MATH 152 Problem set 6 solutions

1. $\mathbb{Z}[\sqrt{-2}]$ *is a Euclidean domain (i.e. has a division algorithm)*: the idea is to approximate the quotient by an element in $\mathbb{Z}[\sqrt{-2}]$. More precisely, let $a+b\sqrt{-2}, c+d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ (of course $a, b, c, d \in \mathbb{Z}$). Then there exists $e + f\sqrt{-2}$, where $e, f \in \mathbb{Q}$, such that

$$\frac{a + b\sqrt{-2}}{c + d\sqrt{-2}} = e + f\sqrt{-2}.$$

Now pick $r, s \in \mathbb{Z}$ such that $|e - r| \leq 1/2$ and $|f - s| \leq 1/2$. Then

$$\begin{aligned} & a + b\sqrt{2} \\ = \;& (c + d\sqrt{-2})(e + f\sqrt{-2}) \\ = \;& (c + d\sqrt{-2})(r + s\sqrt{-2} + (e - r) + (f - s)\sqrt{-2}) \\ = \;& (c + d\sqrt{-2})(r + s\sqrt{-2}) + (c + d\sqrt{-2})((e - r) + (f - s)\sqrt{-2}). \end{aligned}$$

We are done if we find a norm N such that $N(c+d\sqrt{-2}) > N((c+d\sqrt{-2})((e-r)+(f-s)\sqrt{-2}))$. Define our N to be just the standard norm, i.e. $N(x + y\sqrt{-2}) = x^2 + 2y^2$. (This is just the complex Euclidean norm squared.) Then since $|e - r| \leq 1/2$ and $|f - s| \leq 1/2$, $N((e - r) + (f - s)\sqrt{-2}) \leq (1/2)^2 + 2(1/2)^2 = 3/4$. This immediately implies the desired inequality.

Primes in $\mathbb{Z}[\sqrt{-2}]$ *are precisely the irreducibles*: suppose first $z \in \mathbb{Z}[\sqrt{-2}]$ is prime, and suppose $vw = z$. Then either v or w is a multiple of z, so without loss of generality write $w = uz$. Then $vuz = z$, and thus $vu = 1$; in particular v is a unit, showing that z is irreducible.

Conversely, suppose p is irreducible, and that $p \mid ab$. By assumption, the only divisor of p (i.e. an element n such that $p = nm$ for some m) up to unit is p itself. Therefore $(a, p) = 1$ or p, and similarly $(b, p) = 1$ or p. If either $(a, p) = p$ or $(b, p) = p$, then p is prime as desired. If $(a, p) = (b, p) = 1$, then we can write $a = Ap + 1$ and $b = Bp + 1$ for some A and B, which implies $ab = (Ap + 1)(Bp + 1) = ABp^2 + (A + B)p + 1$; but this is not a multiple of p, a contradiction. Therefore we have shown that in $\mathbb{Z}[\sqrt{-2}]$ primes are irreducibles and irreducibles are primes.

Unique factorization: we first show the existence of the factorization. Pick any $z \in \mathbb{Z}[\sqrt{-2}]$. We argue by induction on $N(z)$. If $N(z) = 1$, then z is a unit, and there is nothing to prove. Next assume that every element of $\mathbb{Z}[\sqrt{-2}]$ with norm less than n has a factorization into irreducibles, and suppose that $N(z) = n$. If z is irreducible, we are done. If not, we can write $z = z_1 z_2$, where $N(z_1), N(z_2) < N(z)$. By induction hypothesis, z_1 and z_2 have a factorization into irreducibles, so z has one, too.

To show the uniqueness of the factorization, suppose $p_1 \dots p_n = q_1 \dots q_m$, where p_i's and q_i's are irreducibles (hence primes by our work above), is two unique factorizations of the same element. Since p_1 is prime, at least one q_j is divisible by p_1, and by reordering the subscripts if necessary, we can assume $j = 1$. But then q_1, being irreducible, is only divisible by a unit or q_1 itself; and since p_1 divides q_1 and is not a unit, p_1 and q_1 are equal up to multiplication by a unit (which, in this case, is just ± 1). So we can cancel out p_1 and q_1 from each side and obtain $p_2 \dots p_n = \pm q_2 \dots q_m$. Repeating the same argument with p_2 and q_2 (with some reordering of subscripts), p_3 and q_3, and so on, we will have $n = m$ and $p_i = \pm q_i$ for every i. This proves the unique factorization.

