CPSC 413 Fall 2018 — Assignment 4

Due no later than Friday, November 30, 2018, 10:30am

This assignment consists of one problem. Full answer (100%) is 10 points.

Finding many pairwise relative primes is hard

Consider the following problem.

RELATIVE PRIME SETS

Input: a set of n positive integers $A = \{a_1, a_2, \ldots, a_n\}$, and
an integer t where $1 \leq t \leq n$.

Output: "Yes" if there exists a subset $X \subseteq A$ of t integers that are pairwise relative prime, i.e., for all $x, y \in X$ we have that $\gcd(x, y) = 1$.
"No" otherwise.

Example 1: Suppose the input is $A_1 = \{14, 34, 35, 99, 110, 143, 165, 243\}$ and $t_1 = 4$. The set A_1 contains eight integers. Let $X_1 = \{34, 35, 143, 243\}$. Then X_1 is a subset of A_1 of size 4. We can readily verify that the four integers in X_1 are pairwise prime:

1. $\gcd(34, 35) = 1$ so 34 and 35 are relative prime.
2. $\gcd(34, 143) = 1$ so 34 and 143 are relative prime.
3. $\gcd(34, 243) = 1$ so 34 and 243 are relative prime.
4. $\gcd(35, 143) = 1$ so 35 and 143 are relative prime.
5. $\gcd(35, 243) = 1$ so 35 and 243 are relative prime.
6. $\gcd(143, 243) = 1$ so 143 and 243 are relative prime.

That is, all $6 = \binom{4}{2}$ pairs of integers in X_1 are relative prime. Thus X_1 is a subset of A_1 of four integers that are pairwise relative prime. Since the question is whether there is a subset X_1 of A_1 of four ($t_1 = 4$) integers that are pairwise relative prime, we should thus answer "Yes".

Example 2: Suppose the input is $A_2 = \{2, 3, 4, 6\}$ and $t_2 = 3$. We should answer "No", since there does not exist three integers in A_2 that are pairwise relative prime.

In this assignment, we want to show that Independent Set $\leqslant_m^P$ Relative Prime Sets.

1. Let p_j denote the j^{th} smallest prime, for all $j \geq 1$. For instance $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, and $p_5 = 11$. It is known that $p_j \leq 2j\ln(j)$ for large enough j. Show that this implies that we can generate a list of the J smallest primes in time polynomial in J.

2. Give a many-to-one poly-time reduction f from Independent Set to Relative Prime Sets. Note that the input $\langle G, k \rangle$ to your reduction is a graph G and an integer k. The output $\langle A, t \rangle$ of your reduction is a set A of positive integers and an integer t.

   (*Hint:* Set t to be equal to k. Let n be the number of vertices in the input graph. Construct the set A so that A contains n integers, one integer for each vertex.)

3. For your reduction f, show that if G has an independent set of size k, then A has a set X of t pairwise relative prime integers.

4. For your reduction f, show that if A has a set X of t pairwise relative prime integers, then G has an independent set of size k.

5. Argue that your reduction f runs in polynomial time. (*Hint:* This is not immediately obvious. Use that $p_j \leq 2j\ln(j)$ from the first question to deduce that integer p_j can be written in binary using only of order $O(\log(j))$ bits. Just like e.g. the integer 26 can be written in binary as 11010, which is only $\lceil \log_2(26+1) \rceil = 5$ bits.)

Collaboration and plagiarism

You are welcome to work and discuss the assignment with other students enrolled in this course (i.e., CPSC 413 — Fall 2018). You must **clearly state whom your collaborators are**, if any, for the problems on the assignment.

Verbal collaboration is allowed. **Written collaboration is dis-allowed**. No collaboration can use any form of written material. While discussing this assignment with other enrolled students, the following aids are strictly forbidden: papers, notes, notebooks, textbooks, webpages, email, twitter, facebook, sms, messages, whiteboards, blackboards, etcetera. All written work that you submit must be your own sole work. Anything else will be considered plagiarism. All collaborations must take place on an equal footing, where all parties contribute equally to the discussion. Any conversation must be ended if all parties are not contributing equally.

The use of published literature is allowed. If you use any published literature (texts, articles, websites, etc) to complete your assignment, you must quote your sources. I suggest that you develop your own solutions however, without the use of any published materials. You will be asked to answer similar questions on the exams for this course and during the exams no such sources will be available.

You may read about the regulations on plagiarism in the calendar here:
`http://www.ucalgary.ca/pubs/calendar/current/k-2.html`. If you have any doubt whether a collaboration is allowed or not, ask the lecturer before entering the collaboration.

Cover pages and submission guidelines

The last page in the assignment is a cover page. On Assignment 4, there is one problem and thus only one cover page. Prior to submitting your answers, put your sheets of paper in the following order: (1) Cover page for Problem 1, (2) Answer to Problem 1. Use a single staple in the upper left corner to staple **all** of your sheets of paper together. Put your name and TA lab on the cover page.

Assignments diverging from these guidelines, including being submitted without the cover page, or submitted with incorrectly filled cover page, will be deducted 1 or more points.

Submission

You may turn in your assignment using the drop boxes on the ground floor in the math science building (MS), or by giving your assignment in person to one of the TAs or the instructor. You must submit your assignment on or before Friday, November 30, 2018, 10:30am. No late submissions will be accepted. The deadline is **firm**. Note that 10:30am is in the morning.

Cover page for Problem 1

CPSC 413 Assignment 4 Fall 2018

Name: ____

Lab section:

□	□	□	□	□
T01 Mon 15:00	T02 Tue 11:00	T03 Tue 14:00	T04 Mon 17:00	T05 Mon 11:00

My sources and my collaborators, if any, on this problem were:

Problem 1: ____