"But you can't prove it," said Susan.
Hawk smiled his warm meaningless smile, "Provin' don't matter to me, knowin's enough."
"I want it all."
—R. I. Parker, *Pale Kings and Princes*.

PROMYS Number Theory **Problem Set #7** *Boston University, July 13, 2021*

Reasoning

P1: Consider a subset S of the natural numbers $\mathbb{N}$. The principle of mathematical induction asserts that if 1 is in the set S and if $n+1 \in S$ whenever $n \in S$, then S is the set of all natural numbers. What is the relationship between the well-ordering principle and the principle of mathematical induction? Can you prove one from the other?

Technique of Generalization

P2: Consider the system $\mathbb{Z}_3[x]$ of polynomials with coefficients in $\mathbb{Z}_3$. Is $\mathbb{Z}_3[x]$ a ring under the addition and multiplication of polynomials? Is $\mathbb{Z}_3[x]$ a commutative ring? With (multiplicative) identity? With cancellation law? When should we say that one polynomial divides another in $\mathbb{Z}_3[x]$? What are the units in $\mathbb{Z}_3[x]$? Which of the following polynomials are prime in $\mathbb{Z}_3[x]$: $x^2+x+2,\ x^3+x^2+1,\ x^3+x^2+x+2,\ x^3-x^2+1,\ x^4+1,\ x^4+x+2$? Construct a table of primes of degree 2 in $\mathbb{Z}_3[x]$.

Prove or Disprove and Salvage if Possible

P3: $[x+y] \geq [x]+[y]$. Here x and y are real numbers and $[x]$ is the greatest integer in x.

P4: $[n+x] = n+[x]$ for $n \in \mathbb{Z}$, $x \in \mathbb{R}$.

P5: Two integers a and b are relatively prime $\Leftrightarrow$ there is an integral solution (x,y) of the linear Diophantine equation $ax+by=1$.

P6: An element a in $\mathbb{Z}_m$ is a unit $\Leftrightarrow$ $(a,m)=1$.

P7: U_m has exactly $\varphi(m)$ elements.

P8: If $a|c$, $b|c$ and $(a,b)=1$ then $ab|c$. True in $\mathbb{Z}$.

P9: There exist infinitely many distinct positive rational primes.

P10: Every natural number >1 has a unique prime factorization.

Numerical Problems

P11: Find the continued fraction of $\frac{1+\sqrt{5}}{2}$. What is the relation between the convergents of this continued fraction and the Fibonacci numbers?

P12: From the simple continued fraction expansion of $\sqrt{5}$ find the convergent with the smallest denominator which approximates $\sqrt{5}$ to within one part in 1000.

P13: Find the GCD of $7+11i$ and $3+5i$ in $\mathbb{Z}[i]$. Does our algorithm in $\mathbb{Z}$ suggest a method?

P14: Calculate $\tau(15!)$. Explain.

P15: Consider the polynomial x^2-6x+8 in $\mathbb{Z}_{105}[x]$. Factor this polynomial into linear factors in $\mathbb{Z}_{105}[x]$ in as many ways as possible.