1. (a) Show that if α and β are elements of $\mathbb{Z}[\sqrt{D}]$ such that α is a unit times β, then $N(\alpha) = \pm N(\beta)$.

Solution: If $\alpha = \beta\varepsilon$ with ε a unit, then $N(\alpha) = N(\beta)N(\varepsilon)$ and $N(\varepsilon) = \pm 1$, so $N(\alpha) = \pm N(\beta)$.

(b) Either prove or give a counterexample to the following statement: If α and β are Gaussian integers with $N(\alpha) = N(\beta)$ then α is a unit times β.

Solution: Let $\alpha = a + bi$ and $\beta = c + di$. Then the condition $N(\alpha) = N(\beta)$ says that $a^2 + b^2 = c^2 + d^2$. This equation has many solutions, for example $3^2 + 4^2 = 5^2 + 0^2$, which gives $\alpha = 3 + 4i$ and $\beta = 5$, and obviously $3 + 4i$ is not a unit times 5 since the only units are ± 1 and $\pm i$.

2. Show that a Gaussian integer $x + yi$ with both x and y odd is divisible by $1 + i$ but not by $(1 + i)^2$.

Solution: We have $$\frac{x + yi}{1 + i} = \frac{(x + yi)(1 - i)}{(1 + i)(1 - i)} = \frac{(x + y) + (y - x)i}{2}$$

This is a Gaussian integer if x and y are odd since $x + y$ and $y - x$ are then even. Thus $1+i$ divides $x+yi$ when x and y are odd. For $(1+i)^2$, note that this equals $2i$, so if $x + yi$ was divisible by $2i$ it would be divisible by 2, but $x + yi$ is not divisible by 2 if x and y are odd.

3. There are four different ways to write the number $1105 = 5 \cdot 13 \cdot 17$ as a sum of two squares. Find these four ways using the factorization of 1105 into primes in $\mathbb{Z}[i]$. [Here we are not counting $5^2 + 2^2$ and $2^2 + 5^2$ as different ways of expressing 29 as the sum of two squares. Note that an equation $n = a^2 + b^2$ is equivalent to an equation $n = (a + bi)(a - bi)$.]

Solution: The prime factorization is

$$1105 = 5 \cdot 13 \cdot 17 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)(4 + i)(4 - i)$$

We want to find the various ways we can combine these into two terms $(a+bi)(a-bi)$ by choosing the signs $+$ and $-$ in the various factors:

$(+++)(---)$: $[(2 + i)(3 + 2i)(4 + i)][(2 - i)(3 - 2i)(4 - i)] = (9 + 32i)(9 - 32i)$

$(++-)(--+)$: $[(2 + i)(3 + 2i)(4 - i)][(2 - i)(3 - 2i)(4 + i)] = (23 + 24i)(23 - 24i)$

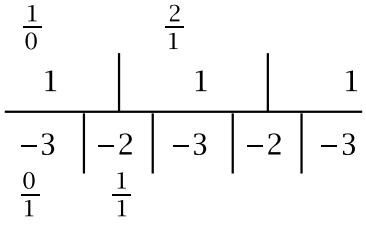
$(+--)(-++)$: $[(2 + i)(3 - 2i)(4 - i)][(2 - i)(3 + 2i)(4 + i)] = (31 - 12i)(31 + 12i)$

$(+-+)(-+-)$: $[(2 + i)(3 - 2i)(4 + i)][(2 - i)(3 + 2i)(4 - i)] = (33 + 4i)(33 - 4i)$

So we get $1105 = 9^2 + 32^2 = 23^2 + 24^2 = 31^2 + 12^2 = 33^2 + 4^2$.

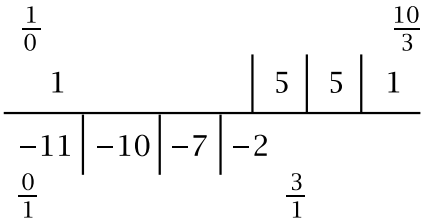
4. (a) Find four different units in $\mathbb{Z}[\sqrt{3}]$ that are positive real numbers, and find four that are negative.

