Monday November 8

For which nonnegative integers n can we make change for n with coins of value 5 cents and 3 cents?

Restating: We can make change for __________, we cannot make change for _______________, and

______________________________________ $\star$

New! Proof by Strong Induction (Rosen 5.2 p337)
To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

Basis Step:	Show the statement holds for b, $b+1$, $\ldots$, $b+j$.
Recursive Step:	Consider an arbitrary integer n greater than or equal to $b+j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b+1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n+1$.

$\mathbb{N}$	The set of natural numbers	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^{\geq b}$	The set of integers greater than or equal a basis element b	$\{b, b+1, b+2, b+3, \ldots\}$

Proof of $\star$ by mathematical induction ($b = 8$)

Basis step: WTS property is true about 8

Recursive step: Consider an arbitrary $n \geq 8$. Assume (as the IH) that there are nonnegative integers x, y such that $n = 5x + 3y$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$. We consider two cases, depending on whether any 5 cent coins are used for n.

Case 1: Assume $x \geq 1$. Define $x' = x - 1$ and $y' = y + 2$ (both in $\mathbb{N}$ by case assumption).

Calculating:

$$5x' + 3y' \overset{\text{by def}}{=} 5(x-1) + 3(y+2) = 5x - 5 + 3y + 6$$
$$\overset{\text{rearranging}}{=} (5x + 3y) - 5 + 6$$
$$\overset{\text{IH}}{=} n - 5 + 6 = n + 1$$

Case 2: Assume $x = 0$. Therefore $n = 3y$, so since $n \geq 8$, $y \geq 3$. Define $x' = 2$ and $y' = y - 3$ (both in $\mathbb{N}$ by case assumption). Calculating:

$$5x' + 3y' \overset{\text{by def}}{=} 5(2) + 3(y-3) = 10 + 3y - 9$$
$$\overset{\text{rearranging}}{=} 3y + 10 - 9$$
$$\overset{\text{IH and case}}{=} n + 10 - 9 = n + 1$$

Proof of $\star$ by strong induction ($b = 8$ and $j = 2$)

Basis step: WTS property is true about $8, 9, 10$

Recursive step: Consider an arbitrary $n \geq 10$. Assume (as the IH) that the property is true about each of $8, 9, 10, \ldots, n$. WTS that there are nonnegative integers x', y' such that $n + 1 = 5x' + 3y'$.

Representing positive integers

Theorem: Every positive integer is a sum of (one or more) distinct powers of 2. *binary expansions exist!*

Proof by strong induction, with $b = 1$ and $j = 0$.

Basis step: WTS property is true about 1.

Recursive step: Consider an arbitrary integer $n \geq 1$. Assume (as the IH) that the property is true about each of $1, \ldots, n$. WTS that the property is true about $n + 1$.

Review

1. Consider the following statement: For $n > 0$, the sum of the first n positive integers, also written as $\sum_{i=1}^{n} i$, is equal to

$$\left(\frac{n \cdot (n+1)}{2}\right)$$

.

For example, when $n = 3$, the statement would mean that $1+2+3 = \left(\frac{3 \cdot (3+1)}{2}\right)$.

Consider the following (start to) a proof of this statement:

Basis Step: Choose $n = 1$ as the basis step. Applying the formula from the original statement, we find that $\frac{1 \cdot (1+1)}{2}$ is equal to 1. Since the total sum of the first positive integer is 1, these are equal and the basis step is complete.

Recursive Step: Consider an arbitrary $k \geq 1$. Towards a direct proof, we assume (as the induction hypothesis) that the sum of the first k positive integers is $\left(\frac{k \cdot (k+1)}{2}\right)$. We want to show that the sum of the first $k+1$ positive integers is

$$\left(\frac{(k+1) \cdot ((k+1)+1)}{2}\right)$$

.

[Proof would continue here...]

