Assignment 1 Question 3

Let G = $\mathbb{Z}[i] = \{a + b \cdot i : a, b \in \mathbb{Z}\}$ denote the set of Gaussian integers.

```
> restart;
```

Part (a)

Why is G an integral domain? Since G is closed under addition and multiplication (easily checked) and 0 and 1 are in G, and since G is a subset of the field of complex numbers C, it follows that G is subring of C. Since C is a field, C has no zero divisors and C is commutative hence G has no zero divisors and G is commutative too. Hence G is an integral domain.

What are the units in G? The elements $\{1, -1, i, -i\}$ have inverses $\{1, -1, -i, i\}$ in G respectively so they are units. To show that there are no more units we proved in class that all units must have the same Euclidean norm and these ones {1,-1,i,-i} are the only ones with norm 1. Alternatively you can show

```
> (a+b*I)*(c+d*I)=1;
```

$$(a + b\,\mathrm{I})\,(c + d\,\mathrm{I}) = 1$$

has no integer solutions for a,b,c,d other than the ones enumerated above. We solve

```
> solve( {a*c-b*d=1,b*c+a*d=0} );
```

$$\left\{c = c,\ d = d,\ b = -\frac{d}{c^2 + d^2},\ a = \frac{c}{c^2 + d^2}\right\}$$

Now we argue that the only integer solutions for a are $c = 0$ or $c = 1$ or $c = -1$. If $c = 0$ then $d = 1$ or $d = -1$ which forces $a = 0,\ b = -1$ and $a = 0,\ b = 1$ respectively. $c = 1$ forces $d = 0$ which means $a = 1,\ b = 0$. And $c = -1$ forces $d = 0$ which means $a = -1$ and $b = 0$. These are the four units.

A better approach would be to use $|a + b \cdot i| = \sqrt{a^2 + b^2}$. For complex numbers A and B we have |AB| = |A||B| and thus if |a+bi| |c+di| = |1| = 1, and since a,b,c,d are integers, the only possibility for a+bi is that |a+bi| = 1. Since |a+bi| = sqrt(a^2+b^2) the only possibility is that (a,b) = (0,1) or (1,0) or (-1,0) or (0,-1) which gives {1,-1,-i,i} are the units.

Part (b)

Let N(a+bi) = $a^2 + b^2$ be the norm of a complex number $a + b\,i$. Now
N(A B) = N((a+bi) (c+di)) = N((ac-bd) + (ad+bc) i) = (ac-bd)^2 + (ad+bc)^2

```
>  N := expand( (a*c-b*d)^2 + (a*d+b*c)^2 );
```

$$N := a^2 c^2 + b^2 d^2 + a^2 d^2 + b^2 c^2$$

```
> factor(N);
```

$$(c^2 + d^2)\,(a^2 + b^2)$$

which is clearly N(A) N(B). Now if A and B are non-zero and A,B are in G with a,b,c,d integers, then N(A) >= 1 and N(B) >= 1 hence N(A) N(B) >= N(A).

Part (c)

The main part of this question is to show that G = $\mathbb{Z}$[i] is a Euclidean domain with $\nu(a+b\,i) = N(a+b\,i) = a^2+b^2$. Note the norm function is simply the square of the magnitude of a complex number which is denoted $|a+b\,i|$. The main thing we need to do is define a remainder function for computing the remainder of A divided B with the required properties. Given A and B we need to define the quotient Q and remainder R that satisfy A = B Q + R with R = 0 or N(R) < N(B). It's easier if we define Q and then R is given by R = A - BQ. Let's work on an example.

To define the remainder operation consider A/B where

```
> A := 63+10*I; B := 7+43*I; C := A/B; evalf(C);
```

$$A := 63 + 10\,\mathrm{I}$$

$$B := 7 + 43\,\mathrm{I}$$

$$C := \frac{67}{146} - \frac{203}{146}\,\mathrm{I}$$

$$0.4589041096 - 1.390410959\,\mathrm{I}$$

We see that a possible Gaussian integer for the quotient Q is -I because the integer part of A/B is -I. I.e. if we ``truncate'' towards zero the real and imaginary parts. So if we choose

```
> Q := trunc(Re(C)) + trunc(Im(C))*I;
```

$$Q := -\mathrm{I}$$

then to satisfy $A = B\,Q + R$ we let

```
> R := A-B*Q;
```

$$R := 20 + 17\,\mathrm{I}$$

Now we also require that either R = 0 or the Euclidean valuation function $\nu(R) < \nu(B)$.

```
> v := z -> Re(z)^2 + Im(z)^2;
```

$$\nu := z \to \Re(z)^2 + \Im(z)^2$$

```
> v(R) < v(B);
```

$$689 < 1898$$

It works.

