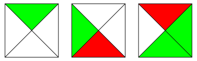
CS2205: Theory of Computation
Problem Class XVI

1. Dr. Toc makes the following assertion: "If a decision problem has only one instance, then that problem must be in **P**." Is the good doctor right? Explain your answer in detail. (Hint: Begin by thinking about what it means to say that a probelm has only one instance.)

2. In lecture 1, we briefly looked at *Tiling Problems*. This question revisits those problems. In a Tiling Problem, you are given a finite set of 1cm × 1cm types of tile, with coloured edges, e.g.:



Tiles are fixed in orientation, i.e. they cannot be rotated.

Here's a problem specification for the Square Tiling Problem:

Problem XVI.1. *SquareTiling*
Parameters: *A finite set $T = \{t_1, \ldots, t_m\}$ of 1cm × 1cm tile types, fixed in orientation, with coloured edges; and G, an n cm × n cm square grid, divided into 1cm × 1cm cells. $m \geq 0; n \geq 0$.*
Returns: *YES if it is possible to tile G with tiles (supply unlimited) taken from among the types in T so that every cell in G contains exactly one tile and the colours on all adjacent tile edges are the same; NO otherwise.*

(a) How many *problem instances* does SquareTiling have?

(b) Is SquareTiling a decision problem?

(c) Here is the outline of an algorithm for solving SquareTiling:


```
while there are untried configurations
{   generate the next configuration (i.e. put a tile into each cell of the grid);
    if there are no clashing edges
    {   return YES;
    }
}
return NO;
```

Give a big-Oh characterisation, in terms of m and n, of the worst-case time complexity of this algorithm. Justify your answer.

(d) The algorithm only tests complete configurations. Imagine instead an algorithm that checks for clashing edges after each tile is placed into the grid. If there is a clash of colours, the algorithm abandons this configuration and moves on to the next one.

Give a big-Oh characterisation, in terms of m and n, of the worst-case time complexity of this algorithm. Justify your answer.

(e) Prove that SquareTiling $\in$ **NP**.

(f) Suppose Dr. Toc carries out a literature survey and finds proofs of the following:

VertexCover $\xrightarrow{\text{poly}}$ SquareTiling and

SAT $\xrightarrow{\text{poly}}$ VertexCover.

Hence, which of the following are true, which are false and which cannot be determined? In each case, explain your answer.

i. SquareTiling is **NP**-hard.
ii. SquareTiling is **NP**-complete.
iii. SquareTiling is in **P**.
iv. SquareTiling is in **NP** but it is not in **P**.

3. Consider the PRIMES decision problem:

Problem XVI.2. *PRIMES*
Parameters: *An integer, n, $n > 1$.*
Returns: *YES if n is prime; NO otherwise.*

For a long time, we have known that PRIMES $\in$ **NP**. We have not known whether PRIMES is **NP**-hard.

In 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxenan published a polynomial-time algorithm to solve PRIMES.

(a) This shows that PRIMES $\in$ **P**. Explain why.

(b) What does the 2002 result tell us about the following problem?

Problem XVI.3. *COMPOSITE*
Parameters: *An integer, n, $n > 1$.*
Returns: *YES if n is composite; NO otherwise. (A composite number is an integer greater than 1 that is not a prime number.)*

(c) *Prove* your answer to the previous question.

(d) What does the 2002 result tell us about whether **P** = **NP**. Explain your answer, considering both the case where PRIMES is not **NP**-hard and the case where one day PRIMES is shown to be **NP**-hard.

(e) Does the 2002 result have any impact in *cryptography*? Explain your answer.

(f) Does the 2002 result have any impact in *cryptanalysis*? Explain your answer.

4. Suppose you want to encrypt the message

$$4; 11; 6; 7$$

using RSA, with $p = 3$, $q = 5$ and $pubKey = 7$. Which of the following lists of numbers would be the encrypted message?

(a) $4^3 \bmod 15; 11^3 \bmod 15; 6^3 \bmod 15; 7^3 \bmod 15$

(b) $4^{15} \bmod 3; 11^{15} \bmod 3; 6^{15} \bmod 3; 7^{15} \bmod 3$

(c) $4^{15} \bmod 21; 11^{15} \bmod 21; 6^{15} \bmod 21; 7^{15} \bmod 21$

(d) $4^7 \bmod 15; 11^7 \bmod 15; 6^7 \bmod 15; 7^7 \bmod 15$

5. Suppose you want to decrypt the message

$$4; 11; 6; 7$$

using RSA with $p = 3$, $q = 5$ and $pubKey = 7$, Which of the four lists of numbers in the previous question would be the result of the decryption? (To answer this will require an amount of trial-and-error.)