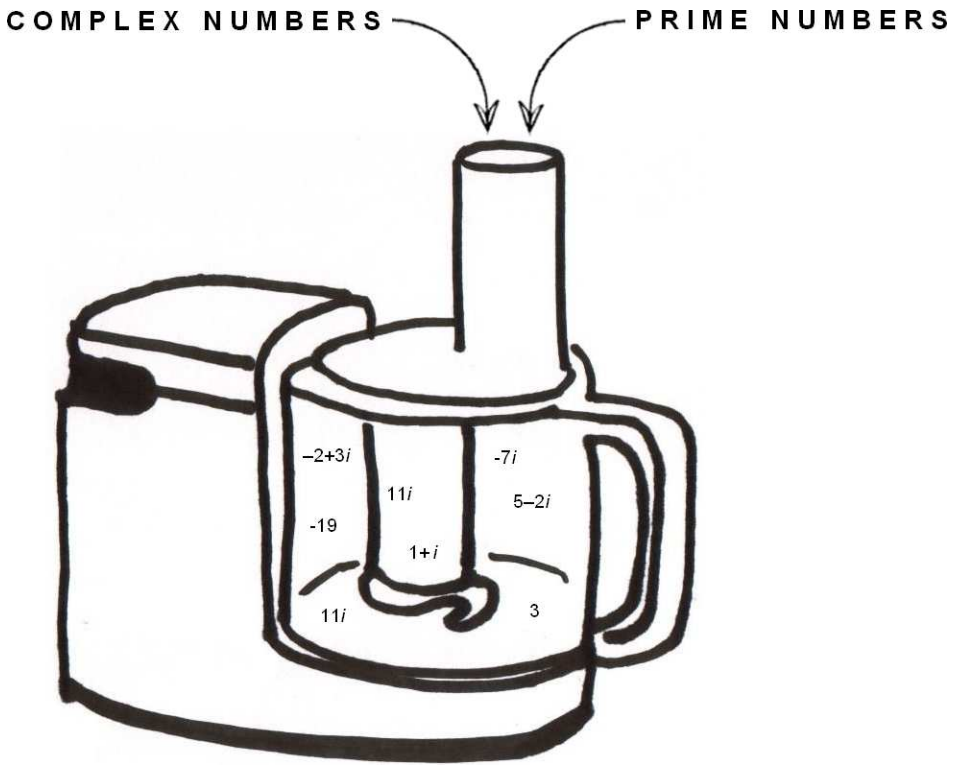
*There's an old saying, "you can't add apples and oranges." Mathematicians hate "can't;" they love to throw apples and oranges into a food processor and see what happens. Sometimes they get amazing results. Here is today's recipe at Café Math.*




Complex Integers[1] are defined as the set of complex numbers whose real and imaginary parts are both integers. For example, 4, 7*i*, and 2 – 3*i* are complex integers.

A Real Prime is an integer > 1 that is only divisible by 1 and itself. We can extend this definition to complex integers and define a Complex Prime[2] as a complex integer whose *modulus*[3] is > 1 and is only divisible by 1, *i*, and itself.

For complex primes the signs of the real and imaginary parts can be positive or negative. Complex primes are symmetrical in the complex plane. We only need to test complex integers $a+bi$ where $a \geq 0, 0 \leq b \leq a$, and can find all the others using symmetry. This group of complex primes $\pm a \pm bi,\ \pm b \pm ai$ are called *associates*. Every complex prime is divisible by some of its associates; these do not count as factors.

[1] These are actually called *Gaussian Integers* in honor of Carl Friedrich Gauss who was the first mathematician to study them.

[2] Actually called *Gaussian Primes*.

[3] The modulus of a complex number $a + bi$ is $\sqrt{a^2+b^2}$ and is written $|a + bi|$.

## Let's find some complex primes.

The smallest[4] complex integer > 1 is $1 + i$ and it is a complex prime since there are no possible divisors between it and 1. By symmetry, $1 - i$ is also a complex prime.