   (a) In a recursive definition of the function that gives the sum of the first n positive integers, the domain is

      i. $\mathbb{N}$
      ii. $\mathbb{Z}^+$
      iii. $\mathbb{Z}$

   (b) In a recursive definition of the function that gives the sum of the first n positive integers, the basis step is

      i. $\sum_{i=1}^{1} i = 1$
      ii. $\sum_{i=1}^{n} 1 = n$
      iii. None of the above.

   (c) In a recursive definition of the function that gives the sum of the first n positive integers, the recursive step is

      i. If n is a positive integer, $\sum_{i=1}^{n} i = n$
      ii. If n is a positive integer, $\sum_{i=1}^{n} i = (\sum_{i=1}^{n} i) + 1$
      iii. If n is a positive integer, $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + 1$
      iv. If n is a positive integer, $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + n$
      v. If n is a positive integer, $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1)$

   (d) The proof technique used here is:

      i. Structural induction
      ii. Mathematical induction

iii. Strong induction

(e) Which of these is both true, and a useful next step in the proof?

i. By the induction hypothesis, we know that

$$\left(\frac{(k+1)\cdot((k+1)+1)}{2}\right) = \left(\frac{k\cdot(k+1)}{2}\right)$$

ii. By the induction hypothesis, we know that

$$\left(\frac{(k+1)\cdot((k+1)+1)}{2}\right) > \left(\frac{k\cdot(k+1)}{2}\right)$$

iii. By the induction hypothesis and the definition of the statement we're proving, we know that

$$\left(\frac{k\cdot(k+1)}{2}\right) + k$$

is the sum of the first $k+1$ positive integers.

iv. By the induction hypothesis and the definition of the statement we're proving, we know that

$$\left(\frac{k\cdot(k+1)}{2}\right) + k + 1$$

is the sum of the first $k+1$ positive integers.

v. None of the above

Recall that an integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p. Fill in the following blanks in the proof of the **Theorem** (Rosen p336): Every positive integer *greater than 1* is a product of (one or more) primes.

Proof: We proceed by ___BLANK for part (a)___.

2. Basis step: We want to show that the property is about 2. Since 2 is itself prime, it is already written as a product of (one) prime.

Recursive step: Consider an arbitrary integer $n \geq 2$. Assume, as the induction hypothesis, that ___BLANK for part (c)___. We want to show that $n+1$ can be written as a product of primes. There are two cases to consider: $n+1$ is itself prime or it is composite. In the first case, we assume $n+1$ is prime and then immediately it is written as a product of (one) prime so we are done. In the second case, we assume that $n+1$ is composite so there are integers x and y where $n+1 = xy$ and each of them is between 2 and n (inclusive). Therefore, the induction hypothesis applies to each of x and y so each of these factors of $n+1$ can be written as a product of primes. Multiplying these products together, we get a product of primes that gives $n+1$, as required. Since both cases give the necessary conclusion, the proof by cases for the recursive step is complete.

(a) The proof technique used here is:

i. Structural induction

ii. Mathematical induction

iii. Strong induction

(b) How many basis steps are used in this proof?

(c) What is the induction hypothesis?

i. That n can be written as a product of (one or more) primes.
ii. That each integer between 0 and n (inclusive) can be written as a product of (one or more) primes.
iii. That each integer between 1 and $n + 1$ (inclusive) can be written as a product of (one or more) primes.
iv. That each integer between 2 and n (inclusive) can be written as a product of (one or more) primes.
v. That each integer between 3 and $n + 1$ (inclusive) can be written as a product of (one or more) primes.

Wednesday November 10

New! Proof by Strong Induction (Rosen 5.2 p337)
To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

Basis Step:	Show the statement holds for b, $b+1$, $\ldots$, $b+j$.
Recursive Step:	Consider an arbitrary integer n greater than or equal to $b+j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b+1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n+1$.

