INTRODUCTION TO NUMBER THEORY. (Fall 2015)

8. EXERCISES (Mo 16.11)

1. Show that the number $1+i$ divides the Gaussin integer $a+bi$ if and only if $a \equiv b \pmod 2$.

2. Show that the number $m \in \mathbf{N}$ divides the Gaussian integer $a+bi$ if and only if $m|a$ and $m|b$.

3. Determine all right angled triangles whose sides are integers and whose perimeter (the sum of the sides) equals 100.

4. Try to find (by whatever means) all (Gaussian) prime factors of the numbers

(i) 10 (ii) $2-7i$.

5. Assume that $\pi \in \mathbf{N}[i]$ is a gaussian prime. Show in detail that if $\pi|\lambda_1 \cdots \lambda_n$, then $\pi|\lambda_i$ for some $i \in \{1,\dots,n\}$.

6. Show by two different ways that the sequence (B_k) (from the proof of Lagranges theorem in lectures pp. 96-97) is bounded.

(i) Start from the formula $B_k = -(\alpha_k)^{-1}(A_k\alpha_k^2 + C_k)$, prove that the numbers α_k stay bounded and apply the (already proven) boundedness of the sequences (A_k) and (C_k).

(ii) Write $f(x,y) = 2Axy + B(x+y) + 2C$ and note that

$$B_k = q_{k-1}q_{k-2}f(\frac{p_{k-1}}{q_{k-1}}, \frac{p_{k-2}}{q_{k-2}}).$$

Note that $f(\alpha,\alpha) = 0$, and imitate the proof given in the lectures for the boundedness of the sequence (A_k).

7*. Prove an analogy for Fermat's little theorem in case of Gaussian integers: if $p \in \mathcal{P}$ is an odd (standard prime) of the form $p = 4k+1$, then $\alpha^{p-1} - 1$ is divisible by p whenever $\alpha \in Z[i]$ fulfils $(\alpha, p) = 1$. Does this hold for $p \in \mathcal{P}$ of the form $4k-1$?

Hints:

E.1-2: [You may e.g. start directly from the definition of divisibility.]

E.5: [Recall the proof in the case of ordinary integers...]

T.6: [[(i): combine exercise 6/8 ja Liouville's theorem lause 5.5 to verify that λ_k:s and hence α_k:s stay bounded. (ii): apply the intermediate theorem for two variables and Corollary 5.12.]

T.7: [Consider number $\alpha^p - \alpha$, write $\alpha = a + ib$ and apply the binomial formula.]