Prime(=irreducible) elements of $\mathbb{Z}[\sqrt{-2}]$: let $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ be a prime. Note that $(a + b\sqrt{-2})(a - b\sqrt{-2})\mathbb{Z}$ is divisible by $a + b\sqrt{-2}$. On the other hand, we can write $(a + b\sqrt{-2})(a - b\sqrt{-2}) = p_1 \dots p_k$, where p_i's are primes in integers. Therefore $p_1 \dots p_k$ is divisible by $a + b\sqrt{-2}$, and by primality one of $p_i := p$ is divisible by $a + b\sqrt{-2}$. Hence we can write

$$p = (a + b\sqrt{-2})(c + d\sqrt{-2}).$$

By applying the norm to both sides, we get $p^2 = N(a + b\sqrt{-2})N(c + d\sqrt{-2})$. Therefore $N(a + b\sqrt{-2}) = p$ or p^2. In the former case, $p = a^2 + 2b^2$, so it is of the form $x^2 + 2y^2$. In the latter case, we have $N(c + d\sqrt{-2}) = 1$, so $a + b\sqrt{-2} = \pm p$, and p is not of the form $x^2 + 2y^2$; otherwise it is factorizable into $(x + y\sqrt{-2})(x - y\sqrt{-2})$.

In summary, if $a + b\sqrt{-2}$ is prime in $\mathbb{Z}[\sqrt{-2}]$, then either it has norm p where p is of the form $x^2 + 2y^2$, or it has norm p^2 and equals p where p is not of the form $x^2 + 2y^2$.

Conversely, if $a + b\sqrt{-2}$ has norm p prime (in integers), then it is necessarily prime, and p is of the form $x^2 + 2y^2$. And if p (prime in integers) is not of form $x^2 + 2y^2$, then p is a prime in $\mathbb{Z}[\sqrt{-2}]$; because otherwise $p = (a + b\sqrt{-2})(a - b\sqrt{-2})$ for some $a, b \in \mathbb{Z}$, and so $p = a^2 + 2b^2$, a contradiction.

Therefore we have the following characterization of primes in $\mathbb{Z}[\sqrt{-2}]$:

1. elements with norm p, where p is an integer prime of the form $x^2 + 2y^2$.
2. integer primes not of the form $x^2 + 2y^2$.

2. $2 = 0 + 2 \cdot 1^2$ is of the form $x^2 + 2y^2$. So let's consider odd primes only. A square of an integer is always 1 or 4 (mod 8). Hence $x^2 + 2y^2$ can only equal 1, 3, 4, 6 (mod 8). Therefore primes 5 or 7 (mod 8) are not of form $x^2 + 2y^2$.

Next we show that primes 1 or 3 (mod 8) are of the form $x^2 + 2y^2$.

Lemma. *$p = 1$ or 3 (mod 8) if and only if $n^2 + 2 \equiv 0$ (mod p) for some integer n.*

Proof. The latter statement holds if and only if -2 is a quadratic residue over p, i.e. $(\frac{-2}{p}) = 1$. And $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$ is easily seen to be 1 if and only if p is 1 or 3 (mod 8). $\square$

By the lemma, if $p \equiv 1$ or 3 (mod 8), then we can find n such that $p \mid n^2 + 2 = (n + \sqrt{-2})(n - \sqrt{-2})$. We want to show that p is reducible, so that $p = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2$ for some $a, b \in \mathbb{Z}$. If p is irreducible, then p divides $n + \sqrt{-2}$ or $n - \sqrt{-2}$, and since p divides the complex conjugate of what it divides, it actually divides both $n + \sqrt{-2}$ and $n - \sqrt{-2}$, and hence divides their differences, $2\sqrt{-2}$. But this is impossible because $N(p) \leq 9$ by assumption and $N(2\sqrt{-2}) = 8$. Therefore we proved that an integer prime p is of the form $x^2 + 2y^2$ if and only if p is congruent to 1 or 3 mod 8.

In general, $n \in \mathbb{Z}$ is of the form $x^2 + 2y^2$ if and only if the unique factorization of n in $\mathbb{Z}[\sqrt{-2}]$ has no odd power of a prime 5 or 7 mod 8. To prove the "if" part, note that in this case we can write $n = c^2 \dots (a + b\sqrt{-2})(a - b\sqrt{-2})$ for some $a, b, c \in \mathbb{Z}$. For the "only if" part, suppose the unique factorization of $n = x^2 + 2y^2$ has an odd power of a prime q congruent to 5 or 7 (mod 8). By dividing both sides by the maximal possible even power of q, assume that q is the maximal power of q dividing n. Then we have $x^2 + 2y^2 \equiv 0$ (mod q), $x, y \not\equiv 0$ (mod q), which gives $(x/y)^2 \equiv -2$ (mod q), that is, -2 is a quadratic residue mod q. But this contradicts the lemma above.

3. *Infinitude of 1 mod 3 primes.* Suppose $p_1, \dots, p_k$ are all the 1 mod 3 primes there are, and consider the expression

$$(2p_1 \dots p_k)^2 + 3. \tag{1}$$

This is divisible only by odd 2 mod 3 primes. Hence (1) equals

$$q_1 \dots q_l \tag{2}$$

where q_i's are odd 2 mod 3 primes. Comparing residues mod 3 of (1) and (2) gives l is even.

