Useful definitions:

- An integer $n$ is *even* if there is an integer $k$ such that $n = 2k$.
- An integer $n$ is *odd* if there is an integer $k$ such that $n = 2k + 1$.
- If $a, b$ are integers and $a \neq 0$ then $a$ *divides* $b$ (written $a \mid b$) if there is an integer $k$ such that $b = ak$. We write $a \nmid b$ if $a$ does not divide $b$.
- A natural number $p > 1$ is *prime* if whenever $p$ divides a product of two integers $p$ divides (at least) one of the two factors. If a natural number $n > 1$ is not prime we call it *composite*.

You may use the following facts without proof or reference:

- Any logical equivalence or equality of sets proved in class or given as homework.
- The axioms for integers given in class.
- The sum of two integers is even iff they have the same parity.
- The product of two integers is even iff at least one of them is even.
- Any reasonable manipulation of inequalities between real numbers, e.g. from $x \leq y$ and $z \leq w$ conclude $x + z \leq y + w$ or from $x \leq y$ and $z \geq 0$ conclude $xz \leq yz$.
- A natural number $p > 1$ is prime iff its only positive factors are 1 and $p$.
- If $p$ is prime then $\sqrt{p}$ is irrational. In particular, $\sqrt{2}$ is irrational.
- (the fundamental theorem of arithmetic) Any natural number $n > 1$ can be written uniquely as a product of (not necessarily distinct) primes. In particular, every natural $n > 1$ has a prime factor.
- (Euclid's theorem) There are infinitely many primes.

If you need to use some other fact you need to either give a proof for it or give a reference to either the lectures or the textbook.

1. Show that $(\sim (P \iff Q)) \implies (P \vee Q)$ is a tautology. [10 pts]

   We can do this by computing the truth table:

| $P$ | $Q$ | $P \iff Q$ | $\sim (P \iff Q)$ | $P \vee Q$ | $\sim (P \iff Q)) \implies (P \vee Q)$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $F$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $T$ | $T$ | $T$ |
| $F$ | $T$ | $F$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $T$ | $F$ | $F$ | $T$ |

   The last column consists only of $T$s and so the statement is a tautology.

2. Let $A, B$ and $C$ be sets. Show that $(A \setminus B) \setminus C = A \setminus (B \cup C)$. [10 pts]

   We need to show that two sets are equal, so we will prove that each one is a subset of the other.

   To prove that $(A \setminus B) \setminus C \subseteq A \setminus (B \cup C)$ let $x$ be an arbitrary element of $(A \setminus B) \setminus C$. By definition this means that $x \in A \setminus B$ and $x \notin C$. Simplifying even more, we get that $x \in A$ and $x \notin B$ and $x \notin C$. Therefore $\sim (x \in B \vee x \in C)$ is true which means that $x \notin B \cup C$. Putting this together we conclude that $x \in A \setminus (B \cup C)$, as required.

   To prove that $A \setminus (B \cup C) \subseteq (A \setminus B) \setminus C$ let $x$ be an arbitrary element of $A \setminus (B \cup C)$. By definition this means that $x \in A$ and $x \notin (B \cup C)$ and thus $x \notin B$ and $x \notin C$. Putting this together gives us $x \in A \setminus B$ and $x \notin C$ and finally $x \in (A \setminus B) \setminus C)$.

3. Show that if $n$ is an integer then either $n^2$ is odd or 4 divides $n^2$. [10 pts]

   (Hint: Split into cases depending on the parity of $n$. Alternatively, split into cases depending on the parity of $n^2$ and use a theorem from class.)

   Let $n$ be an arbitrary integer. Following the hint, let us consider two cases.

   *Case 1*: $n$ is odd.

   If $n$ is odd then there is an integer $k$ such that $n = 2k + 1$. Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

   and thus $n^2$ is odd, so the conclusion of the statement holds.

   *Case 2*: $n$ is even.

   If $n$ is even then there is an integer $k$ such that $n = 2k$. Then $n^2 = 4k^2$ is clearly divisible by 4 and the conclusion of the statement holds.

   **Comments:** We can save a bit of time if we follow the second hint. Namely, consider two cases depending on whether $n^2$ is even or odd. If it is odd we are done immediately, and if it is even then, by theorem from the reference sheet, $n$ must be even. But if $n$ is even the calculation from above shows that 4 divides $n^2$.

4. Show that if $x$ is rational and $y$ is irrational then $xy$ is irrational. [10 pts]

   Assume, toward a contradiction, that there is some nonzero rational $x$ and irrational $y$ such that $xy$ is rational. Then both $x$ and $xy$ can be written as fractions, i.e. $x = \frac{a}{b}$ and $xy = \frac{c}{d}$ for some integers $a, b, c, d$ with $a, b, d \neq 0$. By combining these expressions we get

$$xy = \frac{a}{b}y = \frac{c}{d}$$

   and after solving for $y$ (which we can do since $a \neq 0$)

$$y = \frac{cb}{ad}$$

   which contradicts our assumption that $y$ is irrational.

