Math 40520 Theory of Number
Homework 10

Due Wednesday, 2015-12-09, in class

Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.

1. For a positive integer n let $f(n)\#\{(x,y,z,t)\in\mathbb{Z}^4 \mid n = xyzt\}$ the number of ways to write n as an ordered product of 4 integers. For example 12 can be written in 4 ways as $12\cdot 1\cdot 1\cdot 1$, in 12 ways as $6\cdot 2\cdot 1\cdot 1$, in 12 ways as $4\cdot 3\cdot 1\cdot 1$ and 12 ways as $3\cdot 2\cdot 2\cdot 1$ for a total of $f(12) = 40$.

   (a) Show that $D_f(s) = \zeta(s)^4$.

   (b) Show that
   $$f(n) = \sum_{d^2|n} \tau(n/d^2)^2$$
   (For example $f(12) = 40 = \tau(12)^2 + \tau(3)^2 = 6^2 + 2^2$.) [Hint: Compare the Dirichlet series of τ^2 and f.]

Proof. (a)

$$\zeta(s)^4 = (\sum \frac{1}{n^s})^4 = \sum_{a,b,c,d\geq 1} \frac{1}{(abcd)^s} = \sum_{n\geq 1}\sum_{abcd=n} \frac{1}{n^s} = \sum_{n\geq 1} \frac{f(n)}{n^s} = D_f(s)$$

(b) From the previous homework you already know that $D_{\tau^2} = \zeta(s)^4/\zeta(2s)$ so part (a) implies that

$$D_f(s) = \zeta(s)^4 = \zeta(2s)D_{\tau^2}(s)$$

which implies that

$$\sum \frac{f(n)}{n^s} = \sum \frac{1}{a^{2s}} \sum \frac{\tau(b)^2}{b^s} = \sum_{a,b} \frac{\tau(b)^2}{(a^2b)^s} = \sum_{n\geq 1}\sum_{a^2b=n} \frac{\tau(b)^2}{n^s}$$

which immediately gives

$$f(n) = \sum_{a^2b=n} \tau(b)^2 = \sum_{d^2|n} \tau(n/d^2)^2$$

□

2. Show that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain. [Hint: similar to $\mathbb{Z}[\sqrt{2}]$, but needs one more step.]

Proof. As in class use $d(x) = |N(x)|$ and we need to show that for any rationals a, b with $x = a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$, we can find $q = m + n\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ such that

$$|N(x-q)| < 1$$

This is equivalent to $|N((a-m)+(b-n)\sqrt{3}| = |(a-m)^2 - 3(b-n)^2| < 1$. Take m to be the closest integer to a and n the closest integer to b. Then $|a-m|, |b-n| \leq 1/2$ and so

$$|(a-m)^2 - 3(b-n)^2| \leq |a-m|^2 + 3|b-n|^2 \leq 1/4 + 3/4 = 1$$

and we just need to rule out the case when $|N(x-q)| = 1$. But the only way to get equality is if $|a-m| = |b-n| = 1/2$ and then

$$|N(x-q)| = |(a-m)^2 - 3(b-n)^2| = |1/4 - 3/4| = 1/2 < 1$$

The proposition in class then implies that $d(x)$ is a Euclidean function. $\square$

3. Consider the Euclidean domain $R = \mathbb{Z}[i]$. Find the gcd of $x = 21 + 47i$ and $y = 62 + 9i$ using the Euclidean algorithm.

Proof. Here is a sequence of divisions with remainder

$$\begin{aligned} 9i + 62 &= (47i + 21)(-i + 1) + (-17i - 6) \\ 47i + 21 &= (-17i - 6)(-3) + (-4i + 3) \\ -17i - 6 &= (-4i + 3)(-3i + 2) \end{aligned}$$

with $N(47i + 21) > N(-17i - 6) > N(-4i + 3)$. We conclude that $(x, y) = -4i + 3$ as it is the last nonzero residue.

The way to get these is to follow the procedure from class. For example

$$\frac{9i + 62}{47i + 21} = -\frac{109}{106}i + \frac{69}{106}$$

and the closest element of $\mathbb{Z}[i]$ to this is $-i + 1$. $\square$

4. Consider the Euclidean domain $R = \mathbb{Z}[\sqrt{2}]$ and let $x = 36 - 19\sqrt{2}$ and $y = 35 - 31\sqrt{2}$. Compute the Bézout identity: find the gcd $d = (x, y)$ and two elements $p, q \in \mathbb{Z}[\sqrt{2}]$ such that $d = xp + yq$.