The next smallest complex integer is 2. $2 = (1+i)(1-i)$ so it is not a complex prime.

Next comes $2 + i$. It is not divisible by any of the complex primes found so far so it and its conjugate, $2 - i$, are the next complex primes.

$2 + 2i$ ? It's divisible by 2 so it is not a complex prime.

3 is not divisible by any of the smaller complex primes so it is a complex prime.

$3 + i$ ? It's divisible by $1 + i$.

$3 + 2i$ ? Divide by the complex primes found so far: $1 \pm i$, $2 \pm i$, and 3. It's a complex prime, as is its conjugate, $3 - 2i$.

$3 + 3i$ ? It's divisible by 3 and $1 + i$.

Here are the first few complex primes:

| | | | | | |
|---|---|---|---|---|---|
| (1 + *i*) | 7 | (10 + 9*i*) | (14 + *i*) | (17 + 2*i*) | (19 + 10*i*) |
| (2 + *i*) | (7 + 2*i*) | 11 | (14 + 9*i*) | (17 + 8*i*) | (19 + 14*i*) |
| 3 | (8 + 3*i*) | (11 + 4*i*) | (14 + 11*i*) | (17 + 10*i*) | (19 + 16*i*) |
| (3 + 2*i*) | (8 + 5*i*) | (11 + 6*i*) | (15 + 2*i*) | (17 + 12*i*) | (20 + *i*) |
| (4 + *i*) | (8 + 7*i*) | (12 + 7*i*) | (15 + 4*i*) | (18 + 5*i*) | (20 + 3*i*) |
| (5 + 2*i*) | (9 + 4*i*) | (13 + 2*i*) | (15 + 14*i*) | (18 + 7*i*) | (20 + 7*i*) |
| (5 + 4*i*) | (10 + *i*) | (13 + 8*i*) | (16 + *i*) | (18 + 17*i*) | (20 + 11*i*) |
| (6 + *i*) | (10 + 3*i*) | (13 + 10*i*) | (16 + 5*i*) | 19 | (20 + 13*i*) |
| (6 + 5*i*) | (10 + 7*i*) | (13 + 12*i*) | (16 + 9*i*) | (19 + 6*i*) | (20 + 19*i*) |

Remember that you can flip the signs and swap the real and imaginary parts to get other primes.

There is a graphic in the appendix that shows the locations of complex primes in the complex plane.

## Which Real Primes are not Complex Primes?

~~2~~, 3, ~~5~~, 7, 11, ~~13~~, ~~17~~, 19, 23, ~~29~~, 31, ~~37~~, ~~41~~,
43, 47, ~~53~~, 59, ~~61~~, 67, 71, ~~73~~, 79, 83, ~~89~~, ~~97~~

There is a pattern here. Remember that when you multiply a complex number, $a + bi$, by its conjugate, $a - bi$, you get the real number $a^2 + b^2$. This means that any real prime that is the sum of two squares in not a complex prime.

[4] Smallest meaning lowest *norm*. The *norm* of a complex integer $a + bi$ is $a^2 + b^2$. This is different than the norm of a general complex number which is the same as the modulus: $\sqrt{a^2 + b^2}$.

It turns out that there is an easy way to determine if a prime number is the sum of two squares. Look at the struck out primes in the above list and see if you can find out what they have in common. (Ignore 2; once again it's the oddball prime!)

All of the odd primes that are not complex primes are the sum of an even square and odd square. Even squares all have the form $(2n)^2 = 4n^2$ for some integer $n$. This means that they are all multiples of 4. Odd squares all have the form $(2n+1)^2 = 4n^2 + 4n + 1$. This means that they are all multiples of 4, plus 1. The sum of an even square and an odd square must therefore be a multiple of 4, plus 1.

