For all integers $n \geq 8$, n¢ can be obtained using 3¢ and 5¢ coins.

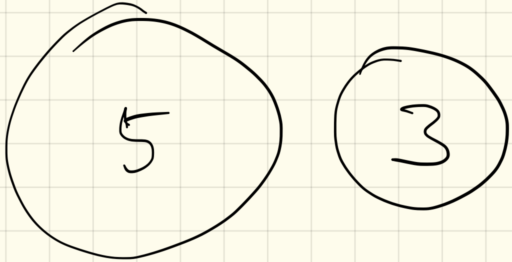
Base Case: For $n = 8$, 8¢ $=$ 3¢ $+$ 5¢.

Inductive Step: Suppose that m¢ can be obtained using 3¢ and 5¢ coins for any $m \geq 8$. We must show that $(m + 1)$¢ can be obtained using 3¢ and 5¢ coins.

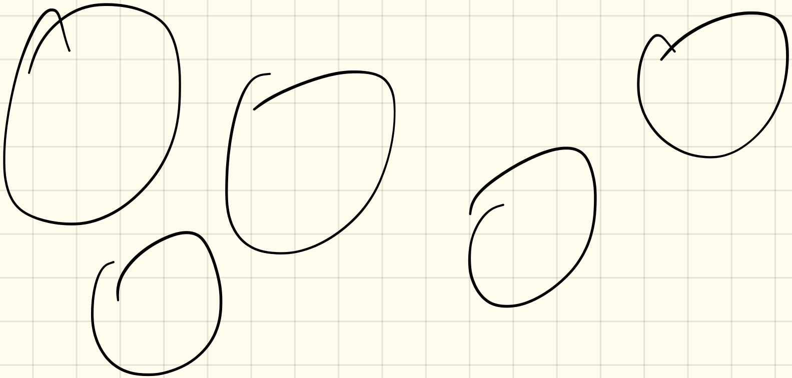
Consider cases

- There is a 5¢ coin among those used to make up the m¢.
  - Replace the 5¢ coin with two 3¢ coins. We obtain $(m + 1)$¢.
- There is no 5¢ coin among those used to make up the m¢.
  - There are three 3¢ coins ($m \geq 8$).
    - Replace the three 3¢ coins with two 5¢ coins