$\mathbb{N}$	The set of natural numbers	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}^{\geq b}$	The set of integers greater than or equal a basis element b	$\{b, b+1, b+2, b+3, \ldots\}$

Definition: An integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Theorem: Every positive integer *greater than 1* is a product of (one or more) primes.

Proof by strong induction, with $b = 2$ and $j = 0$.

Basis step: WTS property is true about 2.

Recursive step: Consider an arbitrary integer $n \geq 2$. Assume (as the IH) that the property is true about each of $2, \ldots, n$. WTS that the property is true about $n+1$.

Case 1:

Case 2:

Review

1. Recall that an integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p. Fill in the following blanks in the proof of the **Theorem** (Rosen p336): Every positive integer *greater than 1* is a product of (one or more) primes.

   Proof: We proceed by ___BLANK for part (a)___.

   Basis step: We want to show that the property is about 2. Since 2 is itself prime, it is already written as a product of (one) prime.

   Recursive step: Consider an arbitrary integer $n \geq 2$. Assume, as the induction hypothesis, that ___BLANK for part (c)___. We want to show that $n+1$ can be written as a product of primes. There are two cases to consider: $n+1$ is itself prime or it is composite. In the first case, we assume $n+1$ is prime and then immediately it is written as a product of (one) prime so we are done. In the second case, we assume that $n+1$ is composite so there are integers x and y where $n+1 = xy$ and each of them is between 2 and n (inclusive). Therefore, the induction hypothesis applies to each of x and y so each of these factors of $n+1$ can be written as a product of primes. Multiplying these products together, we get a product of primes that gives $n+1$, as required. Since both cases give the necessary conclusion, the proof by cases for the recursive step is complete.

   (a) The proof technique used here is:

      i. Structural induction
      ii. Mathematical induction
      iii. Strong induction

   (b) How many basis steps are used in this proof?

(c) What is the induction hypothesis?

i. That n can be written as a product of (one or more) primes.
ii. That each integer between 0 and n (inclusive) can be written as a product of (one or more) primes.
iii. That each integer between 1 and $n+1$ (inclusive) can be written as a product of (one or more) primes.
iv. That each integer between 2 and n (inclusive) can be written as a product of (one or more) primes.
v. That each integer between 3 and $n+1$ (inclusive) can be written as a product of (one or more) primes.

Friday November 12

Definition: An integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

New! Proof by Contradiction
To prove that a statement p is true, pick another statement r and once we show that $\neg p \to (r \wedge \neg r)$ then we can conclude that p is true.
Informally The statement we care about can't possible be false, so it must be true.

Prove or **disprove**: There is a least prime number.

Prove or **disprove**: There is a greatest integer.

Approach 1, De Morgan's and universal generalization:

Approach 2, proof by contradiction:

Extra examples: Prove or disprove that $\mathbb{N}$, $\mathbb{Q}$ each have a least and a greatest element. Prove that there is no greatest prime number.

The **set of rational numbers**, $\mathbb{Q}$ is defined as

$$\left\{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0\right\} \quad \text{or, equivalently,} \quad \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \exists q \in \mathbb{Z}^+ (p = x \cdot q)\}$$

Extra practice: Use the definition of set equality to prove that the definitions above give the same set.

Goal: The square root of 2 is not a rational number. In other words: $\neg \exists x \in \mathbb{Q}(x^2 - 2 = 0)$

Attempted proof: The definition of the set of rational numbers is the collection of fractions p/q where p is an integer and q is a nonzero integer. Looking for a **witness** p and q, we can write the square root of 2 as the fraction $\sqrt{2}/1$, where 1 is a nonzero integer. Since the numerator is not in the domain, this witness is not allowed, and we have shown that the square root of 2 is not a fraction of integers (with nonzero denominator). Thus, the square root of 2 is not rational.

The problem in the above attempted proof is that ____

Proof:

Lemma 1: For every two integers p and q, not both zero, $gcd\left(\frac{p}{gcd(p,q)}, \frac{q}{gcd(p,q)}\right) = 1$.

