CS/Math 240: Introduction to Discrete Mathematics 8/2/2007

Homework 7

Instructor: Jeff Kinne TA: Mike Kowalczyk

This homework is due at the beginning of class on Wednesday August 8, 2007. Mike will hold a (homework/exam) review session sometime later in the day.

Problem 1

Show that for any integers a, b, and c, if $a|b$ and $b|c$ then $a|c$.
Note FYI: this shows that the "divides" relation is transitive. It also has the other properties required for it to form a partial order over the integers.

Problem 2

In class we showed that if a and m are relatively prime, then a has an inverse mod m. In this problem, you we show that this is an "if and only if". That is, show that if $gcd(a, m) > 1$ then a does not have an inverse mod m.
Note FYI: together with what we discussed in class, this shows that $\mathbb{Z}/m$ - the integers mod m - are a field iff m is prime. Fields are very important structures in math (but you don't have to know anything about them for this course).

Problem 3

Prove or disprove the following claim: for any integers a, b, and c, if $a|bc$ then either $a|b$ or $a|c$.

Problem 4

How many zeros are there at the end of (100!)? Justify your answer.

Problem 5

Show that at some point there at least n consecutive composite integers, for any $n > 0$.
Hint: consider the n numbers beginning with $(n + 1)! + 2$.

Problem 6

Show that for $m \geq 2$, if $a \equiv b \pmod{m}$, then $gcd(a, m) = gcd(b, m)$.

Problem 7

Recall the fingerprinting problem discussed in class. Party A has an integer x_1, and party B has another integer x_2. We can think of these integers as representing databases. The two parties want to determine if their databases are equal or not. In class we saw a randomized algorithm to accomplish this task that sends roughly $\log(\log(x_1))$ bits from party A to party B (recall that just sending x_1 would take $\log(x_1)$ bits).

After learning about the Chinese Remainder Theorem, your friend thinks that we should instead use the Chinese Remainder representation of x_1 to accomplish this. We will analyze this approach in this problem.

Part a

Suppose that party A wants to use the Chinese Remainder Theorem to send x_1 to party B. You do this by choosing T large enough so that the product of the primes $\leq T$ is at least x_1. You then compute $x_1 \bmod p_i$ for each of the primes $p_i \leq T$, and send *all of these* values to party B. By the CRT, party B can reconstruct x_1 from these values.

Suppose that we know that $x_1 \leq 2^{1000}$. Use the Prime Number Theorem to give an estimate for the value of T needed to ensure that the product of the primes $\leq T$ is at least x_1.

Part b

Give an estimate for the number of bits that would need to be transmitted in order to use your friend's strategy of using the CRT representation of x_1. Is this better or worse than using the randomized algorithm discussed in class? Is this better or worse than just sending the entirety of x_1?