Each of the questions is worth 10 points. Please turn in solutions to four questions of your choice. Write your name, your student ID, and your TA’s name on the solution sheet.

Please write your solutions clearly and concisely. If you do not explain your answer you will be given no credit. You are encouraged to collaborate on the homework, but you must write your own solutions and list your collaborators on your solution sheet. Copying someone else’s solution will be considered plagiarism and may result in failing the whole course.

Questions

1. Use induction to prove the following statements.

   (a) (3’) For every \( n \geq 4 \), \( n^2 \leq 2^n \).

   **Solution:** Base case \( n = 4 \): \( 4^2 = 16 = 2^4 \).

   **Inductive step:** Assume \( n \geq 4 \) and \( n^2 \leq 2^n \). Then

   \[
   (n + 1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + n = 2^n + 3n \leq 2^n + 2^n = 2^{n+1}.
   \]

   By induction, \( n^2 \leq 2^n \) for all \( n \geq 4 \). (There are other, equally valid, ways to do this proof.)

   (b) (3’) For every \( n \geq 1 \), \( 1^2 - 2^2 + 3^2 + 4^2 - \ldots (+ \text{ or } -) n^2 = (-1)^{n+1}n(n+1)/2 \).

   **Solution:** The sign in front of the \( n^2 \) term is +1 if \( n \) is even and −1 if \( n \) is odd: This is the number \((-1)^{n+1}\).

   **Base case** \( n = 1 \): \( 1^2 = 1 \) and \((-1)^{1+1}(1+1)/2 = 1 \).

   **Inductive step:** Assume \( n \geq 1 \) and \( 1^2 - 2^2 + \ldots (-1)^{n+1}n^2 = (-1)^{n+1}n(n+1)/2 \). Then

   \[
   1^2 - 2^2 + 3^2 + \ldots + (-1)^{n+2}(n+1)^2 = \frac{(-1)^{n+1}n(n+1)}{2} + (-1)^{n+2}(n+1)^2
   
   = (-1)^{n+1}(n + 1) \left(\frac{n}{2} - (n + 1)\right)
   
   = (-1)^{n+1}(n + 1) \left(-\frac{n}{2} - 1\right)
   
   = \frac{(-1)^{n+2}(n+1)(n+2)}{2}.
   \]

   The proposition is true by induction on \( n \).

   (c) (4’) For \( n \geq 3 \), the sum of interior angles of a convex polygon with \( n \) sides is \((n - 2)\pi\). (You can assume that the base case \( n = 3 \) is true.)

   **Solution:** We assume the base case \( n = 3 \) is true, namely the sum of interior angles of every triangle is \( \pi \).

   **Inductive step:** Assume that \( n \geq 3 \) and that the sum of interior angles of every convex polygon with \( n \) sides is \((n - 2)\pi\). Let \( P \) be a convex polygon with \( n + 1 \) sides. Choose any two
2. Use strong induction to prove the following statements.

(a) (5') Every nonnegative integer has a binary representation: Every \( n \geq 0 \) can be written as \( n = n_0 + 2n_1 + 4n_2 + \cdots + 2^k n_k \) for some \( k \geq 0 \), where \( n_0, \ldots, n_k \) are 0 or 1.

**Solution:** We prove the proposition by strong induction on \( n \).

**Base case** \( n = 0 \): Set \( k = 0 \) and \( n_0 = 0 \).

**Inductive step:** Assume every nonnegative integer between 0 and \( n \) has a binary representation. We will show that \( n + 1 \) has one too. The proof is by cases.

Case 1: \( n + 1 \) is even. By our inductive hypothesis, the integer \( (n + 1)/2 \), which is smaller, has a binary representation

\[
\frac{n + 1}{2} = n_0 + 2n_1 + 4n_2 + \cdots + 2^k n_k.
\]

Then \( n + 1 = 1 \cdot 0 + 2 \cdot n_0 + 4 \cdot n_1 + \cdots + 2^{k+1} n_k \), so \( n + 1 \) also has a binary representation.

Case 2: \( n + 1 \) is odd. By our inductive hypothesis, the integer \( n/2 \) has a binary representation

\[
\frac{n}{2} = n_0 + 2n_1 + 4n_2 + \cdots + 2^k n_k.
\]

Then \( n + 1 = 1 \cdot 1 + 2 \cdot n_0 + 4 \cdot n_1 + \cdots + 2^{k+1} n_k \), so \( n + 1 \) also has a binary representation. Therefore the proposition is true for all \( n \geq 0 \).

