
The Golden Ratio



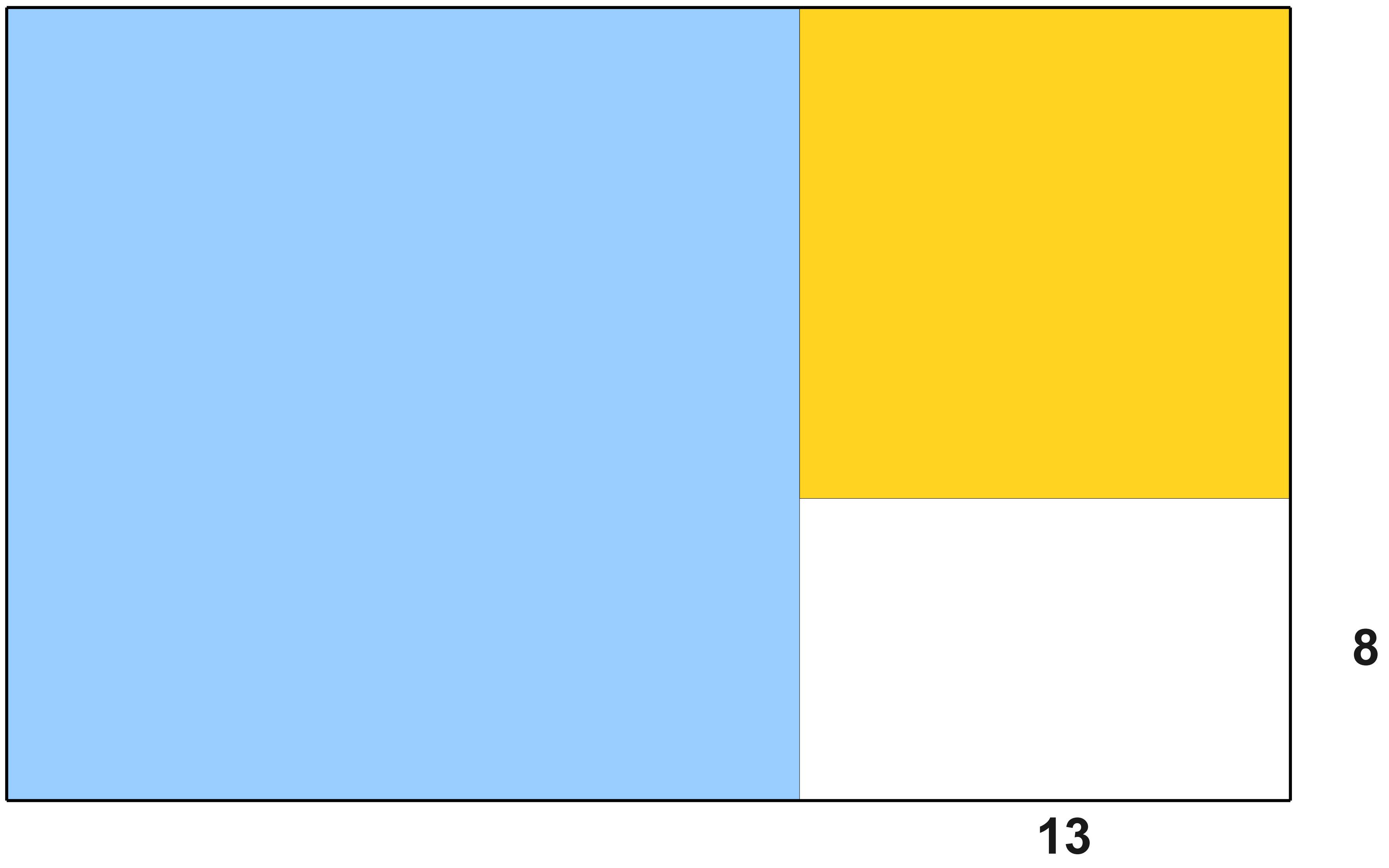
The Golden Ratio



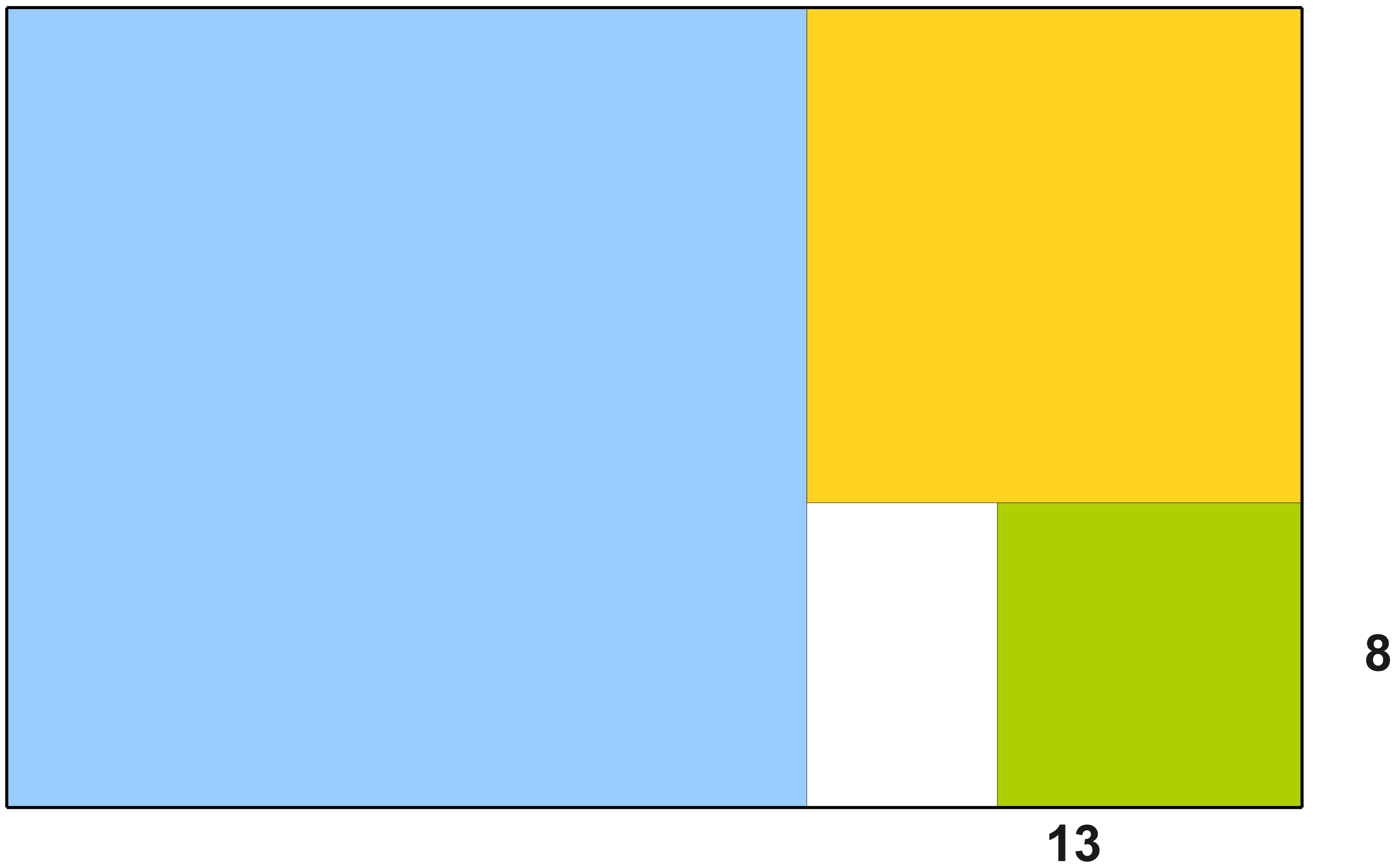
The Golden Ratio



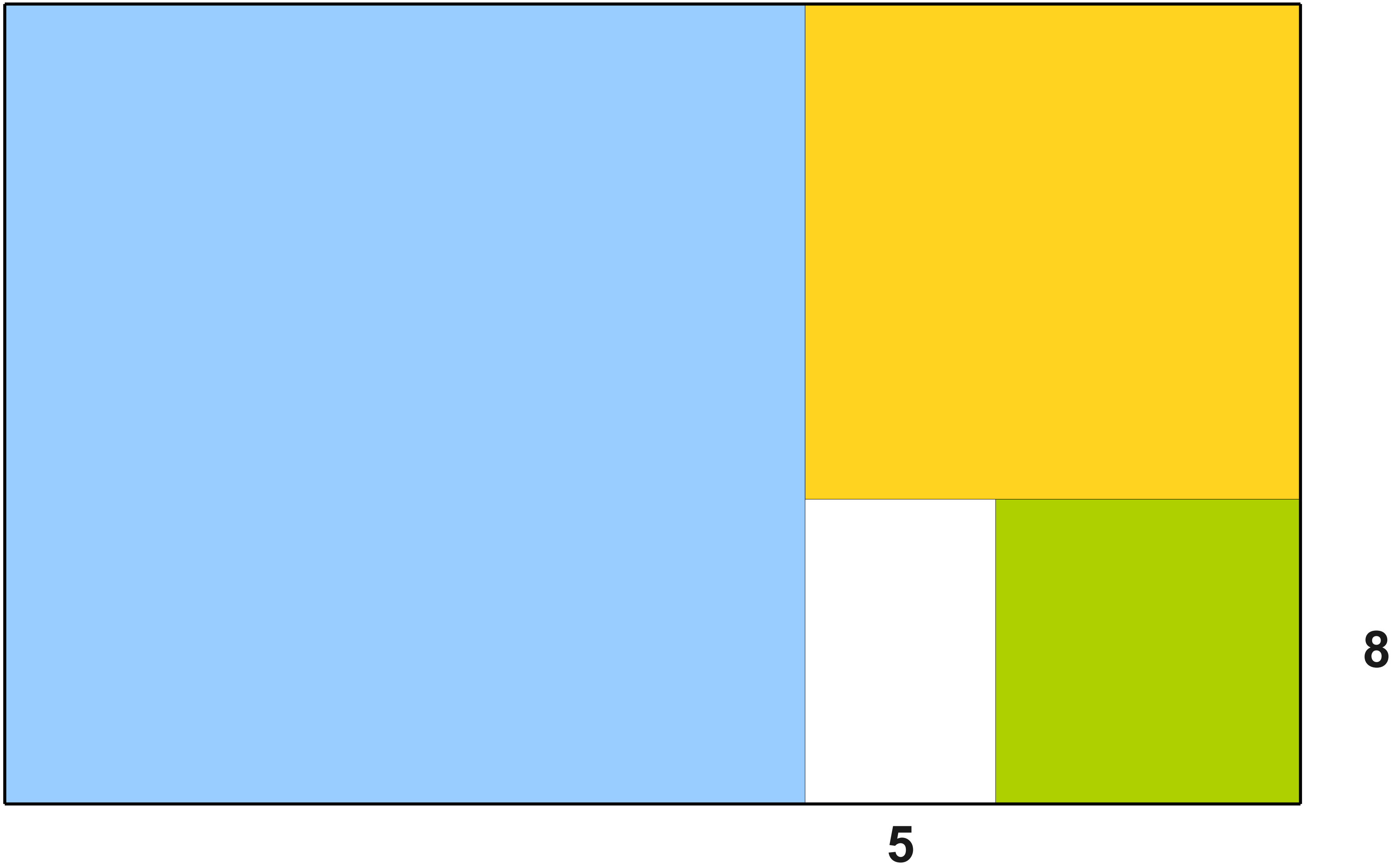
The Golden Ratio



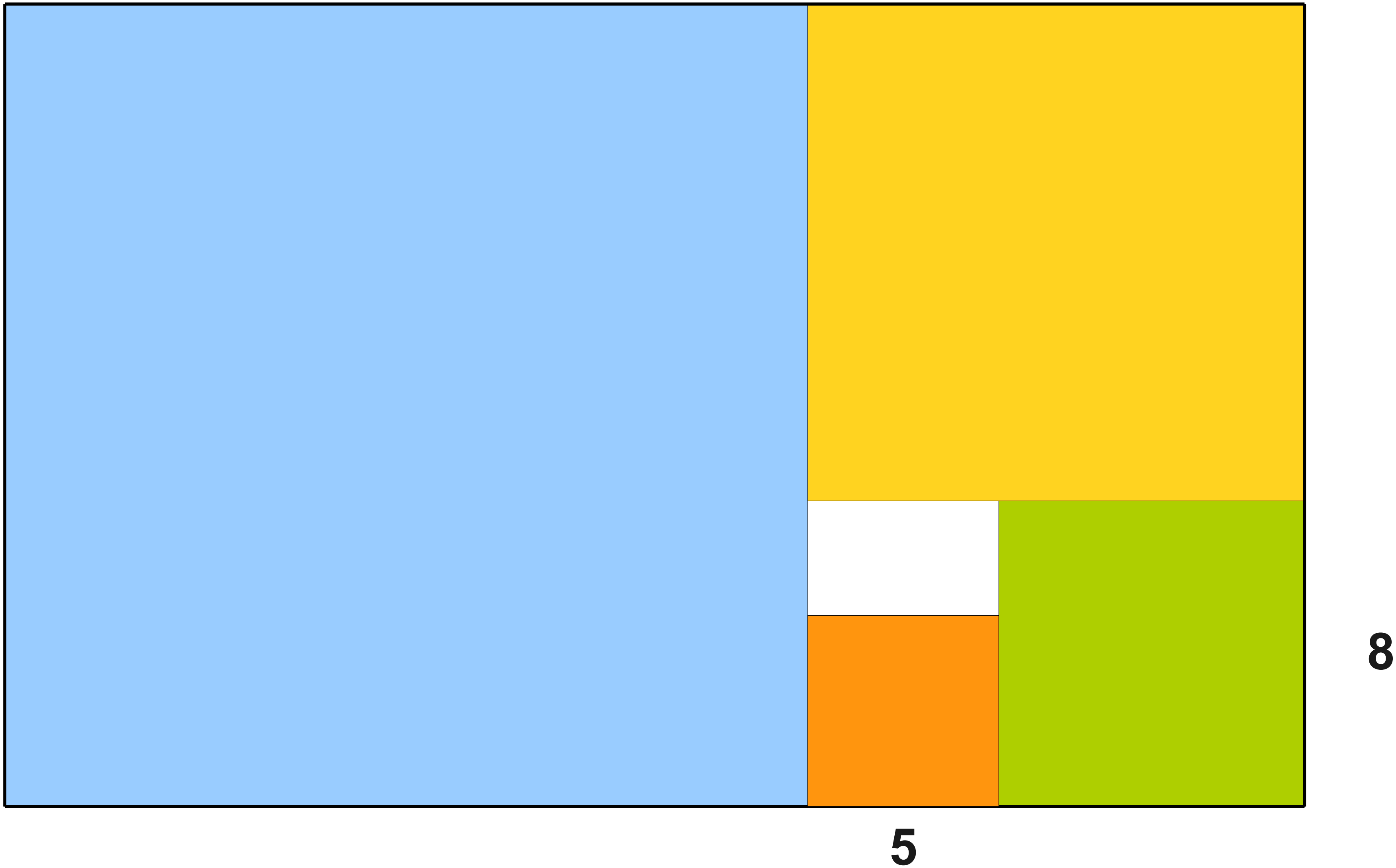
