ASSIGNMENT 3 – ELEMENTARY NUMBER THEORY MATH 392

Eyal Goren, November 6, 1998

In this assignment (and through the course) a "group" means an "abelian group". Answer the following questions:

1. Let $n \in \mathbb{N}$ and write n in the usual decimal expansion:

$$n = a_k \cdots a_2 a_1.$$

That is, the a_i's are just the digits of n. Use the technique of congruences to prove the following:

(A) n is divisible by 3 if and only if $a_1 + a_2 + \cdots a_k$ is divisible by 3. (E.g.: 231231 is divisible by 3 and indeed $2+3+1+2+3+1 = 12$ is divisible by 3).

(B) n is divisible by 11 if and only if $-a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$ is divisible by 11. (E.g.: 231231 is divisible by 11 and indeed $-2+3-1+2-3+1 = 0$ is divisible by 11).

(C) n is divisible by 7 if and only if the number $a_k \cdots a_3 a_2 - 2a_1$ is divisible by 7. (E.g.: 23107 is divisible by 7. The criterion says it is enough to check that $2310 - 2 \cdot 7 = 2296$ is divisible by 7. Iterating, it is enough to prove that $229 - 2 \cdot 6 = 217$ is divisible by 7. Iterating, it is enough to prove $21 - 2 \cdot 7 = 7$ is divisible by 7 and it is !)

2. Prove that every year we must have "Friday the 13-th" (Assume that every month contains precisely 30 days).

3. Do exercise (i) on page 25 in Baker's: :Find an integer x such that

$$2x \equiv 1 \pmod 3, \quad 3x \equiv 1 \pmod 5, \quad 5x \equiv 1 \pmod 7.$$

4. Let G be a group. Prove: (i) $-(-x) = x$; (ii) $-(nx) = n(-x)$ for $n \in \mathbb{N}$, where $nx = x + x + \cdots + x$ (n times).

5. Let G be a group and H_1, H_2 subgroups.

(A) Prove that

$$H_1 + H_2 = \{h_1 + h_2 : h_1 \in H_1, h_2 \in H_2\}$$

is a subgroup.

(B) Prove that $H_1 \cap H_2$ is a subgroup.

(C) Give an example where $H_1 \cup H_2$ is not a subgroup.

(D) Let H be a nonempty *subset* of G such that

$$x, y \in H \Rightarrow x - y \in H.$$

Prove that H is a subgroup.

6. (A) Define the least common multiple of $x, y \in \mathbb{N}$ to be a number f such that $x|f, y|f$ and if $x|h, y|h$ then $f|h$. Prove that such a number exists and unique. It is denoted $lcm(x, y)$.

Prove that we have: $lcm(x, y) = xy/gcd(x, y)$.

(B) consider the subgroups $x\mathbb{Z}$ and $y\mathbb{Z}$ of $\mathbb{Z}$. Prove that

$$x\mathbb{Z} \cap y\mathbb{Z} = f\mathbb{Z}, \;\; x\mathbb{Z} + y\mathbb{Z} = d\mathbb{Z},$$

where $d = gcd(x, y), f = lcm(x, y)$.