Bezout's Theorem - Extended Euclidean Algorithm iterative

Arabic animated intuition

Extended Euclidean algorithm iterative

$ax+by=gcd(a,b)$ (1)

$ax\_prev+by\_prev=r\_prev$ (2)

$ax+by=r\_cur$ (3)

gcd(r_prev,r_cur) r_prev from the first gcd call

a=r_prev, b=r_cur

$r\_new=r\_prev-Q*r\_cur$ (4)

r_new=(ax_prev+ay_prev)-q(ax+ay)

$a(y-qy\_prev)+b(x-qx\_prev)=r\_new$ (5)

from the Euclidean algorithm we know that

gcd(a,b)= gcd(b,a%b)

gcd(a,b)=gcd(b,r)

r is the remainder (R)

r=a-b*Q

so we are continually trading in
the gcd of a pair for
the gcd of a smaller pair.
At the last step, we have gcd

gcd(a,b) =gcd(b,a%b)

gcd(r_prev,r_cur)=gcd(r_cur,0)=r_cur

Extended Euclidean algorithm iterative

$ax+by=gcd(a,b)$ (1)

$ax\_prev+by\_prev=r\_prev$ (2)

$ax+by=r\_cur$ (3)

gcd(r_prev,r_cur) r_prev from the first gcd call

a=r_prev, b=r_cur

$r\_new=r\_prev-Q*r\_cur$ (4)

r_new=(ax_prev+ay_prev)-q(ax+ay)

$a(y-qy\_prev)+b(x-qx\_prev)=r\_new$ (5)

gcd(a,b)=gcd(b,a%b)

gcd(a,b)=gcd(b,r)

r is the remainder

r=a-b*Q (R)

so we are continually trading in
the gcd of a pair for
the gcd of a smaller pair.
At the last step, we have gcd

gcd(r_prev,r_cur)=gcd(r_cur,0)=r_cur

a(1)+b(0)=a x_prev=1 y_prev=0

a(0)+b(1)=b x=0,y=1

X_new=x-qx_prev

Y_new=y-qy_prev