

## Euclidean Domains

[This is the handout for the class period that was spent in the computer classroom, demonstrating the GAP commands for quotients, remainders, norms, factorization into primes, and greatest common divisors. It concludes with a set of exercises.]

### A quickie refresher:

[Here are instructions about how to open GAP in the computer classroom.]

The computer starts with the "gap>" prompt.

You will probably want to save your work in a file. To do that, make up a file name and type

```
LogTo("filename");
```

Remember that GAP is case-sensitive, and that you must end every GAP command with a semicolon.

**GAP recognizes several rings as Euclidean domains and has built-in “norms” for them. For these rings it will perform computations involving quotients, remainders, greatest common divisors, and factorization.**

### **I. The integers**

These computations are simplest in the case of the integers. If you want to find the quotient and remainder when one integer is divided into another, use the command “QuotientRemainder.” For example, if you type

```
QuotientRemainder(75,6);
```

GAP responds with

```
[ 12, 3 ]
```

which tells you that  $75=12(6)+3$ . If you want just the quotient or just the remainder, you can use the commands “EuclideanQuotient” or “EuclideanRemainder,” respectively. If you type

```
EuclideanQuotient(75,6);
```

GAP responds with

12

If you type

```
EuclideanRemainder(75,6);
```

GAP responds with

3

If you want to find the greatest common divisor of 75 and 6, type

```
Gcd(75,6);  
to which GAP responds with
```

3

To express the greatest common divisor as an integer-linear combination of 75 and 6, type

```
Gcdex(75,6);
```

GAP replies

```
rec( gcd := 3, coeff1 := 1, coeff2 := -12, coeff3 := -2, coeff4 := 25 )
```

The first two “coefficients” tell you that  $3=1(75)-12(6)$ .

If you want to factor the integer 123456789 as a product of primes, type

```
Factors(123456789);
```

GAP responds with

```
[ 3, 3, 3607, 3803 ]
```

which tells you that  $123456789=3^2(3607)(3803)$ .

GAP will also find the “norm” of an integer -- which is, of course, its absolute value. The relevant command is “EuclideanDegree.” If you type

```
“EuclideanDegree(-13);
```

GAP responds with

13.

Incidentally, you can also ask GAP whether the integers really are a Euclidean domain. If you type

```
IsEuclideanRing(Integers);
```

GAP replies

true

## II. The Gaussian Integers

The Gaussian integers -- alias  $\mathbf{Z}[i]$  -- are built into GAP, under the name "GaussianIntegers." To save typing, let's give them a shorter name:

```
r:=GaussianIntegers;
```

Just to be sure, let's ask whether this is a Euclidean domain by typing

```
IsEuclideanRing(r);  
to which GAP replies
```

true

GAP's notation for the imaginary number "i" is  $E(4)$  [since  $i$  is the fourth root of the identity]. To save typing, let's give it a name:

```
i:=E(4);
```

The same commands that worked for the integers apply to the Gaussian integers. If you want to find the quotient and remainder when  $15-82i$  is divided by  $2+3i$ , type

```
QuotientRemainder(15-82*i, 2+3*i);
```

GAP responds with

```
[ -17-16*E(4), 1+E(4) ]
```

which tells you that  $15-82i=(-17-16i)(2+3i)+(1+i)$ . To find a greatest common divisor of these two Gaussian integers, type

```
Gcd(15-82*i, 2+3*i);
```

to which GAP responds with

1

You can confirm that 1 is a greatest common divisor of  $15-82i$  and  $2+3i$  by using GAP to perform the Euclidean algorithm, step by step.

[Do it! Do you get 1 as the last non-zero remainder?]

*Some things to bear in mind:* An ordinary integer like 3 has two “norms” -- its norm as a regular integer, and its norm as an element of the Gaussian integers. To compute the latter, use the command

```
EuclideanDegree(r,3);
```

GAP responds with

```
9
```

Similarly, an ordinary integer can be factored in  $\mathbf{Z}$  or in  $\mathbf{Z}[i]$ . If you want to factor 6 in  $\mathbf{Z}[i]$ , type

```
Factors(r,6);
```

GAP replies with

```
[ 1-E(4), 1+E(4), 3 ]
```

which tells you that, in  $\mathbf{Z}[i]$ ,  $6=3(1-i)(1+i)$ . You should also note that the command “Gcdex” does not work for  $\mathbf{Z}[i]$ .

