CSC 282 - Fall 2007 - http://www.cs.rochester.edu/~stefanko/Teaching/07CS282/
Homework #3 - due: **Tuesday, Sep. 25, before class**

1. (4 points) Compute the multiplicative inverse of 27 modulo 89 or prove it does not exist. Show all your work. Just stating the answer is not sufficient.

2. (4 points) Compute the multiplicative inverse of 13 modulo 45 or prove it does not exist. Show all your work. Just stating the answer is not sufficient.

3. (4 points) Find the remainder of $1! + 2! + \ldots + 99! + 100!$ when divided by 12.

4. (6 points) True or false? Prove your answer.

   "If $\gcd(x, 21) = 1$ then $x^{20} \equiv 1 \pmod{21}$."

5. (6 points) Consider the following two congruences.

   $(*)$ $21x \equiv 35 \pmod{60}$

   $(**)$ $12x \equiv 20 \pmod{240}$

   Decide whether or not each of the following holds:

   (a) $(\forall x)((*) \Rightarrow (**))$;

   (b) $(\forall x)((**) \Rightarrow (*))$.

   Prove your answers.

6. (4 points) Let $A = 100000007$ and $B = 100000037$. Both A, and B are primes. Let a be the inverse of A mod B. Let b be the inverse of B mod A. What is $(Aa + Bb)$ modulo (AB)? You don't have to compute a and b. Prove your answer.

7. (4 points) For what values of x is the following statement true:

   $(\forall y)($ if $x \mid 6y$ then $x \mid y)$.

   Prove your answer. You must prove (a) that the good values of x are indeed good; and (b) the bad values are indeed bad.

8. (4 points) Compute 10301^2 modulo 10403. Show your work. Use the result to prove that 10403 is not a prime.

9. (5 points) Prove: if p is a prime number and $p \geq 5$ then $p \equiv \pm 1 \pmod 6$.

10. (6 points) Prove: $(\forall x)(x^7 \equiv x \pmod{21})$.

11. (6 points) Decide whether or not the following system of congruences is solvable. Prove your answer.

    $x \equiv 7 \pmod{10}$

    $x \equiv 8 \pmod{15}$

    $x \equiv 1 \pmod{6}$

12. (5 points) Prove: if x is an odd integer then $x^2 \equiv 1 \pmod{8}$.

13. (6 points) Let p be a prime number and a an arbitrary integer. Prove: if $a^{p+1} \equiv 1 \pmod{p}$ then $a \equiv \pm 1 \pmod{p}$.

14. (4 points) Let B be a positive integer. Let $a_n, a_{n-1}, \ldots, a_1, a_0$ be the decimal digits of B (thus $B = a_0 + 10a_1 + \cdots + 10^n a_n$). Prove: $B \equiv a_0 - a_1 + a_2 - + \cdots + (-1)^n a_n \pmod{11}$. (Hint: Examine the sequence $10^k \pmod{11}$.)

15. (4 points) Compute the multiplicative inverse of 2 modulo $2k + 1$.

16. (6 points) Prove that $x^2 \equiv -1 \pmod{43}$ does not have a solution. (Hint: 43 is a prime, use Fermat's little theorem).

17. (10 points) Give an algorithm, which for an input integer A computes $\lfloor \sqrt{A} \rfloor$. The running time of your algorithm should be $O(n^3)$, where n is the number of bits of A.

18. (10 points) Suppose that there is an efficient algorithm $\mathcal{A}$ which on input N (which is a product of two primes) outputs all x such that $x^2 \equiv 1 \pmod{A}$. Show how you can use the algorithm $\mathcal{A}$ to factor a number N, which is a product of two primes.