Solution: We find the smallest positive solution of Pell's equation $x^2 - 3y^2 = \pm 1$ by looking at the separator line in the topograph for $x^2 - 3y^2$. This gives the solution $(x, y) = (2, 1)$ which gives the unit $2 + \sqrt{3}$. This is a unit since $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$. Another unit is $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, with $(7 + 4\sqrt{3})(7 - 4\sqrt{3}) = 1$. Thus we have four positive units $2 \pm \sqrt{3}$ and $7 \pm 4\sqrt{3}$. The negatives of these numbers give four negative units.



(b) Do the same for $\mathbb{Z}[\sqrt{11}]$.

Solution: This time the separator line is:



The smallest positive solution of $x^2 - 11y^2 = \pm 1$ is $(x, y) = (10, 3)$ so we have the four positive units $10 \pm 3\sqrt{11}$ and $(10 \pm 3\sqrt{11})^2 = 199 \pm 60\sqrt{11}$. Taking the negatives of these gives four negative units.

5. Make a list of all the Gaussian primes $x + yi$ with $-7 \le x \le 7$ and $-7 \le y \le 7$.

Solution: We know the Gaussian primes are the ordinary primes $p = 4k + 3$ (and units times these) and the Gaussian integers $a + bi$ such that $a^2 + b^2$ is a prime in $\mathbb{Z}$, either 2 or $p = 4k + 1$. When $a \le 7$ and $b \le 7$ we have $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$, $61 = 6^2 + 5^2$. We stop here since the next few would be $73 = 8^2 + 3^2$, $89 = 8^2 + 5^2$, $97 = 9^2 + 4^2$. The list of Gaussian primes is then ± 3, $\pm 3i$, ± 7, $\pm 7i$, $\pm 1 \pm i$, $\pm 2 \pm i$, $\pm 1 \pm 2i$, $\pm 3 \pm 2i$, $\pm 2 \pm 3i$, $\pm 4 \pm i$, $\pm 1 \pm 4i$, $\pm 5 \pm 2i$, $\pm 2 \pm 5i$, $\pm 6 \pm i$, $\pm 1 \pm 6i$, $\pm 5 \pm 4i$, $\pm 4 \pm 5i$, $\pm 7 \pm 2i$, $\pm 2 \pm 7i$, $\pm 6 \pm 5i$, $\pm 5 \pm 6i$.

6. Factor the following Gaussian integers into primes in $\mathbb{Z}[i]$: $3 + 5i$, $8 - i$, $10 + i$, $5 - 12i$, $35i$, $-35 + 120i$, $253 + 204i$.

Solution: For $3 + 5i$ we have $N(3 + 5i) = 3^2 + 5^2 = 34 = 2 \cdot 17$. So the possible prime

factors of $3+5i$ are the prime factors of $2=(1+i)(1-i)$ and $17=(4+i)(4-i)$. Testing $i+i$ first, we have

$$\frac{3+5i}{1+i}=\frac{(3+5i)(1-i)}{(1+i)(1-i)}=\frac{8+2i}{2}=4+i$$

Thus we have the prime factorization $3+5i=(1+i)(4+i)$. The two factors are prime since their norms are 2 and 17 which are prime in $\mathbb{Z}$.

$8-i$ has norm $65=5\cdot 13=(2+i)(2-i)(3+2i)(3-2i)$. Testing whether $2+i$ divides $8-i$, we have

$$\frac{8-i}{2+i}=\frac{(8-i)(2-i)}{(2+i)(2-i)}=\frac{15-10i}{5}=3-2i$$

So $8-i=(2+i)(3-2i)$ and these two factors are prime since their norms are 5 and 13 which are prime in $\mathbb{Z}$.

Next, $10+i$ has norm 101 which is prime, so $10+i$ is already a prime.