Lemma 2: For every two integers a and b, not both zero, with $gcd(a, b) = 1$, it is not the case that both a is even and b is even.

Lemma 3: For every integer x, x is even if and only if x^2 is even.

Greatest common divisor Let a and b be integers, not both zero. The largest integer d such that d is a factor of a and d is a factor of b is called the greatest common divisor of a and b and is denoted by $gcd(a, b)$.

Review

1. *Goals for this question: recognize that we can prove the same statement in different ways. Trace proofs and justify why they are valid.*

   By definition, an integer n is **even** means that there is an integer a such that $n = 2a$; an integer n is **odd** means that there is an integer a such that $n = 2a + 1$. Equivalently, an integer n is **even** means $n \mod 2 = 0$; an integer n is **odd** means $n \mod 2 = 1$. Also, an integer is even if and only if it is not odd.

   You can refer to any of the above definitions and claims in your proofs.

   Below are two proofs of the same statement: fill in the blanks with the expressions below.

   Claimed statement: **(a)**________________

   > **Proof 1**: Using De Morgan's law for quantifiers, we can rewrite this statement as a universal of the negation of the body of the statement. Towards a proof by universal generalization, let x be an arbitrary element of $\mathbb{Z}$. Then we need to show that
   >
   > **(b)**________________
   >
   > We proceed by contradiction to show that
   >
   > $$(x \text{ is odd} \wedge x^2 \text{ is even}) \rightarrow \textbf{(c)}\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_$$
   >
   > We assume by direct proof that (x is odd $\wedge$ x^2 is even). Then, (x^2 is even) follows directly from this assumption, so by definition of conjunction, we must show that (x^2 is not even) to complete the proof. From the assumption, we have that (x is odd). Applying the definition of odd, $x = 2k + 1$ for some $k \in \mathbb{Z}$. Then $x^2 = 4k^2 + 4k + 1$. We can rewrite the right hand side to $2(2k^2 + 2k) + 1$. This shows that x^2 is odd by the definition of odd, since choosing $j = 2k^2 + 2k$ gives us $j \in \mathbb{Z}$ with $x^2 = 2j + 1$. Since a number is either even or odd and not both, and x^2 is odd, then it must not be even. This concludes the proof, as we have assumed the negation of the original statement and deduced a contradiction from this assumption.

Proof 2:

1.	**To Show** $\forall x \in \mathbb{Z} \neg(x \text{ is odd} \wedge x^2 \text{ is even})$	Rewriting statement using De Morgan's law for quantifiers
2.	**Choose arbitrary** $x \in \mathbb{Z}$ **To Show (d)**_______________	By **(e)**_______________
3.	**To Show** x is odd $\rightarrow \neg(x^2 \text{ is even})$	Rewrite previous **To Show** using logical equivalence
4.	**Assume** x is odd **To Show** $\neg(x^2 \text{ is even})$	By **(f)**_______________
5.	**To Show** x^2 is odd	Rewrite previous **To Show** using definition of even, odd
6.	**Use the witness** k, an integer, where $x = 2k + 1$	By existential definition of x being odd
7.	**Choose the witness** $j = 2k^2 + 2k$, an integer **To Show** $x^2 = 2j + 1$	Show this new **To Show** is true to prove the existential definition of x^2 being odd
8.	**To Show** $(2k + 1)^2 = 2j + 1$	Rewrite previous **To Show** using definition of k
9.	**To Show** $(2k + 1)^2 = 2(2k^2 + 2k) + 1$	Rewrite previous **To Show** using definition of j
10.	**To Show** T	By algebra: multiplying out the LHS; factoring the RHS
QED		Because we got to T only by rewriting **To Show** to equivalent statements, using valid proof techniques and definitions.

