MATH 2610
Discrete Mathematics for Computer Science
Thursday February, 24 2005

I will collect homework next Wednesday so that you can ask me some questions about this assignment (or any other assignment for that matter). All of the below exercises come from material in section 2.4 of the book.

(1) Let $a, b, c \in \mathbb{Z}$. Prove that if $a|b$ and $b|c$, then $a|c$.

(2) Show that if $a, b, c, d \in \mathbb{Z}$ so that $a|c$ and $b|d$, then $ab|cd$.

(3) Show that if $a, b, c \in \mathbb{Z}$ so that $ac|bc$, then $a|b$.

(4) Find the prime factorization of each of these integers.
  - (a) 39
  - (b) 81
  - (c) 101
  - (d) 143
  - (e) 289
  - (f) 899

(5) Find the prime factorization of $10!$.

(6) Which positive integers less than 30 are relatively prime to 30?

(7) Evaluate these quantities,
  - (a) $-17 \mod 2$.
  - (b) $144 \mod 7$.
  - (c) $-101 \mod 13$.
  - (d) $199 \mod 19$.

(8) List five integers that are congruent to 4 modulo 12.

(9) What are the greatest common divisors of these pairs of integers?
  - (a) $a = 2^2 \cdot 3^3 \cdot 5^5$, $b = 2^5 \cdot 3^3 \cdot 5^2$.
  - (b) $a = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $b = 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$.
  - (c) $a = 17$, $b = 17^{17}$.
  - (d) $a = 2^2 \cdot 7$, $b = 5^3 \cdot 13$.
  - (e) $a = 0$, $b = 5$.
  - (f) $a = 2 \cdot 3 \cdot 5 \cdot 7$, $b = 2 \cdot 3 \cdot 5 \cdot 7$.

(10) What are the least common multiples of the pairs of integers in the previous exercise?

(11) If the product of two integers is $2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}$ and their greatest common divisor is $2^3 \cdot 3^4 \cdot 5$, what is their least common multiple?

(12) Show that if $n|m$ where n and m are positive integers greater than 1, and if $a \equiv b \mod m$, where a and b are integers, then $a \equiv b \mod n$.

(13) What sequence of pseudorandom numbers is generated using the recursive definition $x_{n+1} = 3x_n \mod 11$ with seed $x_0 = 2$?

(14) Decrypt the following messages. (They are encoded using some shifting letter cipher like we did in class.)
  - (a) GQZJ OJFSX
  - (b) WHVW WRGDB (MXUW NLGGLQJ)
  - (c) GCV CV LQGU