(b) (5') \( F_n \geq (3/2)^{n-2} \) for every \( n \geq 1 \), where the sequence \( F_n \) is defined by \( F_1 = 1, F_2 = 1 \) and \( F_n = F_{n-1} + F_{n-2} \) for \( n \geq 3 \).

**Solution:** We prove the proposition by strong induction on \( n \).

**Base case** \( n = 1 \): \( F_1 = 1 \geq 2/3 = (3/2)^{1-2} \).

**Inductive step:** Assume \( n \geq 1 \) and \( F_k \leq (3/2)^{k-2} \) for all \( k \) from 1 to \( n \). Then

\[
F_{n+1} = F_n + F_{n-1} \geq (3/2)^{n-2} + (3/2)^{n-3} = (3/2)^{n-3}(3/2 + 1) = (3/2)^{n-3}(5/2) \geq (3/2)^{n-3}(3/2)^2 = (3/2)^{n-1}
\]

The first inequality is where we used the inductive hypothesis. Therefore the proposition is true for all \( n \geq 1 \).

3. You start with the three numbers \(-2, 0, \) and \( 2 \) and play the following game: In each round, you can take any pair of numbers \( a \) and \( b \) and replace them by \((a + b)/\sqrt{2}\) and \((a - b)/\sqrt{2}\). The third number stays the same. Can you ever end up with the numbers

(a) (2') \(0, 0, \) and \( \sqrt{8}\)?

**Solution:** Yes. Take \( a = 2, b = -2, c = 0 \). \((a + b)/\sqrt{2} = 0, (a - b)/\sqrt{2} = 4/\sqrt{2} = \sqrt{8}\), and \( c = 0 \), so we obtain the triple \(0, 0, \sqrt{8}\).
(b) $(4') - 2, 1, \text{ and } 2$?

**Solution:** No. We will prove that for every $n$, after $n$ rounds the following invariant holds: $a^2 + b^2 + c^2 = 8$. The proof is by induction on $n$. When $n = 0$, we have $(-2)^2 + 0^2 + 2^2 = 8$. Now assume that in round $n$, the three numbers $a, b, c$ satisfy $a^2 + b^2 + c^2 = 8$. In round $n + 1$, the numbers become $(a + b)/\sqrt{2}, (a - b)/\sqrt{2}, c$ and

$$\left(\frac{a + b}{\sqrt{2}}\right)^2 + \left(\frac{a - b}{\sqrt{2}}\right)^2 + c^2 = \frac{(a + b)^2}{2} + \frac{(a - b)^2}{2} + c^2 = a^2 + b^2 + c^2 = 8.$$ 

By induction, the invariant holds in all rounds. It is impossible to ever obtain the triple $-2, 1, 2$ because $(-2)^2 + 1^2 + 2^2 = 9$.

(c) $(4') - \sqrt{3}, \sqrt{2}, \text{ and } \sqrt{3}$?

**Solution:** No. We will prove that for every $n$, after $n$ rounds $a, b, c$ are all of the form $s + t\sqrt{2}$ for some rational numbers $s$ and $t$. When $n = 0$, this is clearly true. Now assume that in round $n$, we have $a = s_a + t_a\sqrt{2}, b = s_b + t_b\sqrt{2}$ and $c = s_c + t_c\sqrt{2}$ for some integers $s_a, t_a, s_b, t_b, s_c, t_c$. Then in round $n + 1$ our three numbers look like this:

$$\frac{a + b}{\sqrt{2}} = (t_a + t_b) + \frac{s_a + s_b}{2}\sqrt{2}, \quad \frac{a - b}{\sqrt{2}} = (t_a - t_b) + \frac{s_a - s_b}{2}\sqrt{2}, \quad c = s_c + t_c\sqrt{2}.$$ 

All these numbers are of the desired form, so by induction the proposition is true for all $n \geq 0$. Now assume, for contradiction, that we ever reach the triple $-\sqrt{3}, \sqrt{2}, \sqrt{3}$. Then $\sqrt{3} = s + t\sqrt{2}$ for some rational numbers $s$ and $t$. Squaring both sides of this equation, we obtain

$$3 = (s + t\sqrt{2})^2 = s^2 + 2st\sqrt{2} + 2t^2$$

so $2st\sqrt{2}$ must be a rational number. This is not possible unless $t = 0$ or $s = 0$. We now proceed by cases.

