Mathematical Induction

Part Two

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

$P(0)$ is true

If it starts …

… and it keeps going …

and

For any $n \in \mathbb{N}$, we have $P(n) \to P(n + 1)$

Then

… then it's always true.

For any $n \in \mathbb{N}$, $P(n)$ is true.

Theorem: For any natural number n, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof: By induction. Let $P(n)$ be

$$P(n) \equiv \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

For our base case, we need to show $P(0)$ is true, meaning that

$$\sum_{i=1}^{0} i = \frac{0(0+1)}{2}$$

Since the empty sum is defined to be 0, this claim is true.

For the inductive step, assume that for some $n \in \mathbb{N}$ that $P(n)$ holds, so

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

We need to show that $P(n + 1)$ holds, meaning that

$$\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

To see this, note that

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Thus $P(n + 1)$ is true, completing the induction. ■

Induction in Practice

- Typically, a proof by induction will not explicitly state $P(n)$.
- Rather, the proof will describe $P(n)$ implicitly and leave it to the reader to fill in the details.
- Provided that there is sufficient detail to determine
  - what $P(n)$ is,
  - that $P(0)$ is true, and that
  - whenever $P(n)$ is true, $P(n + 1)$ is true,

  the proof is usually valid.

Theorem: For any natural number n, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof: By induction on n. For our base case, if $n = 0$, note that

$$\sum_{i=1}^{0} i = \frac{0(0+1)}{2} = 0$$

and the theorem is true for 0.

For the inductive step, assume that for some n the theorem is true. Then we have that

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

so the theorem is true for $n + 1$, completing the induction. ■

A Variant of Induction

n^2 versus 2^n

$0^2 = 0$	$<$	$2^0 = 1$
$1^2 = 1$	$<$	$2^1 = 2$
$2^2 = 4$	$=$	$2^2 = 4$
$3^2 = 9$	$>$	$2^3 = 8$
$4^2 = 16$	$=$	$2^4 = 16$
$5^2 = 25$	$<$	$2^5 = 32$
$6^2 = 36$	$<$	$2^6 = 64$
$7^2 = 49$	$<$	$2^7 = 128$
$8^2 = 64$	$<$	$2^8 = 256$
$9^2 = 81$	$<$	$2^9 = 512$
$10^2 = 100$	$<$	$2^{10} = 1024$

2^n is <u>much</u> bigger here. Does the trend continue?

Theorem: For any natural number $n \geq 5$, $n^2 < 2^n$.

Proof: By induction on n. As a base case, if $n = 5$, then we have that $5^2 = 25 < 32 = 2^5$, so the claim holds.

For the inductive step, assume that for some $n \geq 5$, that $n^2 < 2^n$. Then we have that

$$(n + 1)^2 = n^2 + 2n + 1$$

Since $n \geq 5$, we have

$$\begin{aligned}
(n + 1)^2 &= n^2 + 2n + 1 \\
&< n^2 + 2n + n \quad \text{(since } 1 < 5 \leq n\text{)} \\
&= n^2 + 3n \\
&< n^2 + n^2 \quad \text{(since } 3n < 5n \leq n^2\text{)} \\
&= 2n^2
\end{aligned}$$

So $(n + 1)^2 < 2n^2$. Now, by our inductive hypothesis, we know that $n^2 < 2^n$. This means that

$$\begin{aligned}
(n + 1)^2 &< 2n^2 \quad \text{(from above)} \\
&< 2(2^n) \quad \text{(by the inductive hypothesis)} \\
&= 2^{n + 1}
\end{aligned}$$

Completing the induction. ■

Theorem: For any natural number $n \geq 5$, $n^2 < 2^n$.

Proof: By induction on n. As a base case, if $n = 5$, then we have that $5^2 = 25 < 32 = 2^5$, so the claim holds.

For the inductive step, assume that for some $n \geq 5$, that $n^2 < 2^n$. Then we have that

$$(n + 1)^2 = n^2 + 2n + 1$$

Since $n \geq 5$, we [obscured]

Why is this allowed?