Let us proceed to calculate the GCD of A and B using this definition for the remainder.

```
> REM := proc(A,B) local C,Q,R;
     C := A/B; Q := trunc(Re(C))+trunc(Im(C))*I;
     R := A-B*Q;
  end:
> r0 := A;
```

$$r0 := 63 + 10\,\mathrm{I}$$

```
> r1 := B;
```

$$r1 := 7 + 43\,\mathrm{I}$$

```
> r2 := REM(A,B);
```

$$r2 := 20 + 17\,\mathrm{I}$$

```
> v(r2) < v(r1);
```

$$689 < 1898$$

```
> r3 := REM(r1,r2);
```

$$r3 := 4 + 6\,\mathrm{I}$$

```
> v(r3) < v(r2);
```

$$52 < 689$$

```
> r4 := REM(r2,r3);
```

$$r4 := 2 + 3\,\mathrm{I}$$

```
> v(r4) < v(r3);
```

$$13 < 52$$

```
> r5 := REM(r3,r4);
```

$$r5 := 0$$

The remainder is 0, so $r4 = 2 + 3\,i$ is a GCD(A,B). Let's check that r4 divides A and B exactly.

```
> A/r4, B/r4;
```

$$12 - 13\,\mathrm{I},\ 11 + 5\,\mathrm{I}$$

Now, we still have to prove that the remainder function defined in this way satisfies v(R) < v(B) . In fact, our guess at the quotient function doesn't always give a remainder which satisfies this property. For example, consider

```
> A := 10+122*I;
```

$$A := 10 + 122\,\mathrm{I}$$

```
> B := -105-58*I;
```

$$B := -105 - 58\,\mathrm{I}$$

```
> C := A/B;
```

$$C := -\frac{8126}{14389} - \frac{12230}{14389}\,\mathrm{I}$$

```
> evalf(C);
```

$$-0.5647369518 - 0.8499548266\,\mathrm{I}$$

```
> Q := trunc(C);
```

$$Q := 0$$

```
> R := A-B*Q;
```

$$R := 10 + 122\,I$$

```
> v(R) < v(B);
```

$$14984 < 14389$$

So, what to do in such a case? A definition that does work is to round the real and imaginary parts of A/B to the `nearest integer. What this means is that we are choosing the Gaussian integer in the complex plane which is closest to the complex number A/B for Q the quotient. (Note, there may be more than one choice but the choice we make will not matter). Our previous choice was not the closest, and could be more than one unit away. Note, it is analagous to choosing the integer quotient of 7 divided by 2 to be 3 or 4. So for

```
> C := A/B;
```

$$C := -\frac{8126}{14389} - \frac{12230}{14389}\,I$$

we round both the real and imaginary parts, in this case we get both rounded to -1. I.e.

```
> Q := round(Re(C)) + round(Im(C))*I;
```

$$Q := -1 - I$$

Note, we can use just

```
> Q := round(C);
```

$$Q := -1 - I$$

```
> R := A - B*Q;
```

$$R := -37 - 41\,I$$

```
> v(R) < v(B);
```

$$3050 < 14389$$

Now, to prove that either R=0 or v(R) < v(B).

We have $A = B\,Q + R \Rightarrow R = A - B\,Q = B\,(A/B - Q)$ thus $v(R) = v(B)\,v(A/B - Q)$. To prove that v(R) < v(B) it suffices to show that v(A/B - Q) < 1. Now because of our choice of rounding, the quotient we have the real part of $A/B - Q$ is $\le 1/2$ and the imaginary part of $A/B - Q \le 1/2$.

Thus $v(R) \le \frac{1}{2^2} + \frac{1}{2^2}$ = 1/2.

Part (d)

```
> REM := proc(A,B) local C,Q,R;
      C := A/B;
```

```
    Q := round(A/B);
    R := A-B*Q;
end:
```

```
> r0 := 63+10*I;
```

$$r0 := 63 + 10\,\mathrm{I}$$

```
> r1 := 7+43*I;
```

$$r1 := 7 + 43\,\mathrm{I}$$

```
> r2 := REM(r0,r1);
```

$$r2 := 20 + 17\,\mathrm{I}$$

```
> r3 := REM(r1,r2);
```

$$r3 := 4 + 6\,\mathrm{I}$$

```
> r4 := REM(r2,r3);
```

$$r4 := -2 - 3\,\mathrm{I}$$

```
> r5 := REM(r3,r4);
```

$$r5 := 0$$

So A GCD is $-2-3i$ which is not in the positive quadrant. Since the units in G are 1, -1, i and -i it follows that the possible gcds of A and B are positive quadrant.

```
> r4, -r4, I*r4, -I*r4;
```

$$-2 - 3\,\mathrm{I},\ 2 + 3\,\mathrm{I},\ 3 - 2\,\mathrm{I},\ -3 + 2\,\mathrm{I}$$