If $t = 0$, then $\sqrt{3} = s$, which is rational, contradicting what we proved in Question 4(a) of Homework 2.

If $s = 0$, then $\sqrt{3} = t\sqrt{2}$. Since $t$ is rational, we can write $t = n/d$ for integers $n, d$ with no common factors. After multiplying both sides by $d$ we obtain $d\sqrt{3} = n\sqrt{2}$. Squaring both sides gives $3d^2 = 2n^2$. Since 3 is odd, $d^2$ must be even, so $d$ is even. We can now write $d = 2d'$ for some integer $d'$. After squaring both sides and cancelling a factor of 2, we get $6d'^2 = n^2$. Therefore $n^2$ is even, and so is $n$, and $n$ and $d$ have a common factor, namely 2. Contradiction.

4. Prove the following statements.

(a) $(5')$ For all $n \geq 5$, $n$ is composite if and only if $n$ divides $(n - 1)!$.

**Solution:** Suppose $n \geq 5$ is composite. Then $n = mk$ for some integers $1 < m \leq k < n$.

Case 1: $m < k$. In this case $(n - 1)! = 1 \cdot 2 \cdot \ldots \cdot m \cdot \ldots \cdot k \ldots (n - 1)$, so $n = mk$ divides $(n - 1)!$.

Case 2: $m = k$. Since $n \geq 5$, we have $m > 2$. Consequently $2 < m < m(m - 1) < m^2 = n$. Hence $(n - 1)! = 1 \cdot 2 \cdot \ldots \cdot m \cdot \ldots \cdot m(m - 1) \ldots (n - 1)$ and $n = m^2$ divides $(n - 1)!$.

Conversely, suppose $n \geq 5$ is prime. Then $n$ does not divide any integers between $1$ and $n - 1$, so $n$ does not divide the product of these numbers, which is precisely $(n - 1)!$. 

(b) (5’) For all \( n \), if \( 2^n - 1 \) is a prime, then \( n \) is a prime.

**Answer:** We prove the contrapositive. Assume \( n \) is composite. Then \( n = mk \) for some integers \( 1 < m \leq k < n \). We have

\[
2^n - 1 = (2^m)^k - 1 = (2^m - 1)(1 + 2^m + (2^m)^2 + \cdots + (2^m)^{k-1}).
\]

As \( m, k > 1 \), both of these factors are greater than 1. It follows that \( 2^n - 1 \) is composite.

(c) (2’) (**Extra Credit**) There exists an integer \( n \) such that \( n/2 \) is a square, \( n/3 \) is a cube, and \( n/5 \) is a fifth power of an integer. (Do not just write down a number; explain how you discovered it.)

**Answer:** We search for \( n \) of the form \( 2^a 3^b 5^c \) where \( a, b, c \) are positive integers. To make \( n/2 = 2^{a-1} 3^b 5^c \) a square, \( a - 1 \), \( b \), and \( c \) should all be even. Similarly, for \( n/3 \) to be a cube, \( a, b - 1, c \) should all be divisible by 3; for \( n/5 \) to be a fifth power, \( a, b, c - 1 \) should all be divisible by 5.

Let’s find \( a \) first. \( a \) needs to be odd and divisible by 3 and 5, so a multiple of 15. We can set \( a = 15 \). For \( b \), we are looking for something that is divisible by 2 and 5, so a multiple of 10, and of the form \( 3k + 1 \). \( b = 10 \) works. Finally \( c \) should be divisible by 2 and 3 and of the form \( 5\ell + 1 \), so \( c = 6 \) works.

This suggests the solution \( n = 2^{15} 3^{10} 5^6 \) as one possible answer. Indeed, \( n/2 = (2^7 3^5 5^3)^2 \), \( n/3 = (2^5 3^5 5^2)^3 \), and \( n/5 = (2^3 3^2 5)^5 \).

5. (10’) Show that the Extended Euclid’s Algorithm \( X(n, d) \) (see the Lecture 4 notes) terminates and outputs integers \( (s, t) \) such that \( s \cdot n + t \cdot d = \gcd(n, d) \) whenever \( n > d \geq 0 \).