[Question: Can GAP still help you express a greatest common divisor of  $a$  and  $b$  in  $\mathbf{Z}[i]$  as a linear combination of  $a$  and  $b$ ?]

### III. Polynomial rings

To create the ring  $\mathbf{Q}[x]$ , first give a name to the rationals:

```
q:=Rationals
```

and then use the command

```
p:=PolynomialRing(q,1);
```

GAP replies with

```
<algebra-with-one over Rationals, with 1 generators>
```

which tells you that GAP has created a ring of polynomials in one unknown with coefficients in  $\mathbf{Q}$  and has called that ring “p.” Just to be sure, we can ask whether p is Euclidean by typing

```
IsEuclideanRing(p);
```

To define  $f(x)$  as the polynomial  $x^3-1$  in  $\mathbf{Q}[x]$ , type

```
f:=UnivariatePolynomial(q, [-1,0,0,1]);
```

GAP responds with

```
-1+x_1^3
```

[Note that GAP “thinks” of polynomials as starting with the lowest power of  $x$ , and you must enter zeros for any missing coefficients.]

To find a greatest common divisor of  $f(x)$  and  $g(x)=x^2-1$ , first type

```
g:=UnivariatePolynomial(q, [-1,0,1]);
```

and then

```
Gcd(f,g);
```

GAP responds with

```
-1+x_1
```

which tells you that  $x-1$  is a greatest common divisor of  $f$  and  $g$ .

The other commands work as they did for  $\mathbf{Z}$  and  $\mathbf{Z}[i]$ , with the exception of “Gcdex” and “EuclideanDegree,” which don’t work for polynomial rings.

[Question: Why doesn’t it matter that “EuclideanDegree” doesn’t work on polynomial rings?]

*Other fields*: If you want the coefficients to be in a different field, like  $\mathbf{Z}_7$ , just define that field as follows:

```
z7:=Integers mod 7;
```

GAP “thinks” of  $z7$  as being generated, multiplicatively, by an element that it calls “ $Z(7)$ .” It takes some effort to figure out which generator  $Z(7)$  is. First save typing by defining

```
a:=Z(7);
```

The possible generators of  $z7$  are 2, 3, 4, 5, and 6. To find out which one  $Z(7)$  is, do some computations. If you type

```
a+a;
```

GAP responds with

$Z(7)^3$

This tells you that, whatever  $a$  is,  $2a=a^3$ . Since  $2(2)$  does not equal  $2^3 \pmod{7}$ , this tells you that  $a$  is not 2. By the process of elimination, you find that  $a$  can equal 3 or 4. GAP also tells you that  $3a$  equals  $a^2$ . This allows you to conclude that  $a=3$ . It follows that, in  $Z_7$ ,  $1=a^6$ ,  $2=a^2$ ,  $3=a$ ,  $4=a^4$ ,  $5=a^5$ , and  $6=a^3$ . The polynomial  $f(x)=6x^4-5$  in  $Z_7[x]$  can then be written in GAP-speak as

`f:=UnivariatePolynomial(z7, [-a^5, 0*a, 0*a, 0*a, a^3]);`

### Exercises

1. Factor your social security number into primes.
2. Find the greatest common divisor of your social security number and 2001, and express the g.c.d. as an integer-linear combination of your SSN and 2001.
3. In #1 in Sec. 8.1, you found the following greatest common divisors by hand and expressed them as linear combinations of the two given numbers. Check your work by carrying out the steps with GAP, and check the final answers:  
20 and 13  
69 and 372  
11391 and 5673  
507885 and 60808  
91442056588823 and 779086434385541
4. In #7 in Sec. 8.1, you found the following greatest common divisors in  $Z[i]$ . Check your work with GAP.  
85 and  $1+13i$   
 $47-13i$ ,  $53+56i$
5. Use GAP to find the irreducible factors of  $f(x)=2x^3-4x^2+5x-3$  in  $Q[x]$  and in  $Z_7[x]$ .