Math 437/537 Problem set 4 (due 28/10/09)

Some polynomials

1. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ be a polynomial with integer coefficients of degree $n \geq 1$, and let $r = \frac{p}{q} \in \mathbb{Q}$ be a rational number with $(p,q) = 1$. Assume that $f(r) = 0$.
   (a) Show that $p|a_0$ and $q|a_n$.
   (b) Conclude that if $a_n = 1$ (f is *monic*) then $r \in \mathbb{Z}$.

2. Let $g(x) = x^6 - 53x^4 + 680x^2 - 1156 = (x^2-2)(x^2-17)(x^2-34)$. Show that $g(x) = 0$ has solutions in the real numbers and in $\mathbb{Z}/m\mathbb{Z}$ for all m, but that $g(x) = 0$ has no solutions in the rational numbers.

DEFINITION. Call $f \in \mathbb{Z}[\underline{x}]$ *homogeneous of degree r* (or a *form*) if every monomial appearing in f has total degree r. Call $\underline{a} \in \mathbb{Z}^n$ *primitive* if $\gcd(a_1, \ldots, a_n) = 1$.

3. Let f be a form in n variables. Show that $V_f(\mathbb{Z}) = \bigcup_{d \geq 1} \left(dV_f'(\mathbb{Z}) \right)$ where $V_f'(\mathbb{Z})$ is the set of primitive solutions to the equations $f = 0$.

4. Find all integral solutions to the following equations (*Hint*: reduce mod m for suitably chosen m).
   (a) $x^2 + y^2 = 9z + 3$.
   (b) $x^2 + 2y^2 = 8z + 5$.
   (c) $x^2 + y^2 + z^2 = 2xyz$.
   (d) $x^4 + y^4 + z^4 = 5x^2yz$.
   (e) $x^4 + 2x^3 + 2x^2 + 2x + 5 = y^2$

5. (Rational points)
   (a) Let $f \in \mathbb{Q}[x,y]$ be a cubic and let $g \in \mathbb{Q}[x,y]$ be linear and non-constant. Obtain a correspondence between $V_f(\mathbb{Q}) \cap V_g(\mathbb{Q})$ and the roots of a polynomial of degree at most 3 with rational coefficient, and conclude that this set, if finite, has size at most 3.
   OPTIONAL Explain why the set cannot have size 2, if we count zeroes with multiplicity and include points at infinity.
   From now on let $f(x,y) = x^3 + 2x^2 - y^2$. We will find $V_f(\mathbb{Q}) \subset \mathbb{Q}^2$.
   (b) Let g be a linear polynomial so that $(0,0) \in V_g(\mathbb{Q})$. Show that $V_f(\mathbb{Q}) \cap V_g(\mathbb{Q})$ contains at most one more point.
   (c) Find all $\mathbb{Q}$-rational points on V_f.
   (d) Given $\varepsilon > 0$, show how to find a rational point $(x,y) \in V_f(\mathbb{Q})$ with $0 < |x|, |y| < \varepsilon$.
   (e) Exhibit specific $x, y \in \mathbb{Q}$ such that $y^2 = x^3 + 2x^2$ and $0 < |x|, |y| < \frac{1}{1000}$.

Using $\mathbb{Z}[i]$

6. (The issue at 2)
   (a) Let $w \in \mathbb{Z}[i]$ divide 2. Show that w is associate to one of $1, \pi, \pi^2$ where $\pi = 1 + i$.
   (b) Let$x, y \in \mathbb{Z}$be relatively prime, and let $z = x + iy \in \mathbb{Z}[i]$. Show that $(z, \bar{z})$ divides 2 in $\mathbb{Z}[i]$. Conclude that $(z, \bar{z}) = \pi$ if x, y are both odd, $(z, \bar{z}) = 1$ otherwise.

(c) Now take any $x,y\in\mathbb{Z}$. Show that $(x+iy,x-iy)=(x,y)\cdot\begin{cases}\pi & \frac{x}{(x,y)},\frac{y}{(x,y)} \text{ both odd}\\ 1 & \text{otherwise}\end{cases}$.

7. Let $x,y\in\mathbb{Z}$ satisfy $y^2=x^3-1$.
   (a) Show that y is even and x is odd.
   Hint: reduce the equation modulu 4.
   (b) Let $z=1+iy\in\mathbb{Z}[i]$. Show that $z\bar{z}$ is a cube in $\mathbb{Z}[i]$ and that $(z,\bar{z})=1$ there. Conclude that there exists $w\in\mathbb{Z}[i]$ and $\varepsilon\in\mathbb{Z}[i]^\times=\{\pm1,\pm i\}$ such that $z=\varepsilon\cdot w^3$.
   (c) Examining the real and imaginary parts of the resulting identity, show that $x=1$, $y=0$ is the only solution.

