Exploring Abstract Algebra with Computer Software
PREP Workshop 2004
Section 16: Gaussian Integers

Recall the ring of Gaussian integers, $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$. This ring is an Euclidean domain. In this section we will investigate the irreducible elements of $\mathbf{Z}[i]$. The command for creating $\mathbf{Z}[i]$ is `GaussianIntegers`:

```
gap> R:=GaussianIntegers;
GaussianIntegers
```

The $\sqrt{-1}$ is denoted in GAP by $E(4)$ (since $\sqrt{-1}$ is the fourth root of one).

```
gap> i:=E(4);
E(4)
gap> i^2;
-1
```

We can now factor elements in $\mathbf{Z}[i]$ using the `Factors` command.

```
gap> Factors(R,4);
[ -1-E(4), 1+E(4), 1+E(4), 1+E(4) ]
gap> Factors(R,3+i);
[ 1-E(4), 1+2*E(4) ]
```

Thus we see the irreducible factors of 4 in $\mathbf{Z}[i]$ are $-1 - i$, $1 + i$, $1 + i$ and $1 + i$ and the irreducible factors of $3 + i$ are $1 - i$ and $1 + 2i$.

Careful: If you do not specify the ring, GAP will assume you want the factorization over the integers:

```
gap> Factors(4);
[ 2, 2 ]
```

Section 16, Project

16.1 Make a list of the prime numbers in $\mathbf{Z}$ that are less than 60. For these primes determine whether or not they are irreducible elements in $\mathbf{Z}[i]$.

16.2 For all the primes $p \in \mathbf{Z}$ less than 60 compute p mod 4.

16.3 Make a conjecture stating which $p \in \mathbf{Z}$ are irreducible elements in $\mathbf{Z}[i]$.

16.4 For the primes $p \in \mathbf{Z}$, $p \leq 60$, that are **not** irreducible in $\mathbf{Z}[i]$ find positive integers $a, b \in \mathbf{Z}$ such that $a^2 + b^2 = p$. Is $a + bi$ irreducible in $\mathbf{Z}[i]$? Is $a - bi$ irreducible in $\mathbf{Z}[i]$?

A proposition that is often proved in more advanced algebra courses states that every irreducible element in $\mathbf{Z}[i]$ is one of the following:
i) the elements you found in Exercise 3 (assuming you did the problem correctly)
ii) the elements you found in Exercise 4 (assuming you did the problem correctly).