CSE 321: Discrete Structures
Assignment #4
Due: Friday, October 28

Reading Assignment: Read Sections 3.3 and 3.4

Problems: (8 points each)

1. Prove that if $a|b$ and $b|c$, then $a|c$.
2. Let a, b and c be integers. Prove that if a does not divide bc, then a does not divide c.
3. Prove that any prime number bigger than 3 is congruent to 1 or 5 modulo 6.
4. How many zeros are there at the end of $100!$ Justify your answer. The function $n!$ is the product of all the integers 1 through n. (Hint: Think about the unique factorization of $100!$ into primes. What about this factorization determines the number of zeros at the end of the decimal representation of $100!$?)
5. Using only your brain, pencil, and paper (e.g., no calculator), compute $23^{25} \bmod 31$. Show your intermediate steps (as proof that you used your brain instead of a calculator). (Hint: If you use the method I demonstrated in lecture, you should never need to compute any product greater than $15 \cdot 15$.)
6. Use Euclid's algorithm to compute the following, showing the values of x and y for each iteration of the algorithm.
   (a) $\gcd(1020, 1173)$
   (b) $\gcd(1019, 1173)$
7. Suppose that you want to compute gcd(a, b), where a and b each have n digits. The naive algorithm that first finds the prime factorization of a and b uses approximately $10^{n/2}$ integer divisions to do so, by trying all possible divisors up to $\sqrt{a}$ and $\sqrt{b}$, respectively. In contrast, Euclid's algorithm uses approximately $5n$ divisions. Suppose you were running these two algorithms on a computer that could do 10^9 divisions per second. Put your answers to the following questions into a single 3×2 table:
   - What is the greatest number n of digits that you could handle by each of the two methods in 10^{-6} seconds of computer time?
   - What is the greatest number n of digits that you could handle by each of the two methods in 10^{-3} seconds of computer time?
   - What is the greatest number n of digits that you could handle by each of the two methods in 1 second of computer time?