Practice Midterm 1

1. Prove that for every integer n there exists an integer k such that $|n^2 - 5k| \leq 1$. (**Hint:** What is $n^2 \bmod 5$?)

   Solution: First we check that for all n, $n^2 \bmod 5$ equals 0, 1 or 4:

$n \bmod 5$	0	1	2	3	4
$n^2 \bmod 5$	0	1	4	4	1

   Since $4 \equiv -1 \pmod 5$ it follows that for every n, n^2 is congruent to 0, 1, or -1 modulo 5. Therefore n^2 is of the form $5k$ or $5k-1$ or $5k+1$ for some integer k. In all cases $|n^2 - 5k| \leq 1$.

2. What is $1 + (1+2) + (1+2+3) + \cdots + (1+2+3+\cdots+1000)$?

   Solution: The sum of the first k integers is $k(k+1)/2 = \frac{1}{2}k^2 + \frac{1}{2}k$, so

   $$\begin{aligned} 1 + (1+2) + \cdots + (1+2+3+\cdots+n) &= \tfrac{1}{2}(1^2 + 2^2 + \cdots + n^2) + \tfrac{1}{2}(1 + 2 + \cdots + n) \\ &= \tfrac{1}{2}(\tfrac{1}{3}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{6}n) + \tfrac{1}{2}(\tfrac{1}{2}n^2 + \tfrac{1}{2}n) \\ &= \tfrac{1}{6}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{3}n \end{aligned}$$

   using the formulas for the sum of the first n squares of integers and the sum of the first n integers, respectively. (Notice that this expression gives the correct answer for $n = 0$, 1, and 2.) Plugging in $n = 1000$ we obtain the answer $\frac{1}{6} \cdot 10^9 + \frac{1}{2} \cdot 10^6 + \frac{1}{3} \cdot 10^3 = 167,167,100$.

   Alternative solution: as $1+2+\cdots+n = n(n+1)/2$ we may guess that $1+(1+2)+\cdots+(1+2+3+\cdots+n)$ has the form $an^3 + bn^2 + cn + d$. Plugging in $n = 0,1,2,3$ we get that a, b, c, d must satisfy

   $$\begin{aligned} d &= 0 \\ a + b + c + d &= 1 \\ 8a + 4b + 2c + d &= 1 + (1+2) = 4 \\ 27a + 9b + 3c + d &= 4 + (1+2+3) = 10 \end{aligned}$$

   Eliminating first d and then c we get $6a + 2b = 2$ and $24a + 6b = 7$. This solves to $2b = 1$. Therefore $b = 1/2$. Plugging back in we get $a = 1/6$ and $c = 1/3$.

   We now verify that the sum equals $\frac{1}{6}n^3 + \frac{1}{2}n^2 + \frac{1}{3}n$ by induction on n. The base case $n = 1$ was already checked. As for the inductive step we assume the claim is true for n and verify it for $n+1$:

   $$\begin{aligned} 1 + (1+2) + \cdots + (1 + \cdots + (n+1)) &= \tfrac{1}{6}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{3}n + (1 + \cdots + (n+1)) \\ &= \tfrac{1}{6}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{3}n + \frac{(n+1)(n+2)}{2} \\ &= \tfrac{1}{6}(n^3 + 3n^2 + 3n + 1) + \tfrac{1}{2}(n^2 + 2n + 1) + \tfrac{1}{3}(n+1) \\ &= \tfrac{1}{6}(n+1)^3 + \tfrac{1}{2}(n+1)^2 + \tfrac{1}{3}(n+1). \end{aligned}$$

   Plugging in $n = 1000$ we obtain the same answer as above.

