Mathematics of Computer Science. - M.I.T. opencourseware

Abstract:

number theory is basically integer count system. there are lot of way to create the combination of integer or breakdown the big integer to factors. which can be used in cryptography-system

For the English:

transition, jug, any of the above, desired, obtain, at most, bounds, invariant, quotient

Lec 4. NUMBER THEORY I:

m|a means 'm divides a' / m|0 => for all integer

gallon jug problem. 3 jug and 5 jug

THM = m|a and m|b then m|any result

transition = emptying , filling , pouring

invariant = P(n) If (x, y) is the state after n-transitions the m|x, m|y

base case = (0, 0), m|0 => P(0) true

inductive step = suppose that (x, y) state after n -trans

> P(n) => m|+x and m|y // after another transition each of jug are filled with [0, a, b, x, y, x+y-a, x+y-b] => m|0, m|a, m|b ...
>
> m divides any of the above - the two numbers are prime, it can make any other number

GCD = greatest common divisor

there exist an unique q(quotient) and r(remainder) such that b = q*a + r // 0=< r <

lemma - gcd(a, b) = gcd(rem(b, a), a)

pf [m|a or m|b] => [m|b-qa = rem(b,a) or m|a]

if rem(b, a) != 0, [m|b-qa or m|a] => [m|a or m|b]

if rem(b, a) = 0 // b = qa => m|a => m|b

thm - any linear combination(V*S + V'*S' = V.2) = L s*a + t*b, of a and b // a=<b

> with 0=< L =< b can be reached

ex) y = (-2)*3 + (2)*5 = 4

> S should be positive
>
> \+ 5*3 - 3*5 = 0

= 3*3 - 1*5 = 4 // then now S is positive

pf : notice L = sa + tb = (s+mb)a + (t-ma)b
to obtain L gal, repeat S times
- fill the a jug * S times
- pour into b jug // when it becomes full, empty it out * u times
- continue this process until a jug is empty

Algorithm

r = S'*a − u*b // L = S'*a + t'*b
r = S'*a + t'*b − t'*b − u*b = L - (t'+u)b

0 < L < b // 0=< r =< b

-1 =< -(t' + u)b =< 1

if t' + u != 0 => [r<0 or r>b]
if t' + u = 0 => r = L