Discrete Mathematics – CMSC-37110-1 Homework 7 – October 20, 2005

Instructor: László Babai Ry-164 e-mail: laci[at]cs[dot]uchicago[dot]edu

HOMEWORK. Please print your name on each sheet. Please try to make your solutions readable.

This homework is due THURSDAY, OCTOBER 27. It is a lot of work, do not delay, start working on them right away.

READ: relevant sections of text, especially the Chinese Remainder Theorem (solving systems of congruences with pairwise relatively prime moduli).

DO7.1 Prove the basic properties of congruences. All variables are universally quantified.

1. Prove that congruence modulo m is an equivalence relation on $\mathbb{Z}$. State what property of divisibility you rae using for each.
   (a) $a \equiv a \pmod{m}$
   (b) If If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
   (c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
2. The equivalence classes defined by the previous exercise are called the "residue classes mod m." Prove: there are exactly m residue classes mod m.
3. If $a \equiv b \pmod{m}$ then $at \equiv bt \pmod{m}$.
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
   (a) $a + c \equiv b + d \pmod{m}$
   (b) $a - c \equiv b - d \pmod{m}$
   (c) $ac \equiv bd \pmod{m}$.
5. If $a \equiv b \pmod{m}$ then $at \equiv bt \pmod{mt}$.
6. If $a \equiv b \pmod{m}$ and $n \mid m$ then $a \equiv b \pmod{m}$.
7. If $t \mid a$ and $t \mid b$ and $t \mid m$ then $a \equiv b \pmod{m}$ implies $a/t \equiv b/t \pmod{m/t}$.
8. If $t \mid a$ and $t \mid b$ and $\gcd(m,t) = 1$ then $a \equiv b \pmod{m}$ implies $a/t \equiv b/t \pmod{m}$.
9. If $t \mid a$ and $t \mid b$ and $\gcd(m,t) = d$ then $a \equiv b \pmod{m}$ implies $a/t \equiv b/t \pmod{m}$.

DO7.2 Prove: if $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$. (Hint: induction using one of the fundamental properties stated in DO7.1.)

DO7.3 Prove: if $a \equiv b \pmod{m}$ then $\gcd(a,m) = \gcd(b,m)$.

DO7.4 Recall that a positive integer p has the *prime property* if $p > 1$ and $(\forall a, b)(p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b)$.

Prove the uniqueness of prime factorization (Fundamental Theorem of Arithmetic) based on the result that all prime numbers have the prime property. (Hint: induction.)

Homework (due at the beginning of the class **next Thursday, Oct 27**):

HW7.1 (2 points) If $p \geq 5$ is a prime number then $p \equiv \pm 1 \pmod{6}$.

HW7.2 (5+1 points) (a) Prove: if g is a common divisor of a and b and g can be written as a linear combination of a and b then g is a greatest common divisor of a and b. (b) Why "a" greatest common divisor and not "the" greatest common divisor?

HW7.3 (3 points each) Find the following multiplicative inverses or prove that they don't exist. Use Euclid's algorithm as shown in class; show all steps.

1. $6^{-1} \pmod{73}$
2. $13^{-1} \pmod{21}$
3. $14^{-1} \pmod{98}$.

HW7.4 (3+4+8 points) Find the following multiplicative inverses by guessing and verifying. Your answer should be an integer between 1 and the modulus minus 1. Write the verification in detail.

1. $k^{-1} \pmod{2k+1}$.
2. $(k+1)^{-1} \pmod{k^2}$.
3. $F_n^{-1} \pmod{F_{n+1}}$ where F_n is the n-th Fibonacci number.

HW7.5 (4+8 points) (a) Let p be a prime number. Prove: if $x^2 \equiv 1 \pmod{p}$ then $x \equiv \pm 1 \pmod{p}$. (b) Let p and q be two distinct odd prime numbers. Prove: there exists x such that $x^2 \equiv 1 \pmod{pq}$ but $x \not\equiv \pm 1 \pmod{pq}$. *Hint.* Recall that $a \equiv b \pmod{pq}$ is equivalent to ($a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$). Solve separately modulo each prime; combine using the Chinese Remainder Theorem.

HW7.6 (6 points) Decide whether or not the following system of congruences is solvable. If so, find *all* solutions; state, modulo what integer the solution is unique. If not, prove your answer.

$x \equiv 4 \pmod{7}$

$x \equiv 6 \pmod{11}$

$x \equiv 1 \pmod{6}$

HW7.7 (6 points) Decide whether or not the following system of congruences is solvable. If so, find *all* solutions;state, modulo what integer the solution is unique. If not, prove your answer.

$x \equiv 4 \pmod{8}$

$x \equiv 6 \pmod{10}$

$x \equiv 1 \pmod{5}$

HW7.8 (5 points) Prove: if p is a prime number and $1 \leq k \leq p-1$ then p divides $\binom{p}{k}$. Use the fact that p has the prime property; do not use the uniqueness of prime factorization.

HW7.9 (Challenge problem.) Prove: $(\forall k \geq 1)(\exists x)(x^2 \equiv -1 \pmod{5^k})$.

HW7.10 (Challenge problem.) Let $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$. Let T_n denote the set of integers k such that $1 \leq k \leq n$ and $\gcd(k,n) = 1$. Let $\mu(n) = \sum_{k \in T_n} \omega^k$. Prove: $(\forall n)(\mu(n) \in \{-1, 0, 1\})$.