3. Find a closed-form expression for the recurrence $f(n+1) = 2f(n) + 2^{n-1}$, $f(1) = 0$.

   Solution: We guess a solution for $f(n)$ by iterating the formula:

   $$\begin{aligned} f(n) &= 2f(n-1) + 2^{n-2} \\ &= 2(2f(n-2) + 2^{n-3}) + 2^{n-2} = 2^2 \cdot f(n-2) + 2 \cdot 2^{n-2} \\ &= 2^2 \cdot (2f(n-3) + 2^{n-4}) + 2 \cdot 2^{n-2} = 2^3 \cdot f(n-3) + 3 \cdot 2^{n-2}. \end{aligned}$$

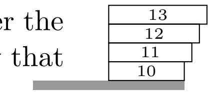
This suggests the guess $f(n) = 2^{n-1} \cdot f(1) + (n-1) \cdot 2^{n-2} = (n-1) \cdot 2^{n-2}$.

We now prove that $f(n) = (n-1) \cdot 2^{n-2}$ by induction on n. When $n = 1$, $f(1) = 0$ and $(n-1) \cdot 2^{n-2} = 0$. Now assume $f(n) = (n-1) \cdot 2^{n-2}$ for some $n \geq 1$. Then

$$f(n+1) = 2f(n) + 2^{n-1} = 2 \cdot (n-1) \cdot 2^{n-2} + 2^{n-1} = n \cdot 2^{n-1}$$

so the formula must be correct for all n.

4. You have overhang blocks 10, 11, up to n units long, one of each kind. They are stacked over the table from smallest to largest so that their left edges align. (See diagram for $n = 13$). Show that the configuration is not stable when n is sufficiently large.



Solution: We assume all blocks have the same weight. If instead a block's weight is proportional its length the calculation is a bit more complicated but the conclusion is similar.

The center of mass of all the blocks, measured from the left edge of the blocks, is at position

$$P(n) = \frac{1}{2n} \cdot (10 + 11 + \cdots + n) = \frac{1}{2n}\big((1 + \cdots + n) - (1 + \cdots + 9)\big) = \frac{1}{2n}\Big(\frac{n(n+1)}{2} - \frac{9 \cdot 10}{2}\Big) = \Omega(n)$$

so when n is sufficiently large, $P(n) > 10$, the center of mass falls to the right of the edge of the table, and the configuration is not stable.

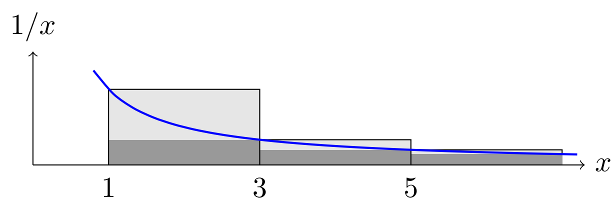
Practice Midterm 2

1. Show that for every integer n, if $n^3 + n$ is divisible by 3 then $2n^3 + 1$ is *not* divisible by 3.

Solution: We can prove this proposition by cases depending on the residue of n^3+n modulo 3. If $n \equiv 0 \bmod 3$ then $n^3 + n$ is divisible by 3, while $2n^3 + 1 \equiv 1 \bmod 3$, so $2n^3 + 1$ is not divisible by 3, so the proposition holds. If $n \equiv 1 \bmod 3$ then $n^3 + n \equiv 2 \bmod 3$, so $n^3 + n$ is not divisible by 3 and the proposition holds again. If $n \equiv 2 \bmod 3$, then $n^3 + n \equiv 1 \bmod 3$ and $n^3 + n$ is not divisible by 3 again.

2. Let $f(n) = 1 + 1/3 + 1/5 + \cdots + 1/(2n-1)$. Show that f is $\Theta(\log n)$.

Solution: $f(n)$ dominates the value of the integral $\int_1^{2n} (1/x)dx$.



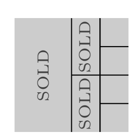
It is dominated by the value of the same integral after subtracting the light gray area which is at most 2. Therefore

$$\int_1^{2n+1} \frac{1}{x} dx \leq f(n) \leq \int_1^{2n+1} \frac{1}{x} dx + 2.$$

The integral evaluates to $\ln(2n+1)$, so $\ln(2n+1) \leq f(n) \leq \ln(2n+1)+2$ so $f(n)$ is $\Theta(\ln(2n+1)) = \Theta(\log n)$.

