Alpha (counting on her fingers furiously): According to my calculations, $62^2 = 3844$, and 3844 is clearly even...

Beta: Hold on. It's not so clear to me that 3844 is even. The definition says that 3844 is even if there exists an integer y such that $3844 = 2y$. If you want to go around saying that 3844 is even, you have to *produce* an integer y that works.

Alpha: How about $y = 1922$.

Beta: Yes, you have a point there. So you've shown that the sentence 'if x is even, then x^2 is even' is true when $x = 17$ and when $x = 62$. But there are *billions* of integers that x could be. How do you know you can do this for every one?

Alpha: Let x be any integer.

Beta: Which integer?

Alpha: Any integer at all. It doesn't matter which one. I'm going to show you, using only the fact that x is an integer and nothing else, that if x is even then x^2 is even.

Beta: All right, go on.

Alpha: So suppose x is even.

Beta: But what if it isn't?

Alpha: If x isn't even, then the statement 'if x is even, then x^2 is even' is vacuously true. The only time I have anything to worry about is when x is even.

Beta: OK, so what do you do when x is even?

Alpha: By the definition of 'even', we know that there exists at least one integer y such that $x = 2y$.

Beta: Only one, actually.

Alpha: I think so. Anyway, let y be an integer such that $x = 2y$. Squaring both sides of this equation, we get $x^2 = 4y^2$. Now to prove that x^2 is even, I have to exhibit an integer, twice which is x^2.

Beta: Doesn't $2y^2$ work?

We can also use our 'and' statement to conclude that y is odd. We write

> Since y is odd, choose an integer v such that $y = 2v + 1$.

Now we need to show that xy is odd. We can do this as follows:

> Then $xy = 4vw + 2v + 2w + 1$. Let $z = 2vw + v + w$; then $xy = 2z + 1$, so xy is odd. □

Next, we will illustrate how to prove and use 'if and only if' statements. The proof of a statement of the form $p \iff q$ usually looks like this:

> ($\Rightarrow$) [proof that $p \Rightarrow q$]
>
> ($\Leftarrow$) [proof that $q \Rightarrow p$]
>
> □

Example. Write a proof that for every integer x, x is even if and only if $x + 1$ is odd.

> Let x be any integer. We must show x is even if and only if $x + 1$ is odd.
>
> ($\Rightarrow$) Suppose x is even. Choose an integer y such that $x = 2y$. Then y is also an integer such that $x + 1 = 2y + 1$, so $x + 1$ is odd.
>
> ($\Leftarrow$) Suppose $x + 1$ is odd. Choose an integer y such that $x + 1 = 2y + 1$. Then y is also an integer such that $x = 2y$, so x is even.
> □

Now we can conclude that for any integer x, the statements 'x is even' and '$x + 1$ is odd' are **interchangeable**; this means that we can take any true statement and replace some occurrences of the phrase 'x is even' with the phrase '$x + 1$ is odd' to get another true statement. For example, mathematicians Alpha and Beta proved in the dialogue that

> For every integer x, if x is even then x^2 is even

So the following is also a true statement:

> For every integer x, if $x + 1$ is odd then x^2 is even.

Remark. All the statements we are proving here about even and odd numbers can be proved more simply using some basic facts about mod 2 arithmetic. However our aim here is to illustrate the fundamental rules of mathematical proofs by giving unusually detailed proofs of some facts which you probably already know.

Exercises.

1. Prove the following statements:

   (a) For every integer x, if x is even, then for every integer y, xy is even.

   (b) For every integer x and for every integer y, if x is odd and y is odd then $x + y$ is even.

   (c) For every integer x, if x is odd then x^3 is odd.

   What is the negation of each of these statements?

2. Prove that for every integer x, $x + 4$ is odd if and only if $x + 7$ is even.

3. Figure out whether the statement we negated in §1.3 is true or false, and prove it (or its negation).

4. Prove that for every integer x, if x is odd then there exists an integer y such that $x^2 = 8y + 1$.

3 More proof techniques

3.1 Proof by cases

We will consider next how to make use of 'or' statements. The first entry in the box in the table is what we call "proof by cases". This is best explained by an example.

Example. For every integer x, the integer $x(x + 1)$ is even.

Proof. Let x be any integer. Then x is even or x is odd. (Some people might consider this too obvious to require a proof, but a proof can be given using the Division Theorem, see §4.2, which here tells us that every integer can be

By assumption this set is nonempty, so it contains a least element n_0. Now $n_0 \neq 1$, because we know that $P(1)$ is true. So $n_0 > 1$. Then $n_0 - 1$ is a positive integer, and since it is smaller than n_0, it is not in the set S. Thus $P(n_0 - 1)$ is true. But $P(n_0 - 1)$ implies $P(n_0)$, so $P(n_0)$ is true. Thus $n_0 \notin S$, a contradiction. □

There are some variants of the well-ordering principle which are easily seen to be equivalent to it. For example any nonempty set of integers (possibly negative) with a lower bound has a least element, and any nonempty set of integers with an upper bound has a largest element. (A **lower bound** on S is a number L such that $x \geq L$ for all $x \in S$. An **upper bound** on S is a number U such that $x \leq U$ for all $x \in S$. A **largest element** of S is an element $x \in S$ such that $x \geq y$ for all $y \in S$.)

A useful application of the well-ordering principle is the following:

Division theorem. If a and b are integers with $b > 0$, then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

(The integer q is the "quotient" when a is divided by b, and r is the **remainder**. In elementary school you learned an algorithm for finding q and r. But let's now prove that they exist and are unique.)

Proof. The idea is that we want q to be the largest integer such that $a \geq qb$. So let

$$S := \{q \in \mathbb{Z} \mid a - qb \geq 0\}.$$

This set is nonempty; for example $-|a| \in S$ since $b > 0$. It also has an upper bound, since $a - qb \geq 0$ implies $q \leq |a|$. So by the well ordering principle, S contains a largest element q. Let $r = a - qb$. Then $r \geq 0$ by definition of S. Also $r < b$, or else we would have $a - (q+1)b = r - b \geq 0$, so $q + 1 \in S$, contradicting the fact that q is the largest element of S. So q and r exist.

Uniqueness is pretty easy to see; if q is any smaller then the remainder will be too big. But let us prove uniqueness using our standard strategy. Suppose $a = qb + r = q'b + r'$ with $0 \leq r, r' < b$. Subtracting we obtain $(q - q')b = r' - r$. We must have $q - q' = 0$, because there is no way to obtain a nonzero multiple of b by subtracting two elements of the set $\{0, 1, \ldots, b-1\}$, because the largest difference between any two elements of this set is $b - 1$. Since $q - q' = 0$, it follows that $r - r' = 0$ also. This proves uniqueness. □

Exercises.