$(n + 1)^2 = $ [obscured]

$< $ [obscured] $5 \leq n$)

$= $ [obscured]

$< n^2 + n^2$ *(since $3n < 5n \leq n^2$)*

$= 2n^2$

So $(n + 1)^2 < 2n^2$. Now, by our inductive hypothesis, we know that $n^2 < 2^n$. This means that

$(n + 1)^2 < 2n^2$ *(from above)*

$< 2(2^n)$ *(by the inductive hypothesis)*

$= 2^{n+1}$

Completing the induction. ■

Why is this Legal?

- Let $P(n)$ be "Either $n < 5$ or $n^2 < 2^n$."
- $P(0)$ is trivially true.
- $P(1)$ is trivially true, so $P(0) \to P(1)$
- $P(2)$ is trivially true, so $P(1) \to P(2)$
- $P(3)$ is trivially true, so $P(2) \to P(3)$
- $P(4)$ is trivially true, so $P(3) \to P(4)$
- We explicitly proved $P(5)$, so $P(4) \to P(5)$
- For any $n \geq 5$, we explicitly proved that $P(n) \to P(n + 1)$.
- Thus $P(0)$ and for any $n \in \mathbb{N}$, $P(n) \to P(n + 1)$, so by induction $P(n)$ is true for all natural numbers n.

Induction Starting at k

- To prove that $P(n)$ is true for all natural numbers greater than or equal to k:
  - Show that $P(k)$ is true.
  - Show that for any $n \geq k$, that $P(n) \to P(n + 1)$.
  - Conclude $P(k)$ holds for all natural numbers greater than or equal to k.
- You don't need to justify why it's okay to start from k.

An Important Observation

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

$\boldsymbol{P(0)}$ **is true**

and

For any $n \in \mathbb{N}$ with $n \neq 0$, if $P(n')$ is true for all $n' < n$, then $P(n)$ is true

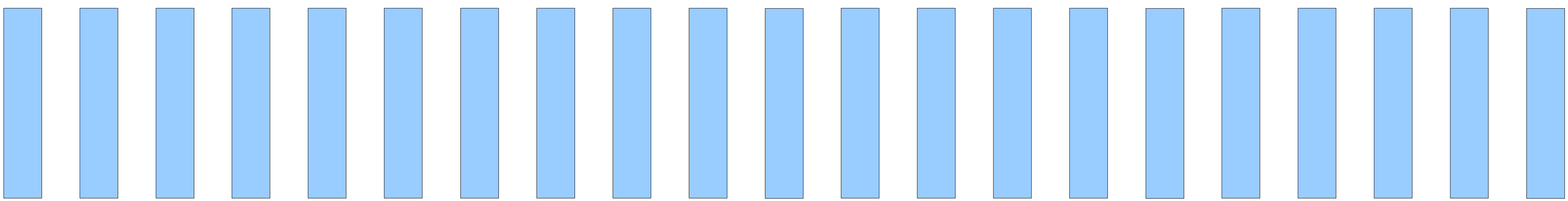
then

For any $n \in \mathbb{N}$, $P(n)$ is true.

