INTRODUCTION TO NUMBER THEORY. (Fall 2015)

2. EXERCISES (Mo 14.9)

1. Prove (Thm 2.4 of lectures): If P is a polynomial of k variables with integer coefficients, then

$$P(x_1, \ldots, x_k) \equiv P(y_1, \ldots, y_k) \pmod{m},$$

whenever $x_j \equiv y_j \pmod{m}$ for all $j = 1, \ldots, k$.

2. (i) Write down the addition and multiplication tables of the rings $\mathbf{Z}_6$ and $\mathbf{Z}_7$.

(ii) Which elements in $[a] \in \mathbf{Z}_6$ possess square root and determine them all (i.e. solutions of $x^2 = [a]$ in $x \in \mathbf{Z}_6$). Do the same in the ring $\mathbf{Z}_7$.

3. **(i)** Let $p, q \in \mathcal{P} \setminus \{2\}$ ja $p \neq q$. Show that then $pq | (2^{(p-1)(q-1)} - 1)$.

(ii) Does part (i) hold if $p = q$?

4. Prove (Thm 2.8 of lectures): Let $m \geq 2$ ja $U \subset \mathbf{Z}$. Then U is a complete residue system (mod m)if and only if at least two of the following conditions hold:

(i) U has m elements,

(ii) elements of U are mutually incongruent (mod m),

(iii) for every $a \in \mathbf{Z}$ there is $u \in U$ so that $a \equiv u \mod m$.

5. Show that $n|m$ implies $\phi(n)|\phi(m)$.

6. (i) Let p be a prime. Show that the binomial coefficient $\binom{p}{k}$ is divisible by p for every $1 \leq k \leq p-1$.

(ii) Verify that (i) implies $a^p + b^p \equiv (a+b)^p \pmod{p}$. Use induction to obtain $(a_1 + \ldots a_\ell)^p \equiv a_1^p + \ldots a_\ell^p \pmod{p}$ for all $a_1, \ldots a_\ell$. Deduce Fermat's little theorem with the choice $a_1 = \ldots = a_\ell = 1$.

7*. Prove the principle of inclusion and exclusion mentioned at lectures.

Vihjeitä:

T.1: [Use Theorem 2.4 separately on each variables.]

T.7: [Laske kuinka monta kertaa jokin tietty alkio tulee lasketuksi kummallakin puolen kaavaa. TAI: Induktio joukkojen lukumäärän suhteen.]