Proof. This is basically the same as for the previous problem but now finding the linear combination is required. Here's the sequence of divisions with remainder together with the linear combinations.

$$\begin{aligned} -19\sqrt{2} + 36 &= (-31\sqrt{2} + 35)(-\sqrt{2} - 1) + (-15\sqrt{2} + 12) & -15\sqrt{2} + 9 &= y + x(\sqrt{2} + 1) \\ -31\sqrt{2} + 35 &= (-15\sqrt{2} + 9)(-\sqrt{2} + 1) + (-7\sqrt{2} - 4) & -7\sqrt{2} - 4 &= y(\sqrt{2} - 1) + 2x \\ -15\sqrt{2} + 9 &= (-7\sqrt{2} - 4)(-2\sqrt{2} + 3) - (2\sqrt{2} + 7) & -(2\sqrt{2} + 7) &= y(-5\sqrt{2} + 8) + x(5\sqrt{2} - 5) \\ -7\sqrt{2} - 4 &= -(2\sqrt{2} + 7) \cdot \sqrt{2} \end{aligned}$$

so $(x, y) = -2\sqrt{2} - 7 = y(-5\sqrt{2} + 8) + x(5\sqrt{2} - 5)$.

$\square$

5. Show that $2, 3, 1 \pm \sqrt{-5}$ are irreducible in the domain $\mathbb{Z}[\sqrt{-5}]$, but they are not prime. Conclude that $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain.

Proof. Suppose 2 is reducible, i.e., we can write $2 = xy$ with x, y not units. Then $4 = N(2) = N(x)N(y)$ where $N(x), N(y) \neq 1$. This implies that $N(x) = N(y) = 2$. Writing $x = a + b\sqrt{-5}$ we'd need $2 = N(x) = a^2 + 5b^2$. This is impossible as 2 is not a quadratic residue mod 5.

Similarly, if 3 were reducible we'd have $3 = xy$ with $N(x) = 3$ in which case $N(x) = N(a + b\sqrt{-5}) = a^2 + 5b^2 = 3$. This, again, is impossible as 3 is not a quadratic residue mod 5.

Now if $1 \pm \sqrt{-5}$ were reducible then $1 \pm \sqrt{-5} = xy$ with $N(x), N(y) \neq 1$. But then $N(x)N(y) = N(1 \pm \sqrt{-5}) = 6$ so $N(x)$ and $N(y)$ are either 2 and 3 or 3 and 2. As we already showed that $N(x)$ can never be 2 or 3 we get another contradiction.

Finally, if $\mathbb{Z}[\sqrt{-5}]$ were a Euclidean domain then $2, 3, 1 \pm \sqrt{-5}$ would be primes. But $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ so $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$. As 2 is a prime it follows that $2 \mid 1 + \sqrt{-5}$ or $2 \mid 1 - \sqrt{-5}$. This would imply that one of $1 \pm \sqrt{-5}$ can be written as $2(a + b\sqrt{-5})$ which is impossible as 1 is odd and $2a$ is not. $\square$

6. Show that if a prime integer p is $\equiv \pm 3 \pmod 8$ then p is a prime element of the domain $\mathbb{Z}[\sqrt{2}]$.

Proof. Suppose p is not a prime element of $\mathbb{Z}[\sqrt{2}]$. As we already know that $\mathbb{Z}[\sqrt{2}]$ is Euclidean from class, p cannot be irreducible as in a Euclidean domain every irreducible is also a prime. Thus $p = xy$ where x and y are not units so $p^2 = N(p) = N(x)N(y)$. Since x, y are not units it follows that $N(x), N(y) \neq \pm 1$ and so either $N(x) = N(y) = p$ or $N(x) = N(y) = -p$.

Write $x = a + b\sqrt{2}$. Then $\pm p = N(a + b\sqrt{2}) = a^2 - 2b^2$. If $p \mid b$ then immediately $p \mid a$ and so $p^2 \mid a^2 - 2b^2 = \pm p$ which is impossible. Thus $a^2 - 2b^2 \equiv 0 \pmod p$ yields $(a/b)^2 \equiv 2 \pmod p$. This is impossible as if $p \equiv 3 \pmod 8$, $\left(\dfrac{2}{p}\right) = -1$. $\square$

7. Consider the set $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$ as a subset of $\mathbb{R}$.

   (a) Show that $\mathbb{Z}[\sqrt[3]{2}]$ is a domain. [Hint: check if it is closed under $+, -, \cdot$.]

   (b) Take for granted that $N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$ satisfies the following two properties: i. $N(xy) = N(x)N(y)$ for all x, y of the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ and ii. $N(x) = 0$ if and only if $x = 0$ (this is a boring exercise). If $a, b, c \in (0, 1/2)$ show that $N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \in (-1, 1)$.

Proof. (a) This subset of $\mathbb{C}$ is clearly closed under $+$ and $-$ and it clearly contains 0 and 1. Also note that

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = (ax + 2bz + 2cy) + (ay + bx + 2xz)\sqrt[3]{2} + (az + by + cx)\sqrt[3]{4}$$

and so the set is closed under multiplications. Therefore it is a domain. $\square$

(b) If $0 < a, b, c < 1/2$ then

$$N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^2 + 2b^3 + 4c^3 - 6abc < a^3 + 2b^3 + 4c^3 < 7/8 < 1$$

and

$$N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^2 + 2b^3 + 4c^3 - 6abc > -6abc > -6/8 > -1$$