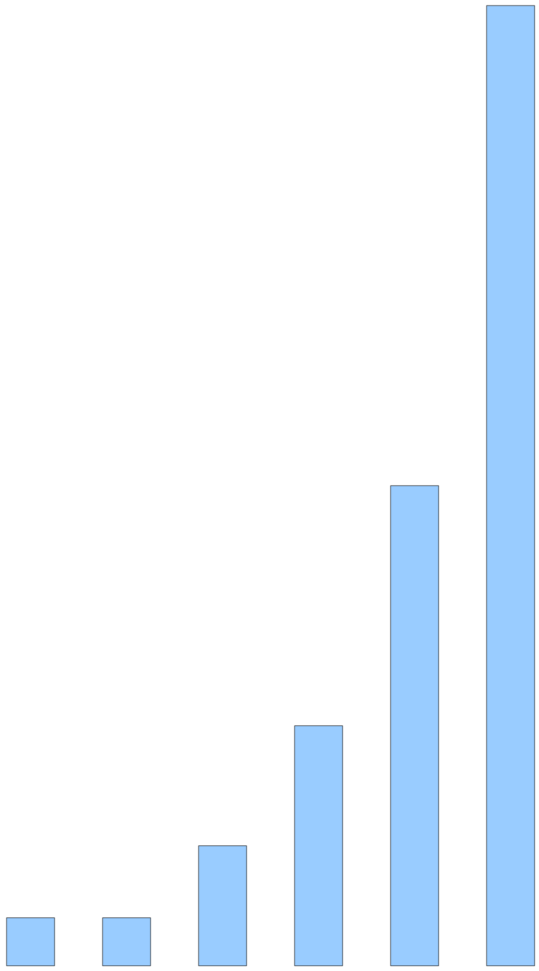
Using Strong Induction

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 $0 \leq n' < n$, that $P(n')$ is true.
  - State what $P(n)$ is. *(this is what you're trying to prove)*
  - Go prove $P(n)$.

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?

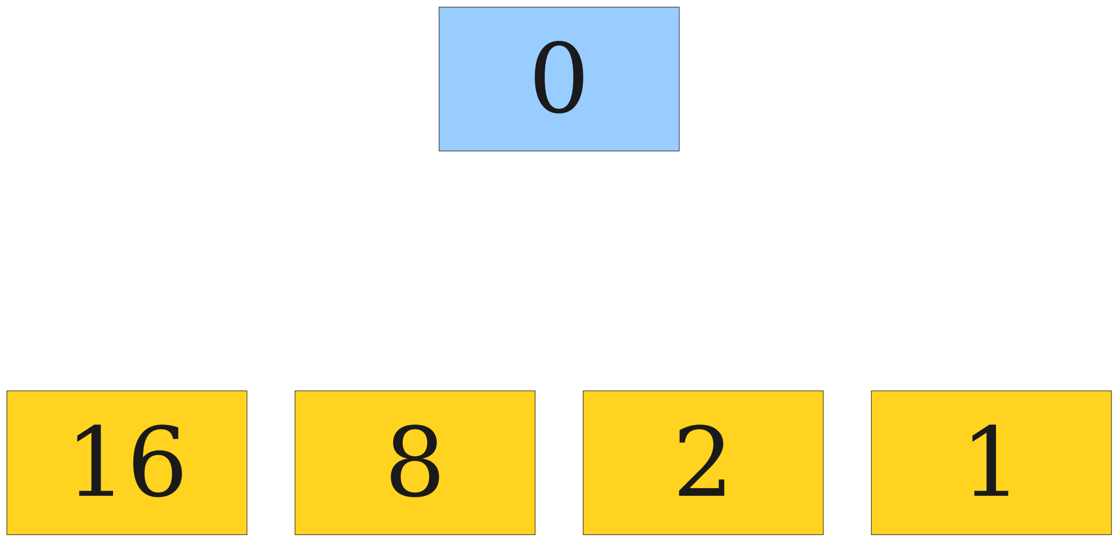
Justifying Binary Numbers

- 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



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 $n \in \mathbb{N}$ is the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n is the sum of distinct powers of two." We prove that P(n) is true for all $n \in \mathbb{N}$.

As our base case, we prove P(0), that 0 is the sum of distinct powers of 2. Since the empty sum of no powers of 2 is equal to 0, P(0) holds.

For the inductive step, assume that for some nonzero $n \in \mathbb{N}$, that for any $n' \in \mathbb{N}$ where $0 \leq n' < n$, that $P(n')$ holds and n' is 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 all natural numbers in the range **$0 \leq n' < n$**. We'll use this fact later on.

Theorem: Every $n \in \mathbb{N}$ is the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n is the sum of distinct powers of two." We prove that P(n) is true for all $n \in \mathbb{N}$.