Alternative solution: On the one hand, $f(n) \leq 1 + 1/2 + 1/3 + \cdots + 1/(2n) = H(2n)$, where $H(n)$ is the n-th harmonic number from Lecture 7. On the other hand, $f(n) \geq 1/2 + 1/4 + 1/6 + \cdots + 1/(2n) = \frac{1}{2}H(n)$. Therefore $\frac{1}{2}H(n) \leq f(n) \leq H(2n)$. In Lecture 7 we showed that $H(n)$ is $\Theta(\log n)$, so $H(2n)$ is also $\Theta(\log 2n) = \Theta(\log n)$. Therefore $f(n)$ must be $\Theta(\log n)$ as well.

3. An $n \times n$ plot of land (n is a power of two) is split in two equal parts by a North-South fence. The Western half is sold and the Eastern half is split in two equal parts by an West-East fence. The same procedure is applied to the remaining $(n/2) \times (n/2)$ plots until 1×1 plots are obtained (see $n = 4$ example). How many units of fence are used?



Solution: The amount $T(n)$ of fence used satisfies the recurrence $T(n) = 2T(n/2) + 3n/2$ for $n > 1$, with $T(1) = 0$. We can unwind the recurrence as follows:

$$\begin{aligned} T(n) &= 2T(n/2) + 3/2 \cdot n \\ &= 2(2T(n/2^2) + 3/2 \cdot n/2) + 3/2 \cdot n = 2^2T(n/2^2) + 3/2 \cdot 2n \\ &= 2^2(2T(n/2^3) + 3/2 \cdot n/2^2) + 3/2 \cdot 2n = 2^3T(n/2^3) + 3/2 \cdot 3n \end{aligned}$$

After $\log n$ steps we expect to obtain $T(n) = n \cdot T(1) + \frac{3}{2}n \log n = \frac{3}{2}n \log n$. We confirm the correctness of this guess by induction. For the base case $n = 1$, $T(1) = 0$ as desired. For the inductive step we assume $T(k) = \frac{3}{2}k \log k$ for all $k < n$ that are powers of two. Then

$$T(n) = 2T(n/2) + 3n/2 = 2 \cdot \frac{3}{2} \cdot \frac{n}{2} \log(n/2) + \frac{3n}{2} = \frac{3n}{2} \cdot (\log n - 1) + \frac{3n}{2} = \frac{3}{2} \cdot n \log n$$

when n is a power of two, concluding the inductive step.

4. Sort these three functions in increasing order of growth: $\sqrt{n} \cdot \log n$, $n/\sqrt{\log n}$, $\sqrt{n \cdot \log n}$. For your sorted list f, g, h show that f is $o(g)$ and g is $o(h)$.

   Solution: $\sqrt{n \log n}$ is $o(\sqrt{n} \log n)$ because the ratio $\sqrt{n \log n}/\sqrt{n} \log n$ equals $1/\sqrt{\log n}$, which eventually becomes and stays smaller than any given constant. $\sqrt{n} \log n$ is $o(n/\sqrt{\log n})$ because the ratio $\sqrt{n} \log n/(n/\sqrt{\log n})$ equals $(\log n)^{3/2}/n^{1/2}$. In Lecture 7 we showed that $(\log n)^a$ is $o(n^b)$ for any constants $a, b > 0$, so this ratio becomes and stays smaller than any constant when n is sufficiently large.

Practice Midterm 3

1. Bob has received from Alice the RSA ciphertext $c = 2$. The modulus is $n = pq$ with $p = 3$ and $q = 5$. The encryption key is $e = 3$.

   (a) Calculate Bob's decryption key d.

