Number Theory Handout

January 3, 2008

Fundamental Theorem of Arithmetic: Every $n \geq 0$ Can be expressed in a unique way as

$$\prod_{1 \leq (i) \leq (k)} p_i^{a_i} = n \text{ With } p_i \text{ prime and } a_i \geq 0.$$

Fermat's little Theorem: For p prime and $(a, p) = 1, a^{p-1} = 1 \pmod p$
Wilson's Theorem: $(p-1)! = -1 \pmod p$

The above are also in the notes by Naoki Sato.

1: a)Prove that for all natural numbers $n, 2n + 1$ and $3n + 1$ are relatively prime.
b) Prove that $kn+1$ and $(k+1)n+1$ are relatively prime, where k is a natural number.

2: Let a, b be two relatively prime positive integers. Prove every integer greated than $ab - a - b$ can be expressed as $ax + by$ for whole numbers x, y. Can you generalize this to n variables?

3: Prove that for p an odd prime such that $p = 1 \pmod 4$, We must have
$((p-1)/2)! = -1 \pmod p$
Hint: Use Wilson's theorem.

3: Prove that for all whole numbers m, n,
$m^3 + mn^3 + n^2 + 3$ cannot divide $m^2 + n^3 + 3n - 1$

4: Prove that $a^2 + b^2 + c^2 = 2012$ has no solutions in positive integers.

5: Prove $n^4 + 4m^4$ isn't prime for $m, n > 1$.

6: Let n be a positive integer relatively prime to 6. Prove that
$2^{-1} + 3^{-1} + 6^{-1} = 1 \pmod n$ Where x^{-1} denotes the multiplicative inverse of x modulo n.

7 : Let $r(n)$ be the sum of the remainders when n is divided by $1, 2, 3, ..n$. Prove that for infinitely many positive integers k, we have $r(k) = r(k-1)$.

8 : For each positive integer n, let $g(n)$ be the numerator of $\frac{n}{\phi(n)}$, and $f(n) = \phi(g(n))^{n^2+1}$. For each n, find $f(f(f(...f(n)...)))$ where there are n iterations of f.
HINT: This is not as terrible as it looks.

9 : Find all natural numbers n such that n divides $2^n - 1$

10 : Find all integer a such that $a^4 + 4^a$ is prime.

11 : Find all integer solutions to $x_1^9 + x_2^9 + ... + x_8^9 = 2005$.

12 : Prove that every positive integer can be written as $x^2+y^2-5z^2$ with x, y, z integers.

13 : Let $P(x)$ be a polynomial with integer coefficients. n is an integer, and define a_i recursively by $a_0 = n, a_i = P(a_{i-1})$. Prove that if $a_k = n$ for some positive integer k, then $a_2 = n$.

14: (APMO 1994) Find all n such that n can be written as $n = a^2 + b^2$ such that every prime not exceeding $\sqrt{n}$ divides ab.

15: Prove that for any $n > 1$, there is a power of 10 with n digits either in base 2 or in base 5, but not in both.

16: Given a set S of 100 positive integers ,prove that there are 11 numbers a_i in S such that EITHER a_1 divides a_2 divides a_3..., OR none of the a_i divide each other. Must there be at least 2 distinct, but not necessarily disjoint such sets?

17: Let $a_1, a_2, ...a_{n+1}$ be a sequence of positive integers with $a_1 = a_{n+1}$. Prove that $\prod_{1 \le i \le n}(a_i + 2a_{i+1})$ is not a power of 2.

The following problems are designed to get you more comfortable working modulo primes

18: Let p be an odd prime. Prove that exactly half of the numbers $1, 2, .., p-1$ are quadratic residue modulo p.

19: Prove that if x is a quadratic non-residue modulo a prime p, and S a set exhausting all quadratic residues, then the set xS, which consists of the elements xs with $s \in S$

exhausts the set of quadratic non-residues modulo p.

20: Let p be an odd prime. Prove that there exists an x such that x^2+1 is not a square modulo p.

21: p is a prime. Prove that every number n can be written as x^2+y^2 modulo p.

22:(IMO 2003, problem 6) Prove that for each prime p, there is a prime q such that $n^p - p$ is not divisible by q for any integer n, by first solving the following 2 problems.

23: Let $N = 1 + p + p^2 + .. + p^{p-1}$. Prove that N has a prime factor q which is not equal to $1 \pmod{p^2}$

24 Prove that q does not divide $p-1$.

Now show that this q solves problem 22