1) C=A+B, A делится на k и B делится на k => докажите, что C делится на k

2) В ОБЩЕЙ СХЕМЕ всех шагов алгоритма Евклида докажите, что r(n+2) является ОД (общим делителем чисел A,B)

Указание1: Двигаться снизу вверх по ОБЩЕЙ СХЕМЕ

Указание2:

а) Доказать, что r[n+1] делится на r[n+2]

б) Доказать, что r[n] делится на r[n+2]

в) Доказать, что r[n-1] делится на r[n+2]

г) Доказать, что B делится на r(n+2)

д) Доказать, что A делится на r(n+2)

3) Докажите, что r(n+2) - НАИБОЛЬШИЙ из делителей чисел A,B

Указание1: От противного

Указание2: Двигаться сверху вниз по ОБЩЕЙ СХЕМЕ

Указание3: Доказать, что r(n+2) делится на делитель больший, чем r(n+2)

если а делится на к ,значит а это хк а б ук значит ук+хк делится на к потомучто с=(х+у)к

2)

$r[n+1]=r[n+2]*q[n+3]$

$r[n]=r[n+1]*q[n+2]+r[n+2]=r[n+2]*q[n+3]*q[n+2]+r[n+2]$

$r[n-1]=r[n]*q[n+1]+r[n+1]$

надо доказать не что среди всех r и q все будут меньшими делителями, а что среди всех на свете чисел не найдется большего делителя, чем r(n+2) для чисел A,B

пусть это не так, т.е. r[n+2] не наибольший, значит есть кто-то больше по имени K, чем r[n+2] и A делится на K и B делится на K

$A=B*q1+r1$ A делится на K и B делится на K $A=xk$ $B=yk$

$A-B*q1=r1$

$xk - yk*q1=r1=k(x-yq1)$

$B=r1*q2+r2$

$B-r1*q2=r2$

$r1=r2*q3+r3$

$r1-r2*q3=r3$

r[n+2] делится на K - противоречие

ОБЩАЯ СХЕМА

A,B, A>B

*делимое=делитель*частное + остаток*

$A=B*q1+r1$

$B=r1*q2+r2$

$r1=r2*q3+r3$

$\dots$

$r[n-1]=r[n]*q[n+1]+r[n+1]$

$r[n]=r[n+1]*q[n+2]+r[n+2]$

$r[n+1]=r[n+2]*q[n+3] + 0$