We can rephrase this so that 2 is also excluded: **a real prime is a complex prime if and only if it is a multiple of 4, plus 3.**

## Is there an easier way to tell if a complex integer is a complex prime?

We've just found a simple test for complex integers whose real or imaginary part is 0. What about the rest of the complex integers?

If a complex integer $z = a + bi$ is prime then its conjugate $\bar{z} = a - bi$ is prime. This means that $z$ and $\bar{z}$ are the only factors of $z\bar{z} = a^2 + b^2$. If $a$ and $b$ are non-zero there are no real factors of $z\bar{z}$. Therefore, if $a^2 + b^2$ is not a real prime, $z$ is not a complex prime.

If a complex integer $z = a + bi$ is not prime it has factors $v$ and $w$ and $z\bar{z} = v\bar{v}\,w\bar{w}$. Because $v\bar{v}$ and $w\bar{w}$ are both real, $z\bar{z}$ has two real factors and is not a real prime. Therefore, if $a^2 + b^2$ is a real prime, $z$ is a complex prime.

Having proved the test for both cases, we can state: **a complex integer $z = a + b$ with $a$ and $b$ non-zero is a complex prime if and only if $a^2 + b^2$ is a real prime.**

## Prime Factoring Complex Integers

When prime factoring complex integers we only want to use factors in the form $a \pm bi$ where $a > 0$ and $-a < b \le a$, and the factor $i^n$ where $n$ = 1, 2, or 3. Using this standard form forces a unique factorization. Factors that are not in this form can be converted into the correct form by multiplying by $i^n$.

Here are some examples:

$$3 + 4i = i(4 - 3i)$$
$$-2 + i = i^2(2 - i)$$
$$1 - i = i^3(1 + i)$$

To find the complex prime factors of a positive integer find its real prime factors. Check if any of the real prime factors are not complex primes. Replace them with the complex conjugate pairs that are their factors:

$$150 = 2 \cdot 3 \cdot 5^2$$
$$= (1+i) \cdot (1-i) \cdot 3 \cdot (2+i)^2 \cdot (2-i)^2$$
$$= (1+i) \cdot i^3 \cdot (1+i) \cdot 3 \cdot (2+i)^2 \cdot (2-i)^2$$
$$\boxed{150 = i^3 \cdot (1+i)^2 \cdot 3 \cdot (2+i)^2 \cdot (2-i)^2}$$

$$12 = 2^2 \cdot 3$$
$$= \left(i^3 \cdot (1+i)^2\right)^2 \cdot 3$$
$$\boxed{12 = i^2 \cdot (1+i)^4 \cdot 3}$$

Factoring a negative integer is the same except that it gets an $i^2$ factor:

$$\boxed{-5 = i^2 \cdot (2+i) \cdot (2-i)}$$

To factor a pure imaginary integer, factor as if it were a real integer and multiply by $i$:

$$\boxed{5i = i \cdot (2+i) \cdot (2-i)}$$

Factoring a complex number is a bit tougher. We need a few preliminary concepts to be able to do this.

The *norm* of a complex integer is defined as $N(a+bi) = a^2 + b^2$.
$N(z)$ is *multiplicative*, that is $N(wz) = N(w)N(z)$.[5]
Given a composite complex integer $z = p_1 \cdot p_2 \cdot \cdots \cdot p_n$, $N(z) = N(p_1) \cdot N(p_2) \cdot \cdots \cdot N(p_n)$.

Notice that the factorization of the norm gives the norms of the factors. Determining the factors is not quite automatic since there are multiple complex integers with the same norm. Also, any prime integer $q$ that is a factor has $q^2$ as its norm.

Factor $z = 123 + 456i$.

$$N(z) = 123^2 + 456^2 = 223065$$

This factors to $3^2 \cdot 5 \cdot 4957$. Factors with even powers are likely the norm of a pure real factor. $N(3) = 3^2$ so 3 is likely a factor (obviously, in this example).

$$\frac{z}{3} = 41 + 152i$$

[5] Try to prove this identity yourself. A proof is shown in the appendix.

confirming that 3 is a factor. Complex primes in standard form whose norms equal 5 are $2 \pm i$.

