THE UNIVERSITY OF SYDNEY
SCHOOL OF MATHEMATICS AND STATISTICS

Solutions to Number Theory and O-Notation – Week 7 Practice Class

MATH1064: Discrete Mathematics for Computing

Here is a list of **problems** for the practice class. Try to solve them before you go to class! There are more problems here than can be solved in the hour, so you should get started on them!

1. Use the Euclidean Algorithm to calculate $\gcd(186, 403)$.

Solution:

$$403 = 2 \times 186 + 31$$
$$186 = 6 \times 31 + 0$$

Hence, $\gcd(186, 403) = 31$.

2.
1. Suppose that n is a positive, composite number. Show that n has a prime factor p which satisfies $p \leq \lfloor \sqrt{n} \rfloor$.
2. Can you give an example of a positive, composite number n such that $p = \lfloor \sqrt{n} \rfloor$ for all of its prime factors p?
3. Can you give an example of a positive, composite number n such that $p > \lceil \sqrt{n}\ \rceil$ for at least one of its prime factors p?
4. What about $p > 2\lceil \sqrt{n}\ \rceil$?

Solution:

1. Consider the prime factorisation of n as follows.

$$n = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}$$

where $x_i \geq 1$ and $p_i \neq p_j$ whenever $i \neq j$. Suppose by contradiction that $p_i > \sqrt{n}$ for all i. Since n is a composite number we know that there are at least two prime factors of n (they may or may not be the same number). Therefore

$$p_1^{x_1} p_2^{x_2} \dots p_n^{x_n} \geq p_i p_j > (\sqrt{n})^2 = n$$

which is a contradiction. Therefore there must exist some j such that $p_j \leq \sqrt{n}$. However p_j is an integer so $p_j \leq \lfloor \sqrt{n} \rfloor$.

2. The prime decomposition of 4 is $4=2^2$.
3. Consider the number 10. We have $\sqrt{10} \approx 3.1623$. The prime decomposition of 10 is $10 = 2 \times 5$ and $5 > \lceil \sqrt{10} \rceil$.
4. The idea is to multiply a relatively large prime number by a small prime number. For example consider $34 = 2 \times 17$. We have $\sqrt{34} \approx 5.8310$. Therefore $\lceil \sqrt{34} \rceil = 6$ and $17 > 12 = 2 \times \lceil \sqrt{34} \rceil$.

3. Compute the following sums, giving the answer in the same base.

1. $(100101)_2 + (111)_2$
2. $(102)_3 + (211)_3$
3. $(7654)_8 + (76543)_8$

Solution:

1. The number $(100101)_2$ can also be represented as $1\times 2^0 + 0\times 2^1 + 1\times 2^2 + 0\times 2^3 + 0\times 2^4 + 0\times 2^5$. The number $(111)_2$ can also be represented as $(1\times 2^0 + 1\times 2^1 + 1\times 2^2)$. Therefore we compute their sum as follows.

$$\begin{aligned} 1\times 2^0 + 0\times 2^1 + 1\times 2^2 + 0\times 2^3 + 0\times 2^4 + 0\times 2^5 + 1\times 2^0 + 1\times 2^1 + 1\times 2^2 \\ = 0\times 2^0 + 0\times 2^1 + 1\times 2^2 + 1\times 2^3 + 0\times 2^4 + 1\times 2^5 \end{aligned}$$

   Therefore the answer is given by $(101100)_2$.

2. $$\begin{aligned} (102)_3 + (211)_3 &= (2\times 3^0 + 0\times 3^1 + 1\times 3^2) + (1\times 3^0 + 1\times 3^1 + 2\times 3^2) \\ &= 3\times 3^0 + 1\times 3^1 + 3\times 3^2 \\ &= 0\times 3^0 + 2\times 3^1 + 0\times 3^2 + 1\times 3^3 \\ &= 0\times 3^0 + 2\times 3^1 + 0\times 3^2 + 1\times 3^3 \end{aligned}$$

   Therefore we write the answer as $(1020)_3$.