5. Let $n$ be an even integer and $m$ an odd integer.

   (a) Find an example of integers $n, m, a, b, c, d$ such that $an + bm$ is even and $cn + dm$ is odd. [5 pts]

   Almost anything you can think of works here. For example we could take $n = 2, m = 3, a = 1, b = 4, c = 6, d = 5$ and get $an + bm = 2 + 12 = 14$ even and $cn + dm = 12 + 15 = 27$ odd.

   (b) If $a, b$ are arbitrary integers, show that $an + bm$ is even iff $b$ is even. [5 pts]

   Let $n$ be even, $m$ odd and $a$ and $b$ arbitrary integers. We can prove the whole biconditional in one fell swoop by using the two powerful theorems on when sums and products of integers are even.

   Since $n$ is even we know that $an$ is also even. We also know that, since $m$ is odd, $bm$ is even iff $b$ is even. Furthermore, since $an$ is even, $an + bm$ is even iff $bm$ is even. Putting this together we can conclude that $an + bm$ is even iff $b$ is even. □

   **Comments:** We could also have proceeded by proving the two directions of the biconditional separately. We would then have had to use various directions of the two theorems several times.

6. Show that $\sum_{k=1}^{n}(k \cdot k!) = (n+1)! - 1$ for any integer $n \geq 1$. [10 pts]

   We proceed by induction. In the base step we check the equality for $n = 1$. Since $\sum_{k=1}^{1}(k \cdot k!) = 1$ and $(1+1)! - 1 = 1$, we can continue.

   In the induction step we assume that $\sum_{k=1}^{n}(k \cdot k!) = (n+1)! - 1$ and prove that $\sum_{k=1}^{n+1}(k \cdot k!) = (n+2)! - 1$. To get this we compute

$$\begin{aligned}\sum_{k=1}^{n+1}(k \cdot k!) &= \sum_{k=1}^{n}(k \cdot k!) + (n+1)(n+1)! \\ &= (n+1)! - 1 + (n+1)(n+1)! = (n+1)!(1+n+1) - 1 \\ &= (n+2)(n+1)! - 1 = (n+2)! - 1\end{aligned}$$

   where we used the induction hypothesis to go from the first to the second line. This finishes the induction and the proof.

7. (a) Show that the sum of two rational numbers is rational. [3 pts]

   (b) Give an example of two irrational numbers whose sum is rational (depending on your example you may want to justify why the sum is rational). [3 pts]

   (c) Given an example of two irrational numbers whose sum is irrational (with a justification why the sum is actually irrational). [4 pts]

   (a) Let $x, y$ be two arbitrary rational numbers. We can write them as fractions, $x = \frac{a}{b}, y = \frac{c}{d}$ for some integers $a, b, c, d$ with $c, d \neq 0$. Then $x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{cd}$ is a rational number.

   (b) For example, $\sqrt{2} + (-\sqrt{2}) = 0$ is rational and we know that $\sqrt{2}$ is irrational and $-\sqrt{2}$ is irrational by problem 4.

   (c) For example, $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} = \sqrt{2}$ is irrational and $\frac{\sqrt{2}}{2}$ is irrational by problem 4.

   **Comments:** There are many possible examples for parts (b) and (c), although it is not the best idea to improvise wildly. Particularly in part (c), we can easily write down numbers which may seem obviously irrational but for which this is still an open mathematical question. For example, it is not known whether $\pi + e$ and $\pi \cdot e$ are irrational (although it is known that they cannot both be rational) and it is unknown whether $\pi^{\pi^{\pi}}$ is even an integer or not.

8. (extra credit)

   (a) Show that if $x, y$ are real numbers and $n \geq 2$ a natural number then [5 pts]

   $$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

   (Hint: This is easier than it looks and you don't need induction. Just try to compute the right side.)

   (b) Use part (a) to show that if $n > 1$ is composite then $2^n - 1$ is composite. [5 pts] (Primes of the form $2^n - 1$ are called *Mersenne primes*. Part (b) shows that the $n$ for any Mersenne prime must be prime itself. There are currently only 48 known Mersenne primes and the largest known prime number is a Mersenne prime.)

   (a) We can multiply out the right side and get a telescoping sum:

   $$\begin{gathered}(x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}) = \\ = x^n - x^{n-1}y + x^{n-1}y - x^{n-2}y^2 + x^{n-2}y^2 - x^{n-3}y^3 + \cdots + x^2y^{n-2} - xy^{n-1} + xy^{n-1} - y^n \\ = x^n - y^n\end{gathered}$$

   (b) Suppose that $n > 1$ is a composite natural number. Therefore we can find two integers $k, l$ such that $n = kl$ and $1 < l < n$. Now consider then number $2^n - 1$. We can rewrite it as

   $$\begin{aligned}2^n - 1 &= 2^{kl} - 1 = (2^k)^l - 1^l \\ &= (2^k - 1)(2^{k(l-1)} + 2^{k(l-2)} + 2^{k(l-3)} + \cdots + 2^k + 1)\end{aligned}$$

using part (a) in the last line. But since $k > 1$, the number $2^k - 1$ is strictly bigger than 1. Therefore $2^n - 1$ has a nontrivial factor $2^k - 1$ which means that $2^n - 1$ is not prime.