The Golden Ratio



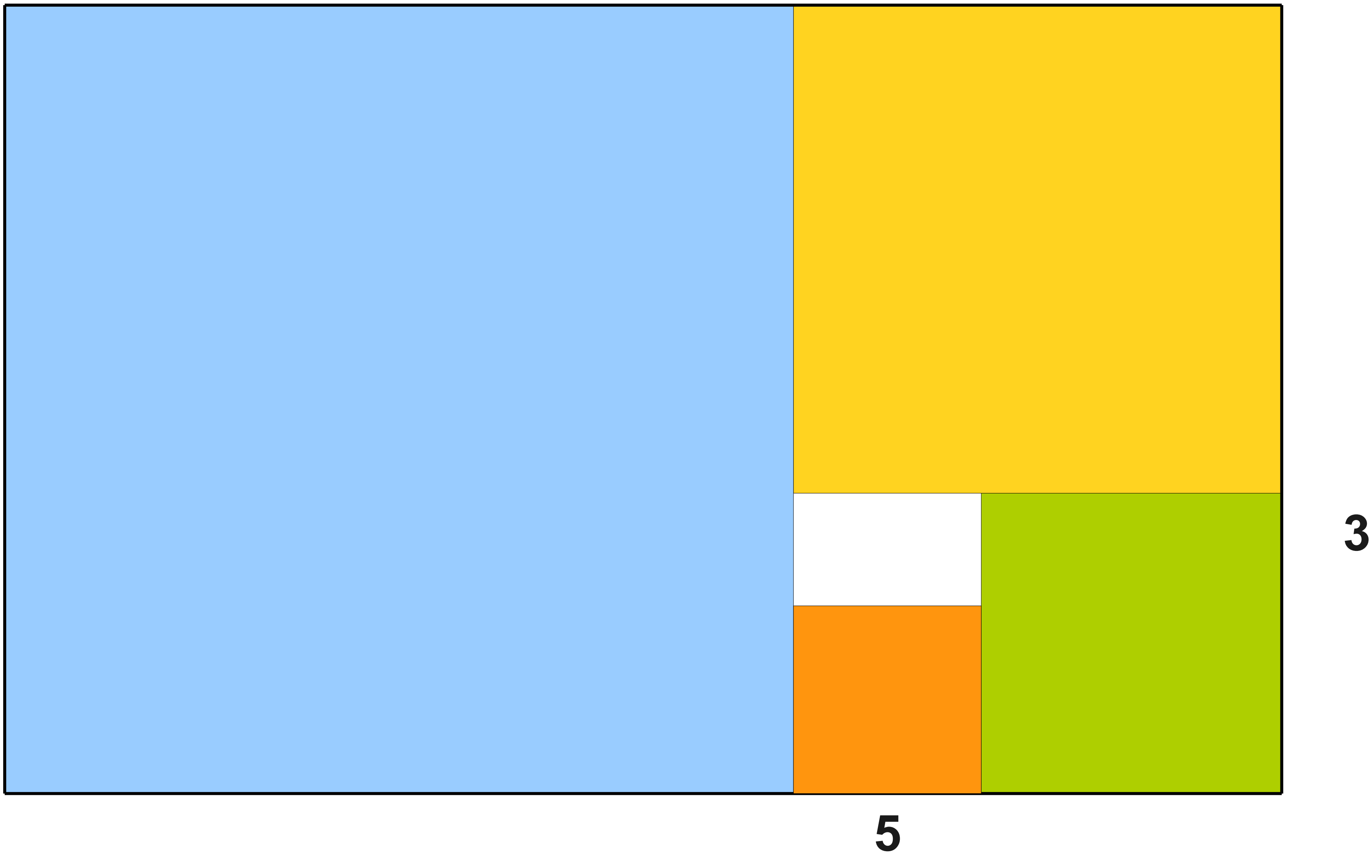
The Golden Ratio



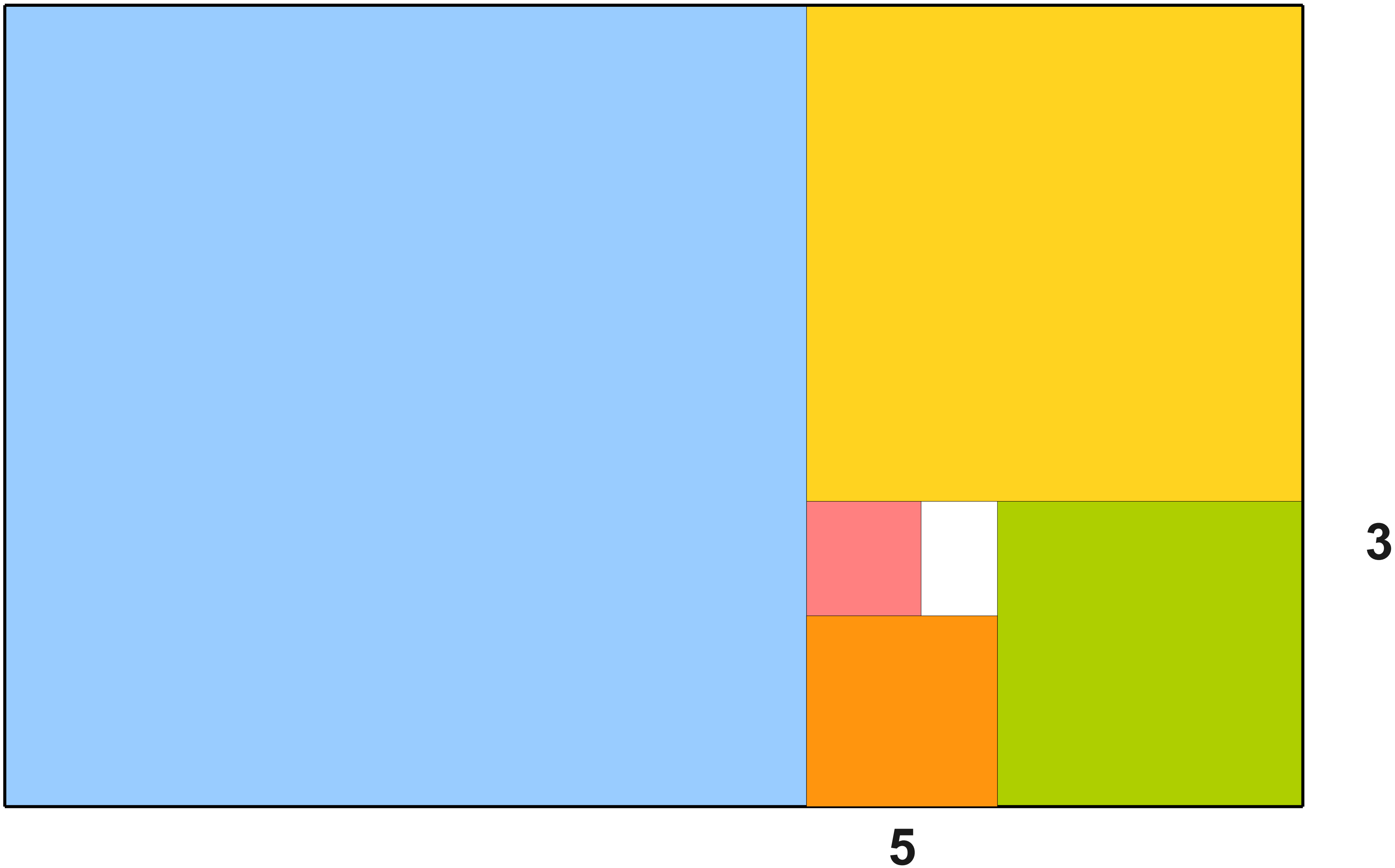
The Golden Ratio



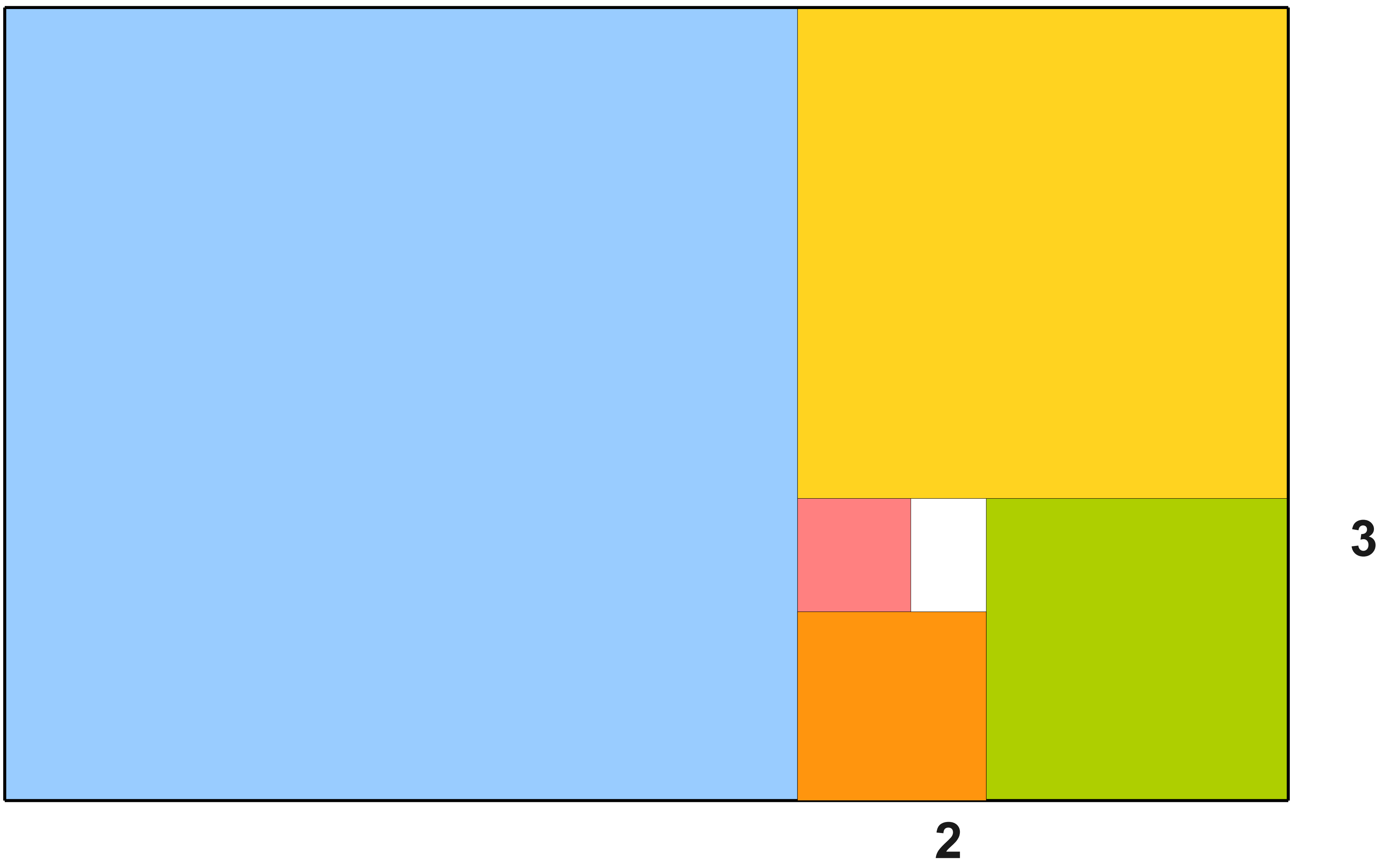
The Golden Ratio