3. $$\begin{aligned} (7654)_8 + (76543)_8 &= (4\times 8^0 + 5\times 8^1 + 6\times 8^2 + 7\times 8^3) \\ &\quad + (3\times 8^0 + 4\times 8^1 + 5\times 8^2 + 6\times 8^3 + 7\times 8^4) \\ &= 7\times 8^0 + 9\times 8^1 + 11\times 8^2 + 13\times 8^3 + 7\times 8^4 \\ &= 7\times 8^0 + 1\times 8^1 + 4\times 8^2 + 6\times 8^3 + 0\times 8^4 + 1\times 8^5 \end{aligned}$$

   The answer is written as $(106417)_8$.

4. Show that $n\log(n) \in O(\log(n!))$.

Solution: Using the definition of O notation, we are required to find positive constants C and k such that

$$|n\log(n)| \leq C|\log(n!)| \quad \forall n > k$$

If $k > 0$ then all terms in the inequality are positive so we can remove the absolute value signs and we are left with

$$n\log(n) = \log(n^n) \leq C\log(n!) = \log(n!)^C \quad \forall n > k$$

Since $\log(x)$ is a monotone increasing function it suffices to find C and k such that

$$n^n \leq (n!)^C \quad \forall n > k$$

First we will show that

$$(n-z)(z+1) \geq n \quad \forall z = 0,1,2,3,\ldots,n-1$$

Think of the value

$$(n-z)(z+1)-n$$

as a function of z for some constant n. Then we have

$$\begin{aligned}(n-z)(z+1) = nz+n-z^2-z \geq n &\iff -z^2+(n-1)z \geq 0\\ &\iff -z^2+(n-1)z \geq 0\\ &\iff z((n-1)-z) \geq 0\end{aligned}$$

The zeroes of the quadratic equation $z((n-1)-z)$ are $z=0$ and $z=(n-1)$. The coefficient of z^2 is negative so this quadratic equation is non-negative for values of z between 0 and $n-1$. In particular, this is true for $z = 0,1,2,\ldots,n-1$.

Now note that we can rewrite $(n!)^2$ as follows

$$\begin{aligned}(n!)^2 &= (n\cdot(n-1)\cdot(n-2)\ldots 2\cdot 1)(n(n-1)(n-2)\ldots 2\cdot 1)\\ &= (n\cdot 1)((n-1)\cdot 2)((n-2)\cdot 3)((n-3)\cdot 4)\ldots(2\cdot(n-1))\cdot(1\cdot n)\end{aligned}$$

Using the fact that $((n-z)(z+1)) \geq n$ for $n = 0,1,2,\ldots,n-1$ we have

$$(n!)^2 \geq n\cdot n\cdot n\ldots n$$

where there are n copies of n on the right hand side. Therefore

$$(n!)^2 \geq n^n$$

As the natural logarithm is an increasing function, we can infer the following inequality.

$$2\log n! = \log((n!)^2) \geq \log(n^n) = n\log(n)$$

Therefore using the witnesses $C=2$ and $k=1$ we have verified the following inequality.

$$n\log(n) \leq C\log(n!) \quad \forall n > k$$

In particular $n\log(n) \in O(\log(n!))$.

5. Determine whether $\log(n!) \in \Theta(n\log(n))$. Justify your answer.

Solution: In the previous question we showed that

$$n\log(n) \leq 2\log(n!) \quad \forall n > 1$$

Rearranging this equation we can write

$$\log(n!) \geq \frac{1}{2}n\log(n) \quad \forall n > 1$$

This shows that $\log(n!) \in \Omega(n\log(n))$. It remains to show that $\log(n!) \in O(n\log(n))$. Using the definition of O notation, we need to show that there exist positive constants C and k such that

$$\log(n!) \leq Cn\log(n) \quad \forall n > k$$

Note that since $\log(n) > 0$ for n sufficiently large, we have dispensed with the absolute value symbols in the definition. To justify this one needs only to choose k sufficiently large to ensure that all terms are positive.

Recall the definition of the factorial

$$n! = n \cdot (n-1) \cdot (n-2) \cdot (n-3) \ldots 3 \cdot 2 \cdot 1$$

It follows that

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

Note that there are n terms in the sum on the right hand side of this equation and that each of those terms is less than $\log(n)$. It follows that we can bound $\log(n!)$ as follows

$$\log(n!) \leq \sum_{k=1}^{n} \log(n) = n\log(n)$$

Therefore we have verified with required inequality. In particular if we set $C = 1$ and $k = 1$ then we have

$$\log(n!) \leq Cn\log(n) \quad \forall n > k$$

This shows that $\log(n!) \in O(n\log(n))$.

