Assignment 1 Question 2

Part (a) Implementing the binary GCD algorithm.

```
> restart;
  BINGCD := proc(A::posint,B::posint)
  local a,b,i,j,g,t;
     a := A;
     b := B;
     for i from 0 while irem(a,2)=0 do a := iquo(a,2) od;
     for j from 0 while irem(b,2)=0 do b := iquo(b,2) od;
     printf("a=%d=2^%d*%d, b=%d=2^%d*%d\n",A,i,a,B,j,b);
     g := 2^min(i,j);
     while true do # a and b are both odd
        if a<b then (a,b) := (b,a); fi;
        printf("a=%d, b=%d\n",a,b);
        a := a-b;
        if a=0 then RETURN( b*g ) fi;
        while irem(a,2)=0 do a := iquo(a,2) od;
     od;
  end:
```

```
> BINGCD(16*3*101,8*3*203);

a=4848=2^4*303, b=4872=2^3*609
a=609, b=303
a=303, b=153
a=153, b=75
a=75, b=39
a=39, b=9
a=15, b=9
a=9, b=3
a=3, b=3
```

$$24$$

Part (b) Timing Maple's igcd command. (This is in Maple 9.5).

```
> a := rand(10^20000)():
> b := rand(10^20000)():
> length(a), length(b);
```

$$20000, 20000$$

```
> time(igcd(a,b));
```

$$0.006$$

This time is too small on my machine. Let's start with 50,000 digits integers.

```
> a := rand(10^100000)():
> b := rand(10^100000)():
> length(a), length(b);
```

$$100000, 100000$$

```
> st := time(): igcd(a,b); T1 := time()-st;
```

$$5$$

$$T1 := 0.071$$

```
> a := a^2:
  b := b^2:
  length(a),length(b);
```

$$200000, 200000$$

```
> st := time(): igcd(a,b); T2 := time()-st;
```

$$25$$

$$T2 := 0.268$$

```
> T2/T1;
```

$$3.774647887$$

```
> a := a^2:
  b := b^2:
  length(a),length(b);
```

$$400000, 400000$$

```
> st := time(): igcd(a,b); T3 := time()-st;
```

$$625$$

$$T3 := 1.102$$

```
> T3/T2;
```

$$4.111940298$$

That's close to a factor of 4 but it should approach 4 from below. Let's do another step

```
> a := a^2:
  b := b^2:
  length(a),length(b);
```

$$800000, 799999$$

```
> st := time(): igcd(a,b); T4 := time()-st;
```

$$390625$$

$$T4 := 4.336$$

```
> T4/T3;
```

$$3.934664247$$

Well, this looks like it's approaching 4.0 which would suggest the algorithm is O(n^2). Let's try one more.

```
> a := a^2:
  b := b^2:
  length(a),length(b);
```

$$1599999, 1599998$$

```
> st := time(): igcd(a,b); T5 := time()-st;
```

$$152587890625$$

$$T5 := 17.247$$

```
> T5/T4;
```

$$3.977629151$$

Obviously we can keep going and wait ...