Math 522 Exam 11 Solutions

1. Set $\alpha = 2^{99}$. Is $\binom{2\alpha-1}{\alpha-1}$ even or odd?
   BONUS: For all $k \in \mathbb{N}_0$, set $\alpha = 2^k$, and determine whether $\binom{2\alpha-1}{\alpha-1}$ is even or odd.

   Recall a useful fact from arithmetic: $1 + 2 + 2^2 + 2^3 + \cdots + 2^w = 2^{w-1} - 1$. *This can be assumed as "common knowledge", or proved as a partial sum of a geometric series, or by induction, or by writing numbers in binary. Note that* $\binom{2\alpha-1}{\alpha-1} = \frac{(2\alpha-1)!}{(\alpha-1)!\alpha!}$.

   It's almost easier to do the bonus first. We need to know how many 2's divide $(2^c)!$ *and* $(2^c - 1)!$, *for every natural number c.*

   The former is $\lfloor 2^c/2 \rfloor + \lfloor 2^c/2^2 \rfloor + \lfloor 2^c/2^3 \rfloor + \cdots = 2^{c-1} + 2^{c-2} + 2^{c-3} + \cdots + 1 = 2^c - 1$. *The latter is* $\lfloor (2^c-1)/2 \rfloor + \lfloor (2^c-1)/2^2 \rfloor + \lfloor (2^c-1)/2^3 \rfloor + \cdots = (2^{c-1} - 1) + (2^{c-2} - 1) + (2^{c-3} - 1) + \cdots + (1 - 1) = (2^{c-1} + 2^{c-2} + 2^{c-3} + \cdots + 1) - c = 2^c - 1 - c$.

   So, the number of 2's that divide $\frac{(2^{k+1}-1)!}{(2^k)!(2^k-1)!}$ *is* $\left(2^{k+1} - k - 2\right) - (2^k - 1) - (2^k - k - 1) = 0$. *Since no 2's are left, the expression is odd for all k.*

2. Prove that there exist infinitely many primes congruent to 3 (mod 4).

   Suppose there were finitely many (say k) such primes; call them $p_1, p_2, \ldots p_k$. *Set* $N = 4p_1p_2 \cdots p_k - 1$, *and consider the prime factorization* $q_1q_2 \cdots q_j$ *of* N. *Suppose that one of the* $q_1, \ldots, q_j$ *(say* q_1*) is congruent to 3 (mod 4). Then it would be among the finite collection* $\{p_1, \ldots, p_k\}$, *and so* $q_1 | N, q_1 | (N + 1)$ *and hence* $q_1 | gcd(N, N + 1) = 1$, *which is impossible since* q_1 *is prime. Hence each of the q's is congruent to 0, 1, or 2 (mod 4). But no product of these can equal 3 (mod 4), which contradicts the fact that* N *is congruent to 3 (mod 4).*

   There is a wonderful theorem of Dirichlet (first conjectured by Gauss) that if $gcd(a, b) = 1$, *then there are infinitely many primes congruent to a (mod b). Further, if we add the reciprocals of these primes, that sum diverges. This theorem is very difficult to prove.*

3. Exam grades: 104, 99, 87, 83, 78, 78, 75, 70, 69, 68, 68, 67, 53