Set # 19
Ross Program, Number Theory
July 8, 2016

By relieving the brain of all unnecessary work, a good notation sets it free to concentrate on more advanced problems, and, in effect, increases the mental power of the race. - Alfred North Whitehead

Terminology

Q1. Look back at Set #15 P6 to see what it means to say that an arithmetic function is *multiplicative* and then give more examples of multiplicative functions.

Prove or Disprove and Salvage if Possible

P1. If p, q are positive odd primes then $\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}}$.

P2. Let f and g be two arithmetic functions with $g(n) = \sum_{d|n} f(d)$. If g is multiplicative, then so is f.

P3. If π is a prime in $\mathbf{Z}[i]$, then the number of elements in $(\mathbf{Z}[i])_\pi$ is $N(\pi)$.

P4. A *translation* of a plane region $\mathcal{S}$ is a rigid shift of it: add a constant vector to all points in $\mathcal{S}$. An *integer translation* is a shift by an integer vector. For instance, if $\mathcal{D}$ is a disk of radius $1/3$ centered at the origin, then any disk of radius $1/3$ centered at a lattice point is an integer translations of $\mathcal{D}$.
Lemma. If Area$(\mathcal{S}) > 1$, then some nonzero integer translation of $\mathcal{S}$ must overlap $\mathcal{S}$.

P5. $\binom{pA}{pB} \equiv \binom{A}{B} \pmod{p}$. Here p is prime and those are binomial coefficients.
More generally: $\binom{pA+a}{pB+b} \equiv \binom{A}{B}\binom{a}{b} \pmod{p}$. Assume here that $0 \le a, b < p$.
The first congruence here seems to be true (mod p^2). Is that correct for every prime p?

Numerical Problems (Some food for thought)

P6. Is 33 a square in $\mathbf{U}_{73}$? Is 35 ? 36 ? 37 ?

P7. Is 17 a square in $\mathbf{Z}_{509}$? Is 105 a square modulo 997 ?

P8. (a) Does the equation $x^2 = 5$ have a solution in $\mathbf{Z}_{119}$?
(b) Does $x^2 - 3x + 7$ have a root in $\mathbf{Z}_{73}$?

P9. Check that 5 is a square in $\mathbf{Z}_{71}$. Now find all elements of $\mathbf{Z}_{71}$ whose square is 5. Can you perform this calculation efficiently? Can you find $\sqrt{171}$ in $\mathbf{Z}_{1123}$?

P10. Check that 38 is a square in $\mathbf{Z}_{73}$. Now find all elements of $\mathbf{Z}_{73}$ whose square is 38. Can you perform this calculation efficiently? Can you find $\sqrt{1771}$ in $\mathbf{Z}_{2017}$?

P11. Find a quadratic polynomial having the real number $[1, 2, 3, 1, 2, 3, \ldots] = [\overline{1, 2, 3}]$ as a root.

P12. Is $(\mathbf{Z}[i])_3$ a field of 9 elements? Is its group of units cyclic? If so, find a generator. How many generators are there?

Counting Techniques

P13. How many zeros are at the end of the decimal expansion of 1000! ? (That's a factorial.)

P14. Find a formula for the power of the prime p appearing in the canonical factorization of $n!$.

P15. What power of p appears in the factorization of $\binom{n}{k}$?

P16. Define $\mu(n)$ as in Set #18 P2. If the prime factorization of n is given, find $\mu(n)$.
To start concretely, evaluate $\mu(p)$, $\mu(p^2)$, $\mu(pq)$, $\mu(p^2q)$, and $\mu(pqr)$, when p, q, r are distinct primes.