ELEMENTARY NUMBER THEORY

TOPICS AND PROBLEMS, SHEET #1

Preliminaries:

(1.1) How many zeroes does 1000! end in?

(1.2) Calculate $\gcd(3073531, 304313)$.

(1.3) Let $S = \{\log_{10} p : p \text{ prime}\}$. Prove that the elements of S are linearly independent over the rationals.

(1.4) A large furniture store sells 6 kinds of dining room suites, whose prices are \$231, \$273, \$429, \$600.60, \$1001, and \$1501.50, respectively. Once a South American buyer came, purchased some suites, paid the total amount due, \$13519.90, and sailed for South America. The manager lost the duplicate bill of sale and had no other memorandum of each kind of suite purchased. Help him by determining the exact number of suites of each kind the South American buyer bought. (You should show your solution is unique.)

(1.5) Prove that for every non-constant polynomial $f(x) \in \mathbb{Z}[x]$, there is an integer m such that $f(m)$ is composite.

Fermat's Theorem, Euler's Theorem, & Co.:

(2.1) Prove that if n is a pseudo-prime, then $2^n - 1$ is a pseudo-prime.

(2.2) Prove that 1729 is a absolute pseudo-prime (a Carmichael number). In other words, prove that 1729 is composite and that $a^{1729} \equiv a \pmod{1729}$ for every positive integer a.

(2.3) Find the smallest positive integer n such that $a^n \equiv 1 \pmod{120}$ for all integers a relatively prime to 120. (The answer is not $\phi(120)$.)

(2.4) Consider the infinite sequence of numbers $31, 331, 3331, \ldots$. Observe that 2 and 3 do not divide any element of this sequence. Determine with proof the smallest integer > 1 which does divide some element of this sequence.

(2.5) Prove that if ℓ is a positive integer with the property that $\phi(k) \neq \phi(\ell)$ for all positive integers $k \neq \ell$, then $\ell > 10^{10}$. (It is unknown whether any such ℓ exists.)

Chinese Remainder Theorem:

(3.1) A squarefree number is an integer n which is not divisible by the square of a prime. Show that for every integer k, there exists an integer m such that $m+1, m+2, \ldots, m+k$ are all NOT squarefree.

(3.2) Lattice points are points (a, b) where both a and b are integers. A lattice point (a, b) is said to be visible from the origin if a small particle sitting at $(0, 0)$ would be able to see it without its view being obstructed by another lattice point. Convince yourself that a lattice point (a, b) is visible from the origin if and only if $\gcd(a, b) = 1$. Then prove that there exist arbitrarily large circles in the plane such that all the lattice points inside the circle are NOT visible from the origin.

(3.3) Calculate the remainder when $123456789101112\ldots1979$ is divided by 1980?

(3.4) Define a sequence by $a_1 = a$, $a_2 = b$, and $a_{n+2} = a_{n+1} + a_n$ for $n \geq 1$. Find positive relatively prime integers a and b such that a_n is composite for all $n \geq 1$.

ELEMENTARY NUMBER THEORY

TOPICS AND PROBLEMS, SHEET #2

Quadratic Residues and Quadratic Reciprocity:

(4.1) Calculate the Legendre symbols $\left(\dfrac{30}{71}\right)$ and $\left(\dfrac{-56}{103}\right)$.

(4.2) Prove that for every prime p, there is an $a \in \{1, 2, \ldots, 9\}$ such that both a and $a + 1$ are squares modulo p.

(4.3) Prove that there are no integers x and y such that $y^2 = x^3 + 7$.

(4.4) (a) For every odd prime p, prove either $\left(\dfrac{-1}{p}\right) = 1$, $\left(\dfrac{2}{p}\right) = 1$, or $\left(\dfrac{-2}{p}\right) = 1$.

(b) Prove that $x^4 + 1$ is reducible modulo p for every prime p.

(4.5) Prove that for every positive integer N, there is an integer a such that a is not a square modulo p for every prime $p \leq N$.

(4.6) Let p be an odd prime, and let a be the least quadratic nonresidue modulo p. Prove that a is a prime.

Miscellaneous:

(5.1) Using the Chinese Remainder Theorem, find the least positive integer n such that $5|(2^n - 2)$, $7|(2^n - 4)$, $31|(2^n - 8)$, and $127|(2^n - 16)$.

(5.2) (a) Evaluate $\left(\dfrac{15}{107}\right)$.

(b) Using Euler's Criterion and (a), deduce that $15^{53} \equiv -1 \pmod{107}$.

(c) Using (b), prove that 15 is a primitive root modulo 107.

(5.3) Find all primes which have exactly 32 primitive roots.

(5.4) Find all the incongruent roots of $x^5 + x^3 + 5x + 15 \equiv 0 \pmod{135}$.

More Advanced Topics:

(6.1) Let $S = \{n_1, n_2, \ldots\}$ be a set of positive integers such that $\sum_{j=1}^{\infty} 1/n_j$ converges. Define $S(x) = |\{n \leq x : n \in S\}|$. Prove $\lim_{x\to\infty} S(x)/x = 0$.

(6.2) Let $T = \{p_1, p_2, \ldots\}$ be an infinite set of primes for which $\sum_{j=1}^{\infty} 1/p_j$ converges. Define $T(x) = |\{p \leq x : p \in T\}|$.

(a) Prove that $\liminf_{x\to\infty} T(x)/\pi(x) = 0$.

(b) Prove, by example, that it is possible to have $\limsup_{x\to\infty} T(x)/\pi(x) = 1$.

(6.3) Prove that a positive proportion of the positive integers n have a prime factor $> \sqrt{n}$. More specifically, show $\liminf_{x\to\infty} |\{n \leq x : n \text{ has a prime factor } > \sqrt{n}\}|/x > 0$.

(6.4) Using that $\pi(x) = \mathrm{Li}(x) + O(x/\log^3 x)$, show that there is an x_0 such that if $x \geq x_0$, then $\pi(x) > x/\log x$. (It is known that $x_0 = 17$, but you don't need to determine a value for x_0.)

(6.5) It is known that the number of twin primes $\leq x$ is $< cx/\log^2 x$ for some constant $c > 0$. Using this fact, explain why the sum of the reciprocals of the twin primes converges.