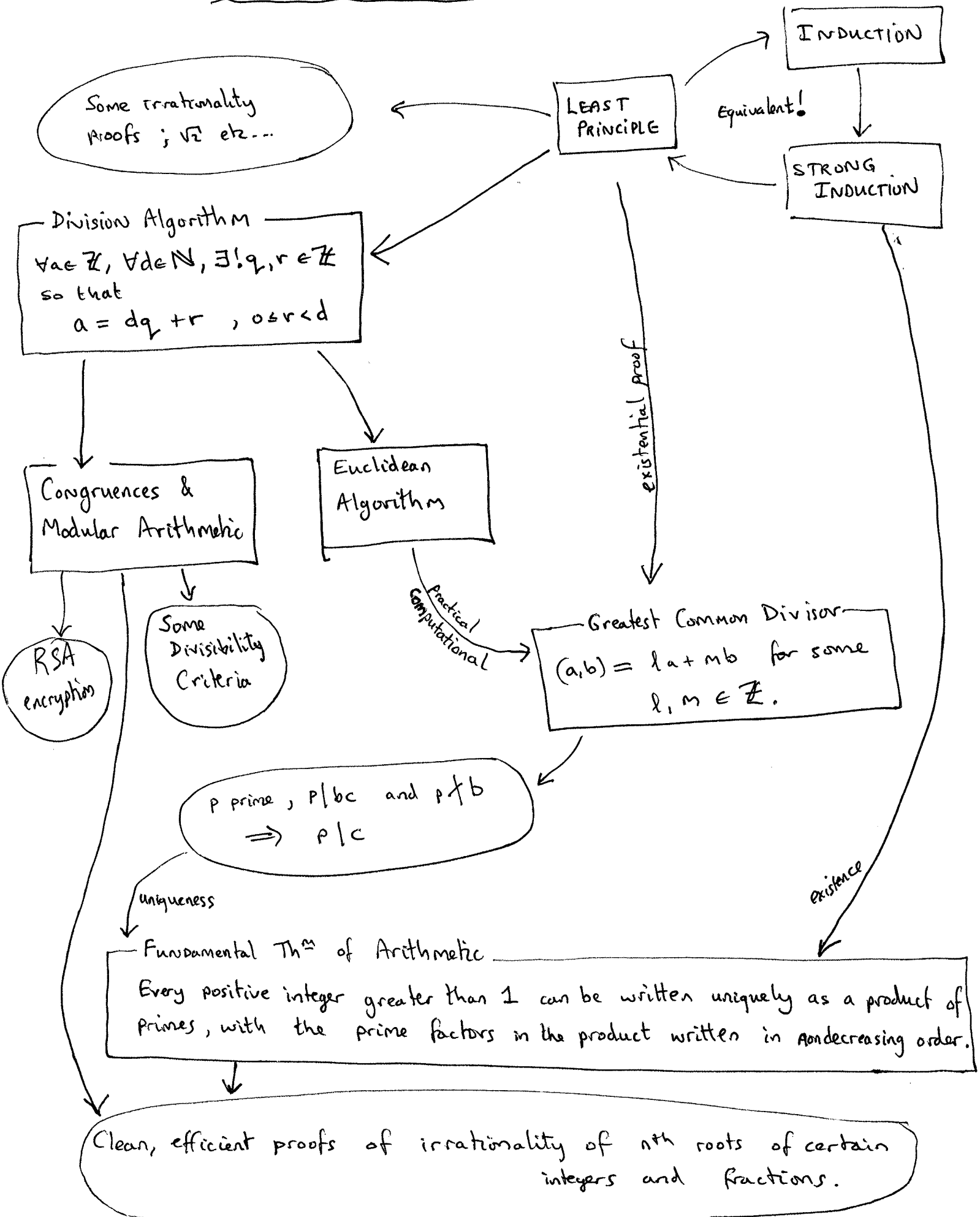


# Flowchart of Ideas



Some irrationality proofs ;  $\sqrt{2}$  etc...

Division Algorithm  
 $\forall a \in \mathbb{Z}, \forall d \in \mathbb{N}, \exists! q, r \in \mathbb{Z}$   
 so that  
 $a = dq + r, 0 \leq r < d$

Congruences & Modular Arithmetic

RSA encryption

Some Divisibility Criteria

Euclidean Algorithm

Greatest Common Divisor  
 $(a,b) = la + mb$  for some  
 $l, m \in \mathbb{Z}$ .

$p$  prime,  $p|bc$  and  $p \nmid b$   
 $\Rightarrow p|c$

Fundamental Th<sup>m</sup> of Arithmetic  
 Every positive integer greater than 1 can be written uniquely as a product of primes, with the prime factors in the product written in nondecreasing order.

Clean, efficient proofs of irrationality of  $n$ th roots of certain integers and fractions.