It is an error to believe that rigor in the proof is the enemy of simplicity. On the contrary, . . . the rigorous method is at the same time the simpler and the more easily comprehended. The very effort for rigor forces us to discover simpler methods of proof. It also frequently leads the way to methods which are more capable of development than the old methods of less rigor.
—David Hilbert

PROMYS Number Theory **Problem Set #4** *Boston University, July 8, 2021*

Reading Search

Q1: For $a \in \mathbb{R}$ what is the "greatest integer function" $[a]$? Calculate $\left[\sqrt{5}\right]$, $\left[-\sqrt{2}\right]$, $\left[\frac{\sqrt{7}}{2}\right]$, $\left[2+\sqrt{3}\right]$.

Exploration

P1: $\mathbb{Z}_3[x]$ is very much like $\mathbb{Z}$ in regard to the addition and multiplication of polynomials. Note that x^2+1 is in $\mathbb{Z}_3[x]$ and write down all the elements of $F = (\mathbb{Z}_3[x])_{x^2+1}$. Here F is the system of remainders obtained upon division by x^2+1. Calculate $(x+1)(x+2)$ in F, $\frac{1}{x}$ in F, $\frac{1}{x^2+2}$ in F, $\frac{1}{x^2+2x+2}$ in F.

Prove or Disprove and Salvage if Possible

P2: $ac = bc \Rightarrow a = b$. True in $\mathbb{Z}$. True in $\mathbb{Z}_m$. True in $\mathbb{Z}[i]$.

P3: Let a, b be integers. Then $ab \in \mathbb{N} \Leftrightarrow a \in \mathbb{N}$ and $b \in \mathbb{N}$.

P4: If $a \neq 0$ then $a^2 > 0$. True in $\mathbb{Z}$.

P5: Given two rational integers a and b, there exist integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.

P6: Every integer > 1 has a prime divisor.

P7: There is no integer which lies strictly between 0 and 1.

P8: Let a and n be positive integers greater than 1. If $a^n - 1$ is prime then $a = 2$ and n is a prime.

Numerical Problems

P9: Use Euclid's algorithm to compute $(7469, 2464)$.

P10: Find an integral solution (x, y) of the equation $7469x + 2464y = 77$.

P11: Find all solutions of $2464x = 11$ in $\mathbb{Z}_{7469}$. Find all solutions of $2464x = 9$ in $\mathbb{Z}_{7469}$.

P12: Make a table of logarithms for U_{29}. Use your table to find all solutions of the following equations in $\mathbb{Z}_{29}$:
(a) $13x^3 = 21$; (b) $x^4 = 7$; (c) $x^7 = 18$; (d) $x^7 = 1$.

P13: Find all the primitive roots in U_{19}.

Technique of Generalization

P14: Describe Euclid's Algorithm in a way which would make it possible to apply the process in P6, P7, P8 from Set #2 to $\sqrt{3}$ and other irrationals.

The Art of Counting

P15: Write $|A|$ for the number of elements in a finite set A. Show:
(a) $|A \cup B| = |A| + |B| - |A \cap B|$;
(b) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$;
(c) $|A \cup B \cup C \cup D| = ?$

Ingenuity

P16: In the *decimal* expansion of 100! (100 factorial) how many zeroes occur at the end? How many zeroes are at the end of the *binary* expansion of 100! (that's, one hundred factorial)?