As our base case, we prove P(0), that 0 is the sum of distinct powers of 2. Since the empty sum of no powers of 2 is equal to 0, P(0) holds.

For the inductive step, assume that for some nonzero $n \in \mathbb{N}$, that for any $n' \in \mathbb{N}$ where $0 \le n' < n$, that $P(n')$ holds and n' is the sum of distinct powers of two. We prove $P(n)$, that n is the sum of distinct powers of two.

Let 2^k be the greatest power of two such that $2^k \le n$. Consider $n - 2^k$.

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

$$0 \le n - 2^k < n$$

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

Theorem: Every $n \in \mathbb{N}$ is the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n is the sum of distinct powers of two." We prove that P(n) is true for all $n \in \mathbb{N}$.

As our base case, we prove P(0), that 0 is the sum of distinct powers of 2. Since the empty sum of no powers of 2 is equal to 0, P(0) holds.

For the inductive step, assume that for some nonzero $n \in \mathbb{N}$, that for any $n' \in \mathbb{N}$ where $0 \leq n' < n$, that $P(n')$ holds and n' is the sum of distinct powers of two. We prove $P(n)$, that n is the sum of distinct powers of two.

Let 2^k be the greatest power of two such that $2^k \leq n$. Consider $n - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n - 2^k < n$. Since $2^k \leq n$, we know $0 \leq n - 2^k$. Thus, by our inductive hypothesis, $n - 2^k$ is the sum of distinct powers of two.

Here is where strong induction kicks in. We use the fact that any smaller number can be written as the sum of distinct powers of two to show that $n - 2^k$ can be written as the sum of distinct powers of two.

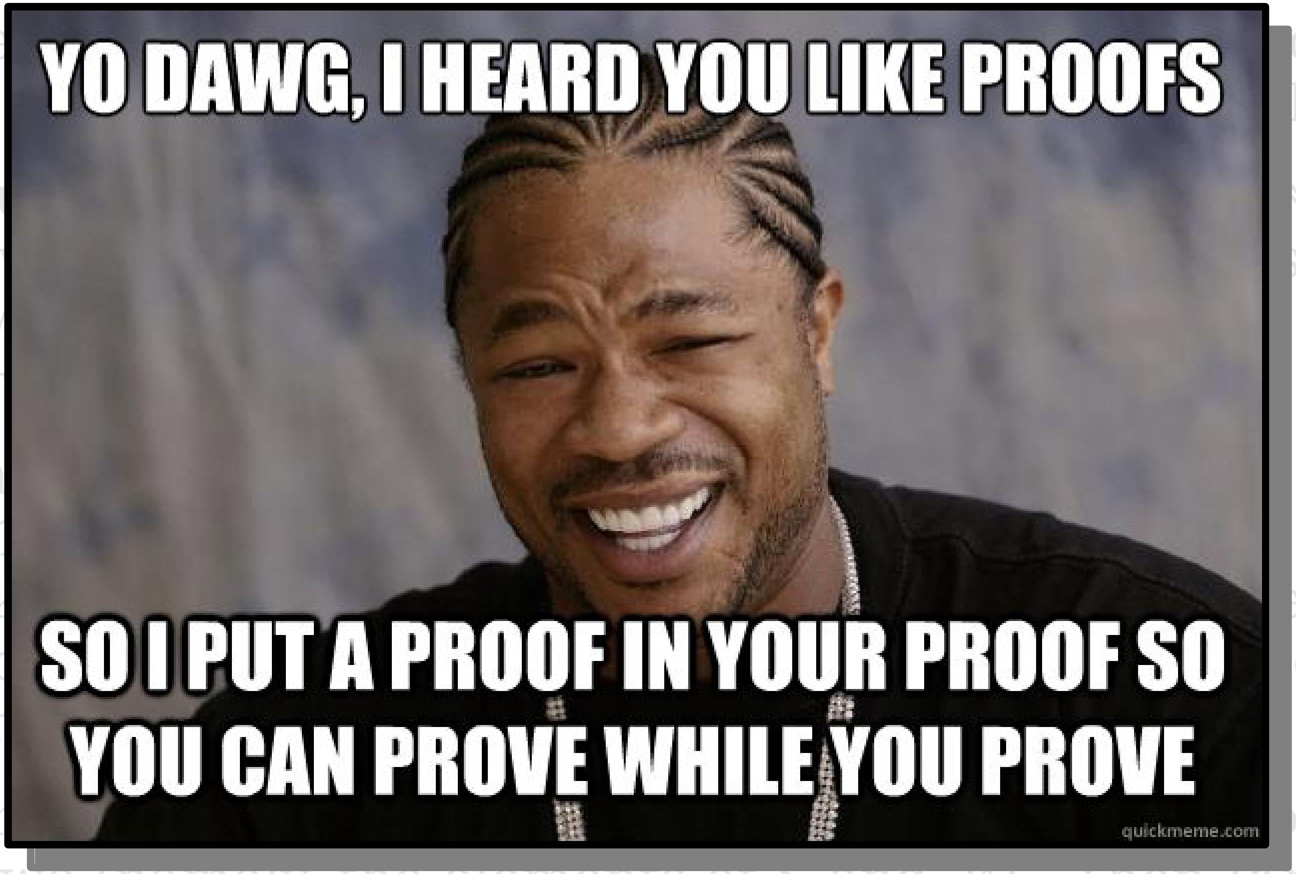
Theorem: Every $n \in \mathbb{N}$ is the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n is the sum of distinct powers of two." We prove that P(n) is true for all $n \in \mathbb{N}$.