**Answer:** We use strong induction on \( d \). When \( d = 0 \), the algorithm returns \((1, 0)\) and \( 1 \cdot n + 0 \cdot 0 = n = \gcd(n, 0) \) and terminates. Now assume the algorithm terminates and outputs \((s, t)\) such that \( s \cdot n + t \cdot d' \) for all input pairs \((n, d')\), where \( n > d' \) and \( 0 \leq d' \leq d \). Consider the algorithm on input \((n, d + 1)\). The algorithm writes \( n = q(d + 1) + r \) with \( 0 \leq r < d + 1 \), obtains \((s, t)\) as the output of \( X(d + 1, r) \), and outputs \((t, s - qt)\).

Since \( X(d + 1, r) \) terminates by our inductive hypothesis, \( X(n, d + 1) \) must also terminate. We now need to show that its output \((t, s - qt)\) satisfies

\[
t \cdot n + (s - qt) \cdot (d + 1) = \gcd(n, d + 1).
\]

By our inductive assumption, we know that \( s \cdot (d + 1) + t \cdot r = \gcd(d + 1, r) \), which we showed in class equals \( \gcd(n, d + 1) \). Therefore

\[
t \cdot n + (s - qt) \cdot (d + 1) = t \cdot n + s \cdot (d + 1) - t \cdot q(d + 1)
\]

\[
= s \cdot (d + 1) + t \cdot (n - q(d + 1))
\]

\[
= s \cdot (d + 1) + t \cdot r
\]

\[
= \gcd(d + 1, r)
\]

\[
= \gcd(n, d + 1)
\]

which is what we needed to prove.
6. You will show that

\[ S(n) = \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \]

is not an integer for every \( n \geq 2 \).

(a) (2') Express the sum \( S(5) \) as a fraction. Show that the denominator does not divide the numerator. (It may be easier if you do not simplify the numerator.)

Answer:

\[
S(5) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{2 \cdot 3 \cdot 4 \cdot 5 + 1 \cdot 3 \cdot 4 \cdot 5 + 1 \cdot 2 \cdot 4 \cdot 5 + 1 \cdot 2 \cdot 3 \cdot 5 + 1 \cdot 2 \cdot 3 \cdot 4}{5!} = \frac{4(2 \cdot 3 \cdot 5 + 1 \cdot 3 \cdot 5 + 1 \cdot 2 \cdot 3) + 2(1 \cdot 3 \cdot 5)}{8(1 \cdot 3 \cdot 5)}.
\]

Note that the largest power of 2 dividing the numerator is 1 but that of the denominator is 3, so \( S(5) \) is not an integer.

(b) (4') Let \( n \geq 2 \) and \( 2^m \) be the largest power of 2 between 1 and \( n \). Show that \( 2^m \) does not divide any number between 1 and \( n \) except itself.

Answer: Let \( k \neq 2^m \) be a number between 1 and \( n \).

Case 1: \( 1 \leq k < 2^m \). Clearly \( 2^m \) does not divide \( k \) as \( k \) is smaller.

Case 2: \( k < 2^m \leq n \). Suppose \( 2^m \) divides \( k \). Then we can write \( k = 2^m n_0 \) where \( n_0 > 1 \) is an integer such that \( \gcd(2, n_0) = 1 \), then \( n \geq 2^m n_0 > 2^{m+1} \) and this would contradict the definition of \( m \), thus \( 2^m \) does not divide \( k \).

(c) (4') Prove that \( S(n) \) is not an integer for every \( n \geq 2 \).

Answer: We write

\[
S(n) = \sum_{k=1}^{n} \frac{1}{k} = \sum_{k=1}^{n} \frac{n! / k}{n!}.
\]

and consider each term \( n! / k \) in the numerator.

Let \( 2^m \) be the largest power of 2 between 1 and \( n \) and \( t \) be the largest power of 2 dividing \( n! \).

For \( k \neq 2^m \), we know from part (b) that the largest power of 2 dividing \( k \) is at most \( m - 1 \), so the largest power of 2 dividing \( n! / k \) is at least \( t - m + 1 \). The largest power of 2 dividing \( n! / 2^m \) is \( t - m \). Therefore the largest power of 2 dividing the numerator is \( t - m \).

On the other hand, the largest power of 2 dividing the denominator is \( t \). Since \( t - m < t \), \( S(n) \) cannot be an integer.