can multiply it by ± 1 or $\pm i$ and obtain another δ of the same absolute value which also divides α and β. This gives four possibilities. In what follows we will consider any one of those four possibilities to be "the" g.c.d.

Notice that any complex number can be written as a Gaussian integer plus a complex number whose real and imaginary parts are each between $\frac{1}{2}$ and $-\frac{1}{2}$. Show that this means that we can divide one Gaussian integer α by another one β and obtain a Gaussian integer quotient along with a remainder which is less than β in absolute value. Use this fact to devise a Euclidean algorithm which finds the g.c.d. of two Gaussian integers. Use this Euclidean algorithm to find (a) $g.c.d.(5+6i,\ 3-2i)$, and (b) $g.c.d.(7-11i,\ 8-19i)$. In each case express the g.c.d. as a linear combination of the form $u\alpha + v\beta$, where u and v are Gaussian integers.

15. The last problem can be applied to obtain an efficient way to write certain large primes as a sum of two squares. For example, suppose that p is a prime which divides a number of the form b^6+1. We want to write p in the form $p = c^2 + d^2$ for some integers c and d. This is equivalent to finding a nontrivial Gaussian integer factor of p, because $c^2+d^2 = (c+di)(c-di)$. We can proceed as follows. Notice that

$$b^6+1 = (b^2+1)(b^4-b^2+1), \qquad \text{and} \qquad b^4-b^2+1 = (b^2-1)^2+b^2.$$

By property 4 of divisibility, the prime p must divide one of the two factors on the right of the first equality. If $p|b^2+1 = (b+i)(b-i)$, then you will find that $g.c.d.(p,\ b+i)$ will give you the desired $c+di$. If $p|b^4-b^2+1 = \big((b^2-1)+bi\big)\big((b^2-1)-bi\big)$, then $g.c.d.(p,\ (b^2-1)+bi)$ will give you your $c+di$.

Example. The prime 12277 divides the second factor in the product $20^6+1 = (20^2+1)(20^4-20^2+1)$. So we find $g.c.d.(12277,\ 399+20i)$:

$$\begin{aligned} 12277 &= (31-2i)(399+20i) + (-132+178i), \\ 399+20i &= (-1-i)(-132+178i) + (89+66i), \\ -132+178i &= (2i)(89+66i), \end{aligned}$$

so that the g.c.d. is $89+66i$, i.e., $12277 = 89^2+66^2$.

(a) Using the fact that $19^6+1 = 2\cdot 13^2\cdot 181\cdot 769$ and the Euclidean algorithm for the Gaussian integers, express 769 as a sum of two squares.

(b) Similarly, express the prime 3877, which divides 15^6+1, as a sum of two squares.

(c) Express the prime 38737, which divides $2^{36}+1$, as a sum of two squares.