We have shown that $\log(n!) \in \Omega(n\log(n))$ and $\log(n!) \in O(n\log(n))$. Therefore $\log(n!) \in \Theta(n\log(n))$.

6. Give a O–estimate for the number of operations (comparison or multiplication, but ignoring the comparisons to test the for loops) in the following segement of an algorithm:

$m := 0$

`for` $i := 1$ `to` n

  `for` $j := i+1$ `to` n

    $m :=$`max`$(a_i a_j, m)$

Here, $a_1, \ldots, a_n$ are positive real numbers.

Solution: For each choice of i and j we perform the following two operations:

1. Calculate $a_i a_j$.
2. Compare $a_i a_j$ to m in order to see which one is larger.

Therefore the total number of operations is twice the number of pairs of numbers i and j considered by the algorithm. We calculate this number as follows.

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=i+1}^{n} 2 &= 2\sum_{i=1}^{n}\sum_{j=i+1}^{n} 1 \\ &= 2\sum_{i=1}^{n}(n-i) \\ &= 2\left(\sum_{i=1}^{n} n - \sum_{i=1}^{n} i\right) \\ &= 2n^2 - 2(\frac{n(n+1)}{2}) \\ &= n^2 - n\end{aligned}$$

Therefore the number of operations is $O(n^2-n) = O(n^2)$.

7. Devise an algorithm that finds all equal pairs of sums of two terms of a sequence of n integers, and determine the worst-case complexity of your algorithm.

Solution: My algorithm is as follows.

for $i := 1$ to n
  for $j := i+1$ to n
    for $k := 1$ to n
      for $\ell := k+1$ to n
        if $a_i + a_j = a_k + a_\ell$ and $(i,j) \neq (k,l)$
          then output the pairs (a_i, a_j) and (a_k, a_l)

I claim that the worst-case complexity for this algorithm is $O(n^4)$. To verify this claim, note that for each pair of pairs (i,j) and (k,l) we perform three operations.

1. Calculate $a_i + a_j$.
2. Calculate $a_k + a_\ell$.
3. Check if $a_i + a_j = a_k + a_\ell$

Therefore the number of operations required is calculated as follows.

$$\begin{aligned}
\sum_{i=1}^{n}\sum_{j=i+1}^{n}\sum_{k=1}^{n}\sum_{\ell=k+1}^{n} 3 &= \sum_{i=1}^{n}\sum_{j=i+1}^{n}\sum_{k=1}^{n} 3(n-k) \\
&= \sum_{i=1}^{n}\sum_{j=i+1}^{n} 3\left(n^2 - \frac{n(n+1)}{2}\right) \\
&= \sum_{i=1}^{n}\sum_{j=i+1}^{n} \frac{3}{2}(n^2-n) \\
&= \frac{3}{2}(n^2-n)\sum_{i=1}^{n}\sum_{j=i+1}^{n} 1 \\
&= \frac{3}{2}(n^2-n)\sum_{i=1}^{n}(n-i) \\
&= \frac{3}{2}(n^2-n)\left(n^2 - \frac{n(n+1)}{2}\right) \\
&= \frac{3}{2}(n^2-n)\left(\frac{n^2}{2} - \frac{n}{2}\right) \\
&= \frac{3}{4}(n^2-n)^2 = \frac{3}{4}n^2(n-1)^2
\end{aligned}$$

Therefore the worst-case complexity of this algorithm is $O\left(\frac{3}{4}n^2(n-1)^2\right) = O(n^4)$.

8. 1. Suppose we have n subsets $S_1, \ldots, S_n$ of the set $\{1, \ldots, n\}$. Express a brute-force algorithm that determines whether there is a disjoint pair of these subsets.

2. Give an O–estimate for the number of times the algorithm needs to determine whether an integer is in one of the subsets.

Solution:

1. My algorithm is as follows

```
for i := 1 to n
    for j := i + 1 to n
        m := True
        for k := 1 to n
            if k ∈ S_i and k ∈ S_j
                then m = False
            if m
                then output the pair (S_i, S_j)
```

2. The algorithm tests whether the integer k is in the subset S_i and the subset S_j for each pair (i, j) under consideration. Therefore the total number of such checks is

calculated as follows.

