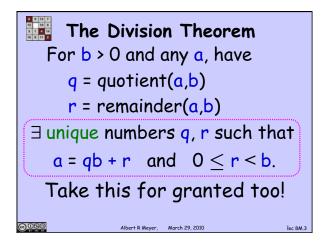
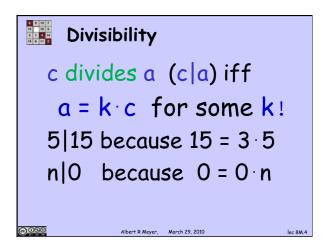
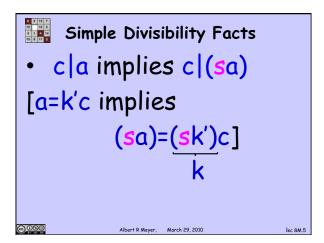


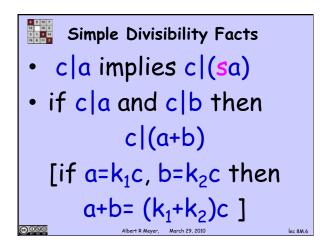
Arithmetic Assumptions assume usual rules for $+, \cdot, -:$ a (b+c) = ab + ac, ab = ba,(ab)c = a (bc), a - a = 0,a + 0 = a, a+1 > a, ...

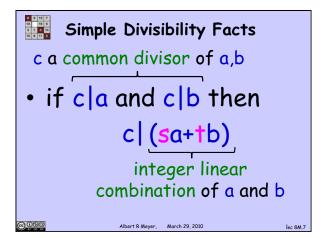
Albert R Meyer, March 29, 2010

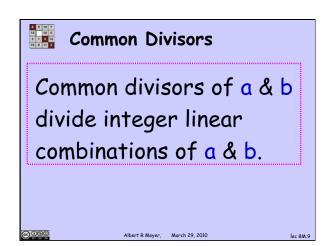




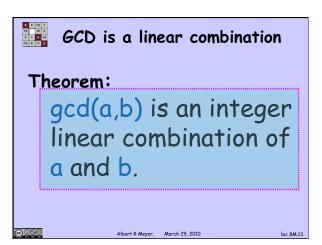




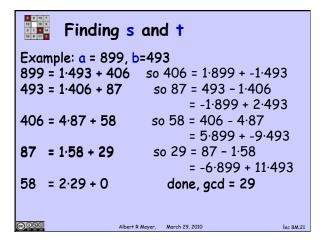


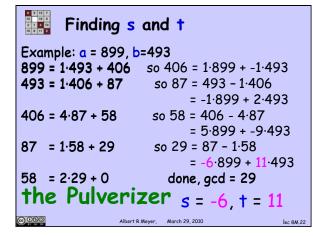


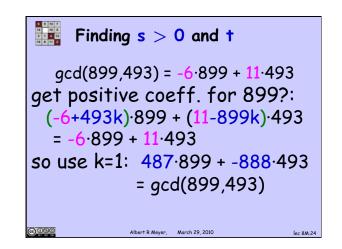
GCD
gcd(a,b) ::= the greatest
common divisor of a and b
lemma: p prime implies
gcd(p,a) = 1 or p
proof: The only divisors
of p are ±1 & ±p.

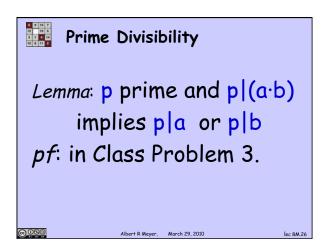


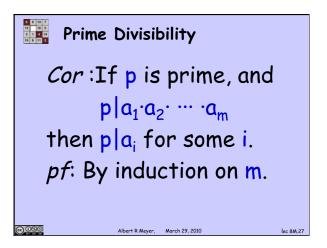
gcd(a,b) = sa+tb
Proof: Show how to find
coefficients s,t.
Method: apply Euclidean
algorithm, finding
coefficients as you go.

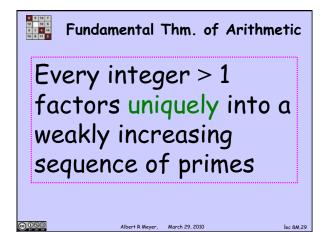


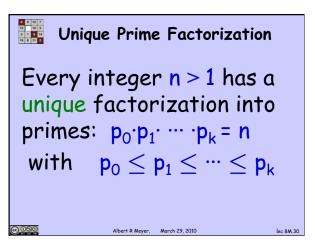


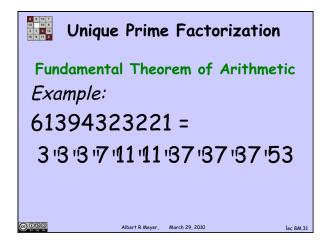


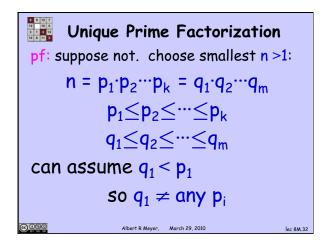


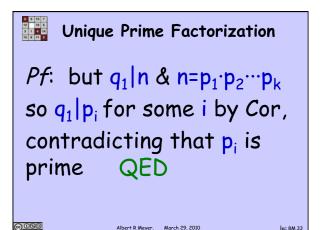


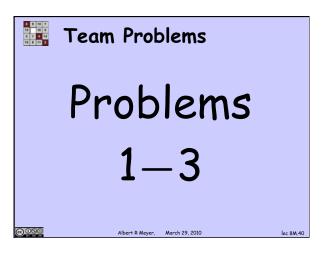












6.042J / 18.062J Mathematics for Computer Science Spring 2010

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.