Homework Set Two

Due Thursday, April 28.

Question 1. Find $g = \gcd(4340, 918)$ and the values x and y such that $4340x + 918y = g$.

Question 2. Let K be a field. Given two polynomials $f(x)$ and $g(x)$ in $K[x]$, we define the *greatest common divisor* of $f(x)$ and $g(x)$, denoted $\gcd(f(x), g(x))$, to be the unique monic polynomial of highest degree dividing both $f(x)$ and $g(x)$. Here, 'monic' means the leading coefficient is 1.

(a) Find the greatest common divisor of $f(x) = 2x^2 - \frac{1}{2}$ and $g(x) = 2x^3 - x^2 - 2x + 1$.

(b) The analog of a prime number for polynomials is an irreducible polynomial. A polynomial $p(x)$ in $K[x]$ of degree at least 1 is *irreducible* if its only divisors are c and $cp(x)$ where c is a nonzero constant. Show that $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible in $\mathbb{C}[x]$.

(c) Prove the following theorem (Euclid's Lemma):

Theorem. Let $p(x)$ in $K[x]$ be irreducible and consider two polynomials $f(x), g(x)$ in $K[x]$. If $f(x)g(x)$ is divisible by $p(x)$, then $p(x)$ divides $f(x)$ or $p(x)$ divides $g(x)$. (Hint: You may use that an analog of the Euclidean algorithm holds for $K[x]$.)

Question 3. The *Gaussian integers* is the set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication of $\mathbb{C}$ (making it a ring). For $\alpha = a + bi \in \mathbb{Z}[i]$ the *conjugate* of α, denoted $\overline{\alpha}$ is $\overline{\alpha} = a - bi$ and the *norm* N on $\mathbb{Z}[i]$ is the map

$$N\colon \mathbb{Z}[i] \to \mathbb{Z}, \qquad (a + bi) \mapsto N(a + bi) := \alpha\overline{\alpha} = a^2 + b^2.$$

(a) Show the norm is multiplicative. That is, show $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Z}[i]$.

(b) Suppose $\alpha, \beta \in \mathbb{Z}[i]$. We say α divides β if there exists a $\gamma \in \mathbb{Z}[i]$ such that $\beta = \alpha\gamma$. An element $\alpha \in \mathbb{Z}[i]$ is a *unit* of $\mathbb{Z}[i]$ if their exists an element β in $\mathbb{Z}[i]$ such that $\alpha\beta = 1 = \beta\alpha$. Show the following are equivalent:

  (i) $\alpha \in \{\pm 1, \pm i\}$

  (ii) α is a unit

  (iii) $N(\alpha) = 1$.

(c) A non-unit Gaussian integer $\alpha \neq 0$ is said to be *reducible* if there exist non-unit elements $\beta, \gamma \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma$. The element α is called *irreducible* if it is not reducible.

  (i) Show that a prime $p \in \mathbb{Z}$ is reducible in $\mathbb{Z}[i]$ if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

  (ii) Show that if α divides β in $\mathbb{Z}[i]$, then $N(\alpha)$ divides $N(\beta)$ in $\mathbb{Z}$.

  (iii) Show that $\alpha = 4 + i$ is a irreducible.

(iv) Show that $\alpha = 2$ is not a irreducible.

(d) (Bonus.) Recall that the reason the Euclidean algorithm works is that given integers a and b with $b \neq 0$, we may write

$$a = qb + r$$

where q and r are integers and $0 \leq r < b$. Show that $\mathbb{Z}[i]$ has the analogous property that given $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ such that

$$\alpha = q\beta + r$$

and $0 \leq N(r) < N(\beta)$. (Hint: Consider $\frac{\alpha}{\beta}$. This number is not necessarily in $\mathbb{Z}[i]$, but you can show that it is of the form $x + iy$ where x and y are rational numbers. Show that there is a Gaussian integer $a + bi$ such that $N(\frac{\alpha}{\beta} - (a + bi)) \leq \frac{1}{2}$. Now consider the Gaussian integer $r = \alpha - \beta(a + bi)$. For example, what is its norm?)