As our base … ct powers
of 2. Since … P(0) holds.

For the ind… $\mathbb{N}$, that for
any $n' \in \mathbb{N}$ … sum of
distinct pow… distinct
powers of t…

Let 2^k be th… ider $n - 2^k$.
Since $2^k \geq$ … $< n$. Since
$2^k \leq n$, we … esis, $n - 2^k$
is the sum … e powers
of two, ther…



If we can sh… f distinct
powers of two (namely, the elements of S and 2^k). Then $P(n)$ will hold,
completing the induction.

We show $2^k \notin S$ by contradiction; assume that $2^k \in S$.

Theorem: Every $n \in \mathbb{N}$ is the sum of distinct powers of two.

Proof: By strong induction. Let P(n) be "n is the sum of distinct powers of two." We prove that P(n) is true for all $n \in \mathbb{N}$.

As our base case, we prove P(0), that 0 is the sum of distinct powers of 2. Since the empty sum of no powers of 2 is equal to 0, P(0) holds.

For the inductive step, assume that for some nonzero $n \in \mathbb{N}$, that for any $n' \in \mathbb{N}$ where $0 \leq n' < n$, that $P(n')$ holds and n' is the sum of distinct powers of two. We prove $P(n)$, that n is the sum of distinct powers of two.

Let 2^k be the greatest power of two such that $2^k \leq n$. Consider $n - 2^k$. Since $2^k \geq 1$ for any natural number k, we know that $n - 2^k < n$. Since $2^k \leq n$, we know $0 \leq n - 2^k$. Thus, by our inductive hypothesis, $n - 2^k$ is the sum of distinct powers of two. If S be the set of these powers of two, then n is the sum of the elements of S and 2^k.

If we can show that $2^k \notin S$, we will have that n is the sum of distinct powers of two (namely, the elements of S and 2^k). Then $P(n)$ will hold, completing the induction.

We show $2^k \notin S$ by contradiction; assume that $2^k \in S$. Since $2^k \in S$ and the sum of the powers of two in S is $n - 2^k$, this means that $2^k \leq n - 2^k$. Thus $2^k + 2^k \leq n$, so $2^{k+1} \leq n$. This contradicts that 2^k is the largest power of two no greater than n. We have reached a contradiction, so our assumption was wrong and $2^k \notin S$, as required. ■

Application: **Continued Fractions**

Continued Fractions

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

Continued Fractions

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

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

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

π 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 π

$\pi = 3$

$3 = \mathbf{3}.0000\ldots$

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 π

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

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

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

Greek mathematician **Archimedes** knew of this approximation, circa 250 BCE

Approximating π

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

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

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

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

355/113 = **3.141592**92...

