//

MAT315 HOMEWORK #1 Rui Qiu #999292509

1. Solution

Then answer is no.

Suppose there are infinitely many so that say $p, p+2, p+4$ is one of these prime triplets.

Three possibilities:

$$p \equiv 0 \bmod 3 \quad \text{or} \quad 1 \bmod 3 \quad \text{or} \quad 2 \bmod 3$$

since p is prime, $p \equiv 0 \bmod 3$ is not possible

if $p \equiv 1 \bmod 3$ then $p+2 \equiv 0 \bmod 3$, not a prime!

if $p \equiv 2 \bmod 3$ then $p+4 \equiv 0 \bmod 3$, not a prime!

Hence, either way, there would be at least a non-prime number in the triplets.

2. Solutions:

(a). Suppose linear line $y=kx+b$ passes $(1,1)$

i.e. $y=kx+(1-k)$

plug it in $x^2+y^2=2$

$$x^2+(kx+(1-k))^2=2$$

$$x=\frac{-2k(1-k)\pm\sqrt{4k^2(1-k)-4(1+k^2)((1-k)^2-2)}}{2(1+k^2)}$$

$$=\frac{k^2-k\pm(k+1)}{1+k^2}$$

$$=1 \quad \text{or} \quad \frac{k^2-2k-1}{1+k^2}$$ where k is the slope

note: when $k=-1$, $x=1$

$$\text{Hence } y=kx-k+1=\frac{-k^2-2k+1}{1+k^2}$$

So all rational points satisfying our conditions are

$$\left(\frac{k^2-2k+1}{1+k^2}, \frac{-k^2-2k+1}{1+k^2}\right)$$

except $(1,-1)$ (when $k\to\infty$), where k is a rational number.

Rui Qiu
#999282509

(b). Suppose there are rational points.
Then $x=\frac{a}{b}$, $y=\frac{c}{d}$, $\gcd(a,b)=\gcd(c,d)=1$

$(ad)^2+(bc)^2=3(bd)^2$
let $u=ad$, $v=bc$, $w=bd$
$u^2+v^2=3w^2$
then we need to check whether we can find integer solution for u, v and w.

Both sides should satisfy:
$u^2+v^2\equiv 3w^2$
since $3\mid 3w^2$
u^2+v^2 should be divisible by 3 as well.
if u, v both divisible by 3, it would be simple.
Note: $\forall m\in\mathbb{Z}$, $3\nmid m$, either $m\equiv 1 \bmod 3$ or $m\equiv 2 \bmod 3$.
if $m\equiv 1 \bmod 3 \Rightarrow m^2\equiv 1 \bmod 3$
if $m\equiv 2 \bmod 3 \Rightarrow m^2\equiv 4\equiv 1 \bmod 3$
So no matter what combination u and v have, $u^2+v^2\not\equiv 0 \bmod 3$
Therefore the only possibility is $3\mid u$ and $3\mid v$.
let $u=3x$, $v=3y$, $x,y\in\mathbb{Z}$
$u^2+v^2=9x^2+9y^2=3w^2 \Rightarrow 3\mid w$ as well.
So $3\mid ad$, $3\mid bc$, $3\mid bd$
So $3\mid a$ or $3\mid d$
$3\mid b$ or $3\mid c$
$3\mid b$ or $3\mid d$

I. cannot have $3\mid a$, $3\mid b$ at the same time since $\gcd(a,b)=1$
II. cannot have $3\mid c$, $3\mid d$ at the same time since $\gcd(c,d)=1$
III. cannot have $3\mid b$, $3\mid d$ at the same time.
since $3\nmid a$, $3\nmid c$
then for $(ad)^2+(bc)^2=3(bd)^2$
$9\mid (ad)^2$, $9\mid (bc)^2$ and $243\mid 3(bd)^2$
$\Rightarrow 243\mid (ad)^2$, $243\mid (bc)^2$
$\Rightarrow \sqrt{243}\mid d$, $\sqrt{243}\mid b$ $\Rightarrow$ impossible.
Therefore, contradiction in any scenario, there are no rational points.

Rui Qiu
#999292509

3. Solution:

$$\begin{cases} x^2-y^2=1 \\ y=mx+b \text{ through } (-1,0) \end{cases}$$

$-m+b=0$, $b=m$

$y=mx+m$

$x^2-(mx+m)^2=x^2-m^2x^2-2m^2x-m^2=1$

$(1-m^2)x^2-2m^2x-m^2-1=0$

$x=\frac{m^2\pm1}{1-m^2}=-1$ or $\frac{1+m^2}{1-m^2}$ where $m\neq\pm1$

correspondingly, $y=m\cdot\frac{m^2\pm1}{1-m^2}+m=0$ or $\frac{2m}{1-m^2}$

so $(x,y)=\left(\frac{1+m^2}{1-m^2},\frac{2m}{1-m^2}\right)$ or $(-1,0)$ with $m\neq\pm1$

The intersection we need is $\left(\frac{1+m^2}{1-m^2},\frac{2m}{1-m^2}\right)$, $m\neq\pm1$.

