Problem Set 1

Due: January 30th, 5pm

1. **Primes in Arithmetic Progressions.**

   Let $a, d \in \mathbb{Z}_{>0}$, and consider the arithmetic progression

   $$a,\ a+d,\ a+2d,\ a+3d,\ \ldots$$

   Using computational experimentation, investigate for which pairs (a, d) the arithmetic progression $a+nd$ contains infinitely many prime numbers. Try at least 6 different pairs (a, d).

   You are strongly encouraged to use SageMath. In SageMath, the expression `i in Primes()` returns `True` if i is prime and `False` otherwise.

   Based on your experiments, state a conjecture characterizing all pairs (a, d) for which the arithmetic progression contains infinitely many primes. Provide clear computational evidence supporting your conjecture (for example, tables, plots, or explicit data).

   You are not expected to prove your conjecture.

2. **The Well-Ordering Principle.**

   Let $S \subseteq \mathbb{R}$. The *Well-Ordering Principle* for S is the statement:

   > Every nonempty subset of S has a least element (with respect to the usual order on $\mathbb{R}$).

   Give an explicit example of a nonempty subset $S \subseteq \mathbb{R}$ for which the Well-Ordering Principle does not hold, and explain carefully why it fails.

3. **Divisibility Statements.**

   Let a, b, c be integers. Determine whether each statement is true or false. If true, give a proof. If false, give a counterexample.

   (a) If $a \mid c$ and $b \mid c$, then $a+b \mid c$.

   (b) If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$.

4. **Linear Diophantine Equations.**

   Find *all* integer solutions to the equation

$$252x + 198y = 18.$$

5. **Congruences.**

   Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{Z}_{>0}$. We say that $a \equiv b \pmod{n}$ or that a is *congruent to* b *modulo* n if $n \mid (b - a)$. Using this definition, prove the following properties.

   (a) Find $a \in \{0, 1, \ldots, 11\}$ such that $7^5 + a \equiv 2 \pmod{12}$.

   (b) Using the definition, prove the following properties:

      (i) $a \equiv a \pmod{n}$

      (ii) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

      (iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

      (iv) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ for all $c \in \mathbb{Z}$.

6. **The Euclidean Algorithm.**

   Let a and b be positive integers with $a > b$, and let

$$b = r_0, r_1, r_2, \ldots$$

   be the successive remainders in the Euclidean algorithm applied to a and b.

   (a) Show that after every two steps, the remainder is reduced by at least one half. In other words, verify that

$$r_{i+2} < \frac{1}{2} r_i$$

   for every $i = 0, 1, 2, \ldots$.

   (b) Conclude that the Euclidean algorithm terminates in at most $2\log_2(b)$ steps, where $\log_2$ denotes the logarithm to the base 2.

   (c) Deduce that the number of steps is at most seven times the number of decimal digits of b.

   Hint: What is the value of $\log_2(10)$*?*

7. **The $3n + 1$ Algorithm.**

   The $3n + 1$ *algorithm* works as follows. Start with any positive integer n.

   - If n is even, divide it by 2.
   - If n is odd, replace it with $3n + 1$.

Repeat this process indefinitely.

For example, starting with 5 we obtain

$$5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$$

and starting with 7 we obtain

$$7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \ldots$$

Notice that if the algorithm ever reaches 1, the sequence repeats $4, 2, 1$ forever.

In general, one of the following two possibilities occurs:

1. The sequence eventually repeats a number that appeared earlier. In this case, the block of numbers between the two occurrences repeats indefinitely. We say that the algorithm *terminates* at the last nonrepeated value, and the number of distinct entries is called the *length* of the algorithm.

2. The sequence never repeats any value, in which case we say that the algorithm does not terminate.

(a) Verify that the algorithm terminates at 1 for the starting values 5 and 7, and compute the length of the algorithm in each case.

(b) Write a short program or use computational software to test the algorithm for many starting values. What do you observe?

(c) State a conjecture about whether the $3n + 1$ algorithm terminates for all positive integers.