Homework 0

1. **Estimating Sums.** In this problem we estimate two summations.
   - (8 + 8 points) $S = \sum_{i=1}^{n} \frac{1}{i}$. Obtain (meaningful) upper and lower bounds for S using integrals.
   - (9 points) In the lecture, we saw that if f is a concave upwards function then the following is true.

     $$\frac{f(x-1)+f(x)}{2} \geqslant \int_{x-1}^{x} f(t)\,\mathrm{d}t$$

     Prove that, for a concave upwards function f, we have

     $$f(1)+f(2)+\cdots+f(n) \geqslant \frac{f(1)+f(n)}{2} + \int_{1}^{n} f(t)\,\mathrm{d}t$$

2. **Some Group Theory.** In this problem we shall derive some basic results based on the definition of groups introduced in the lectures. Let $(G, \circ)$ be a group and let e be the identity element of the group.
   - (5 points) Prove that it is impossible that there exists $a, b, c \in G$ such that $a \neq b$ but $a \circ c = b \circ c$.
   - (5 points) Suppose $a, b \in G$. Let $\mathsf{inv}(a)$ and $\mathsf{inv}(b)$ be the inverses of a and b, respectively (i.e., $a \circ \mathsf{inv}(a) = e$ and $b \circ \mathsf{inv}(b) = e$). Prove that $\mathsf{inv}(a) = \mathsf{inv}(b)$ if and only if $a = b$.
   - (10+5 points) Let $G = \{x_1, x_2, \ldots, x_n\}$, i.e. G is a finite group. Suppose G also has the **commutativity** property, i.e., for all $a, b \in G$, we have $a \circ b = b \circ a$ (such groups are called Abelian). Define $x = x_1 \circ x_2 \circ \cdots \circ x_n$. Prove that $x \circ x = e$. Give an example of a commutative group where $x \neq e$.

     (Comment: This demonstrates that the result is tight!)

3. **Some properties of $(\mathbb{Z}_p^*, \times)$.** Recall that $\mathbb{Z}_p^*$ is the set $\{1, \ldots, p-1\}$ and $\times$ is integer multiplication $\mod p$, where p is a prime. For example, if $p = 5$, then 2×3 is 1. In this problem we shall show that $(\mathbb{Z}_p^*, \times)$ is a group. The only part missing in the lecture was the proof that every $x \in \mathbb{Z}_p^*$ has an inverse. We will find the inverse of any element x.

- (10 points) Recall $\binom{p}{k} := \frac{p!}{k!(p-k)!}$. For a prime p, prove that p divides $\binom{p}{k}$, if $k \in \{1, 2, \ldots, p-1\}$.
- (5 points) Recall that $(1+x)^p = \sum_{k=0}^{p} \binom{p}{k} x^k$. Prove by induction that, for any $x \in \mathbb{Z}_p^*$, we have

$$\overbrace{x \times x \times \cdots \times x}^{p\text{-times}} = x$$

- (10 points) For $x \in \mathbb{Z}_p^*$, prove that the inverse of x is given by

$$\overbrace{x \times x \times \cdots \times x}^{(p-2)\text{-times}}$$

4. **Efficient Exponentiation Algorithm.** (25 points) Suppose $(G, \circ)$ is a group that is generated by g. In the lecture notes, we have seen an algorithm that constructs the list

$$n[0] = g, n[1] = g^2, n[2] = g^4, \ldots, n[k] = g^{2^k}$$

using the $\circ$ operation only k times.

Suppose i is an integer in the range $\{0, 1, \ldots, 2^{k+1} - 1\}$. Give an algorithm that computes g^i from the list presented above using at most $(k+1)$ additional uses of the $\circ$ operator.