Set # 16
Ross Program, Number Theory
July 8, 2014

The problem with young people nowadays is that they don't think that they should be doing math all day, every day. – Paul Sally

Prove or Disprove and Salvage if Possible

P1. If $\mathcal{M} \subseteq \mathbf{Z}$ is a subset closed under addition and subtraction, then $\mathcal{M} = d\mathbf{Z}$ for some $d \geq 0 \in \mathbf{Z}$.
If $a, b \in \mathbf{Z}$, then $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ and $a\mathbf{Z} \cap b\mathbf{Z} = \ell\mathbf{Z}$, for suitable $d, \ell \in \mathbf{Z}$.
Does $(a\mathbf{Z})(b\mathbf{Z}) = ab\mathbf{Z}$? Why is $a\mathbf{Z} \cup b\mathbf{Z}$ of less interest here?

P2. There exist infinitely many primes congruent to $-1 \pmod 4$. Congruent to $-1 \pmod 3$.

P3. Euler's function φ is multiplicative.

P4. If π is a prime in $\mathbf{Z}[i]$, then $N\pi$ is a prime in $\mathbf{Z}$.

P5. If $a, b \in \mathbf{Z}^+$ are odd and relatively prime then: $\displaystyle\sum_{\substack{0<x<b/2 \\ x\in\mathbf{Z}}} \left\lfloor \frac{ax}{b} \right\rfloor + \sum_{\substack{0<y<a/2 \\ y\in\mathbf{Z}}} \left\lfloor \frac{by}{a} \right\rfloor = \frac{a-1}{2} \cdot \frac{b-1}{2}.$

Hint: Draw a picture.

P6. If p is prime then every c can be expressed as a sum of two squares: $x^2 + y^2 \equiv c \pmod p$.

Numerical Problems (Some food for thought)

P7. Recall Legendre's symbol from **Set #14** P9: $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbf{U}_p \\ -1 & \text{if } a \text{ is not a square in } \mathbf{U}_p \end{cases}$.

Then: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$; and $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

Evaluate the sum $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)$. Investigate the sum $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a$ for primes $p < 25$.

P8. Find all polynomials $f(x), g(x)$ satisfying $(2x^3+1)f(x) + (x^2+3x+1)g(x) = 1$ in $\mathbf{Z}_5[x]$. Are there any solutions where neither f nor g has a constant term?

Exploration

P9. Observe that $(x+1)(x+2) = (x+4)(x+5)$ in $\mathbf{Z}_6[x]$. Does this mean that $\mathbf{Z}_6[x]$ does not have unique factorization?

P10. If $ad - bc \neq 0$, then for every r, s, the system $\begin{cases} ax + cy = r \\ bx + dy = s \end{cases}$ has a unique solution (x, y).

Find an explicit formula for x, y, showing: $a, b, c, d, r, s \in \mathbf{Z} \Rightarrow x, y \in \mathbf{Q}$.
What conditions on a, b, c, d guarantee that x, y will be integers for every $r, s \in \mathbf{Z}$?
Interpret this as a statement about the lattice generated by vectors $\vec{v} = \binom{a}{b}$ and $\vec{w} = \binom{c}{d}$.
How does this generalize to systems of 3 equations in 3 unknowns?