INTRODUCTION TO NUMBER THEORY. (Fall 2015)

3. EXERCISES (Mo 21.9)

1. Solve a version of the problem of Chinese mathematician Sun Tzu (from 3:rd century): How many soldiers (at least) are in the army of general Han Xing? It is known that if the army marches in rows of 7 soldiers, only five soldiers remain for the last row. And if in rows of 10 or in rows of 11, in both cases nine remains over.

2. List all the units (i.e. invertible elements) in the rings Z_{12}, Z_{20} and find their inverses. Check that the number of units in these cases is in accordance with the result of lectures (which says that it is $\varphi(m)$ in Z_m).

3. Find all numbers $n \geq 2$ such that $\varphi(n) = 12$.

4. Prove in detail the fact used in the second proof of Lagrange's theorem: Assume that $m \in \mathcal{P}$ and f is a polynomial of degree $n \geq 2$ with coefficients in Z_m, and $P([a]) = [0]$. Then there exists a polynomial g polynomial of degree $n-1$ with coefficients in Z_m and such that $f([x]) = ([x]-[a])g([x])$.

5. Let $n \geq 2$ be an integer. Show that $2^n - 1$ can be a prime only if n itself is a prime.

6. Consider the claim: $a^{\varphi(m)+1} \equiv a \pmod{m}$ for all $a \in \mathbf{Z}$.

(i) Show that the claim holds if m is a prime or a product of distinct primes

(ii) Does the claim hold true for all m?

7. Given a number $k \geq 2$ show that there are k consecutive numbers $n, n+1, \ldots, n+(k-1)$ such that first of these numbers is divisible by a second power of a prime, second one by a third power of some prime,..., and finally the k:th one is divisible by $(k+1)$:th power of a prime.

8*. Assume that $P(x)$ is a polynomial of degree n (with real coefficients). Show $P(n) \in \mathbf{Z}$ for all $n \in \mathbf{Z}$ if and only if P is of the form

$$P(x) = \sum_{k=0}^{n} c_k \binom{x}{k} \qquad \text{where} \quad c_k \quad \text{is and integer for all} \quad k = 0, 1, \ldots, n.$$

Hints:

E.4 & E.5: [use the identity$x^n - a^n = (x - a)(x^{n-1} + x^{n-2}a + \ldots + a^{n-1}]$

E.6: [(i): Consider separately divisibility by any of the primes that divide m]