MA 638 - Section 8.1 Homework

1. (The postage stamp problem) Let a and b be two relatively prime positive integers. Prove that every sufficiently large positive integer N can be written as a linear combination $ax + by$ of a and b where x and y are both nonnegative. (i.e. there exists an integer N_0 such that for all $N \geq N_0$ the equation $ax + by = N$ can be solved with both x and y nonnegative integers.) Prove in fact that the integer $ab - a - b$ cannot be written as a positive linear combination of a and b, but that every integer greater than $ab - a - b$ is a positive linear combination of a and b. (so every "postage" greater than $ab - a - b$ can be obtained using only stamps in denominations a and b.)

Proof: To see that $ab-a-b$ cannot be written as a nonnegative linear combination of a and b suppose for contradiction that it can. So let $ab-a-b = am+bn$ where $m, n \in \mathbb{Z}^{\geq 0}$. First note that, since $(a, b) = 1$ this implies that in the multiplicative group of integers mod a, i.e. $\mathbb{Z}_a^*$, the element b has a multiplicative inverse. Likewise in $\mathbb{Z}_b^*$ the element a has a multiplicative inverse. This implies

$$\begin{aligned} ab - a - b \pmod{a} &= am + bn \pmod{a} \quad \Rightarrow \\ -b \pmod{a} &= bn \pmod{a} \quad \Rightarrow \\ -1 \pmod{a} &= n \pmod{a} \end{aligned}$$

and

$$\begin{aligned} ab - a - b \pmod{b} &= am + bn \pmod{b} \quad \Rightarrow \\ -a \pmod{b} &= am \pmod{b} \quad \Rightarrow \\ -1 \pmod{b} &= m \pmod{b}. \end{aligned}$$

From this we can infer that $n = -1 + ap$ and $m = -1 + bq$ for some integers p, q. Since a and b are each positive integers and m, n each nonnegative, then we must have that both p and q are positive.

Next we observe that, from the above,

$$\begin{aligned} ab - a - b &= a(-1 + bq) + b(-1 + ap) \quad \Rightarrow \\ ab &= abq + abp \quad \Rightarrow \\ 1 &= p + q. \end{aligned}$$

But now p and q cannot both be positive, a contradiction. $\lightning$ Hence $ab - a - b$ cannot be written as a nonnegative linear combination of a, b.

Next we show that for any positive integer k, the number $n = ab - a - b + k$ can be written as a positive linear combination of a and b. First note that from Bezout's lemma there exist x_0, y_0 such that

$$ax_0 + by_0 = 1.$$

Because of this we have

$$nax_0 + nby_0 = n$$

and so $x_1 = nx_0$ and $y_1 = ny_0$ are integer solutions to

$$ax_1 + by_1 = n$$

Moreover, for every integer z we have

$$a\left(x_1 + z\frac{b}{(a,b)}\right) + b\left(y_1 - z\frac{a}{(a,b)}\right) = ax_1 + by_1 + zab - zab = n.$$

Since this holds for every integer, we can choose z to be the least integer such that $x_1 + zb \geq 0$. Note that the minimality of z also requires that $x_1 + zb \leq b - 1$. Therefore

$$n = a(x_1 + zb) + b(y_1 - za).$$

Further note that

$$(a-1)(b-1) = ab - a - b + 1 \leq ab - a - b + k = n.$$

Hence

$$(a-1)(b-1) \leq a(x_1 + zb) + b(y_1 - za) \quad \Rightarrow$$

$$\begin{aligned} b(y_1 - za) &\geq (a-1)(b-1) - a(x_1 + zb) \\ &\geq (a-1)(b-1) - a(b-1) \\ &= -(b-1). \end{aligned}$$

But this implies $y_1 - za \geq -\frac{b-1}{b}$ and since for all positive integers b we must have $\frac{b-1}{b} < 1$. Therefore $y_1 - za > -1$ and since $y_1 - za$ is an integer we must have $y_1 - za \geq 0$.

Since we have shown that $n = a(x_0 + zb) + b(y_0 - za)$ this therefore shows that n is a nonnegative linear combination of a and b. Since n was selected arbitrarily from all integers $n \geq ab - a - b + 1$, therefore all such numbers are nonnegative linear combinations of a and b. □

2. Find a generator for the ideal $(85, 1 + 13i) \subseteq \mathbb{Z}[i]$, i.e. the gcd for 85 and $1 + 13i$, by the Euclidean Algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.

Calculuation of $(85, 1 + 13i)$*:* Since 85 has a greater norm than $1 + 13i$ we compute

$$\frac{85}{1+13i} \cdot \frac{1-13i}{1-13i} = \frac{1}{2} - \frac{13}{2}i$$

and arbitrarily choose to round the first one down, and the second we round up. We therefore set $p = 0, q = -6$. We are therefore calling the quotient $0 - 6i$ and the remainder we compute as

$$(1 + 13i)\left(\frac{1}{2} - \frac{1}{2}i\right) = 7 + 6i.$$

Therefore this iteration of the Euclidean algorithm gives us

$$\overbrace{85}^{b} = \overbrace{(1 + 13i)}^{a}\overbrace{(-6i)}^{q_1} + \overbrace{(7 + 6i)}^{r_1}$$

We next compute the quotient and remainder for the pair $1 + 13i$ and $7 + 6i$. Then

$$\frac{1+13i}{7+6i} \cdot \frac{7-6i}{7-6i} = 1 + i.$$

We therefore set $p = 1, q = 1$. We are therefore calling the quotient $1 + i$ and the remainder we compute as

$$(7+6i)(0)=0.$$

Therefore this iteration of the Euclidean algorithm gives us

$$\overbrace{1+13i}^{a}=\overbrace{(7+6i)}^{r_1}\overbrace{(1+i)}^{q_2}+\overbrace{(0)}^{r_2}.$$

Since the remainder is zero the algorithm now terminates, and we conclude that a greatest common divisor is $7+6i$. Therefore the ideal $(85, 1+13i)$ is the same as $(7+6i)$.

