Homework #9. Solutions to selected problems.

1. Let p be a prime of the form $4k+3$.

(a) Prove that if $p \nmid a$ or $p \nmid b$, then $p \nmid (a^2+b^2)$.

(b) Use (a) to prove that $ord_p(a^2+b^2)$ is even for any $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$.

Solution: (a) If p divides one of the numbers a and b (but not the other), then clearly p does not divide a^2+b^2. So, we can assume that $p \nmid a$ and $p \nmid b$. Suppose that $p \mid (a^2+b^2)$, so $a^2+b^2 = pm$ for some $m \in \mathbb{Z}$. Hence $b^2 = pm - a^2$. Take Legendre symbols over p of both sides. Since $\left(\frac{-1}{p}\right) = -1$ (as $p \equiv 3 \mod 4$) and $\left(\frac{x}{p}\right) = \left(\frac{x+pm}{p}\right)$ for any x, we get

$$\left(\frac{b^2}{p}\right) = \left(\frac{pm-a^2}{p}\right) = \left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right) = -\left(\frac{a^2}{p}\right). \qquad (***)$$

Since $p \nmid a$ and $p \nmid b$, both Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are equal to ± 1, so $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = 1$ and similarly $\left(\frac{b^2}{p}\right) = 1$. This contradicts (***).

(b) Let p^k be the highest power of p which divides both a and b. Thus $a = p^k c$ and $b = p^k d$ for some $c, d \in \mathbb{Z}$, and at least one of the numbers c and d is not divisible by p, so by part (a), $p \nmid (c^2+d^2)$. Since $a^2+b^2 = p^{2k}(c^2+d^2)$, we conclude that $ord_p(a^2+b^2) = 2k$.

2. Let ω be a complex number such that $\omega \notin \mathbb{Z}$ and $\omega^2 = n_1\omega + n_2$ for some $n_1, n_2 \in \mathbb{Z}$. For instance, if d is a positive integer which is not a perfect square, we can take $\omega = \sqrt{d}$ or $\omega = i\sqrt{d}$. Define

$$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\} \quad \text{and} \quad \mathbb{Q}[\omega] = \{a + b\omega : a, b \in \mathbb{Q}\}.$$

(a) Prove that $\mathbb{Z}[\omega]$ is a commutative ring with 1 and that $\mathbb{Q}[\omega]$ is a field.

For the remaining parts of this problem assume that $\omega = \sqrt{d}$ or $\omega = i\sqrt{d}$ for some d as above.

(b) Define the conjugation map $\iota : \mathbb{Q}[\omega] \to \mathbb{Q}[\omega]$ by $\iota(a+b\omega) = a - b\omega$ Prove that ι is a ring isomorphism.

(c) Prove that $u \cdot \iota(u) \in \mathbb{R}$ for any $u \in \mathbb{Q}[\omega]$.

(d) Define the norm map $N : \mathbb{Q}[\omega] \to \mathbb{R}_{\geq 0}$ by $N(u) = |u \cdot \iota(u)|$. Prove that $N(uv) = N(u)N(v)$.

(e) Prove that $N(u) \in \mathbb{Z}$ for any $u \in \mathbb{Z}[\omega]$ and $N(u) = 0 \iff u = 0$.

(f) Let $u \in \mathbb{Z}[\omega]$. Prove that $N(u) = 1 \iff u$ is a unit of $\mathbb{Z}[\omega]$.

Solution: (d) By part (b) we have $\iota(uv) = \iota(u)\iota(v)$ for all $u, v \in \mathbb{Q}[\omega]$, so

$$N(uv) = |uv \cdot \iota(uv)| = |uv \cdot \iota(u)\iota(v)| = |u\iota(u)| \cdot |v\iota(v)| = N(u)N(v).$$

Note that the explicit formula for the norm function N is

$$N(a+b\omega) = a^2 + db^2 \text{ if } \omega = i\sqrt{d} \text{ and } N(a+b\omega) = |a^2 - db^2| \text{ if } \omega = \sqrt{d}. \quad (!!!)$$

(f) "$\Rightarrow$" Suppose that $N(u) = 1$. Since $N(u) = |\iota(u) \cdot u|$, we have $\iota(u) \cdot u = \pm 1$, so $(\pm\iota(u)) \cdot u = 1$. Hence $u^{-1} = \pm\iota(u) \in \mathbb{Z}[\omega]$, so u is a unit of $\mathbb{Z}[\omega]$.
Conversely, suppose that u is a unit of $\mathbb{Z}[\omega]$, so $uv = 1$ for some $v \in \mathbb{Z}[\omega]$. Taking norms of both sides, we get $N(uv) = N(1) = 1$, so $N(u)N(v) = 1$. Since both $N(u)$ and $N(v)$ are non-negative integers (which is clear from formula (!!!) above), we have $N(u) = N(v) = 1$.
Remark: If $\omega = i\sqrt{d}$, the ring $\mathbb{Z}[\omega]$ has very few units. Indeed, the only pair of integers (a, b) satisfying $a^2 + db^2 = 1$ are $(\pm 1, 0)$ and $(0, \pm 1)$ if $d = 1$ and $(\pm 1, 0)$ if $d > 1$.
On the other hand, if $\omega = \sqrt{d}$, there are infinitely many units in $\mathbb{Z}[\omega]$, as we saw when describing solutions to Pell's equation.

3. Prove that $\mathbb{Z}[i\sqrt{2}]$ is a Euclidean domain.

Solution: Let $R = \mathbb{Z}[i\sqrt{2}]$ and $F = \mathbb{Q}[i\sqrt{2}]$. Define the norm function $N : F \to \mathbb{Q}$ by $N(a + bi\sqrt{2}) = a^2 + 2b^2$. By the same argument as in Problem 2, $N(fg) = N(f)N(g)$ for all $f, g \in F$. Also note that $N(f) \in \mathbb{Z}$ for $f \in R$.