$5-12i$ has norm $5^2+12^2=13^2=(3+2i)^2(3-2i)^2$. To see whether $5-12i$ is divisible by $3+2i$ we compute

$$\frac{5-12i}{3+2i}=\frac{(5-12i)(3-2i)}{(3+2i)(3-2i)}=\frac{-9-46i}{13}$$

This is not in $\mathbb{Z}[i]$ so it must be $3-2i$ that divides $5-12i$, and in fact $5-12i=(3-2i)^2$. This is the prime factorization since the norm of $3-2i$ is 13, a prime in $\mathbb{Z}$.

$35i=5\cdot 7i=(2+i)(2-i)(7i)$ and these are primes since $N(2\pm i)=5$ is prime and 7 is congruent to 3 mod 4.

$-35+120i=5(-7+24i)=(2+i)(2-i)(-7+24i)$. We have $N(-7+24i)=7^2+24^2=25^2=5^4=(2+i)^4(2-i)^4$. We know that $-7+24i$ is divisible by either $(2+i)^4$ or $(2-i)^4$ since if it were divisible by some mixture of powers of $2+i$ and $2-i$ it would be divisible by $(2+i)(2-i)=5$, which it obviously isn't. A calculation shows that $(2+i)^4=-7+24i$, so the final factorization is $-35+120i=(2+i)^5(2-i)$.

$253+204i$. Using a calculator one computes that this has norm $105625=5^4 13^2=(2+i)^4(2-i)^4(3+2i)^2(3-2i)^2$. Then one computes

$$\frac{253+204i}{2+i}=142+31i \qquad \frac{142+31i}{2+i}=63-16i \qquad \frac{63-16i}{2+i}=22-19i$$

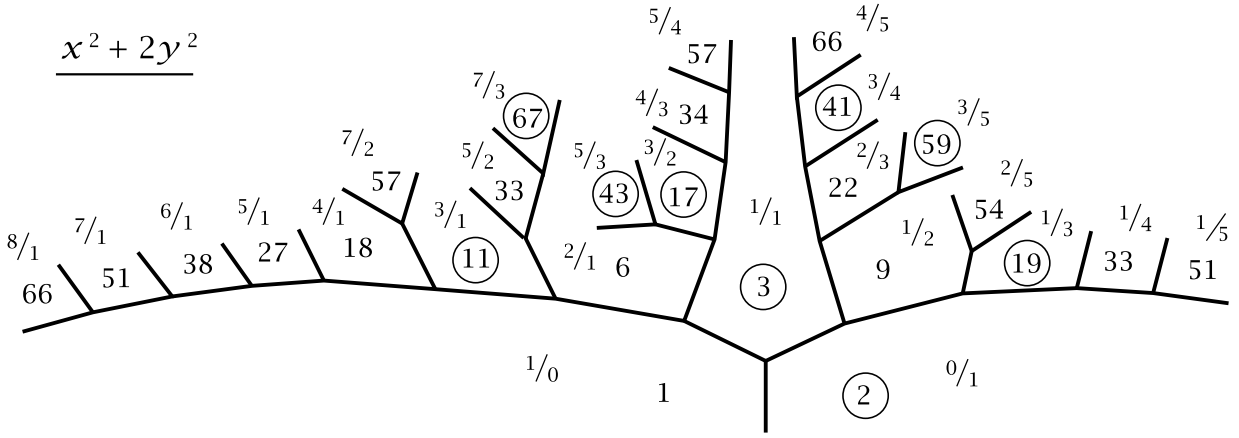
$$\frac{22-19i}{2+i}=5-12i$$

We also have $5-12i=(3-2i)^2$ so the final factorization is:

$$253+204i=(2+i)^4(3-2i)^2$$

7. In this problem we consider $\mathbb{Z}[\sqrt{-2}]$. To simplify notation, let $\omega = \sqrt{-2}$, so elements of $\mathbb{Z}[\omega]$ are sums $x + y\omega$ with $x, y \in \mathbb{Z}$ and with $\omega^2 = -2$. We have $N(x + y\omega) = x^2 + 2y^2 = (x + y\omega)(x - y\omega)$.

