Exercise Sheet 1 **Topics in Number Theory**

2012 C. Elsholtz

Ex. 1
An integer n can be written as a sum of two integer squares, if and only if in the standard prime factorization the exponents of all primes $q \equiv 3 \bmod 4$ are even. From this classification of the integers n, which can be written as a sum of two squares, we only proved the case of $p \equiv 1 \bmod 4$.
Complete the proof that is
show that integers with the "allowed" prime factorisation have a representation as $n = x^2 + y^2$,
and show that integers with a "forbidden" factorisation do not have a representation.
Explain: if $n_1 = x_1^2 + y_1^2$ and $n_2 = x_2^2 + y_2^2$, then $n_1 n_2 = (...)^2 + (...)^2$ by means of complex numbers.

Ex. 2
Classify those integers which can be written in the form $n = x^2 + 2y^2$. Prove your statement for primes. (Hint: for which primes p is $x^2 \equiv -2 \bmod p$ soluble? (most of you will know this from the Legendre symbol $\left(\frac{-2}{p}\right)$.)

Ex. 3
Let $A = \{x^2 + y^2 : x, y \in \mathbb{N}_0\}$ denote the set of integers which are sums of two squares.
Let $A(N) = \sum_{a \in A, n \leq N} 1$ denote the counting function.
Write a computer program to evaluate $A(N)$ for $N = 10^i$, $i = 1, 2, 3, \ldots$ (as far as you reasonably can go). From this deduce a conjecture about the asymptotic growth of $A(N)$.
Give an estimate for the computational complexity to compute $A(N)$, as a function of N. (How many steps does your program need, roughly?)
For the integers $n \leq 1,000$ verify the "if and only if" of the Sum of two squares theorem.

Ex. 4
Let $r_2(n)$ denote the number of representations as sums of two squares, $x, y \in \mathbb{Z}$, i.e. negative integers allowed. For example $r_2(5) = 8$, as $5 = (\pm 1)^2 (\pm 2^2) = \pm 2^2 \pm 1^2$. Estimate the average value of $r_2(N)$, i.e., $\lim_{N \to \infty} \frac{\sum_{n \leq N} r_2(n)}{N}$. Make a conjecture, and prove it. (Also a computation of these values for $n = 10^i$ with a similar computer programme (simple modification of the one above) may be of interest).
Let p_1, p_2, p_3 be distinct primes. Evaluate $r_2(p_1 p_2 p_3)$ (several cases!) What happens if the p_i are not distinct?
Let $d_1(n)$ be the number of *divisors* d of n with $d \equiv 1 \bmod 4$, and let d_3 be the number of *divisors* d of n with $d \equiv 3 \bmod 4$. Try to find a connection between $r_2(n)$ and $d_1(n), d_3(n)$.
Study those values of n with large values of $r_2(n)$. How large can these values be? (Can you give any lower/upper bounds, even if only with a "guess"?)