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=i+1}^{n} 2n &= 2n\sum_{i=1}^{n}(n-i)\\ &= 2n\left(n^2-\frac{n(n+1)}{2}\right)\\ &= n^3-n^2\end{aligned}$$

Therefore an O-estimate for the number of times the algorithm needs to check whether an integer is in one of the subsets S_i is $O(n^3)$.

9. Prove using induction that for all $n \in \mathbb{N}$, the product $n(n+1)(n+2)$ is divisible by three. Can you find a simpler proof that does *not* use induction?

Solution: First we prove the statement by induction. First let $n = 1$ so we have

$$n(n+1)(n+2) = 6$$

which is divisible by three.

Now assume that $n(n+1)(n+2) = 3k$ for some $k \in \mathbb{Z}$.

$$\begin{aligned}(n+1)(n+2)(n+3) &= n(n+1)(n+2)+3(n+1)(n+2)\\ &= 3k+3(n+1)(n+2)\\ &= 3(k+(n+1)(n+2))\end{aligned}$$

which is clear divisible by 3 so the result holds.

To see that $n(n+1)(n+2)$ is divisible by 3 without using induction, we need only note that n, $n+1$ and $n+2$ are three consecutive integers so one of them must be divisible by 3. Therefore the product $n(n+1)(n+2)$ must also be divisible by 3.

10. Prove that for all integers $n \geq 2$, $2n+1 < n^3$.

Solution: We proceed by induction. First let $n = 2$ then

$$5 = 2n+1 < n^3 = 8$$

so the statement holds in this case.

Now suppose that $2n+1 < n^3$ for some n. We want to show that $2(n+1)+1 < (n+1)^3$. We have the following

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

So the statement in the question is true if the following are true

$$2n+1+3n^2+3n+1 > 2(n+1)+1$$

However this simplifies to the following

$$3n^2 + 3n > 1$$

which is clearly true because of the assumption that $n \geq 2$. The result therefore follows by induction.

11. A sequence $b_0, b_1, b_2, \ldots$ is defined recursively by:

$$b_0 = 7, \quad b_k = b_{k-1} - 4 \text{ for all integers } k \geq 1.$$

Use induction to prove the general formula $b_n = 7 - 4n$ for all integers $n \geq 0$.

Solution: We first verify the case $n = 0$. We are given $b_0 = 7$ which agrees with the formula $b_n = 7 - 4n$.

Now assume that $b_n = 7 - 4n$. We would like to show that $b_{n+1} = 7 - 4(n+1)$. We do using the recurrence relation as follows

$$\begin{aligned} b_{n+1} &= b_n - 4 \\ &= 7 - 4n - 4 \\ &= 7 - 4(n+1) \end{aligned}$$

so the statement follows.

12. Let $(b_n)_{n \in \mathbb{N}}$ be the sequence defined recursively by:

$$b_1 = 2, \quad b_2 = 4, \quad b_k = 5b_{k-1} - 6b_{k-2} \text{ for each } k \geq 3.$$

Prove using strong induction that $b_n = 2^n$ for all $n \in \mathbb{N}$.

Solution: We are using strong induction so we need to prove more than one base case in this proof. First show that the statement is true for $k = 1$ and $k = 2$. If $k = 1$ then $b_n = 2$ and if $k = 2$ then $b_n = 4$ which verifies the formula in these cases.

Now suppose that $b_n = 2^n$ and $b_{n_1} = 2^{n-1}$. We would like to show that $b_{n+1} = 2^{n+1}$. We do so using the recurrence relation as follows.

$$\begin{aligned} b_{n+1} &= 5b_n - 6b_{n-1} \\ &= 5 \cdot 2^n - 6 \cdot 2^{n-1} \\ &= 5 \cdot 2^n - 3 \cdot 2^n \\ &= 2 \cdot 2^n \\ &= 2^{n+1} \end{aligned}$$

which verifies the formula. Therefore the result follows by strong induction.

13. A sequence of numbers $x_1, x_2, x_3, \ldots$ is defined recursively by the following rules:

$$x_1 = 1 \qquad \text{and} \qquad x_{n+1} = 1 + \frac{x_n}{3}$$

for each $n \geq 2$.