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

Approximating π

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

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

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

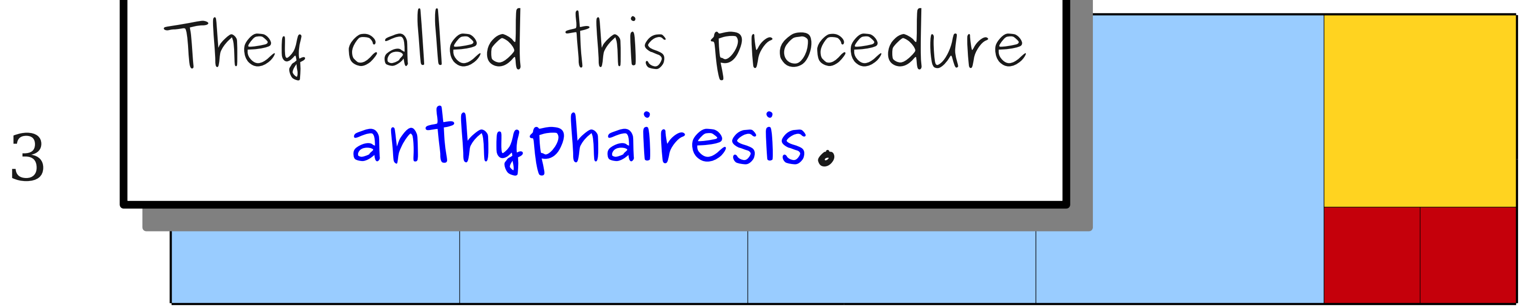
336/106 = **3.1415**094...

355/113 = **3.141592**92...

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

More Continued Fractions

The Ancient Greeks knew about this connection. They called this procedure anthyphairesis.