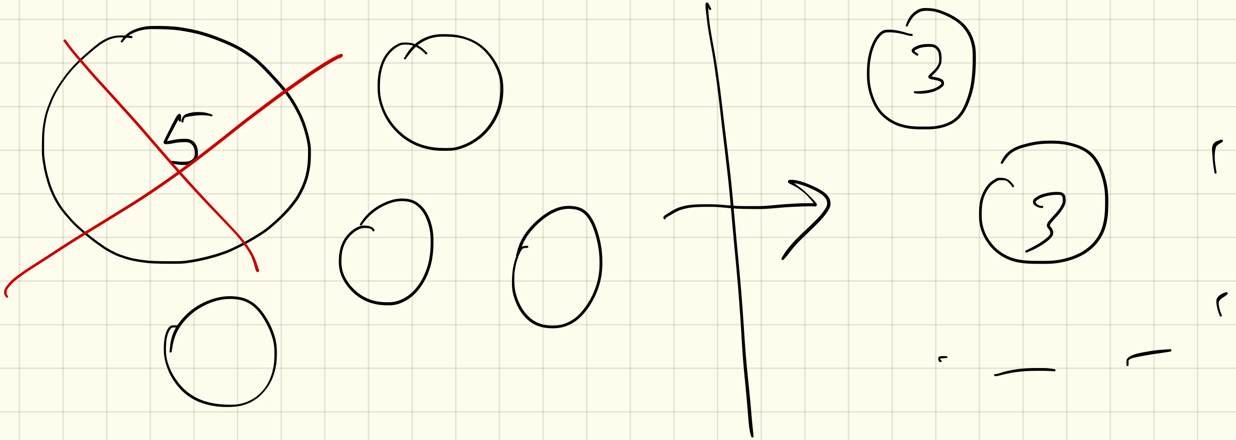
Base case for $n=8$



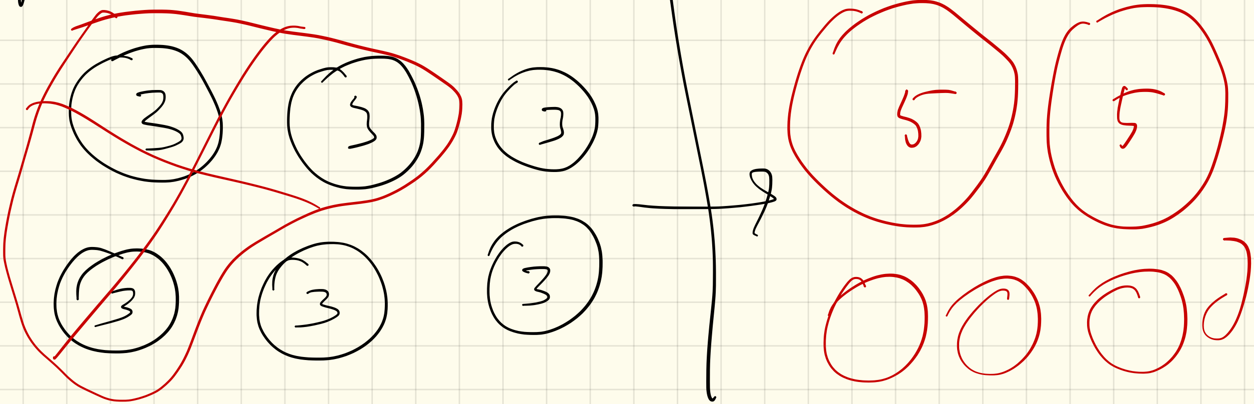
Inductive step Suppose you can give $n=m$ cents in 3 and 5 cent coins. Then you can give $n=m+1$ cents.



Case 1 There's one 5¢ coin



Case 2: No 5¢ coin on the table



Example: Proof by induction

For every integer $n \geq 3$, $4^n > 2^{n+2}$.

Base Case: Take $n = 3$. Then $4^n = 4^3 = 64$. Also, $2^{n+2} = 2^5 = 32$. So $4^n > 2^{n+2}$.

Inductive Step: For any $m \geq 3$, assume that the statement $4^m > 2^{m+2}$ is true. (This is called the "inductive hypothesis".) Now consider $n = m + 1$. We must show that $4^{m+1} > 2^{(m+1)+2} = 2^{m+3}$.

Here is the calculation. $4^{m+1} = 4 \times 4^m$. But by the inductive hypothesis, $4 \times 4^m > 4 \times 2^{m+2}$. Finally,

$$4 \times 2^{m+2} > 2 \times 2^{m+2} = 2^{m+3}.$$

For now define $\forall\, n \geq 1$, n is a natural number

$$n! = 1 \times 2 \times 3 \times \ldots \times n$$

Examples

$$1! = 1$$

$$2! = 1 \times 2 = 2$$

$$3! = 1 \times 2 \times 3 = 6$$

$$4! = 1 \times 2 \times 3 \times 4 = 24$$

$$\ldots$$

```
def fac(n):
    if n==1:
        return 1
    else:
        return n* fac(n-1)
```

Statement:

$\forall$ natural $n \geq 1$

fac(n) computes $n!$

Proof We prove this statement by mathematical induction

Base case: $n=1$ Then $fac(n) = fac(1) = 1 = 1!$

Inductive step

Assume that $fac(n) = n!$ for some $n = m$.

We need to show that $fac(n) = n!$ for $n = m+1$.

$fac(m) = m!$

$fac(m+1) = (m+1) * fac(m)$. By induction hypothesis,

$$fac(m+1) = (m+1) * m! = (m+1) * 1 * 2 * \ldots * m =$$

$$1 * 2 * \ldots * m * (m+1) = (m+1)!$$

So, $fac(n)$ computes $n!$

What does the following program do?

my list

```
i = 0
M = 0
mylist = [1, 2, 6, 3, 4, 5]
while i < len(mylist):
        M = max(M, mylist[i])
        i = i + 1
print M
```

iterations

	0	1	2	3	4	5	6	7
i	0	1	2	3	4	5	6	
M	0	1	2	6	6	6	6	

```
i = 0
M = 0
mylist = [1, 2, 6, 3, 4, 5]
while i < len(mylist):
        M = max(M, mylist[i])
        i = i + 1
print M
```

Property: After the statement M = max(M , mylist[i]) gets executed, the value of M is max(mylist[0],...,mylist[i]).

