INTRODUCTION TO NUMBER THEORY. (Fall 2015)

4. EXERCISES (Mo 5.10)

1. Verify the converse direction of Wilson's Thm: if $p \geq 2$ is not a prime, then $p \not| ((p-1)!+1)$.

2. Find all the primitive roots mof p when

(i) p=11 (ii) p=18.

3. Determine $\mathrm{ord}_{73}(2)$ and $\mathrm{ord}_{73}(7)$. Can use use this information to guess a primitive root mod 73?

4. Find all the roots of the congruence

$$x^3 - 3x^2 + 27 \equiv 0 \pmod{1125}$$

by using the method developed in the lectures.

5. Try to deduce that all rational numbers of the form $1/p$, where $(p, 10) = 1$ can be written with a periodic decimal expansion by using the division algorithm taught in high schools.

6. Let f be a polynomial with integer coefficients. Show that $\dfrac{f^{(k)}(y)}{k!} \in \mathbf{Z}$ for all $a \in \mathbf{Z}$ and $k \geq 0$.

7. Give the details to the following proof (due to Gauss) of Wilson's Theorem: Let $p \geq 5$ be a prime. Consider the follwing elements of Z_p: $\{\overline{2}, \overline{3}, \ldots, \overline{p-2}\}$. Show that they can be paired in such a way that the two elements of each pair are (multiplicative) inverses of each others. Then Wilson's Theorem follows easily.

8*. Show that if p is an odd prime and $\mathrm{ord}_p(a) = 3$, then $\mathrm{ord}_p(a+1) = 6$

Hints:

E.5: [Recall the division algorithm, compute several examples and look what happens!]

E.6: [Consider first single monomials.]