$\frac{41+152i}{2+i}$ does not work, but $\frac{41+152i}{2-i} = -14+69i$.

We can convert the final factor into standard form by dividing it by *i*.

$$\frac{-14+69i}{i} = 69+14i$$

This gives the factorization

$$\boxed{123+456i = i \cdot 3 \cdot (2-i) \cdot (69+14i)}.$$

Factor $z = 35-85i$.

$$N(z) = 8450$$

This factors to $2 \cdot 5^2 \cdot 13^2$. The first factor has norm 2 so it must be $1+i$.

$$\frac{35-85i}{1+i} = -25-60i$$

$5^2$ indicates that 5 is a likely factor, but 5 is not a complex prime so we need two factors of the form $2 \pm i$.

$\frac{-25-60i}{2+i} = -22-19i$, $\frac{-22-19i}{2+i}$ does not work, $\frac{-22-19i}{2-i} = -5-12i$

so $2+i$ and $2-i$ are factors. 13 is not a complex prime so we need two factors of the form $3 \pm 2i$.

$$\frac{-5-12i}{3+2i} = -3-2i = i^2 \cdot (3+2i)$$

so there are two $3+2i$ factors and a final factor of $i^2$.

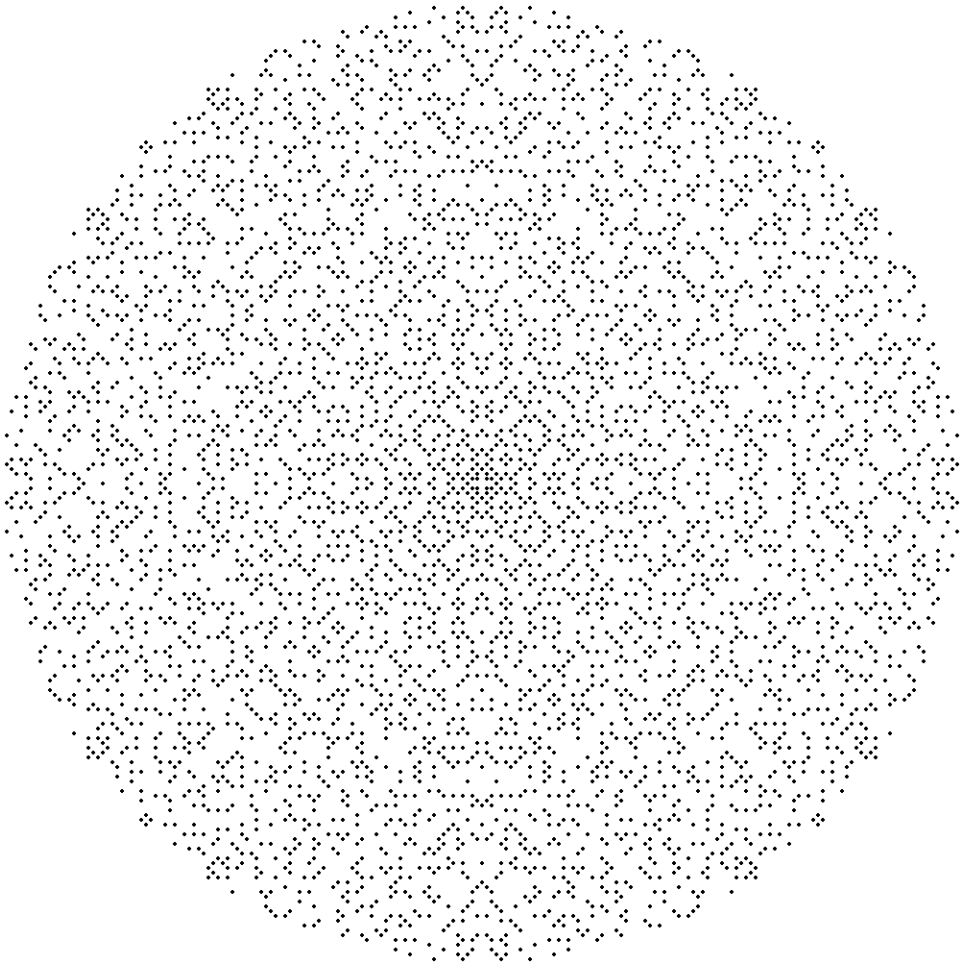
This gives the factorization

$$\boxed{35-85i = i^2 \cdot (1+i) \cdot (2+i) \cdot (2-i) \cdot (3+2i)^2}.$$

# A p p e n d i x

Complex primes with modulus less than 100 on the complex plane:



Proof that $N(z)$ is multiplicative:

$$N(wz) = N(w)N(z)$$
$$N((a+bi)(c+di)) = N(a+bi)N(c+di)$$
$$N(ac-bd+(ad+bc)i) = N(a+bi)N(c+di)$$
$$(ac-bd)^2+(ad+bc)^2 = (a^2+b^2)(c^2+d^2)$$
$$a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2 = a^2c^2+a^2d^2+b^2c^2+b^2d^2$$
$$a^2c^2+b^2d^2+a^2d^2+b^2c^2 = a^2c^2+a^2d^2+b^2c^2+b^2d^2$$

# TI-83/84 Program to Compute Gaussian (Complex) Prime Factors

```
1    Prompt Z
2    Z+0i→Z
3    6→L

4    √(abs(Z))→M
5    1+i→F
6    Lbl N
7        0→E
8        Z/F→W
9        While fPart(real(W))=0 and fPart(imag(W))=0
10           E+1→E
11           W→Z
12           Z/F→W
13           End

