Lecture 1: GCD and Euclidean Algorithm

Def: Given integers *a*,*b* the greatest common divisor or gcd(a,b) is the largest integer d such that $d \mid a$ **and** $d \mid b$

Ex.
(1) gcd(180,72) = 36 (180 = 5*36, 72 = 2*36)

One way of computing gcd(but very slow) is to look at the divisors of the numbers. Note that divisors() is a Sage command

divisors(180)
1,2,3,45,6,9,10,12,15,18,20,30,36,45,60,90,180

divisors(72)
1,2,3,4,6,8,9,12,18,24,36,72

The largest number appearing in both lists is 36

(2) Using the Sage command gcd
gcd(31571776,443085702) = 1346

Note: 31571776 = 1346*23456, 443085702 = 1346*329187

Def. Given positive integers *a*,*b*. There exists integers *q*,*r* such that

$$a = qr + b \text{ where } 0 \le r < b$$

Euclidean algorithm

Let *a*,*b* be positive integers with $b \le a$. The following algorithm computes gcd(a,b). Compute the sequence $r_0, r_1, r_2, \ldots$ as follows:

Step 1: let $r_0 = a, r_1 = b$

Step 2: Let $i = 1$

Step 3: Compute r_{i+1} by dividing r_{i-1} by r_i as follows

$$r_{i-1} = q * r_i + r_{i+1} \text{ where } 0 \le r_{i+1} < r_i$$

Step 4: If $r_{i+1} = 0$

then $\gcd(a,b) = r_i$

else let $i = i + 1$ and repeat Step 3

The running time of the algorithm is O(log b)

Ex:

(1) gcd(101,97)

101 = 1*97 +4 Now divide 97 by 4
97 = 24*4 + 1 Now divide 4 by 1
4 = 4*1 + 0 Done, **gcd(101,97) = 1** (the remainder at the previous step)

(2) gcd(42823,6409)

42823 = 6*6409 + 4369 Now divide 6409 by 4369
6409 = 1*4369 + 2040 Now divide 4369 by 2040
4369 = 2*2040 + 289 Now divide 2040 by 289
2040 = 7*289 + 17 Now divide 289 by 17
289 = 17*17 + 0 Done **gcd(42823,6409) = 17** (the remainder at the previous stage)

Extended Euclidean Algorithm
Given positive integers *a*,*b*. There exists integers *u*,*v* such that

$$\boldsymbol{ua + vb = \gcd(a,b)}$$

Start with the next to last step of the Euclidean algorithm. Solve for the gcd(a,b). Then keep substituting from the previous equations until reaching *a*,*b*.

Ex:
(1) 101,97
101 = 1*97 +4
97 = 24*4 + 1
4 = 4*1 + 0

1 = 97 – 24*4 = 97 – 24*(101 – 97) = 25*97 – 24*101 (so *u* = 25, *v* = -24)

(2) 42823,6409
42823 = 6*6409 + 4369
6409 = 1*4369 + 2040
4369 = 2*2040 + 289
2040 = 7*289 + 17
289 = 17*17 + 0

17 = 2040 – 7*289 = 2040 – 7*(4369-2*2040) = 15*2040 – 7*4369 = 15*(6409-4369) -7*4369
= 15*6409 – 22*4369 = 15*6409 – 22*(42823-6*6409) = 147*6409 – 22*42823
(so *u* = 147, *v* = -22)