(a) Draw the topograph of $x^2 + 2y^2$ including all values less than 70 (by symmetry, it suffices to draw just the upper half of the topograph). Circle the values that are prime (prime in $\mathbb{Z}$, that is). Also label each region with its x/y fraction.



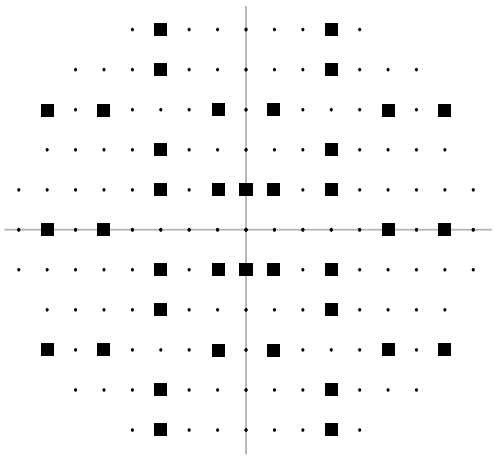
(b) Which primes in $\mathbb{Z}$ factor in $\mathbb{Z}[\omega]$?

Solution: These are the primes that are represented by the norm form $x^2 + 2y^2$. From the topograph we can see that these are 2 (which is the only prime dividing the discriminant $\Delta = -8$) and the primes $p \equiv 1, 3$ modulo 8.

(c) Using the information in part (a), list all primes in $\mathbb{Z}[\omega]$ of norm less than 70.

Solution: We know that $\mathbb{Z}[\omega]$ has unique factorization since it has a Euclidean algorithm. Therefore the primes in $\mathbb{Z}[\omega]$ are of two types: First there are the primes in $\mathbb{Z}$ that stay prime in $\mathbb{Z}[\omega]$. These are the primes not represented by $x^2 + 2y^2$, which are the primes congruent to 5 or 7 modulo 8. The only two that have norm less than 70 are 5 and 7. And second there are the numbers $x + y\omega$ such that $x^2 + 2y^2 = p$, a prime in $\mathbb{Z}$. Reading from the circled entries in the topograph in the order of increasing norm we get $\pm\omega, \pm1 \pm \omega, \pm3 \pm \omega, \pm3 \pm 2\omega, \pm1 \pm 3\omega, \pm3 \pm 4\omega, \pm5 \pm 3\omega, \pm3 \pm 5\omega, \pm7 \pm 3\omega$.

(d) Draw a diagram in the xy-plane showing all elements $x + y\omega$ in $\mathbb{Z}[\omega]$ of norm less than 70 as small dots, with larger dots or squares for the elements that are prime in $\mathbb{Z}[\omega]$.



(e) Show that the only primes $x + y\omega$ in $\mathbb{Z}[\omega]$ with x even are $\pm\omega$. (Your diagram in part (d) should give some evidence that this is true.)

Solution: The primes in $\mathbb{Z}$ that stay prime in $\mathbb{Z}[\omega]$ are congruent to 5 or 7 mod 8 so they are odd and hence don't have the form $x + y\omega$ with x even. The other primes in $\mathbb{Z}[\omega]$ are of the form $x + y\omega$ with $x^2 + 2y^2$ prime in $\mathbb{Z}$. If x is even then $x^2 + 2y^2$ is even, and the only even prime in $\mathbb{Z}$ is 2, so we have $x^2 + 2y^2 = 2$ whose only solutions are (0 ± 1), corresponding to $\pm\omega$.

(f) Factor $4 + \omega$ into primes in $\mathbb{Z}[\omega]$.

Solution: The norm of $4+\omega$ is $(4+\omega)(4-\omega) = 18 = 2\cdot 3^2 = -\omega^2(1+\omega)^2(1-\omega)^2$. So the prime factorization of $4+\omega$ will be either $\pm\omega(1+\omega)^2$ or $\pm\omega(1-\omega)^2$. Multiplying these products out, we see that the correct factorization is $4 + \omega = -\omega(1 + \omega)^2$.