

@ **①** @

March 6, 2015

pulverizer.1



GCD is a linear combination

Theorem:

qcd(a,b) is an integer linear combination of a and b.

$$gcd(a,b) = sa+tb$$

 \odot \odot

Albert R Mever

March 6, 2015

pulverizer.2



GCD is a linear combination

Corollary:

The multiples of gcd(a,b) are exactly the linear combinations of a and b.



Albert R Meyer



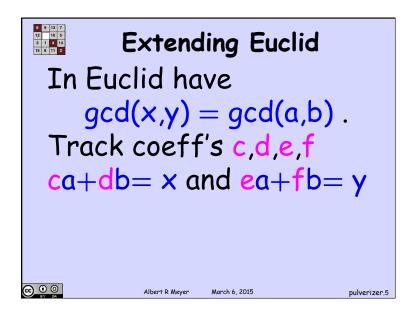
gcd(a,b) = sa+tb

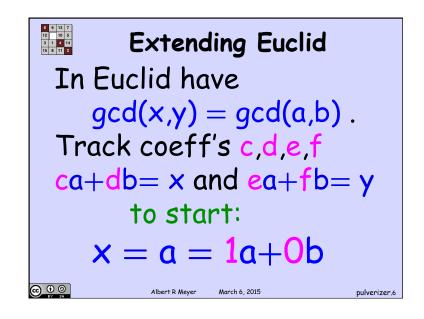
Proof: Show how to find coefficients s,t.

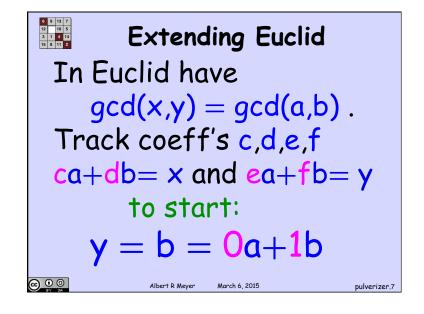
Method: apply Euclidean algorithm, finding coefficients as you go.

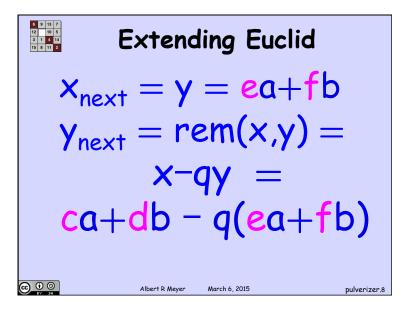


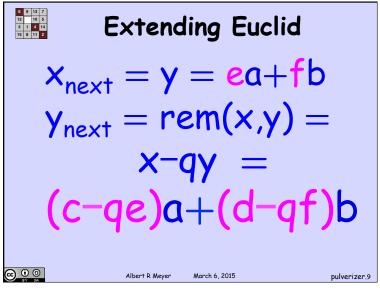
Albert R Meyer

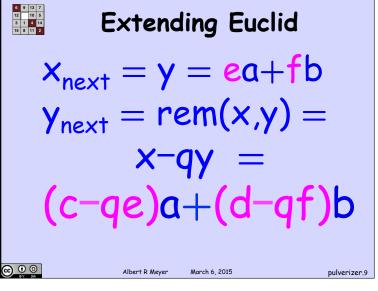


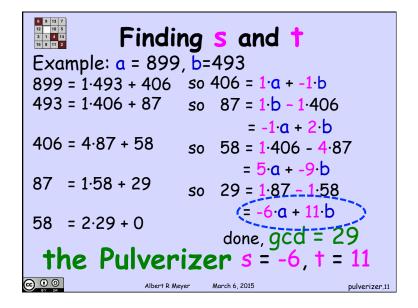


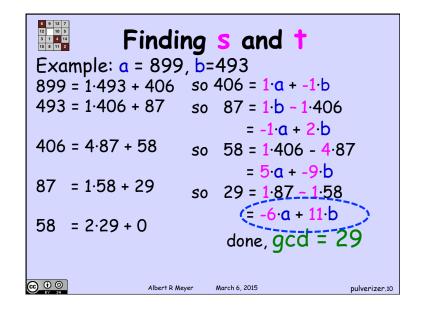


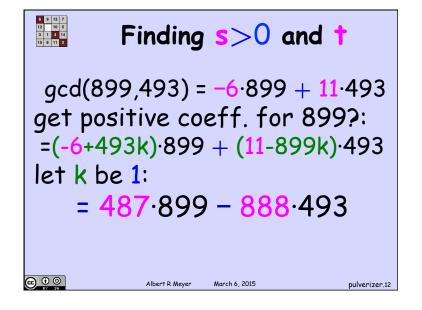


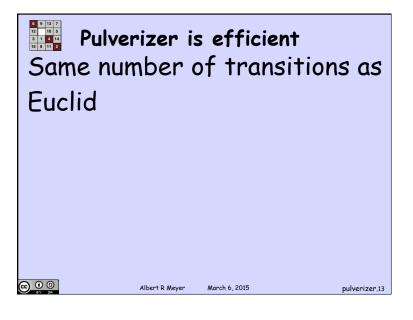












Pulverizer is efficient

Same number of transitions as

Euclid, a few more adds/mults

per transition.

So halts after at most

10log₂ b operations