Calculation of $(47-13i, 53+56i)$*:*

Since the norm of $53+56i$ is larger, we compute

$$\frac{53+56i}{47-13i}\cdot\frac{47+13i}{47+13i}=\frac{43}{58}+\frac{81}{58}i$$

We therefore set $p=1, q=1$. We are therefore calling the quotient $1+ii$ and the remainder we compute as

$$(47-13i)\left(-\frac{15}{58}+\frac{23}{58}i\right)=-7+22i$$

Therefore this iteration of the Euclidean algorithm gives us

$$\overbrace{53+56i}^{b}=\overbrace{(47-13i)}^{a}\overbrace{(1+i)}^{q_1}+\overbrace{(-7+22i)}^{r_1}$$

We next compute the quotient and remainder for the pair $47-13i$ and $-7+22i$. Then

$$\frac{47-13i}{-7+22i}\cdot\frac{-7-22i}{-7-22i}=-\frac{15}{13}-\frac{23}{13}i.$$

We therefore set $p=-1, q=-2$. We are therefore calling the quotient $-1-2i$ and the remainder we compute as

$$(-7+22i)\left(-\frac{2}{13}+\frac{3}{13}\right)=-4-5i.$$

Therefore this iteration of the Euclidean algorithm gives us

$$\overbrace{47-13i}^{a}=\overbrace{(-7+22i)}^{r_1}\overbrace{(-1-2i)}^{q_2}+\overbrace{(-4-5i)}^{r_2}.$$

We next compute the quotient and remainder for the pair $-7+22i$ and $-4-5i$. Then

$$\frac{-7+22i}{-4-5i}\cdot\frac{-4-5i}{-4-5i}=-2-3i.$$

We therefore set $p=-2, q=-3$. We are therefore calling the quotient $-2-3i$ and the remainder we compute as

$$(-7-22i)\,(0)=0.$$

Therefore this iteration of the Euclidean algorithm gives us

$$\overbrace{-7+22i}^{r_1}=\overbrace{(-4-5i)}^{r_2}\overbrace{(-2-3i)}^{q_3}+\overbrace{(0)}^{r_3}.$$

Since the remainder is zero we conclude that a greatest common divisor of $47-13i$ and $53+56i$ is $-4-5i$. Hence the ideal $(47-13i, 53+56i)$ is the same as $(-4-5i)$.

3. Prove the quadratic integer ring $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to the norm given by the absolute value of the field norm N given in the last example of section 7.1 from the textbook (i.e. the standard norm).

Proof: Let $\alpha=a+b\sqrt{2}, \beta=c+d\sqrt{2}$. We use the norm $N(a+b\sqrt{2})=|a^2-2b^2|$. Next define

$$r=\frac{ac-2bd}{c^2-2d^2}$$
$$s=\frac{ad+bc}{c^2-2d^2}.$$

Note that it is impossible for $c^2-2d^2=0$ since this would imply $\left(\frac{c}{d}\right)^2=2$. This in turn would imply that $\sqrt{2}$ is a rational number, which we know it is not. So r and s are each rational numbers and

$$\alpha=\beta(r+s\sqrt{2}).$$

Next define p to be the integer nearest to r and define q to be the integer nearest to s. Set $\theta=(r-p)+(s-q)\sqrt{2}$ and set $\gamma=\beta\theta$. Since β and θ each have integer coefficients then γ must also have integer coefficients. Moreover

$$\gamma=\beta(r+s\sqrt{2})-\beta(p+q\sqrt{2})=\alpha-\beta(p+q\sqrt{2})\quad\Rightarrow$$

$$\alpha=\beta(p+q\sqrt{2})+\gamma$$

so that if we show $N(\beta)>N(\gamma)$ then $p+q\sqrt{2}$ is our quotient and γ is our remainder satisfying the properties of a Euclidean norm. But notice that by the triangle inequality

$$N(\theta)=|(r-p)^2-2(s-q)^2|\leq|r-p|^2+2|s-q|^2$$

and from the construction of p and q we have that $|r-p|\leq\frac{1}{2}$ and $|s-q|\leq\frac{1}{2}$. Therefore

$$N(\theta)\leq\frac{1}{4}+2\cdot\frac{1}{4}=\frac{3}{4}.$$

Since the norm is multiplicative then

$$N(\gamma)=N(\beta\theta)=N(\beta)N(\theta)=\frac{3}{4}N(\beta)<N(\beta).$$

This shows that N is an appropriate norm to make $\mathbb{Z}[\sqrt{2}]$ a Euclidean domain. □