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

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

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

1 / 1

2 / 1

3 / 2

5 / 3

8 / 5

13 / 8

21 / 13

34 / 21

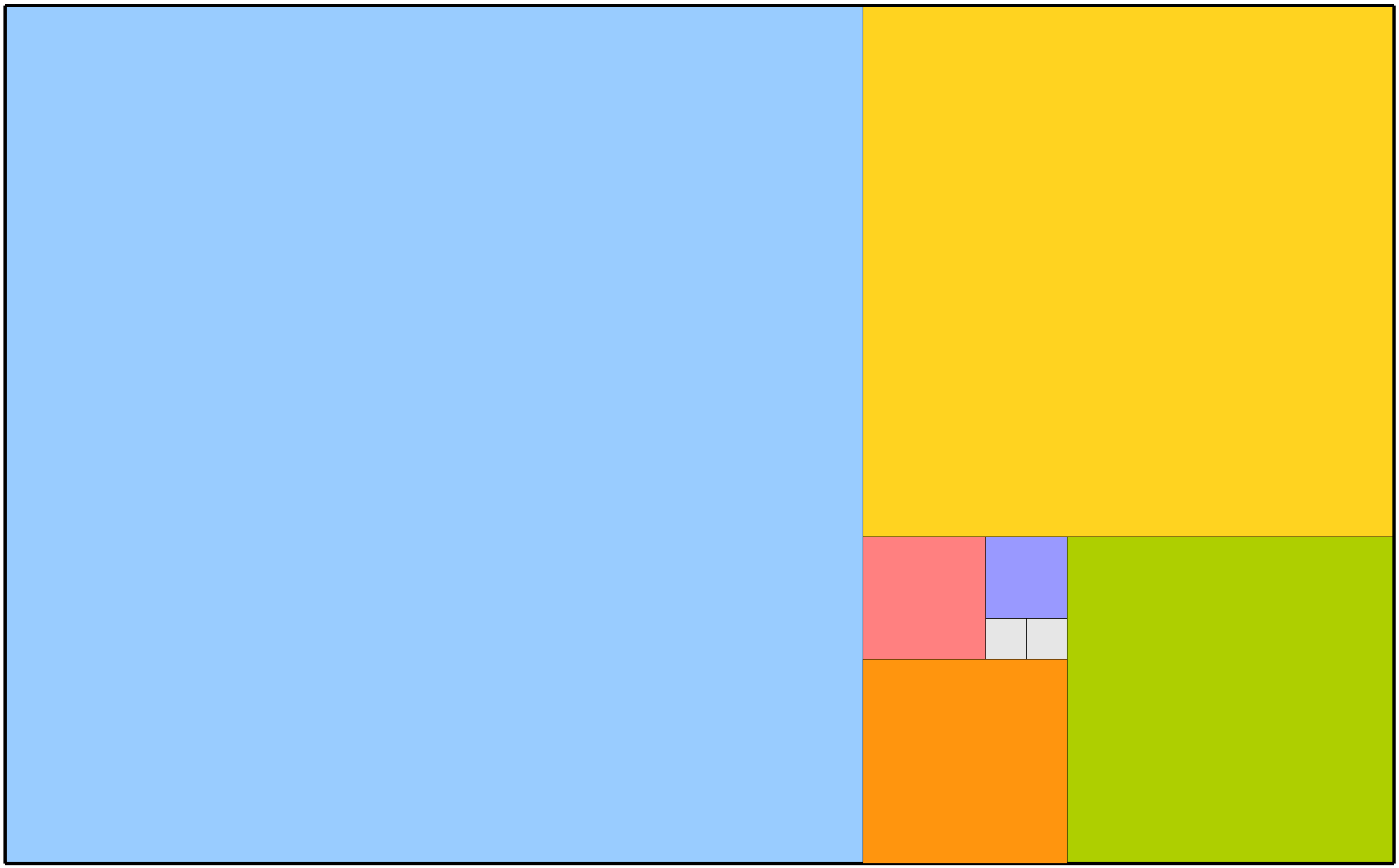
Each fraction is the ratio of consecutive Fibonacci numbers!

