MATH 418/818, Number Theory and Cryptography, Winter 2022
Homework 1
(Due: January 25 11:59 PM (Kingston time), upload on Crowdmark)

Textbook problems.

(1) Exercise 1.3.
(2) Exercise 1.11 (a)-(d).
(3) Exercise 1.18 (a),(c),(f),(g).
(4) Exercise 1.21.
(5) Exercies 1.24.

Properties of integers. Recall the Euclidean algorithm for finding greatest common divisors.

(6) Using the Euclidean algorithm, calculate $\gcd(4235, 792)$.
(7) The second-to-last step of your algorithm from problem (4) should read "$242 - 7 \cdot 33 = 11$." In this equation, substitute for 33 using the previous step: $33 = 275 - 1 \cdot 242$, and repeat plugging in previous steps. (Next you will substitute for 242.) After no more substitutions are possible, you will have an equation $11 = \ldots$. After simplifying, "$\ldots$" is of the form $4235x + 792y$, and x and y are integers. What are they?
(8) Look up the statement of Bézout's identity (for instance, see `https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity`). What does this have to do with the above problems?

The Euler totient function. We recall the Euler φ-function which is defined as

$$\varphi(n) = \#\{a \in \mathbb{Z} : 1 \leq a \leq n \quad \text{and} \quad \gcd(a, n) = 1.\}.$$

(9) Calculate the values $\phi(n)$ for $n \in \{3, 4, 5, 8, 45, 46\}$.
(10) If p is a prime and $k > 0$, prove that

$$\varphi(p^k) = p^k - p^{k-1}.$$

Does the formula match with your results in (9)?
(11) Note that the Euler φ-function is multiplicative, in other words, we have

$$\varphi(mn) = \varphi(m)\varphi(n), \quad \text{when } \gcd(m, n) = 1.$$

Using this property of φ, prove that, for any integer $n > 1$, we have

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct primes p dividing n. (Hint: use induction!)

Modular arithmetic. Let $n \in \mathbb{N}$ be a positive integer. Define a relation $\sim_n$ on $\mathbb{Z}$ as follows: $a \sim_n b$ if and only if $a \equiv b \pmod{n}$.

(12) Prove that $\sim_n$ is an equivalence relation for all $n \in \mathbb{N}$.
(If you want to recall the definition of the equivalence relation and equivalence classes, see `https://en.wikipedia.org/wiki/Equivalence_relation`)
(13) Determine the number of equivalence classes with respect to $\sim_n$.
(14) Write some elements of the equivalence class with respect to $\sim_7$ that contains 3.
(15) Let C and D be equivalence classes of $\sim_n$. Prove that if $c_1, c_2 \in C$ and $d_1, d_2 \in D$, then all four sums $c_1 + d_1, c_2 + d_1, c_1 + d_2, c_2 + d_2$ are in the same equivalence class of $\sim_n$.