# CS222: Assignment 6 - Modular arithmetic and Extended Euclid's algorithm

1. Submission deadline: Sunday, 28 March at 11:59 pm.
2. Follow good coding practices to gain more marks.
3. No copying among the students or from the Internet or any other source.
4. The assignment can be submitted in groups of size $\leq 3$.
5. Submit two `.cpp` files and two `.pdf` files.
6. Write the names and roll numbers of the students at the top of each file.
7. The files should be called
   `noModN_firstRollNumber_secondRollNumber_thirdRollNumber.cpp`,
   `extendedEuclid_firstRollNumber_secondRollNumber_thirdRollNumber.cpp`,
   `noModN_firstRollNumber_secondRollNumber_thirdRollNumber.pdf`,
   `extendedEuclid_firstRollNumber_secondRollNumber_thirdRollNumber.pdf`,
8. The pdf should contain the output obtained when each program was run.
9. In case you do not know about C++ templates, check `https://www.learncpp.com/cpp-tutorial/template-non-type-parameters/`. We can also discuss it on Thursday.
10. For more information about question 1: `https://stackoverflow.com/questions/66546257/in-c-can-we-create-a-class-for-each-integer`

---

1. (25 points) Recall the modular arithmetic that we studied in the class. Create a `class noModN`[1] using a C++ template with non-type parameter for $N$. It has a single private data which is an integer between 0 and $N - 1$. This data should be initialised using a constructor that takes an arbitrary integer(may be positive or negative) and converts it to modulo $N$ representation. Do not use `%` operator.

   For this, you will need to implement the `divide(int, int)` algorithm which returns the quotient and the remainder. You can use an array or `struct` for returning two values.

   Also create a default constructor.

   Overload the operators `+`, `*` and `++`[2] for this class.

   Recall that in multiplication, you should go modulo $N$ in each of the intermediate steps.

   Now, in the `main` procedure, take integer inputs $a, b, c$ from the user and create objects of the `class noModN`. Output `(a+b)*c, a++, ++a` in this exact sequence. The output should be clearly understandable.

[1] short for number modulo $N$.

[2] Recall that there are two versions of the `++` operator: prefix `++` as in `++i` and postfix `++` as in `i++`

[If you are brave, you can output/input using `cout/cin`. I.e. by overloading the `<<` and `>>` operators. Write in the common assignment comment on Google classroom whether you have implemented it. No credits for this!]

2. (15 points) Write a recursive program that takes $a$ and $b$ as input from the user and outputs $\gcd(a, b)$ and the integers $x, y$ such that $\gcd(a, b) = ax + by$. The output should be clearly understandable. Example:

```
Input the two numbers:  3 2.

The gcd of 3 and 2 is 1.

1 = (1) * 3 + (-1) * 2.
```