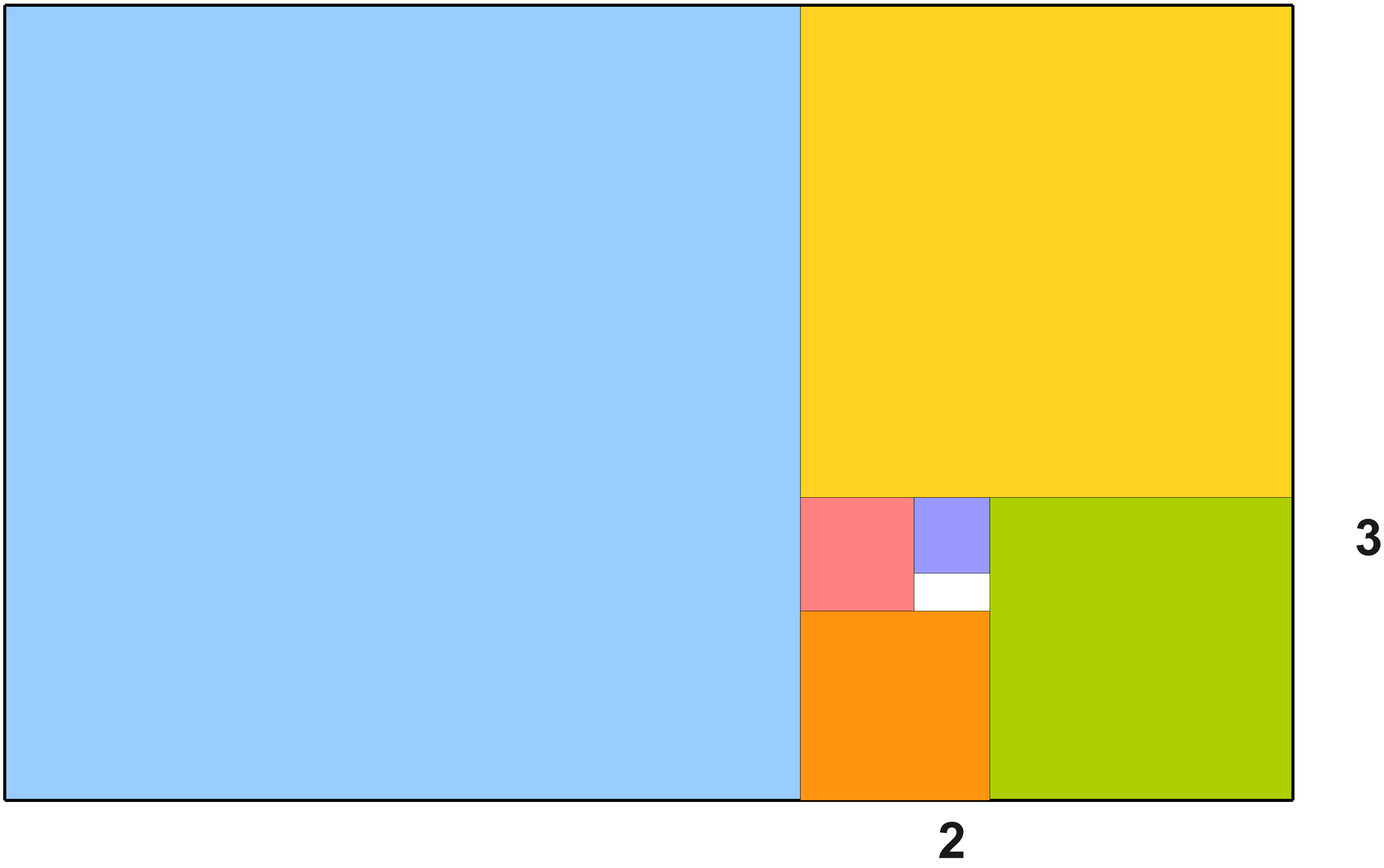
The Golden Ratio



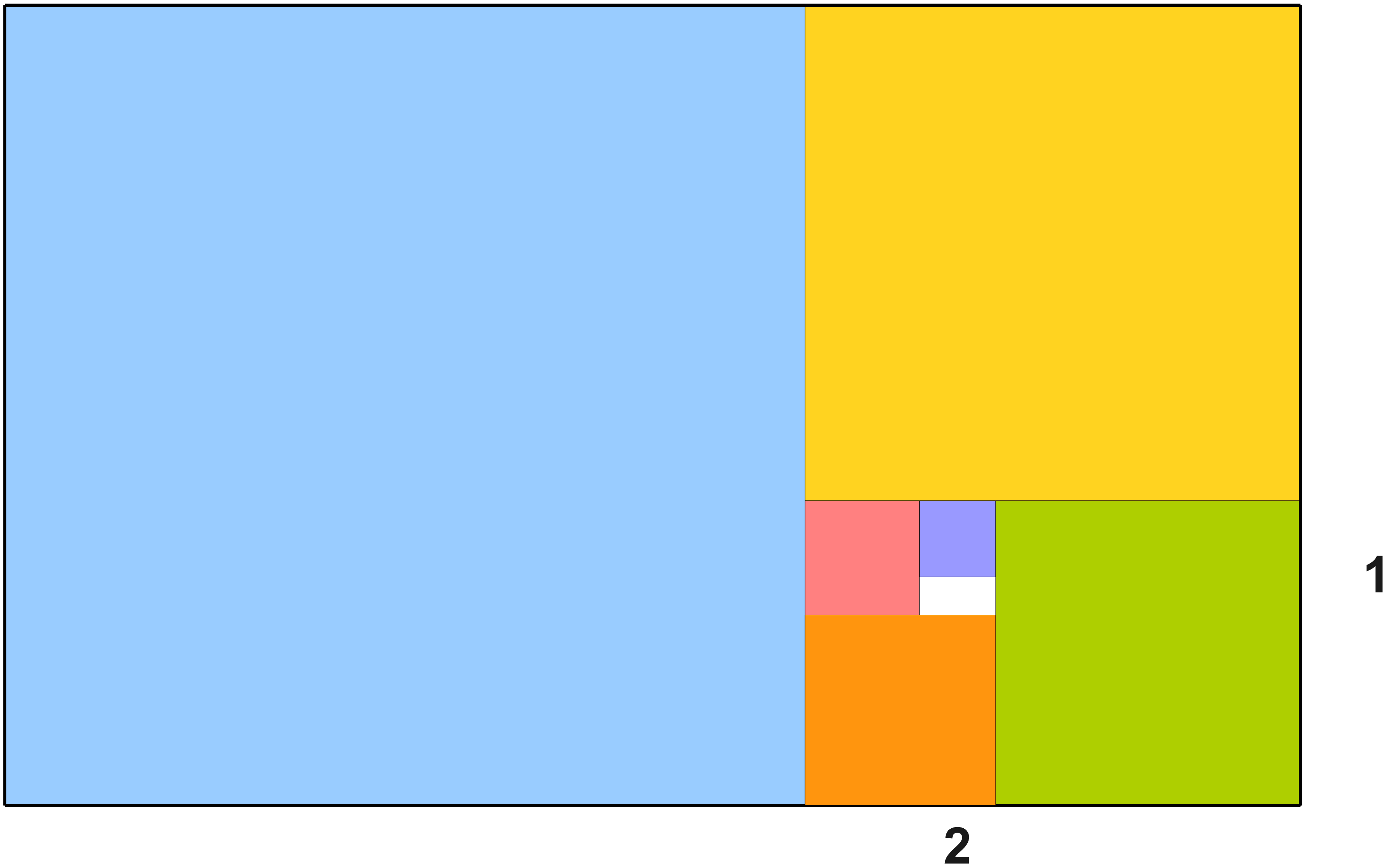
The Golden Ratio



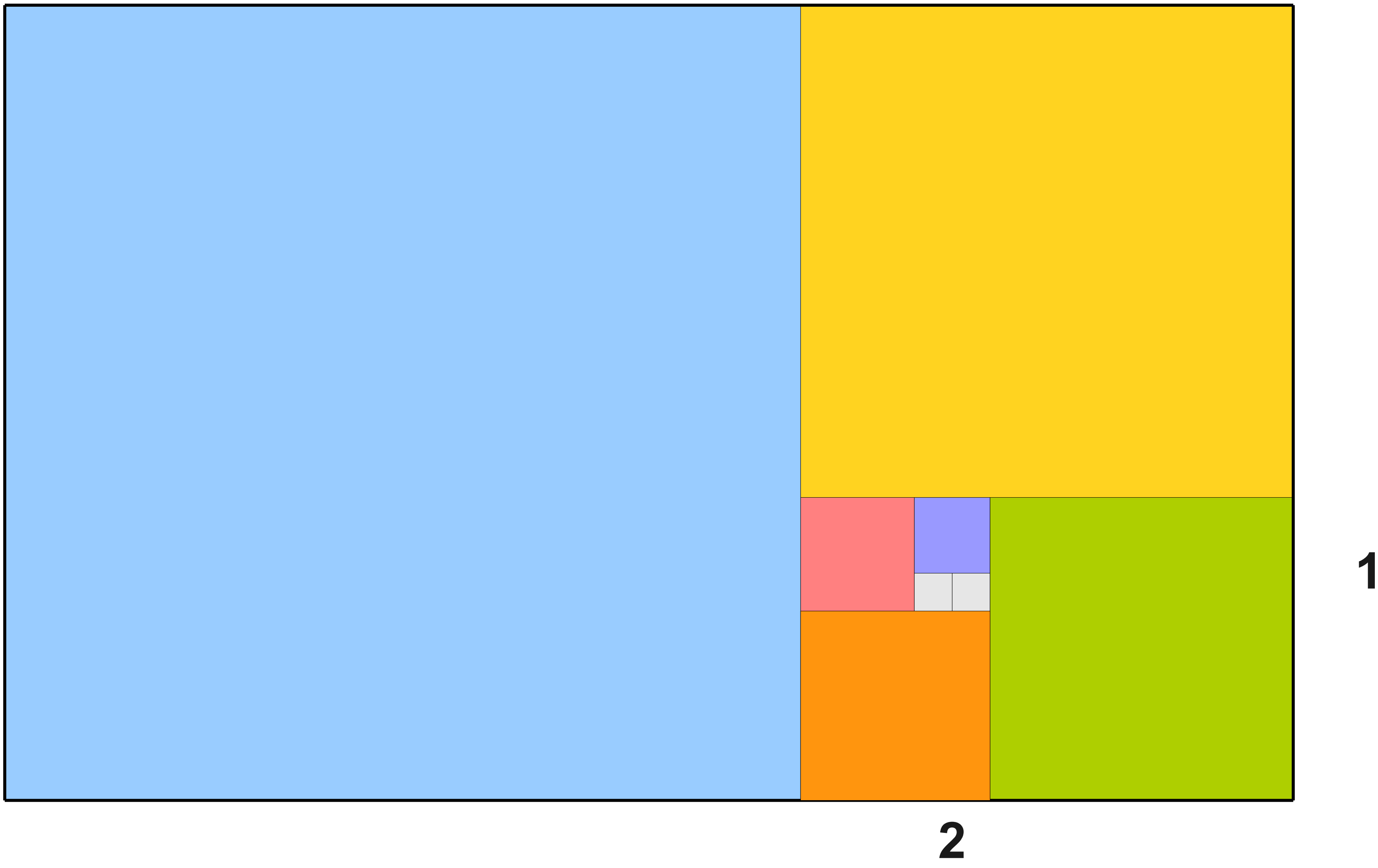
The Golden Ratio



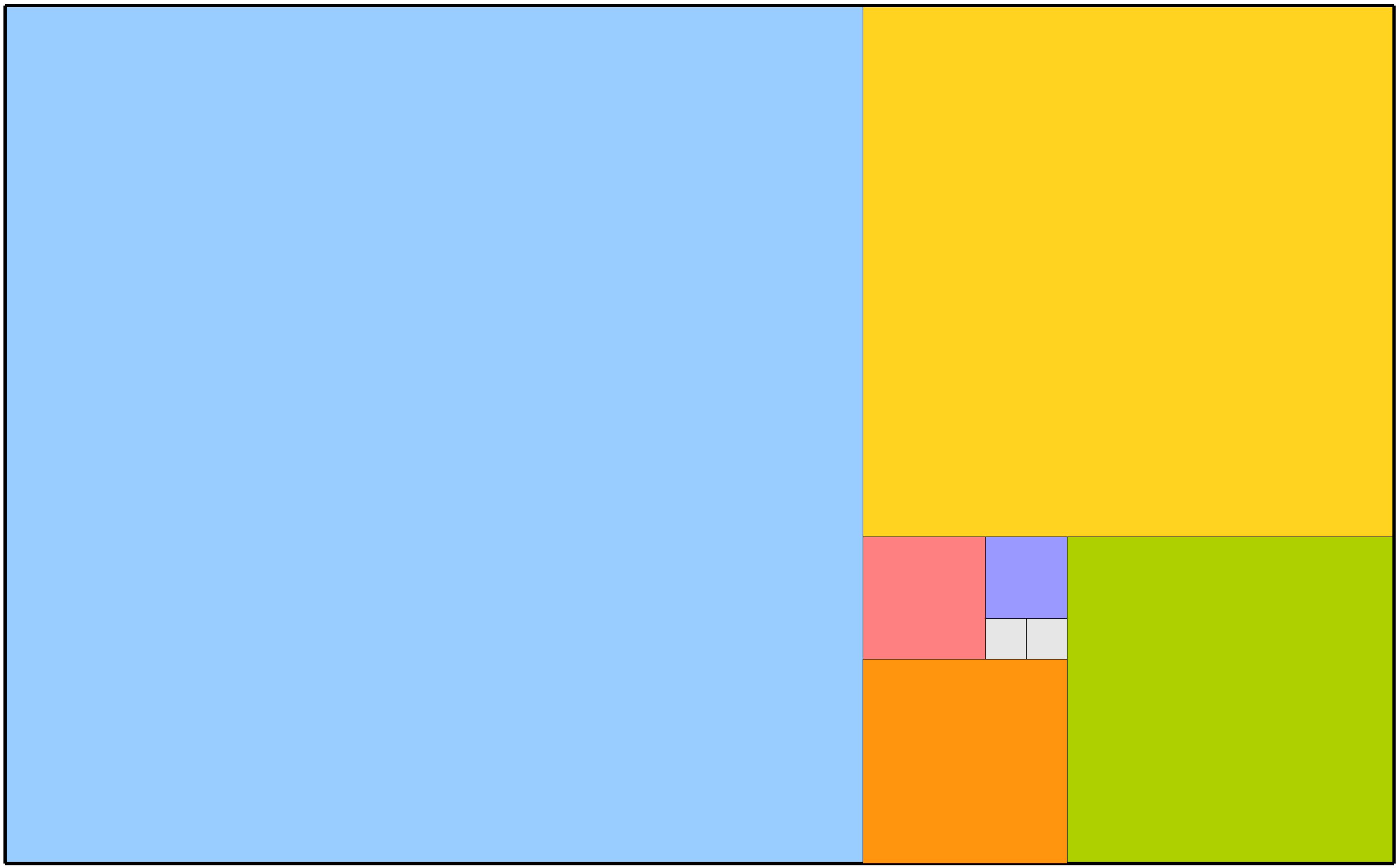
The Golden Ratio



The Golden Ratio



The Golden Ratio



The Division Algorithm

- For any integers a and b, with $b \neq 0$, there exists **unique** integers **q** and **r** such that

$$a = \mathbf{q}b + \mathbf{r}$$

and

$$0 \leq \mathbf{r} < b$$

- **q** is the **quotient** and **r** is the **remainder**.
- If both a and b are nonnegative, then both **q** and **r** are nonnegative.
- Given $a = 11$ and $b = 4$: $11 = \mathbf{2} \cdot 4 + \mathbf{3}$
- Given $a = 137$ and $b = 42$: $137 = \mathbf{3} \cdot 42 + \mathbf{11}$

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be “any nonnegative rational number with denominator n can be represented as a continued fraction.”

