Math 7770 Spring 2011
Homework 3
Due: February 7, 2011

You are welcome to work together but everyone needs to write up **distinct** solutions. If you use any books outside of our textbook or other people, please make sure to give them credit. Make sure your solutions are complete. If your handwriting is atrocious, I am happy to give you a basic introduction to LaTeX.

Warmup

- §2.1 #19. Prove that $n^6 - 1$ is divisible by 7 if $(n, 7) = 1$.
- §2.2 # 4. The fact that the product of any three consecutive integers is divisible by 3 leads to the identical congruence $x(x+1)(x+2) \equiv 0 \bmod 3$. Generalize this, and write an identical congruence modulo m.
- §2.2 # 6. How many solutions are there to each of the following congruences:
  (a) $15x \equiv 25 \bmod 35$
  (b) $15x \equiv 24 \bmod 35$
  (c) $15x \equiv 0 \bmod 35$
- §2.3 #1, #2, #3. Any of these are good practice for using the Chinese Remainder Theorem.
- §2.3 #4. Find all integers that give the remainders $1, 2, 3$ when divided by $3, 4, 5$, respectively.

Problems

1. §2.1 # 53. Show that there are infinitely many n such that $n! - 1$ is divisible by at least two distinct primes.
2. §2.2 # 2. Denoting the number of solutions of $f(x) \equiv k \bmod m$ by $N(k)$, prove that $\sum_{k=1}^{m} N(k) = m$.
3. §2.2 # 9. Show that the congruence $x^2 \equiv 1 \bmod 2^\alpha$ has one solution when $\alpha = 1$, two solutions when $\alpha = 2$, and precisely the four solutions $1, 2^{\alpha-1} - 1, 2^{\alpha-1} + 1, -1$ when $\alpha \geq 3$.
4. §2.3 # 7. Determine whether the congruences $5x \equiv 1 \bmod 6$ and $4x \equiv 13 \bmod 15$ have a common solution and find them if they exist.
5. §2.3 # 19. Let m_1, m_2, …, m_r be relatively prime in pairs. Assuming that each of the congruences $b_i x \equiv a_i \bmod m_i$, $i = 1, 2, \ldots, r$ is solvable, prove that the congruences have a simultaneous solution.

Challenge

I. §2.1 #46. For any prime p, if $a^p \equiv b^p \bmod p$, prove that $a^p \equiv b^p \bmod p^2$.

II. §2.1 #56. Let p be a prime number, and suppose that x is an integer such that $x^2 \equiv -2 \bmod p$. By considering the numbers $u + xv$ for various pairs (u, v), show that at least one of the equations $a^2 + 2b^2 = p$, $a^2 + 2b^2 = 2p$ has a solution