14       If E≠0: Then
15           Disp {F,E}
16           L-1→L: If L≤0: Pause
17           √(abs(Z))→M
18           End

19       If imag(F)>0: Then
20           conj(F)→F
21           Goto N
22           End

23       conj(F)+2i→F
24       If imag(F)<real(F) and abs(F)≤M
25           Goto N

26       real(F)+1→F
27       If fPart(F/2)=0
28           F+i→F
29       If abs(F)≤M
30           Goto N
```

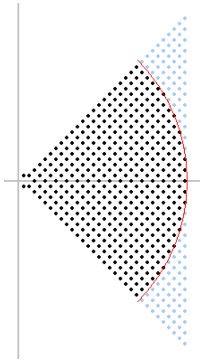
```
31   0→E
32   While real(Z)<0 or abs(real(Z))<abs(imag(Z))
33       Z/i→Z
34       E+1→E
35       End

36   If Z≠1+0i: Then
37       Disp {Z,1}
38       L-1→L: If L≤0: Pause
39       End

40   If E>0
41       Disp {i,E}
```

Notes:

Line 2 converts *Z* into a complex number if a real number was entered. This is required to prevent "Data Type" errors in comparisons. This is the same reason line 36 compares against 1+0*i*.

Lines 6 through 30 are the factor test loop. The factors tested are 1±*i*, 2±*i*, 3, 3±2*i*, 4±*i*, 4±3*i*, 5, 5±2*i*, 5±4*i*,… In particular, there is no need to test any Gaussian integer whose components are both even or both odd. (Just as 2 is the only even real prime, 1+*i* is the only "even" Gaussian prime.)

Throughout the factor test loop, *M* is the square root of the modulus of *Z*. No factor of *Z* can have a modulus greater than *M*. The test against *M* in line 24 eliminates about 21% of the trial divisions, as shown in the figure to the right..



When the factor test loop exits, *Z* is prime or a power of *i*. However, *Z* may not be in the form we want; its real part may be negative or its imaginary part may be greater than its real part. Lines 31-35 rotate *Z* until it is in the correct form, keeping track of the power of *i* needed as the final factor.