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be m / 1 = m. Since m is a valid continued fraction and m = m / 1, P(1) holds.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be m / 1 = m. Since m is a valid continued fraction and m = m / 1, P(1) holds.

For our inductive step, assume that for all 1 ≤ n' < n, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(*n*) is true by showing that any nonnegative rational number with denominator *n* has a continued fraction.

Consider any nonnegative rational number with denominator *n*; let it be m / n.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let $P(n)$ be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, $P(n')$ is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that $P(n)$ is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$.

The division algorithm is the mathematically rigorous way to justify getting a quotient and a remainder.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be m / 1 = m. Since m is a valid continued fraction and m = m / 1, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$.

Case 2: $r \neq 0$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$.

Case 2: $r \neq 0$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be “any nonnegative rational number with denominator n can be represented as a continued fraction.” We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \le n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \le r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.
Since $1 \le r < n$, by our inductive hypothesis there is some continued fraction for n / r; call it F.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(n) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all p

For our base … with denominator … rational number with … fraction and m = m /

For our indu… nonnegative … We prove that P(n) is t… minator n has a contin…

Consider an… . Using the division … ses:

Notice how we're using the fact that $r < n$ to justify using the inductive hypothesis.

Since our induction starts at 1, we also have to show that $r \geq 1$. Otherwise we might be out of the range of where the inductive hypothesis holds.

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.
Since $1 \leq r < n$, by our inductive hypothesis there is some continued fraction for n / r; call it F.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.
Since $1 \leq r < n$, by our inductive hypothesis there is some continued fraction for n / r; call it F.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.
Since $1 \leq r < n$, by our inductive hypothesis there is some continued fraction for n / r; call it F. Then $q + 1 / F$ is a continued fraction for m / n.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.
Since $1 \leq r < n$, by our inductive hypothesis there is some continued fraction for n / r; call it F. Then $q + 1 / F$ is a continued fraction for m / n.

In either case, we find a continued fraction for m / n, so P(n) holds, completing the induction.

Theorem: Every nonnegative rational number can be expressed as a continued fraction.

Proof: By strong induction. Let P(*n*) be "any nonnegative rational number with denominator n can be represented as a continued fraction." We prove that P(n) is true for all positive natural numbers.

For our base case, we prove P(1); that is, any nonnegative rational number with denominator 1 has a continued fraction. Consider an arbitrary nonnegative rational number with denominator 1; let it be $m / 1 = m$. Since m is a valid continued fraction and $m = m / 1$, P(1) holds.

For our inductive step, assume that for all $1 \leq n' < n$, P(n') is true; that is, any nonnegative rational number with denominator n' has a continued fraction. We prove that P(n) is true by showing that any nonnegative rational number with denominator n has a continued fraction.

Consider any nonnegative rational number with denominator n; let it be m / n. Using the division algorithm, write $m = qn + r$, where $0 \leq r < n$. We consider two cases:

Case 1: $r = 0$. Then $m = qn$, so $m / n = q$. Then q is a continued fraction for m / n.

Case 2: $r \neq 0$. Given that $m = qn + r$, we have that $\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{n/r}$.
Since $1 \leq r < n$, by our inductive hypothesis there is some continued fraction for n / r; call it F. Then $q + 1 / F$ is a continued fraction for m / n.

In either case, we find a continued fraction for m / n, so P(n) holds, completing the induction. ■

For more on continued fractions:

http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/cfINTRO.html

The Well-Ordering Principle

Extremal Cases

- Our proof about powers of two relied on a key step:

Let 2^k be the largest power of two less than or equal to $n + 1$.

- Many proofs work by picking some *extremal objects* (the largest *x* such that..., the smallest *y* such that..., etc.)

The Well-Ordering Principle

- The **well-ordering principle** is the following:

  Any nonempty set of natural numbers has a least element.

- Examples:
  - The least element of $\{1, 2, 3\}$ is 1.
  - The least element of $\mathbb{N}$ is 0.
  - There is no least element of $\mathbb{Z}$, but $\mathbb{Z}$ is not a set of natural numbers.
  - There is no least element of $\emptyset$, but $\emptyset$ is empty.

Proof by Well-Ordering

- Many proofs by induction or strong induction can be rewritten as proofs using the well-ordering principle.
- To prove that P(*n*) is true for all natural numbers *n*:
  - Consider the set $S = \{ n \mid n \in \mathbb{N}$ and $P(n)$ is false$\}$ of all natural numbers for which P(*n*) is false.
  - Assume, for the sake of contradiction, that *S* is nonempty.
  - Using the well-ordering principle, take the smallest element of *S*, call it n_0.
  - Derive a contradiction with n_0.
  - Conclude that *S* must be empty, so P(*n*) is always true.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$.

This set S is the set of all natural numbers n where the theorem isn't true. If this set is empty, we're done. So our goal now is to show that it has to be empty.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{\, n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that *S* must be empty by contradiction; assume that *S* is nonempty.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that *S* must be empty by contradiction; assume that *S* is nonempty. By the well-ordering principle, there is a least element of *S*, call it n_0.

An important detail here is that we're picking the smallest element of S, not just any arbitrary element of S. We'll use this fact later on.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that *S* must be empty by contradiction; assume that *S* is nonempty. By the well-ordering principle, there is a least element of *S*, call it n_0.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$.

Case 2: $n_0 > 0$.

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that *S* must be empty by contradiction; assume that *S* is nonempty. By the well-ordering principle, there is a least element of *S*, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$.

This is notationally dense, but we're just pulling off the last term of the sum. Since we know that $n_0 > 0$, the upper bound on this sum is still a natural number.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0 + 1} - 1$.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0-1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0-1} 2^i) + 2^{n_0} \neq 2^{n_0+1} - 1$$

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that *S* must be empty by contradiction; assume that *S* is nonempty. By the well-ordering principle, there is a least element of *S*, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0 + 1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0} \neq 2^{n_0 + 1} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0 + 1} - 2^{n_0} - 1$$

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0} \neq 2^{n_0+1} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0+1} - 2^{n_0} - 1 = 2(2^{n_0}) - 2^{n_0} - 1$$

Theorem: For any natural number *n*, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let *S* be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that *S* must be empty by contradiction; assume that *S* is nonempty. By the well-ordering principle, there is a least element of *S*, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0-1} 2^i) + 2^{n_0} \neq 2^{n_0+1} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0+1} - 2^{n_0} - 1 = 2(2^{n_0}) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0} - 1$$

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1 \}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0} \neq 2^{n_0+1} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0+1} - 2^{n_0} - 1 = 2(2^{n_0}) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0} - 1$$

This means that the theorem is false for $n_0 - 1$, which in turn means that $n_0 - 1$ has to be in the set S.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0 + 1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0} \neq 2^{n_0 + 1} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0 + 1} - 2^{n_0} - 1 = 2(2^{n_0}) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0} - 1$$

