Introduction to Number Theory. Problem set I .

Due date: October 24, 2017.

1. We proved that every prime number congruent to 1 modulo 4 can be written in the form x^2+y^2, where x, y are nonnegative integers. Prove that such a representaion is unique up to a permutation of summands.

2. Find all integral solutions to the equation $x^2+1=y^3$.

3. Prove that every ideal in the rings $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{6}]$ is principal. Give an example of a non-principal ideal in $\mathbb{Z}[\sqrt{-3}]$. Finally, show that every ideal in $\mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-3}}{2}$, is principal.

4. Prove that a prime number p can be written in the form x^2+3y^2, $x, y \in \mathbb{Z}$, if and only if $p=3$ or $p \equiv 1 \, mod \, 3$.

5. (a) Show that equations $x^2-2y^2=-1$, $x^2-2y^2=1$ have infinitely many solutions in integers.
(б) Prove that, for p of the form $\pm 1+8k$, equations $x^2-2y^2=-p$, $x^2-2y^2=p$ have infinitely many solutions in integers.

6. Prove that for every odd prime number p, one has

$$\sum_{i=1}^{p-1} (i/p) = 0.$$

(Here (i/p) is the Legendre symbol.)

7. Let n be a nonzero integer. Prove that there is a unique homomorphism $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \to \{1,-1\}$ (where $(\mathbb{Z}/4n\mathbb{Z})^*$ is the group of invertible elements in $\mathbb{Z}/4n\mathbb{Z}$), such that, for every odd prime p, with $(n,p)=1$, one has

$$(n/p) = \chi([p]).$$

(Here $[p]$ is the class of p in $(\mathbb{Z}/4n\mathbb{Z})^*$.)

8. Let R be a finitely generated commutative ring (*i.e.*, R adimits a surjective homomorphism $\mathbb{Z}[x_1 \cdots, x_n] \to R$.) Prove that for every maximal ideal $m \subset R$ the quotient R/m is finite.

Definition: For a finitely generated commutative ring R define its zeta function to be

$$\zeta_R(s) = \prod_{m \subset R} \frac{1}{1-|R/m|^{-s}},$$

where the product is taken over all maximal ideals in R. (Note that $|R/m|$ is finite by Problem 8.) One can show that the product converges for large s.

9. Let R be a finitely generated commutative algebra over $\mathbb{F}_p$. For an integer $k>0$, let N_k be the number algebra homomorphisms

$$R \to \mathbb{F}_{p^k}.$$

(Why N_k is finite?) Show that

$$\zeta_R(s) = exp(\sum_{k\geq 1} \frac{N_k}{k} p^{-ks}).$$

10. Prove that

$$\zeta_{\mathbb{F}_p[x]}(s) = \frac{1}{1-p^{1-s}}.$$

11. Define a function $\chi : \mathbb{Z} \to \{0, 1, -1\}$ as follows: $\chi(d) = 1$ if d is congruent to 1 modulo 4, $\chi(d) = -1$ if d is congruent to 3 modulo 4, and $\chi(d) = 0$ for every even d. Prove that the number of integral solutions to the equation $x^2 + y^2 = n$, $(n \geq 0)$, with $x > 0, y \geq 0$, is equal to

$$\sum_{d|n} \chi(d),$$

where the summation runs over all positive divisors of n.