Exercise set 5 **Number Theory**
Tuesday OCT 18 2011 at 4 pm. Sharp **in MaD-302**

1. *Use the divisibility criterion to decide whether 123456789 is divisible by*
   (a) *3 or 9*
   (b) *11.*
   (c) *Is* 476271 *a prime ? (No division!)*

2. *Invent or find the div. criteria and find which of the numbers 222222, 600560 and 3416 are divisible by*
   (i) *4*
   (ii) *8*

3. *This is an exercise in Algebra. sta tiedetään, että*

Def: *The order of a (finite) group G is $\#G$.*

Def: *The order of an element $a \in G$ is* $\min\{n \in \mathbb{N} \mid a^n = 1\}$ *(=$\#\langle a\rangle$.)*

Exx: *ord* $\mathbb{Z}_5^* = 4$, *ord* $\mathbb{Z}_{10}^* =$ *ord* $\{a \in Z_{10} \mid a$ *is invertible*$\} =$ *ord* $\{\{a \in Z_{10} \mid (a, 10) = 1\} =$ *ord* $\{1, 3, 7, 9\} = 4$. *Generally ord* $\{\mathbb{Z}_n^* \varphi(n)$.

ord $1 \in \mathbb{Z}_{10}^* = 1$ *since* $1^1 = 1$.

ord $3 \in \mathbb{Z}_{10}^*$ *kertaluku on 4 since* $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^3 = 27 = 7 \neq 1$ *and finally* $3^4 = 81 = 1$.

ord $9 \in \mathbb{Z}_{10}^* = 2$ *since* $9^1 = 9 \neq 1$, *but already* $9^2 = 81 = 1$.

Lagrange's *theorem: ord* $a \mid$ *ord* G.

Prove Euler's thm by Lagrange's.

4. (a) *Solve the linear congruence* $3x \equiv 5 \pmod 7$,
   (b) *Solve the linear congruence* $6x \equiv 5 \pmod{12}$.
   (c) *How many solutions (classes) exist for* $943x \equiv 381 \pmod{2576}$,
   (d) *How many solutions (classes) exist for* $1375x \equiv 242 \pmod{5625}$*?*

Perustele.

5. *Solve the linear congruence* $6x \equiv 4 \pmod{10}$ *by 3 methods.*

6. *If a number is divided*
   (i) *by 2, 1 remains*
   (ii) *by 3, 2 remain,*
   (iii) *by 7, nothing remains*

Find the number(s).

7. *Solve the simultaneous congruences:*

a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{12} \end{cases}$ b) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$ c) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 8 \pmod{12} \end{cases}$ d) $\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 6 \pmod{10} \\ x \equiv 9 \pmod{11} \end{cases}$

NEWPAGE

8. *Let p and q be different primes. Prove*

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Assume $p \in \mathbb{P}$. Prove

(a) $(a+b)^p \equiv a^p + b^p \pmod{p}$, *(Use Fermat's little thm)*
(b) $(a+b)^p \equiv a^p + b^p \pmod{p}$, *(Do NOT use Fermat!)*
(c) $a^p \equiv a \pmod{p}$ *by (2) (Prove Fermat's little thm by (b).)*