Consider the following expressions as options to fill in the two proofs above. Give your answer as one of the numbers below for each blank a-c. You may use some numbers for more than one blank, but each letter only uses one of the expressions below.

i. $\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x^2 \text{ is even})$
ii. $\neg\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x^2 \text{ is even})$
iii. $\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x \text{ is even})$
iv. $\neg\exists x \in \mathbb{Z}\,(x \text{ is odd} \wedge x \text{ is even})$
v. $\exists x \in \mathbb{Z}\,(x^2 \text{ is odd} \wedge x^2 \text{ is even})$
vi. $\neg\exists x \in \mathbb{Z}\,(x^2 \text{ is odd} \wedge x^2 \text{ is even})$
vii. $(x^2 \text{ is even} \wedge x^2 \text{ is not even})$
viii. $\neg(x \text{ is odd} \wedge x^2 \text{ is even})$
ix. $(x \text{ is odd} \wedge x^2 \text{ is even})$
x. $(x \text{ is odd} \wedge x \text{ is not odd})$
xi. $\neg(x \text{ is odd} \wedge x \text{ is not odd})$
xii. x^2 is even
xiii. x^2 is odd
xiv. universal generalization
xv. proof by cases
xvi. direct proof
xvii. proof by contraposition
xviii. proof by contradiction

2. *Goals for this question: Reason through multiple nested quantifiers. Fluently use the definition and properties of the set of rationals.*

   Recall the definition of the set of rational numbers, $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$. We define the set of **irrational** numbers $\overline{\mathbb{Q}} = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.

   (i) $\forall x \in \mathbb{Q}\ \forall y \in \mathbb{Q}\ \exists z \in \mathbb{Q}\ (x + y = z)$

   (ii) $\forall x \in \mathbb{Q}\ \forall y \in \mathbb{Q}\ \exists z \in \mathbb{Q}\ (x + z = y)$

   (iii) $\forall x \in \mathbb{Q}\ \forall y \in \mathbb{Q}\ \exists z \in \mathbb{Q}\ (x \cdot y = z)$

   (iv) $\forall x \in \mathbb{Q}\ \forall y \in \mathbb{Q}\ \exists z \in \mathbb{Q}\ (x \cdot z = y)$

   (v) $\forall x \in \overline{\mathbb{Q}}\ \forall y \in \overline{\mathbb{Q}}\ \exists z \in \overline{\mathbb{Q}}\ (x + y = z)$

   (vi) $\forall x \in \overline{\mathbb{Q}}\ \forall y \in \overline{\mathbb{Q}}\ \exists z \in \overline{\mathbb{Q}}\ (x + z = y)$

   (vii) $\forall x \in \overline{\mathbb{Q}}\ \forall y \in \overline{\mathbb{Q}}\ \exists z \in \overline{\mathbb{Q}}\ (x \cdot y = z)$

   (viii) $\forall x \in \overline{\mathbb{Q}}\ \forall y \in \overline{\mathbb{Q}}\ \exists z \in \overline{\mathbb{Q}}\ (x \cdot z = y)$

   (a) Which of the statements above (if any) could be **disproved** using the counterexample $x = \frac{1}{2}$, $y = \frac{3}{4}$?

   (b) Which of the statements above (if any) could be **disproved** using the counterexample $x = \sqrt{4}$, $y = \sqrt{3}$?

   (c) Which of the statements above (if any) could be **disproved** using the counterexample $x = 0$, $y = 3$?

   (d) Which of the statements above (if any) could be **disproved** using the counterexample $x = \sqrt{2}$, $y = 0$?

   (e) Which of the statements above (if any) could be **disproved** using the counterexample $x = \sqrt{2}$, $y = -\sqrt{2}$?

   Hint: we proved in class that $\sqrt{2} \notin \mathbb{Q}$. You may also use the facts that $\sqrt{3} \notin \mathbb{Q}$ and $-\sqrt{2} \notin \mathbb{Q}$.

   Bonus - not to hand in: prove these facts; that is, prove that $\sqrt{3} \notin \mathbb{Q}$ and $-\sqrt{2} \notin \mathbb{Q}$.

