Exercises 1.1: 3, 4(a)(b)(c) (I do not insist that you prove these by induction – any logically correct proof will do!).

3. Prove that the square of an even number is even and the square of an odd number is odd.

By definition, an integer \( a \) is even if you can write \( a = 2n \) for some \( n \in \mathbb{Z} \), and odd if you can write \( a = 2n + 1 \) for some \( n \in \mathbb{Z} \).

Suppose \( a \) is even, so \( a = 2n \). Then \( a^2 = 4n^2 = 2.2n^2 \). Since this is 2 times another integer, so it is even.

Suppose \( a \) is odd, so \( a = 2n + 1 \). Then \( a^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1 \). Since this is 2 times an integer plus 1, it is odd.

4(a) I did this one in class on Monday.

4(b) The sum of the first \( n \) odd integers is \( n^2 \).

Proceed by induction on \( n \). We need to show that

\[
1 + 3 + \cdots + (2n-1) = n^2.
\]

Base case: If \( n = 1 \), LHS = 1 and RHS = 1\(^2\) = 1 so true.

Induction step: Assume the formula is true for \( n = k \), i.e.

\[
1 + 3 + \cdots + (2k-1) = k^2.
\]

Now using this we need to deduce that the formula is true for \( n = k + 1 \). Add \((2k + 1)\) to both sides to get

\[
1 + 3 + \cdots + (2k-1) + (2k + 1) = k^2 + 2k + 1.
\]

Factorizing the RHS gives

\[
1 + 3 + \cdots + (2k-1) + (2k + 1) = (k + 1)^2.
\]

This is exactly the formula we want for \( n = k + 1 \), so now we are done by induction.

4(c) The sum of the squares of the first \( n \) positive integers is \( \frac{1}{6}n(n+1)(2n+1) \).

Proceed by induction on \( n \).

Base case: \( 1 = 1 \), surely true!

Induction step: Assume the formula is true for \( n = k \), i.e.

\[
1^2 + 2^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1).
\]

Add \((k + 1)^2\) to both sides to get

\[
1^2 + 2^2 + \cdots + k^2 + (k + 1)^2 = \frac{1}{6}k(k+1)(2k+1) + (k + 1)^2.
\]
Now we simplify the RHS

\[
\frac{1}{6} k(k+1)(2k+1) + (k+1)^2 = \frac{1}{6} (k+1)(k(2k+1) + 6(k+1))
\]

\[
= \frac{1}{6} (k+1)(2k^2 + 7k + 6)
\]

\[
= \frac{1}{6} (k+1)(k+2)(2k+3).
\]

We have now shown that

\[
1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{1}{6} (k+1)(k+2)(2(k+1) + 1)
\]

which is the formula we were after with \(n = k+1\). Now we are done by induction.

- Exercises 1.2: 1(a)(c)(e), 3, 4, 6
  1(a) Write \(\text{GCD}(14, 35)\) as \(m.14 + n.35\) for integers \(m, n\).
  Write 35 = 2.14 + 7. Since 7|14, we stop here, the GCD equals 7. Moreover, 7 = 35 − 2.14.
  1(c) I did this one in class – look back through your notes!
  1(e) Write \(\text{GCD}(512, 360)\) as \(m.512 + n.360\).
  We have

\[
\begin{align*}
512 &= 360 + 152 \\
360 &= 2.152 + 56 \\
152 &= 2.56 + 40 \\
56 &= 40 + 16 \\
40 &= 2.16 + 8
\end{align*}
\]

Since 8|16 we stop, the GCD equals 8. Now rewrite these equations...

\[
152 = 512 - 360
\]

\[
56 = 360 - 2.152 = 360 - 2(512 - 360) = 3.360 - 2.512
\]

\[
40 = 152 - 2.56 = (512 - 360) - 2(3.360 - 2.512) = 5.512 - 7.360
\]

\[
16 = 56 - 40 = (3.360 - 2.512) - (5.512 - 7.360) = 10.360 - 7.512
\]

\[
\]

We are done, the GCD 8 can be written as 19.512 − 27.360.

CHECK: 8 = 19.512 − 27.360.

3. Prove that whenever \(m \neq 0\), \(\text{GCD}(0, m) = |m|\).

Suppose \(m \neq 0\). By definition, \(\text{GCD}(0, m)\) is the biggest integer that divides both 0 and \(m\). Since everything divides 0, that is simply the biggest integer that divides \(m\). Obviously that is \(|m|\), since nothing bigger that \(|m|\) divides \(m\).

4(a) Prove that if \(a|x\) and \(b|y\) then \(ab|xy\).
Suppose $a | x$ and $b | y$. This means that $x = am$ and $y = bn$ for integers $m, n \in \mathbb{Z}$. Hence, $xy = ambn = (ab)(mn)$. So $xy$ is an integer multiple of $ab$, hence $xy | ab$.

4(b) Prove that if $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Let $d = \gcd(a, b)$. By Theorem 3 in class, there are integers $m, n$ such that $d = ma + nb$. Divide both sides by $d$ to get that $1 = m\frac{a}{d} + n\frac{b}{d}$. By Theorem 4 in class this shows that $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime, i.e. $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

6. Give a counterexample to the statement: If there are integers $m, n$ so that $d = am + bn$ then $d = \gcd(a, b)$.

We need to find integers $a, b, m, n, d$ such that $d = am + bn$ but $d \neq \gcd(a, b)$. For instance, take $a = b = m = n = 2$. Then $d = am + bn = 8$ which is certainly not $\gcd(2, 2)$. 