Note Title 1/25/2012

$E_K[R]$, $E_K[E_K(R)]$, $E_K[E_K[E_K(R)]]$, ...

$C_1 = S_1 \otimes P_1$

$C_2 = S_1 \otimes P_2$

$C_1 \otimes C_2 = P_1 \otimes P_2$

$15 = 3 \times 5$

a	412	260	152	108	44	20	4
b	260	152	108	44	20	4	0

GCD(412, 260) = GCD(260, 412 mod 260)
↳ 152

= GCD(152, 108) = GCD(108, 152 mod 108)
↳ 44

= GCD(44, 108 mod 44)