Proof by induction

Property: After the statement M = max(M, mylist[i]) gets executed, the value of M is max(mylist[0],...,mylist[i]).

Base Case: Take i=0. Before the statement, M=0, so the statement assigns M to be the maximum of 0 and mylist[0], which is mylist[0].

Inductive Step: Assume that the statement is true for i=m for some m$\geq$ 0. Now consider i=m+1. The statement assigns M to be the maximum of mylist[m+1] and max(mylist[0],...,mylist[m]), so after the statement, M is max(mylist[0],...,mylist[m+1]).

- Prove that the property holds for the natural number $n = 0$.
- Prove that **if** the property holds for $n = \cancel{0, 1, 2, \ldots,}\, m$ (and not just for m!) **then** it holds for $n = m + 1$.

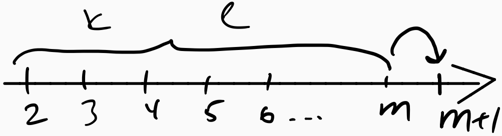
  $0, 1, 2, \ldots m$

Can also be used to prove a property for all integers greater than or equal to some particular natural number b

Every natural number $n \geq 2$, is a prime or a product of primes.

Base Case: Take $n = 2$. Then n is a prime number.

Inductive Step: Assume that the property holds for $n = m$ so *every* number i s.t. $2 \leq i \leq m$ is a prime or a produce of primes. Now consider $n = m + 1$.



Case 1: m+1 is prime

There is nothing to prove

Case 2 m+1 is composite. Then there exist k, l

natural numbers, k>1, l>1

Then k is either prime or a product of primes

ℓ is either prime or a product of primes.

But then $k \cdot \ell$ is a product of primes.

Example: Number of multiplications

For any integer $n \geq 1$, if $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

$$(\,:(((x_1 * x_2) * x_3) * x_4) \ldots * x_4)$$

$$(\ldots) * (\ldots)$$

Bad proofs: Arguing from example

An incorrect “proof” of the fact that the sum of any two even integers is even.

> *This is true because if $m = 14$ and $n = 6$, which are both even, then $m + n = 20$, which is also even.*

Bad proofs: Using the same letter to mean two different things

Consider the following "proof" fragment:

> *Suppose m and n are any odd integers. Then by definition of odd, $m = 2k + 1$ and $n = 2k + 1$ for some integer k.*

Bad proofs: Jumping to a conclusion

To jump to a conclusion means to allege the truth of something without giving an adequate reason.

> *Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then $m + n = 2r + 2s$. So $m + n$ is even.*

Bad proofs: Circular reasoning

To engage in circular reasoning means to assume what is to be proved.

> *Suppose m and n are any odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd.*

Bad proofs: Confusion between what is known and what is still to be shown

Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that

$$mn = 2s + 1.$$

Also by definition of odd, there exist integers a and b such that

$$m = 2a + 1 \; and \; n = 2b + 1.$$

Then

$$mn = (2a + 1)(2b + 1) = 2s + 1.$$

So, since s is an integer, mn is odd by definition of odd.

Good proofs in practice[2]

State your game plan.

> *A good proof begins by explaining the general line of reasoning, for example, "We use case analysis" or "We argue by contradiction."*

[2] *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.

Good proofs in Practice

Keep a linear flow.

> *Sometimes proofs are written like mathematical mosaics, with juicy titbits of independent reasoning sprinkled throughout. This is not good. The steps of an argument should follow one another in an intelligible order.*

Good proofs in practice

A proof is an essay, not a calculation.

> *Many students initially write proofs the way they compute integrals. The result is a long sequence of expressions without explanation, making it very hard to follow. This is bad. A good proof usually looks like an essay with some equations thrown in. Use complete sentences.*

Good proofs in practice

Structure your proof

- Theorem—A very important true statement.
- Proposition—A less important but still interesting statement.
- Lemma—A true statement used to prove other statements.
- Corollary—A simple consequence of a theorem or a proposition.

Finish

At some point in a proof, you'll have established all the essential facts you need. Resist the temptation to quit and leave the reader to draw the "obvious" conclusion. Instead, tie everything together yourself and explain why the original claim follows.