December 23, 2004

Review for Final Exam Math 431

Example *There exists infiitely many primes of the form* $2^r k + 1, r \in \mathbf{N}$.

Proof. The case $r = 1$ means that there are infinitely many odd primes which is certainly true. Suppose there are finitely many primes of the form $4k + 1$ then we we may label them all as $\{p_1, ..., p_n\}$. Let $N = (2p_1...p_n)^2 + 1$ and suppose that N is not a prime then there is a prime factor p, i.e., $N = 0 \pmod p$. It is clear that p is odd and $p \neq p_i$ for all $i = 1, ..., n$; indeed we have

$$(2p_1...p_n)^2 = -1 \pmod p. \tag{1}$$

Squaring yields $(2p_1...p_n)^4 = 1 \pmod p$. Let $d = (4, p-1)$ be the greatest common divisor then $d = 1, 2$ or 4. By the Corollary $(2p_1...p_n)^d = 1 \pmod p$ hence, in view of (1), $d \neq 1$ and $d \neq 2$. Thus 4 divides $p - 1$ and so p must be one of the p_i. This absurdity means that there must be infinitely many primes of the form $4k + 1$.

Problem 1. Complete the proof of the preceding Example.

Problem 2. The Fermats numbers are of the form $F_n = 2^{2^n} + 1$. it is easily checked that F_n is prime for $n = 1, 2, 3$ and 4. Use Fermat's Theorem and its Corollary to show that F_5 is not a prime. (Hint: First show that if p is a prime factor of $2^{2^n} + 1$ then $2^{2^{n+1}} = 1 \pmod p$. Next show that the GCD of 2^{n+1} and $p - 1$ must be 2^{n+1}. This means that p must be of the form $2^{n+1}k + 1$. Set $n = 5$ and use brute force to find a prime factor of F_5.)

Problem 3. Find n so that $3^n + 2^n$ is divisible by 7.

Problem 4. If $m = p_1 p_2$ where p_1 and p_2 are primes. Show that $\phi(1) + \phi(p_1) + \phi(p_2) + \phi(p_1 p_2) = m$.

Problem 5. Extend the preceding problem to the case where m is the product of 3 primes.

Problem 6. Find another Carmichael number.

Problem 7. If $p - 1 = 6k$ how many solutions does the equation $x^{6k} = 1$ (respectively $x^{3k} = 1, x^{3k} = -1$) $\pmod p$ have?

Problem 8. Find all positive integer solutions of the equation $x^2 - 3y^2 = 1$.