1) показать из алгоритма Евклида, что если НОД(a,b)=k, то найдутся такие ЦЕЛЫЕ числа x,y , что ax+by=k

Указание1:Двигаться снизу вверх по ОБЩЕЙ СХЕМЕ

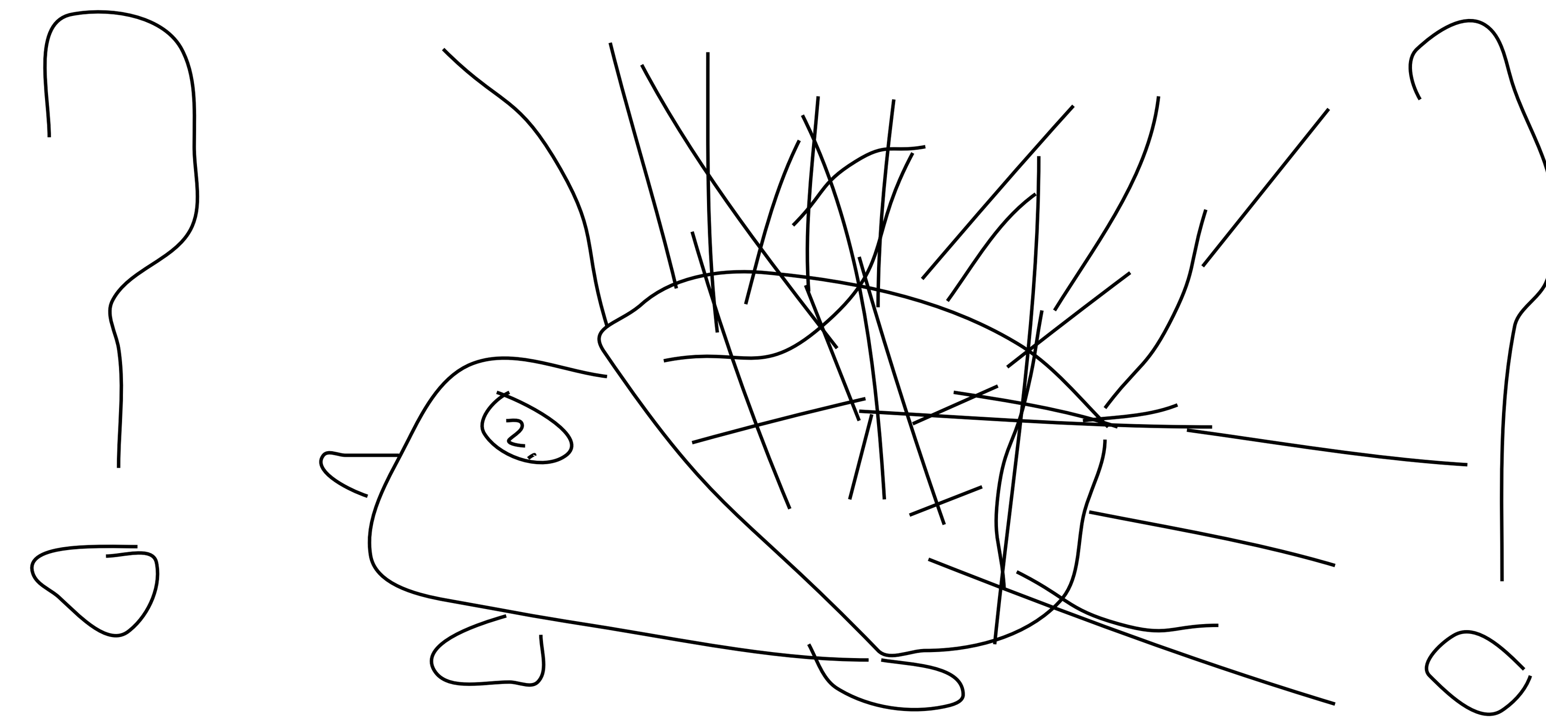
Указание2:

а) r(n+2) выр через rn, r(n+1)

б) r(n+2) выр через r(n-1), rn

в) r(n+2) выр через r(n-2), r(n-1)

г) r(n+2) выр через A, B



2) если произведение ab двух целых чисел a и b делится на простое число p, то хотя бы один из множетелей делится на p

Указание1: От противного

a=px+y

b=pf+t

они оба не делятся на p

Указание2: НОД(a,p)=1 => ax+py=1

Указание3: Домножить равенство ax+py=1 на b

axb+pyb=b=> b делится на p => противоречие

$$r(n)= u^* r(n+2)$$

$$r(n+2)=r(n)-r(n+1)^*q(n+2)=r(n)^*T + r(n+1)^*Q$$

$$r(n+2)=r(n)-[r(n-1)-r(n)^*q(n+1)]^*q(n+2)=$$

$$=r(n)-r(n-1)q(n+2)+r(n)q(n+1)q(n+2)=$$

$$=r(n)[1-q(n+1)q(n+2)]-r(n-1)q(n+2)=$$

$$=r(n)^*U + r(n-1)W$$

$$=A^*x + B^*y$$

$$r(n+1)=r(n-1)-r(n)^*q(n+1)$$

НОД(15,5)=5

15x+5y=5

x=0 y=1

12345*x+6789*y=НОД

12345*-903+6789*1642=3

ОБЩАЯ СХЕМА

A,B, A>B

*делимое=делитель*частное + остаток*

*A=B*q1+r1*

*B=r1*q2+r2*

*r1=r2*q3+r3*

…

*r(n-2)=r(n-1)*q(n)+r(n)*

*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*