1. Show using induction that $x_n < \frac{3}{2}$ for all $n \in \mathbb{N}$.
2. Using (a), show that the sequence of numbers is strictly increasing, i.e., that $x_{n+1} > x_n$ for all $n \in \mathbb{N}$. (Hint: consider $x_{n+1} - x_n$.)

Solution:

1. We are given that $x_1 = 1$ therefore the statement is immediately true for $n = 1$. Now suppose that $x_n < \frac{3}{2}$. We would like to show that $x_{n+1} < \frac{3}{2}$. We do so by using the recurrence relation as follows.

$$\begin{aligned} x_{n+1} &= 1 + \frac{x_n}{3} \\ &< 1 + \frac{3}{6} = \frac{3}{2} \end{aligned}$$

   and the result follows for all n by induction.

2. We use the definition of x_{n+1} as follows

$$x_{n+1} = 1 + \frac{x_n}{3}$$

   Therefore

$$3x_{n+1} - x_n = 3$$

   and

$$x_{n+1} - x_n = 3 - 2x_{n+1}$$

   However from part $a)$ we know that $x_{n+1} < \frac{3}{2}$. Therefore

$$x_{n+1} - x_n = 3 - 2x_{n+1} > 3 - 2\frac{3}{2} = 0$$

   which is demonstrates the result.

14. Have another look at the Tower of Hanoi, which you saw back in lectures 6 and 11. We *guessed* that the minimal number of moves required to move a tower of n discs from one peg to another has the following explicit formula:

$$T_n = 2^n - 1.$$

Prove this by induction on the number of discs.

Solution: The statement is clearly true for $n = 1$. Now we suppose that it is true for some n. As in the question we let T_n denote the minimal number of moves to move a tower of n discs from one peg to another. We would like to show that $T_{n+1} = 2^{n+1} - 1$.

Suppose we have a tower with $n+1$ discs. In order to move all discs onto another peg then we must, at some point, move the bottom disc. In order to do so we must first move the top $n-1$ discs onto another peg so that there is one peg free and one peg which has only the bottom disc on it. By induction, this takes at least 2^n-1 moves. We then move the bottom disc onto the free peg. To complete the solution we must then put the top n pegs onto the bottom peg. Again, the fewest possible moves this can take is 2^n-1. The total number of moves we have made is given as follows.

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

This shows that there exists a solution to the problem which takes $2^{n+1}-1$ moves. That is, we have shown that $T_{n+1}\leq 2^{n+1}-1$. However the bottom disc must be moved at least once so the only way to produce a shorter solution would be to move the top n discs to another peg in fewer than 2^n-1 moves, which would contradict the induction assumption. Therefore $T_{n+1}=2^{n+1}-1$.

Puzzles on next page!

Here are two **puzzles** that you can think about during the week. Feel free to ask your tutors or lecturer for more hints!

I Egyptian fractions: The ancient Egyptians had the habit of writing fractions in the form:

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\dots,$$

where $a,b,c,\dots$ are whole numbers and *no two of them are equal to each other*. For instance,

$$\frac{3}{8} = \frac{1}{4}+\frac{1}{8} = \frac{1}{3}+\frac{1}{24} = \frac{1}{3}+\frac{1}{33}+\frac{1}{88}.$$

Write $\frac{9}{13}$ in Eqyptian form!

J You have two numbers x and y, and you have written x, y, $x+y$ and $x-y$ each in base 10 and base 2. Unfortunately you were caught in wild stormy weather last Friday, and you dropped your notebook whilst wading through the puddles to get to the train station. Most of the digits have been smudged, and all you can read now is:

Base 10:	$x = **$	$y = **$	$x+y = **$	$xy = 3**$
Base 2:	$x = *0***$	$y = ****$	$x+y = *****1$	$xy = ******1**$

Each $*$ indicate a digit that has been smudged. What were the original numbers x and y?

Puzzle hints:

Stuck on the puzzles from sheet 4? Here are some hints!

G There are not many three-digit multiples of 99. What possible values do they give for the number in B across?

H You can use the equation to prove some properties of f. What can you conclude by setting $x = y = 0$? What can you conclude by setting $y = -x$? Can you prove something about $f(x)$ for all *integers* x?