The key lemma is that all the q_i's are 1 mod 4. If any $q_i := q$ is 3 mod 4, then $(\frac{3}{q}) = 1$, because by quadratic reciprocity $(\frac{3}{q})(\frac{q}{3}) = -1$ and $(\frac{q}{3}) = (\frac{2}{3}) = -1$. Now observe that $(2p_1 \dots p_k)^2 + 3 \equiv 0 \pmod q$. 3 is a quadratic residue $\pmod q$, so this is a sum of two squares. We can lift this equality in $\mathbb{Z}$, so that $x^2 + y^2 = cq$ for some $x, y, c \in \mathbb{Z}$ and $c < q$. But this contradicts the two squares theorem.

Hence all the q_i's are 1 mod 4, and so (2) is 1 mod 4. But (1) is 3 mod 4, a contradiction. This proves that there are infinitely many primes 1 mod 3.

infinitude of 2 mod 3 primes Now suppose $q_1, \dots, q_k$ are all the 2 mod 3 primes. Consider the quantity $(q_1 \dots q_k)^2 + 1$. By assumption this is not divisible by any 2 mod 3 primes. But then this is congruent to 2 mod 3, so some 2 mod 3 prime must divide it, a contradiction.

4. When $s > 1$, the series $\sum_{n=1}^{\infty} \mu(n) n^{-s}$ is bounded by $\sum_{n=1}^{\infty} n^{-s}$, a convergent series. Therefore our series also converges when $s > 1$.

Note that formally, $\sum_{n=1}^{\infty} \mu(n) n^{-s}$ equals $1/\zeta(s) = \prod_p (1 - p^{-s})$. Since both of these converge when $s > 1$, they must equal. In addition, $\zeta(s)/\zeta(2s) = \prod_p (1 - p^{-2s})/(1 - p^{-s}) = \prod_p (1 + p^{-s}) = \sum \mu(n)^2/n^s$.

y 5. (i) Suppose m and n are coprime. A multiple of a divisor of m and a divisor of n is always a divisor of mn, so $d(mn) \geq d(m)d(n)$. Conversely, suppose x is a divisor of mn, and let $x = p_1^{a_1} \dots p_k^{a_k}$ be the prime factorization of x with p_i's all distinct. Since m and n are coprime, each $p_i^{a_i}$ divides precisely one of either m or n. Collecting the factors that divide only m and the factors that divide only n, we see that x is a multiple of a divisor of m and a divisor of n. This implies $d(mn) \leq d(n)d(m)$. Therefore $d(mn) = d(m)d(n)$.

$d(p^a) = a + 1$ for any prime power p^a: this is easy because p^a has divisors precisely $1, p, p^2, \dots, p^a$.

(ii) If $n = \prod_i p_i^{a_i}$, then we have $d(n)/n^\epsilon = \prod_i (a_i + 1)/p_i^{a_i \epsilon}$. The key observation is that $(a_i + 1)/p_i^{a_i \epsilon}$ is bounded by 1 for all but finitely many pairs of $a_i \in \mathbb{N}$ and p_i prime; this is because for all p_i sufficiently large (e.g. $p_i^\epsilon > 10000$), $(a_i + 1)/p_i^{a_i \epsilon} < 1$ for all a_i; if p_i is not large enough, then for all sufficiently large a_i, $(a_i + 1)/p_i^{a_i \epsilon} < 1$, because this quantity approaches zero as $a_i \to \infty$. Therefore for any n, we have

$$\frac{d(n)}{n^\epsilon} \leq \prod \frac{a_i + 1}{p_i^{a_i \epsilon}},$$

where the product is taken over all the pairs (a_i, p_i) for which $(a_i + 1)/p_i^{a_i \epsilon} \geq 1$ (we just showed that the number of such pairs is finite).

(iii) If $s \leq 1$ then $\sum d(n)/n^s$ is bounded below by $\sum 1/n^s$, which diverges. If $s > 1$, then by the previous exercise, for any $\epsilon < s - 1$ we have $\sum d(n)/n^s \sum C(\epsilon) n^{\epsilon - s}$, which converges because $\epsilon - s < -1$. Therefore $\sum d(n)/n^s$ converges precisely when $s > 1$.

Next, in the range of convergence, note that we can write

$$\sum \frac{d(n)}{n^s} = \prod_p \left(1 + \frac{d(p)}{p^s} + \frac{d(p^2)}{p^{2s}} + \dots\right),$$

which equals

$$\prod_p \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \dots\right).$$

Using the Taylor expansion

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 \dots (|x| < 1),$$

we see that this equals

$$\prod_p \frac{1}{(1-p^{-s})^2} = (\zeta(s))^2.$$