Class Exercises: 2019-10-08

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

1. Consider arithmetic modulo 30, in the domain $\mathbb{Z}_{30}$. For each of the following numbers, find

   1.1. its inverse modulo 30;

   1.2. the smallest positive power of the number that is congruent to 1 modulo 30.

$$1,\ 10,\ 13,\ 19,\ 27,\ 29\,.$$

   Some of your answers might be "does not exist." You may use a calculator and/or the Python 'egcd' function from class.

Recall some notation from the lecture notes:

$$\mathbb{Z}_m^* := \{a \in \mathbb{Z} :\ 0 \le a < m \text{ and } \gcd(a,m) = 1\}\,; \quad \phi(m) = |\mathbb{Z}_m^*|\,.$$

Let's introduce an important piece of mathematical vocabulary. Consider a set S and an operation "op" on elements on S. We say that S is closed under "op" if the result of applying "op" to elements of S always produces an element of S. The concept is best understood through concrete examples.

- The set $\mathbb{N}$ is closed under the *addition* operation, because if $x, y \in \mathbb{N}$, then $x + y \in \mathbb{N}$.
- Similarly, $\mathbb{N}$ is closed under *multiplication*.
- However, $\mathbb{N}$ is not closed under *subtraction*, because there do exist $x, y \in \mathbb{N}$ such that $x - y \notin \mathbb{N}$.
- On the other hand, the larger set $\mathbb{Z}$ is indeed closed under subtraction.

2. Prove that $\mathbb{Z}_m^*$ is closed under multiplication modulo m, for all $m \in \mathbb{N}^+$.

3. Let p and q be two distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

4. Suppose that p and q are distinct primes and $n \in \mathbb{Z}$ is such that $p \mid n$ and $q \mid n$. Prove that $pq \mid n$.
   Hint: Use the GCD Linear Combination Theorem and write $n = n(kp + \ell q)$.