The Golden Ratio

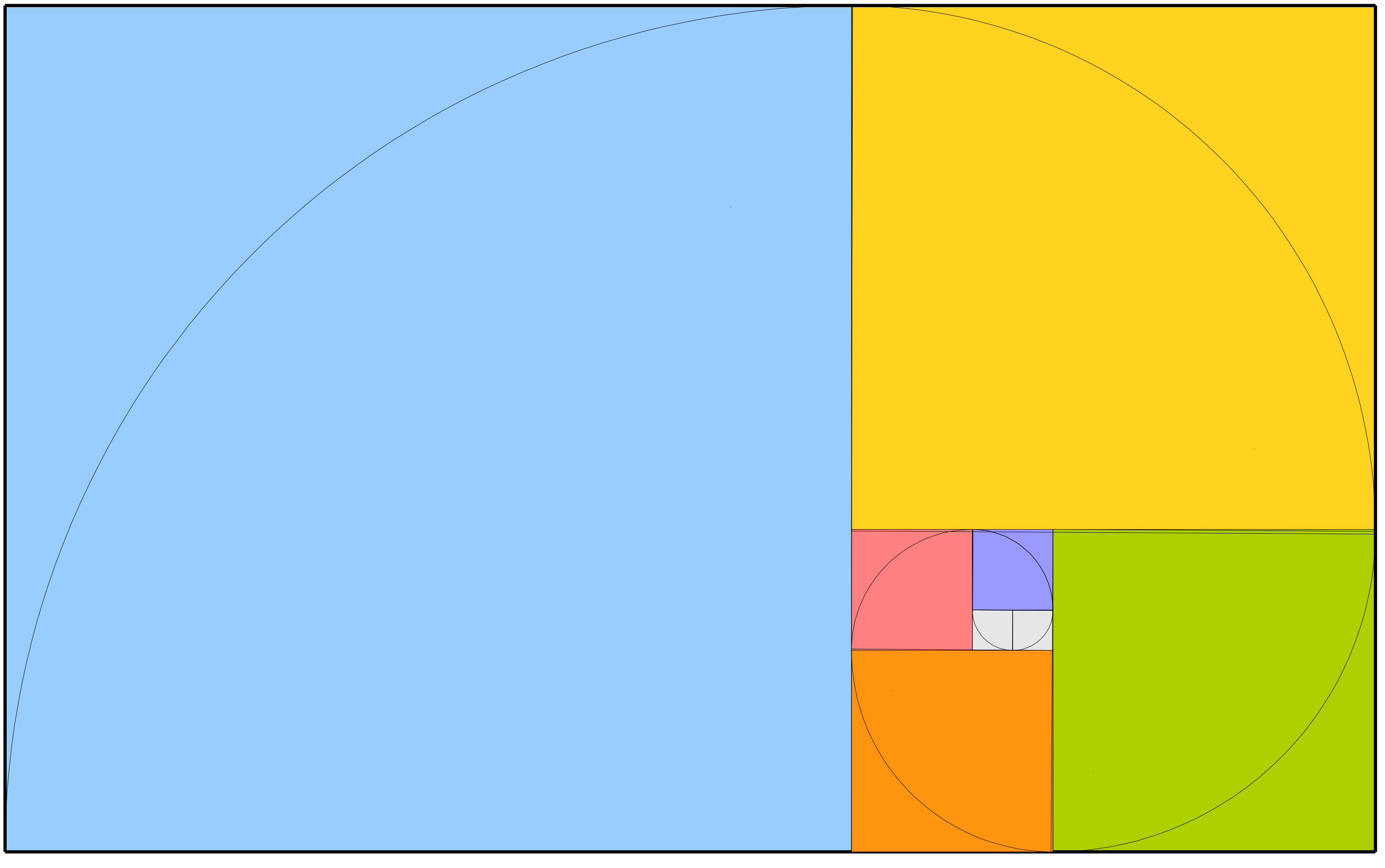
$$\varphi = \frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}}$$

$$\varphi \approx 1.61803399$$

The Golden Ratio



The Golden Spiral



How do we prove all rational numbers have continued fractions?

Constructing a Continued Fraction

$$\frac{7}{9} = 0 + \cfrac{1}{\cfrac{9}{7}}$$

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

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

Constructing a Continued Fraction

$$\frac{7}{9} = 0 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

Constructing a Continued Fraction

$$\frac{7}{\mathbf{9}} = 0 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}$$

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

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

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

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

The Division Algorithm

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

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

and

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

- $\boldsymbol{q}$ is the **quotient** and $\boldsymbol{r}$ is the **remainder**.
- Given $a = 11$ and $b = 4$: $11 = \mathbf{2} \cdot 4 + \mathbf{3}$
- Given $a = -137$ and $b = 42$: $-137 = \mathbf{-4} \cdot 42 + \mathbf{31}$

Theorem: Every rational has a continued fraction.

Proof: By strong induction. Let $P(d)$ be "any rational with denominator d has a continued fraction." We prove that $P(d)$ is true for all positive natural numbers. Since all rationals can be written with a positive denominator, this proves that all rationals have continued fractions.

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

For our inductive step, assume that for some $d \in \mathbb{N}$ with $d > 1$, that for any $d' \in \mathbb{N}$ where $1 \leq d' < d$, that $P(d')$ is true, so any rational with denominator d' has a continued fraction. We prove $P(d)$ by showing that any rational with denominator d has a continued fraction.

Take any rational with denominator d; let it be n / d. Using the division algorithm, write $n = qd + r$, where $0 \leq r < d$. We consider two cases:

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

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

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

For more on continued fractions:

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

Next Time

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