~~Since m is rational,~~

4. Solution: $y^2=x^3+8$

Suppose the line passing through $(1,-3)$ and $(-\frac{7}{4},\frac{13}{8})$

$y=mx+b$

$$\begin{cases} m+b=-3 \\ -\frac{7}{4}m+b=\frac{13}{8} \end{cases} \qquad m=\frac{-37}{22},\ b=-\frac{29}{22}$$

So $y=-\frac{37}{22}x+(-\frac{29}{22})$

So $(-\frac{37}{22}x-\frac{29}{22})^2=x^3+8$

$\Rightarrow$ $\boxed{\begin{array}{l}\text{constant term LHS = RHS} \\ (+\frac{7}{4})(-1)(-x)=8-(\frac{29}{22})^2 \\ \frac{7}{4}x=8-(\frac{29}{22})^2\end{array}}$ *

$-x^3+\frac{1369}{484}x^2+\frac{1073}{242}x-\frac{3031}{484}=0$

$(x+\frac{7}{4})(x-1)(x-\frac{433}{121})=0$

so the third intersection pt is $(\frac{433}{121},-\frac{9765}{1331})$

By (*) $\Rightarrow x$ is rational. $\Rightarrow y$ is rational as well.

Hence the intersection is rational point.

Rui Qiu
#999292509

5. Solution:

Let $a = r_{-1}$, $b = r_0$

$$r_j = q_{j+2} r_{j+1} + r_{j+2} \geq r_{j+1} + r_{j+2} > 2r_{j+2}$$

we are done. (because remainder is always the "smaller one" that left out after a division).

① When $n = 2k+1$, $k \in \mathbb{Z}$

$$b = r_0 > 2r_1 > 2^2 r_3 > 2^3 r_5 > \cdots > 2^{\frac{n+1}{2}} r_n > 2^{\frac{n+1}{2}} \quad (\text{since } r_n > 1)$$

$$\log_2(b) > \frac{n+1}{2} \Rightarrow 2\log_2(b) > n+1 > n$$

② When $n = 2k$, $k \in \mathbb{Z}$

$$b = r_0 > 2r_1 > 2^2 r_3 > 2^3 r_5 > \cdots > 2^{\frac{n}{2}} r_{n-1} > 2^{\frac{n}{2}}$$

$$\log_2(b) > \frac{n}{2} \Rightarrow 2\log_2(b) > n$$

Say b has certain digits x (e.g. if $b=1234$, $x=4$)
then the largest b can achieve won't exceed 10^x.

$$b < 10^x$$

$$\log_2 b < \log_2 10^x$$

$$\log_2 b < x \log_2 10$$

$$2\log_2 b < 2\log_2 10 \cdot x < 7 \cdot x$$

So the number of steps is at most 7 times the number of digits in b.

6. Solution

(1). $LCM(8,12)=24$

$LCM(51,68)=204$

(2). ~~gcd~~

$$LCM(a,b)=\frac{a\cdot b}{gcd(a,b)}$$

check $LCM(8,12)=\frac{8\times 12}{4}=24$

$LCM(51,68)=\frac{51\times 68}{17}=204$

(3). $LCM(a,b)$ must be multiple of both a and b.

so $a\cdot b$ is such a multiple

But the $gcd(a,b)$ is counted twice in the multiple $a\cdot b$

Since we want $LCM(a,b)$ minimal, we need to divide by $gcd(a,b)$.

Explicitly:

need to show $LCM(a,b)$:

① is the multiple of a,b

② is the smallest one.

① $LCM(a,b)=\frac{ab}{gcd(a,b)} \Rightarrow a \mid LCM(a,b)$ and $b \mid LCM(a,b)$

② Suppose $LCM(a,b)=x_0$, other multiples x_i are all greater than x_0, for $i\geq 1$.

Equivalently, we need to show $x_0 \mid x_i$, $\forall i\geq 1$

$a \mid x_i \Rightarrow x_i=a\cdot s$

$b \mid x_i \Rightarrow x_i=b\cdot t$ for some $s,t\in\mathbb{Z}$

$\Rightarrow x_i=a\cdot gcd(a,b)\cdot p$

$x_i=b\cdot gcd(a,b)\cdot q$, p,q are "unique parts" of a and b.

$\Rightarrow ap=bq$

we know $gcd(p,q)=1$

so $q \mid a$, let $a=jq$, $j\in\mathbb{N}$

$\Rightarrow x_i=j\cdot q\, gcd(a,b)\cdot p=j x_0=j\,LCM(a,b) \Rightarrow x_0 \mid x_i$ ■

(4). $LCM(301337, 307829)$

$307829 = 301337 \times 1 + 6492$

$301337 = 6492 \times 46 + 2705$

$6492 = 2705 \times 2 + 1082$

$2705 = 1082 \times 2 + 541$

$1082 = 541 \times 2$

$$LCM = \frac{301337 \times 307829}{541} = 171460753$$

(5). $gcd(m,n) = 18$

$LCM(m,n) = 720$

$$LCM(m,n) = \frac{mn}{gcd(m,n)} = 720$$

$mn = 720 \times 180 = 12960$

$m = 2 \times 3^2 \cdot x$

$n = 2 \times 3^2 \cdot y$

$mn = 2^2 \times 3^4 xy$

$xy = 40$

Since x, y are co-prime

Then $\begin{cases} x=1 \\ y=40 \end{cases}$ $\begin{cases} x=5 \\ y=8 \end{cases}$ $\begin{cases} x=8 \\ y=5 \end{cases}$ $\begin{cases} x=40 \\ y=1 \end{cases}$

Hence there are 4 sets of solutions:

$(18, 720)$, $(90, 144)$, $(144, 90)$, $(720, 18)$