20 August 2023 11:03

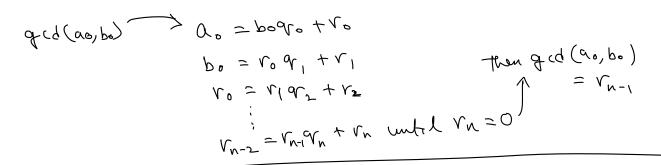
$$\frac{g_{-}}{P_{2}(x)} = \frac{1}{2} - \frac{3x^{2} + x + 1}{2}$$

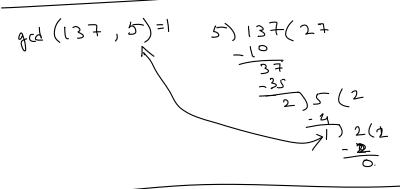
$$\frac{g_{-}}{P_{2}(x)} = \frac{1}{2} - \frac{1}{2} -$$

Q: If P & prime then show that
$$q(d(a,p) \in \{1,p\})$$
 $a(x \leq b)$
Aw: $-(a \times 2! - p) = q(a,p) = 1$

$$a(x \leq b)$$

(ax L. pla = gcd (a,p)=1 $x \in \{a,b\}$ $\frac{\text{Cave 3'-}}{\text{alp}} \Rightarrow \text{a=lonp} \Rightarrow \text{gcd(a,p)} \in \{l,p\}$ x=a on x=b Eucled's Division Algorithm: Think of gcd in terms of Common prime factors $m = P^2 \Upsilon$ $qcd(m,n) = P \Upsilon$ N = Par2r $m_{1} = P^{2} q + P q^{2} r = P q (P + q r)$ In general, the part we can take common outside of m+n & gcd(m,n) g:-qcd(a+b,b)=qcd(a,b) -> True on felix? $g' - gcd(a+3b,b) = gcd(a,b) \rightarrow True or false?$ Speneralizing!-Let a, b be integers. We can write a = bq + r for integers q, r and 0 < r < b. Then we can say that, gcd(a, b) = gcd(r, b)Proof: As in notes Number Theory 1. dcg(orp) = dcg(pd+1,p) = dcg(pd+1-pd,p) = dcg(rp) This process is called Euclid's Division Algorithm (Iterested until r=0) $a_{(d)}(210, 50) \rightarrow 210 = 50 \times 4 + 10$ $a_{(d)}(210, 50) \rightarrow 210 = 50 \times 4 + 10$ $a_{(d)}(20, 10) \rightarrow 50 = 10 \times 5 + 0$ $a_{(d)}(20, 10) \rightarrow 20 = 10$ $a_{(d)}(20, 10) \rightarrow 20 = 10$





0'-Prove that Euclid's, Algorithm terminates in finite step for finite a, b = 7.

Aus! - O& r & b for a = boy + r

This means r & decreasing in each step by at least 1.

This means as a, b are finite so r will be O in finite step

That a when i algorithm stops.

g'-qcd(-120,10) = qcd(0,10) = 10 g'-qcd(-120,10) = qcd(6,7) = qcd(1,6) = qcd(0,1) = 1g'-qcd(-120,7) = qcd(6,7) = qcd(1,6) = qcd(0,1) = 1

0,- dcq(-150)-+)= (4cq(150)+)=1

H.W:- Q:- Show that $gcd(4n+3,2n) \in \{1,3\}$ B:- Let $a,b \in \{2\}$. Then we can write a=bqr+r, $0 \le r \le b$ $qr,r \in \{2\}$. Then is lcm(a,b) = lcm(r,b)-True or false?

I for your solution ar 1/12/c+7,6/c+2) Easy Selution:

In your solution

qcd(12k+7,6k+2)

= qcd(6k+5,6k+2)

=qcd(3,6k+2) & {1,3}

Easy Solution: -

gcd (4n+3,2n) = gcd (3,2n) € [1,3]