To prove that R is a Euclidean domain, it suffices to check that

(i) $N(x) = 0 \iff x = 0$

(ii) For any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$ and $N(r) < N(b)$.

Property (i) is obvious. To prove (ii), take any $a, b \in R$ with $b \neq 0$. Since F is a field, $\frac{a}{b} = x + yi\sqrt{2}$ for some $x, y \in \mathbb{Q}$.

We can find INTEGERS m and n such $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. We set $q = m + ni\sqrt{2}$ and $r = a - bq$. Then automatically $a = bq + r$, and it remains to check that $N(r) < N(b)$. We have $r = a - bq = b(\frac{a}{b} - q) = b((x + yi\sqrt{2}) - (m + ni\sqrt{2})) = b((x - m) + (y - n)i\sqrt{2})$. Note that

$$N((x-m) + (y-n)i\sqrt{2}) = (x-m)^2 + 2(y-n)^2 \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4}.$$

Therefore,

$$N(r) = N(b((x-m)+(y-n)i\sqrt{2})) = N(b)N((x-m)+(y-n)i\sqrt{2}) \leq \frac{3}{4}N(b) < N(b).$$

4.

(a) Determine which primes are representable in the form $a^2 + 2b^2$ with $a, b \in \mathbb{Z}$.

(b) (bonus) Describe all integers representable as $a^2 + 2b^2$ with $a, b \in \mathbb{Z}$.

Solution: We claim that a prime p is representable as $p = a^2 + 2b^2$ if and only if $p = 2$ or $p \equiv 1$ or $3 \bmod 8$.
First suppose that $p \equiv 5$ or $7 \bmod 8$. From the equality $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)$ and the formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ we proved earlier, we get $\left(\frac{-2}{p}\right) = -1$. Arguing as in Problem 1, we conclude that $ord_p(a^2+2b^2)$ is even for any pair $(a, b) \neq (0, 0)$. In particular, $a^2 + 2b^2$ cannot equal p.
One can also give a more elementary argument: by direct computation for any $x \in \mathbb{Z}$ we have $x^2 \equiv 0, 1$ or $4 \bmod 8$, so $a^2 + 2b^2$ can only be congruent to $0, 1, 4, 2, 3$ or $6 \bmod 8$.

Note that $2 = 0^2 + 2 \cdot 1^2$ is representable in the desired form. Now suppose that $p \equiv 1$ or $3 \bmod 8$. We will first show that p is NOT prime as an element of the ring $\mathbb{Z}[i\sqrt{2}]$.
Again by direct computation $\left(\frac{-2}{p}\right) = 1$, so there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -2 \mod p$ and thus $p \mid (x^2+2)$. Note that $(x^2+2) = (x+i\sqrt{2})(x-i\sqrt{2})$. Since $\frac{x+i\sqrt{2}}{p} = \frac{x}{p} + \frac{1}{p}i\sqrt{2} \notin \mathbb{Z}[i\sqrt{2}]$ and similarly $\frac{x-i\sqrt{2}}{p} \notin \mathbb{Z}[i\sqrt{2}]$, we conclude that p does not divide $x \pm i\sqrt{2}$ in $\mathbb{Z}[i\sqrt{2}]$, so p is not prime in $\mathbb{Z}[i\sqrt{2}]$.
Since $\mathbb{Z}[i\sqrt{2}]$ is a Euclidean domain by Problem 3, irreducible elements of $\mathbb{Z}[i\sqrt{2}]$ are prime, so p is not irreducible in $\mathbb{Z}[i\sqrt{2}]$. Since $p \neq 0$ and p is not a unit by Problem 2(f), $p = fg$ for some non-units $f, g \in \mathbb{Z}[i\sqrt{2}]$.

Taking norms of both sides, we get $N(f)N(g) = p^2$. Since f and g are non-units, $N(f)$ and $N(g)$ are both larger than 1, so we must have $N(f) = N(g) = p$. Thus if $f = a + bi\sqrt{2}$, then $p = N(f) = a^2 + 2b^2$, as desired.

(b) Answer: an integer $n > 1$ is representable in the form $a^2 + 2b^2$ with $a, b \in \mathbb{Z} \iff$ all primes congruent to 5 or 7 mod 8 appear in the prime factorization of n with even exponent. The proof is completely analogous to that of the corresponding result about representations of integers as sums of squares.

5. Let $R = \mathbb{Z}[\sqrt{5}]$. Find an element of R which is irreducible but not prime and prove your assertion.

Solution: We start with equality $2 \cdot 2 = (\sqrt{5} + 1)(\sqrt{5} - 1) = 4$. Since $\frac{\sqrt{5}\pm 1}{2} \notin R$ while $2 \mid 4$, we conclude that 2 is not prime in R.

Now we will show that 2 is irreducible. We shall use the norm function from Problem 2, which in this case is given by $N(a + b\sqrt{5}) = |a^2 - 5b^2|$.

Suppose that 2 is not irreducible. Clearly, $2 \neq 0$ and 2 is not a unit since $N(2) = 4 \neq 1$; hence the only possibility is that $2 = fg$ for some non-units f and g. Then, as in the solution to Problem 4(a) we have $N(f)N(g) = 4$, so $N(f) = N(g) = 2$.

If $f = a + b\sqrt{5}$, we have $|a^2 - 5b^2| = 2$, so $a^2 - 5b^2 = \pm 2$, whence $a^2 \equiv 2$ or 3 mod 5. On the other hand, by direct computation $x^2 \equiv 0, 1$ or 4 mod 5 for any $x \in \mathbb{Z}$, so we reached a contradiction.