Math 553 Homework 6

Due Fri. Oct. 12, 2012

1. Let α and β be rational numbers, with $|\alpha| \le 1/2$, and let $m > 0$ be an integer such that $\alpha^2 - m\beta^2 = -1 - \delta$ where $0 \le \delta < 1$. Set $\epsilon := 1$ if $\alpha \ge 0$ and -1 if $\alpha < 0$. Show that if m is not of the form $5n^2$ ($n \in \mathbb{Z}$) then $|(\alpha+\epsilon)^2 - m\beta^2| < 1$.

Deduce that $\mathbb{Z}[\omega]$ is norm-Euclidean when $\omega = \sqrt{6}$, when $\omega = \sqrt{7}$, or when $\omega^2 - \omega + q = 0$ with $q = -4$,-5 or -7.

2. (Fermat). Find all solutions in positive integers of the equation $y^3 = x^2 + 4$.

Hint. Prove and use the following facts about Gaussian integers.
(i) $a + bi$ is divisible by $1 + i \iff a - b$ is even.
(ii) If $y^3 = x^2 + 4$ ($x, y \in \mathbf{Z}$), then

$$(x+2i,\, x-2i) = \begin{cases} 1 & \text{if } x \text{ is odd} \\ (1+i)^3 & \text{if } x \text{ is even.} \end{cases}$$

(iii) If $y^3 = x^2 + 4$ then $x + 2i = i^n(a+bi)^3$ for some n, a, b.

3. Let $\omega \in \mathbb{C}$ satisfy $\omega^2 - p\omega + q = 0$ where p and q are integers such that $p^2 - 4q$ is not the square of an integer. The *norm* of $a + b\omega \in \mathbb{Z}[\omega]$ is

$$N(a+b\omega) := (a+b\omega)(a+b\bar{\omega}) := \big(a+b\omega)(a+b(p-\omega)\big).$$

Prove for any integers a and b that $n := |N(a+b\omega)|$ is the cardinality of $\mathbb{Z}[\omega]/(a+b\omega)\mathbb{Z}[\omega]$; and deduce that if $(a,b) = 1$ then there is an isomorphism of rings

$$\mathbb{Z}/N(a+b\omega)\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[\omega]/(a+b\omega)\mathbb{Z}[\omega].$$

Hint. Show that the cardinality of $\mathbb{Z}[\omega]/(a+b\omega)\mathbb{Z}[\omega]$ is the same as that of $\mathbb{Z}[\omega]/(a+b\bar{\omega})\mathbb{Z}[\omega]$, and that multiplication by $a+b\omega$ gives a group isomorphism

$$\mathbb{Z}[\omega]/(a+b\bar{\omega})\mathbb{Z}[\omega] \xrightarrow{\sim} (a+b\omega)\mathbb{Z}[\omega]/n\mathbb{Z}[\omega].$$

Then use that the cardinality of $\mathbb{Z}/n\mathbb{Z}$ is n^2. (Why?)

(OVER)

4. Let $\omega \neq -1$ be a complex number satisfying $\omega^3 = -1$. We showed in class that $\mathbb{Z}[\omega]$ is a Euclidean domain.

(a) Let $p > 3$ be an odd prime in $\mathbb{Z}$. Show that:

$$p \equiv 1 \pmod 6 \iff -1 \text{ has three cube roots in } \mathbb{Z}/p \iff -3 \text{ is a square in } \mathbb{Z}/p.$$

(b) Prove that every prime $p > 0$ in $\mathbb{Z}$ of the form $p = 6n + 1$ can be represented in the form $p = a^2 + ab + b^2$ $(a > b > 0)$ in *one and only one* way.

(c) Prove that every prime $p > 0$ in $\mathbb{Z}$ of the form $p = 6n + 1$ can be represented in the form $p = a^2 + 3b^2$ $(a, b > 0)$ in *one and only one* way.

(d) Prove that every *odd* prime p in $\mathbb{Z}$ factors into primes in $\mathbb{Z}[\sqrt{-3}]$. What about $p = 2$?

5. (a) Let $n > 1$ be an integer. Prove that a prime p in $\mathbb{Z}$ has at most one representation of the form $p = a^2 + nb^2$ with a, b positive integers.

(b) Show that p as in (a) is of the form $a^2 + 2b^2$ if and only if -2 is a square in $\mathbb{Z}/pZ$.

(c) Let F be a field in which $2 \neq 0$. Show that F has an element of multiplicative order 8 if and only if both -1 and 2 are squares in F.

(d) (Stated by Fermat about 350 years ago; first published proof by Euler over 100 years later.) Prove that every prime $p > 0$ in $\mathbf{Z}$ of the form $p = 8n + 1$ can be represented in the form $p = a^2 + 2b^2$ $(a > 0,\ b > 0)$.

(e) Repeat problem (b) for $p = 8n + 3$.

You will need that 2 is not a square in $\mathbf{Z}/p$. Here is a sketch of one way to see this:

Let F be any finite field, of odd cardinality q $\quad (\Rightarrow 2 \neq 0$ in $F)$.

Let $S \subset F$ be the set of all x such that x and $x + 1$ are both nonzero squares, and let s be the cardinality of S.

i) Show that $x \in S \Leftrightarrow 1/x \in S$; and deduce that s is odd iff 2 is a square in F.

ii) Show that $\sigma \mapsto (\sigma + \sigma^{-1} - 2)/4$ is a two-to-one map from the set Σ of all squares $\sigma \neq 0, 1, -1$ in F onto S.

iii) The cardinality of Σ is $\dfrac{q-3}{2}$ if -1 is not a square, and $\dfrac{q-5}{2}$ otherwise. (Why?)

iv) Deduce that 2 is a square in $F \iff q \equiv \pm 1 \bmod 8$.