   Solution: e and d must satisfy the equation $ed \equiv 1 \pmod{(p-1)(q-1)}$, so $3d \equiv 1 \pmod{8}$. Therefore d is the multilpicative inverse of 3 modulo 8. We find it using extended Euclid's algorithm: $8 = 2 \cdot 3 + 2$ and $3 = 2 + 1$, so $1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = -8 + 3 \cdot 3$. Therefore $d = 3$.

   (b) Decrypt Alice's message m.

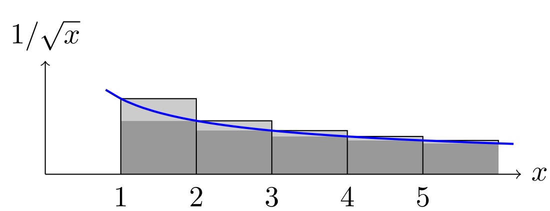
   Solution: The decrypted message is $c^d = 2^3 = 8 \pmod{15}$. (You can verify that $m^e = 8^3 \equiv 2 = c \pmod{15}$.)

2. What is the largest integer n for which

$$n \leq 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{9999}}?$$

   Solution: Let S denote the sum on the right. The area under the first 9999 rectangles is at least as large as the area under the curve, so

$$S \geq \int_1^{10000} \frac{dx}{\sqrt{x}} = 2\sqrt{x}\Big|_1^{10000} = 200 - 2 = 198.$$



If the area L under the light rectangles is removed from S then the dark rectangles fit under the curve, so $S - L \leq 198$. The light rectangles stack up to a rectangle of width 1 and height less than 1, so $L < 1$. Therefore $198 \leq S < 199$ and $n = 198$.

3. Find a closed-form expression for the recurrence $f(n) = 3f(n-1) + 4$, $f(0) = 0$.

   Solution: We unwind the recurrence:

$$\begin{aligned}
f(n) &= 3f(n-1) + 4 = 3(3f(n-2) + 4) + 4 \\
&= 3^2 f(n-2) + 2 \cdot 4 + 4 = 3^2(3f(n-3) + 4) + 3 \cdot 4 + 4 \\
&= 3^3 f(n-3) + (3^2 + 3 + 1) \cdot 4 \\
&\vdots \\
&= 3^n f(0) + (3^{n-1} + 3^{n-2} + \cdots + 1) \cdot 4 \\
&= \frac{3^n - 1}{2} \cdot 4 \\
&= 2 \cdot (3^n - 1).
\end{aligned}$$

   Alternative solution: We try the homogenization $g(n) = 3g(n-1)$, $f(n) = g(n) + c$. Solving for c we obtain $c = 3c + 4$ from where $c = -2$. Therefore $g(n) = 3g(n-1) = \cdots = 3^n g(0) = 3^n(f(0) + 2) = 2 \cdot 3^n$, so $f(n) = 2 \cdot 3^n - 2$.

4. Let $f(n)$ be the number of all length-n strings with symbols $\{\texttt{A}, \texttt{B}, \texttt{C}\}$ in which every `B` is immediately followed by a `C` (e.g., `BCAC` is counted but `ACAB` is not). Find the value of a for which $f(n)$ is $\Theta(a^n)$.

   Solution: There are three types of strings counted by $f(n)$: Those that start with an `A` of which there are $f(n-1)$, those that start with a `C` of which there are also $f(n-1)$, and those that start with a `B` immediately followed by a `C`, of which there are $f(n-2)$. Therefore f satisfies the recurrence $f(n) = 2f(n-1) + f(n-2)$ for all $n \geq 2$. Solutions of the form $f(n) = x^n$ must therefore satisfy $x^2 - 2x - 1 = 0$. There are two such solutions: $x_1 = 1 + \sqrt{2}$ and $x_2 = 1 - \sqrt{2}$. The solution of the recurrence must then be of the form $f(n) = c(1+\sqrt{2})^n + d(1-\sqrt{2})^n$, where c and d should be chosen to satisfy the initial conditions. Regardless of the values of c and d, $f(n)$ is $\Theta((1+\sqrt{2})^n)$, so $a = 1 + \sqrt{2}$.