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = \left(\sum_{i=0}^{n_0-1} 2^i\right) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$\left(\sum_{i=0}^{n_0-1} 2^i\right) + 2^{n_0} \neq 2^{n_0+1} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0+1} - 2^{n_0} - 1 = 2\left(2^{n_0}\right) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0} - 1$$

But this means that $n_0 - 1 \in S$, contradicting the fact that n_0 is the least element of S.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0 + 1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0} \neq 2^{n_0 + 1} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0 + 1} - 2^{n_0} - 1 = 2(2^{n_0}) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0 - 1} 2^i \neq 2^{n_0} - 1$$

But this means that $n_0 - 1 \in S$, contradicting the fact that n_0 is the least element of S. We have reached a contradiction, so our assumption must have been wrong and S is empty.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = \left(\sum_{i=0}^{n_0-1} 2^i\right) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$\left(\sum_{i=0}^{n_0-1} 2^i\right) + 2^{n_0} \neq 2^{n_0+1} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0+1} - 2^{n_0} - 1 = 2\left(2^{n_0}\right) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0} - 1$$

But this means that $n_0 - 1 \in S$, contradicting the fact that n_0 is the least element of S. We have reached a contradiction, so our assumption must have been wrong and S is empty. Thus for any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

Theorem: For any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof: Let S be the set $\{ n \in \mathbb{N} \mid \sum_{i=0}^{n} 2^i \neq 2^{n+1} - 1\}$. We prove that S must be empty by contradiction; assume that S is nonempty. By the well-ordering principle, there is a least element of S, call it n_0. We consider two cases:

Case 1: $n_0 = 0$. But this is impossible, since we know that $\sum_{i=0}^{0} 2^i = 1$

Case 2: $n_0 > 0$. Then $\sum_{i=0}^{n_0} 2^i = (\sum_{i=0}^{n_0 - 1} 2^i) + 2^{n_0}$. Since $n_0 \in S$, we know that $\sum_{i=0}^{n_0} 2^i \neq 2^{n_0+1} - 1$. Therefore,

$$(\sum_{i=0}^{n_0-1} 2^i) + 2^{n_0} \neq 2^{n_0+1} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0+1} - 2^{n_0} - 1 = 2(2^{n_0}) - 2^{n_0} - 1$$

$$\sum_{i=0}^{n_0-1} 2^i \neq 2^{n_0} - 1$$

But this means that $n_0 - 1 \in S$, contradicting the fact that n_0 is the least element of S. We have reached a contradiction, so our assumption must have been wrong and S is empty. Thus for any natural number n, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$. ■

Irrational Numbers Revisited

- A **rational number** is a number *r* that can be written as

$$r = \frac{p}{q}$$

where

  - *p* and *q* are integers,
  - $q \neq 0$, and
  - *p* and *q* have no common divisors other than ±1.

Irrational Numbers Revisited

- A **rational number** is a number r that can be written as

$$r = \frac{p}{q}$$

where

  - p and q are integers,
  - $q \neq 0$, and
  - p and q have no common divisors other than ± 1.
- This last condition is troubling. What if we get rid of it?

Irrational Numbers Revisited

- A **rational number** is a number *r* that can be written as

$$r = \frac{p}{q}$$

  where

  - *p* and *q* are integers,
  - $q \neq 0$, and
  - ~~*p* and *q* have no common divisors other than ±1.~~
- This last condition is troubling. What if we get rid of it?

One Simplifying Assumption

- For general rational numbers, p and q can be integers.
- We will assume that the square root of two is positive.
- Because of this, p and q can be assumed to be natural numbers.

Theorem: $\sqrt{2}$ is irrational.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p \,/\, q = \sqrt{2} \}.$$

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p \mathbin{/} q = \sqrt{2}\}.$$

Notationally this is quite dense, but it just says that S is the set of denominators in an expression of the square root of two as a ratio.

Theorem: $\sqrt{2}$ is irrational.

Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \,\}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \,\}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0.

Again, notice that we're picking q_0 as the least element of S, not an arbitrary element of S.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \,\}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2}q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p \,/\, q = \sqrt{2} \,\}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2}q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Since both p and q_0 are even, this means that $p / 2$ and $q_0 / 2$ are natural numbers.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Since both p and q_0 are even, this means that $p / 2$ and $q_0 / 2$ are natural numbers. Note that $(p / 2) / (q_0 / 2) = p / q_0 = \sqrt{2}$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Since both p and q_0 are even, this means that $p / 2$ and $q_0 / 2$ are natural numbers. Note that $(p / 2) / (q_0 / 2) = p / q_0 = \sqrt{2}$. Since $q_0 \neq 0$, we have that $q_0 / 2 \neq 0$, and so $q_0 / 2 \in S$.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Since both p and q_0 are even, this means that $p / 2$ and $q_0 / 2$ are natural numbers. Note that $(p / 2) / (q_0 / 2) = p / q_0 = \sqrt{2}$. Since $q_0 \neq 0$, we have that $q_0 / 2 \neq 0$, and so $q_0 / 2 \in S$. However, $q_0 / 2 < q_0$, contradicting the fact that q_0 is the least element of S.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{\, q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2}q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Since both p and q_0 are even, this means that $p / 2$ and $q_0 / 2$ are natural numbers. Note that $(p / 2) / (q_0 / 2) = p / q_0 = \sqrt{2}$. Since $q_0 \neq 0$, we have that $q_0 / 2 \neq 0$, and so $q_0 / 2 \in S$. However, $q_0 / 2 < q_0$, contradicting the fact that q_0 is the least element of S. We have reached a contradiction, so our assumption must have been wrong and S is empty.

Theorem: $\sqrt{2}$ is irrational.
Proof: Consider the set

$$S = \{ q \in \mathbb{N} \mid q \neq 0 \text{ and there exists a } p \in \mathbb{N} \text{ such that } p / q = \sqrt{2} \}.$$

If this set is empty, then $\sqrt{2}$ is irrational, because there is no choice of p / q with $q \neq 0$ such that $p / q = \sqrt{2}$.

We prove that S is empty by contradiction; assume that S is nonempty. Then by the well-ordering principle, it has a least element q_0. By our choice of S, $q_0 \neq 0$, and there exists some $p \in \mathbb{N}$ such that $p / q_0 = \sqrt{2}$. This means that $p = \sqrt{2} q_0$, so $p^2 = 2q_0^2$. Since q_0^2 is an integer, p^2 is even. By our earlier result, this means that p is even, so there exists some $k \in \mathbb{Z}$ such that $p = 2k$.

Therefore, $2q_0^2 = p^2 = (2k)^2 = 4k^2$, and so $q_0^2 = 2k^2$. Since k^2 is an integer, this means that q_0^2 is even, so by our earlier result q_0 is even.

Since both p and q_0 are even, this means that $p / 2$ and $q_0 / 2$ are natural numbers. Note that $(p / 2) / (q_0 / 2) = p / q_0 = \sqrt{2}$. Since $q_0 \neq 0$, we have that $q_0 / 2 \neq 0$, and so $q_0 / 2 \in S$. However, $q_0 / 2 < q_0$, contradicting the fact that q_0 is the least element of S. We have reached a contradiction, so our assumption must have been wrong and S is empty. ■

Next Time

- **Graphs and Relations**
  - Representing structured data.
  - Categorizing how objects are connected.