Math 124 Homework 7 Solutions

by Luke Gustafson

Fall 2003

1a. Let $\alpha = a + b\frac{1+\sqrt{-p}}{2}$, with $a, b \in \mathbb{Z}$. We have

$$N(\alpha) = \left(\frac{2a+b+b\sqrt{-p}}{2}\right)\left(\frac{2a+b-b\sqrt{-p}}{2}\right)$$

$$= \frac{(2a+b)^2 + pb^2}{4}$$

Now, if $b = 0$, then $N(\alpha) = a^2 \neq q$ so $b \neq 0$. In particular, $b^2 \geq 1$, and we have $N(\alpha) \geq \frac{1+p}{4}$.

1b. Since $-p$ is a quadratic residue, that means there is a solution to $x^2 \equiv -p \pmod{q}$. Thus x^2+p is divisible by q. Suppose that x^2+p is divisible by q^2; i.e. $x^2+p \equiv 0 \pmod{q^2}$. Then $(x+q)^2+p \equiv x^2+p+2q+q^2 \equiv 2q \pmod{q^2}$. Since $q \neq 2$, $2q \not\equiv 0 \pmod{q^2}$. Conclude that either x^2+p or $(x+q)^2+p$ is divisible by q but not q^2. Letting $m = x$ or $m = x+q$ and $n = 1$ gives the desired result.

1c. Consider $x \in R$ with $x = a + b\frac{1+\sqrt{-p}}{2}$, $a, b \in \mathbb{Z}$.

First, observe that q cannot divide n. If $q|n$, then since $q|m^2+pn^2$, we must have $q|m$. However, then $q^2|m^2+pn^2$, a contradiction.

Therefore q and $2n$ are relatively prime. Let c, d be integers such that $cq + 2dn = -b$. Then

$$x + cq\frac{1+\sqrt{-p}}{2} + d(m + n\sqrt{-p}) = a + b/2 + cq/2 + dm$$

is an integer (since $b + cq = 2dn$ is even). Therefore, there exists an integer e such that

$$a + b/2 + cq/2 + dm + eq$$

is between 0 and $q-1$.

Now let $-i = cq\frac{1+\sqrt{-p}}{2} + d(m + n\sqrt{-p}) + eq \in I$. Then, using the above results, $x - i$ is an integer k between 0 and $q-1$, so $x = i + k$ as desired.

1d. First, suppose that the representation in part (c) is not unique. Suppose

$x = i_1 + k_1 = i_2 + k_2$. Then $k_1 - k_2 = i_2 - i_1 \in I$. If $k_1 \neq k_2$, then q does not divide $k_1 - k_2$. Then $k_1 - k_2$ and q are both in I, and they are relatively prime, so $1 \in I$ and $I = R$. Then $I = R$, and so it is prime.

Now suppose the representation in part (c) is unique. Then we can define a map $\phi : R \to \mathbb{Z}/q$ that maps $i+k$ to k. In fact, one can see that $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$, and $\phi(1) = 1$, so ϕ is a homomorphism to $\mathbb{Z}/q$. It is surjective because $0, 1, \ldots, q-1$ must map to themselves by the uniqueness we assumed. The kernel of ϕ is clearly I. Hence, $R/I \cong \mathbb{Z}/q$, which is a field. That means I is a maximal ideal, so I is prime.

1e. Recall that the norm of an ideal is the greatest common divisor of the norms of all elements in the ideal. Consider $m + n\sqrt{-p}$: $N(m + n\sqrt{-p}) = m^2 + pn^2$, which is divisible by q but not q^2. On the other hand, $N(q) = q^2$. Then we get $q = \gcd(N(q), N(m + n\sqrt{-p}))$, so $N(I)|q$. Therefore $N(I) = 1$ or q.

If $N(I) = 1$, then $1 \in I$. However, we claim $1 \notin I$. Suppose $1 = a(m + n\sqrt{-p}) + bq$, where $a, b \in R$. Then $N(1 - bq) = N(a(m + n\sqrt{-p})) = N(a)N(m + n\sqrt{-p})$, and this is divisible by q. Now let $b = x + y\frac{1+\sqrt{-p}}{2}$, with $x, y \in \mathbb{Z}$.

$$\begin{aligned} N(1 - bq) &= N\left(1 - qx - \frac{qy}{2} - \frac{qy\sqrt{-p}}{2}\right) \\ &= \left(1 - qx - \frac{qy}{2}\right)^2 + p\left(\frac{qy}{2}\right)^2 \end{aligned}$$

Multiplying by 4 gives

$$(2 - 2qx - qy)^2 + p(qy)^2 \equiv 4 \pmod{q}$$

Since $q \neq 2$, that means $N(1 - bq)$ is not divisible by q. That gives a contradiction, so $1 \notin I$.

Therefore $N(I) = q$. From class, we know that $N(\alpha) = N(I)$, which gives the desired result.

1f. If $\left(\frac{-p}{q}\right) = 1$, then parts (b)-(d) imply the ideal I exists and is prime. By part (e), since the ideal is principal, $I = (\alpha)$ for some α such that $N(\alpha) = q$. By part (a), $4q \geq p + 1$. That proves the contrapositive of the desired result.

1g. For $p = 23$, use $q = 3$ and we have $\left(\frac{-23}{3}\right) = 1$, so by part (f) R is not a principal ideal domain. For $p = 31$, $q = 5$ gives $\left(\frac{-31}{5}\right) = 1$. For $p = 47$, $q = 3$ gives $\left(\frac{-47}{3}\right) = 1$.

Now look at $p = 23$. We construct a non-principal ideal I as given in parts (b)-(c). As in part (b), we chose $q = 3$ and then $m = 1$, $n = 1$. Then consider the ideal $I = (1 + \sqrt{-23}, 3)$. If it is principal, then by part (e) there exists $\alpha \in R$ such that $N(\alpha) = 3$. However,

$$N(\alpha) = N\left(x + y\frac{1 + \sqrt{-23}}{2}\right)$$

$$= \frac{1}{4}((2x+y)^2 + 23y^2)$$

It is easy to check that there is no solution to $(2x+y)^2 + 23y^2 = 12$, so no α can exist. Therefore, I is not principal.