Week 2 Math

Lecture 3 The rational numbers

A normal form and the Euclidean algorithm

```
x <- a
y <- b
while ( y != 0 ) {
    r <- x mod y
    x <- y
    y <- r }
return x
```

The extended Euclidean algorithm and finite fields

lcf(a,b) = u×a+v×b

```
x <- a
y <- b
u_x <- 1; v_x <- 0
u_y <- 0; v_y <- 1
while ( y != 0 ) {
    r <- x mod y; k <- x div y
    u <- u_x; v <- v_x
    u_x <- u_y; v_x <- v_y
    u_y <- u - k*u_y; v_y <- v - k*v_y
    x <- y
    y <- r }
return x, u_x, v_x
```