[B]eware the mathematician and others who make false prophecies. The danger already exists that the mathematicians have made a pact with the Devil to darken the spirit and confine Man within the bonds of Hell.
—St. Augustine

PROMYS Number Theory **Problem Set #3** *Boston University, July 7, 2021*

Reading Search

Q1: What is meant by the canonical decomposition of an integer into positive primes?

Q2: Use the sieve of Eratosthenes to make a list of all primes less than 200.

Exploration

P1: Consider the complex numbers $a + bi$ with a and b in $\mathbb{Z}$ (where $i = \sqrt{-1}$). These numbers form under addition and multiplication a mathematical system not unlike $\mathbb{Z}$. This system is usually denoted by $\mathbb{Z}[i]$. Which of the properties in P3–P8 of Problem Set #1 and in P2–P5 of Problem Set #2 hold true in $\mathbb{Z}[i]$?

Prove or Disprove and Salvage if Possible

Make an inventory of properties of $\mathbb{Z}$ which you think gives a good description of this mathematical system. Does your inventory suffice to derive everything about $\mathbb{Z}$ which you have proved so far?

P2: If a and b are positive integers and $a|b$ then $a \leq b$.

P3: $ab|ac \Rightarrow b|c$ for all integers a, b, c.

P4: If $a > b$ and $c < 0$ then $ac < bc$. True in $\mathbb{Z}$.

P5: If $a|b$ and $a|(b + c)$ then $a|c$.

P6: Given any pair of natural numbers $a, b \in \mathbb{N}$, there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.

P7: If $a|bc$ and $a \nmid b$ then $a|c$.

P8: If $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots,\ p_n$ are the first n primes then $P_n = p_1 p_2 p_3 \cdots p_n + 1$ is a prime for every n.

Numerical Problems (*Some food for thought*)

P9: Write down all the elements of U_{22}, of U_{23}, of U_{25}, of U_{105}. Which have primitive roots? Any conjectures?

P10: Construct a table of logarithms for U_{19}. Find all the perfect squares in U_{19}.

P11: Describe (and justify, if possible) the process represented by the following table for calculating the successive convergents in P8 of the continued fraction in P7 of Problem Set #2.

		2	1	1	1	3
0	1	2	3	5	8	29
1	0	1	1	2	3	11

Have you noticed anything interesting about the 2×2 determinants

$$\begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 2 & 3 \\ 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} 3 & 5 \\ 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 5 & 8 \\ 2 & 3 \end{vmatrix}, \quad \begin{vmatrix} 8 & 29 \\ 3 & 11 \end{vmatrix} \quad ?$$

P12: Proceed with the fraction $\frac{7469}{2463}$ as in P6, P7, and P8 of Set #2. Plot the values of all of the convergents on the real line and observe carefully relations between the convergents and the fraction itself as well as the relations of the convergents to one another. In approximating the fraction by the convergents of its simple continued fraction expansion, is the price for accuracy in each case unexpectedly high? low?

P13: Use your results in the last two problems to find an integral solution to each of the linear Diophantine equations: $29x + 11y = 1$ and $7469x + 2463y = 1$.

Ingenuity

P14: Consider a rectangular Cartesian coordinate system in a plane. Points with integral coordinates we call *lattice points*. Show that no triangle whose vertices are all lattice points can be an equilateral triangle.