8. Let $(x,y,z)\in\mathbb{Z}^3$ be primitive and satisfy $x^2+y^2=z^2$.
   (a) Show that x,y have different parities. WLG we'll assume that x is odd, y is even.
   (b) Show that $x+iy\in\mathbb{Z}[i]$ has the form $\varepsilon(m+in)^2$ for some relatively prime $m,n\in\mathbb{Z}$ and $\varepsilon\in\mathbb{Z}[i]^\times$.
   (c) Conclude that $(x,y,z)=\left(m^2-n^2,2mn,m^2+n^2\right)$.
   - Note how the choice of root of unity corresponds to the choice of which of x,y is even.

Sums of two squares

9. Let $r_2(n)=\#\left\{(a,b)\in\mathbb{Z}^2 \mid a^2+b^2=n\right\}$ and set $s(n)=\frac{1}{4}r_2(n)$.
   (a) Show that $s(n)$ is integral and multiplicative.
   Hint: Adapt problem 6(a) from PS1 to $\mathbb{Z}[i]$.
   (b) For $k\geq 1$, and primes $p\equiv 1\,(4)$ and $q\equiv 3\,(4)$ show that $s(2^k)=1$, $s(p^k)=k+1$, $s(q^k)=\begin{cases}1 & k\equiv 0\,(2)\\ 0 & k\equiv 1\,(2)\end{cases}$.
   (c) Find the smallest integer n so that $r_2(n)=60$.

10. Define a function $\chi_4\colon\mathbb{Z}_{\geq1}\to\{0,\pm1\}$ by setting $\chi_4(n)=\begin{cases}1 & n\equiv 1\,(4)\\ -1 & n\equiv 3\,(4)\\ 0 & 2|n\end{cases}$.
    (a) Show that $\chi_4(ab)=\chi_4(a)\chi_4(b)$ for all $a,b\in\mathbb{Z}$.
    (b) Show that $n\mapsto\sum_{d|n}\chi_4(d)$ is multiplicative.
    (c) show that $s(n)=\sum_{d|n}\chi_4(d)$ for prime powers n.
    (d) Show that $r_2(n)=4\sum_{d|n}\chi_4(d)$ for all n.

Some arithmetic

11. The most recently discovered perfect number is $N=2^{p-1}(2^p-1)$, where $p=42,643,801$. Determine how many digits N has, and find the first three digits (on the left) and the last three digits (on the right). You may use the equivalent of an abacus (e.g. a simple electronic calculator) to do the arithmetic, but not the equivalent of a general-purpose computer – for example do not evaluate N directly!

Roots of unity

Let $e(x) = e^{2\pi i x}$. For an integer m Let $\zeta_m = e(\frac{1}{m})$, $\zeta_m^k = e\left(\frac{k}{m}\right)$. Let $\mu_m = \left\{\zeta_m^k\right\}_{k\in\mathbb{Z}} \subset \mathbb{C}$.

12. Show that μ_m is the set of solutions to $z^m = 1$ in $\mathbb{C}$, and that it is closed under multiplication. Show that the map $k \mapsto \zeta_m^k$ induces a bijection $\mathbb{Z}/m\mathbb{Z} \to \mu_m$ mapping addition to multiplication. Fixing k, show that $\mu_m = \left\{\zeta_m^{kj}\right\}_{j\in\mathbb{Z}}$ iff $(k,m) = 1$. In that case we call ζ_m^k a *primitive* root of unity of order m.

13. Given $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ and $j \in \mathbb{Z}/m\mathbb{Z}$ set $\hat{f}(k) = \sum_{j(m)} f(j)\zeta_m^{-jk} = \sum_{a(m)} f(a)e(\frac{ak}{m})$. We call $\hat{f}$ the *Discrete Fourier Transform* of f.
    (a) Show that $\sum_{k(m)} \zeta_m^{kj} = m\delta_{j,0}$.
    (b) Show that $\hat{\hat{f}}(k) = f(-k)$ ("Fourier inversion").
    (c) Show that $\sum_{j(m)} |f(j)|^2 = \frac{1}{m}\sum_{k(m)} \left|\hat{f}(k)\right|^2$ ("Parseval's identity").