L19P1

CODE
BC

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Which of the following statements is false?

A) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \leq b \ \wedge \ \gcd(a,b) \leq a)$

B) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \neq 0 \implies (a \neq 0) \ \vee \ (b \neq 0))$

C) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (\gcd(a,b) \mid a \ \wedge \ \gcd(a,b) \mid b)$

D) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (((c \mid a) \ \wedge \ (c \mid b)) \implies c \leq \gcd(a,b))$

E) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \gcd(a,b) \geq 0$

A is False $a=-12$ $b=0$ $\gcd(-12,0)=12 > 0^{> -12}$.

B True $\gcd(a,b)=0 \iff a>b=0$.

C True

D is false $a=b=0$ and $c=10$

E is true.

Recall:

Let $a, b \in \mathbb{Z}$.

1. (Bezout's Lemma/Identity) If $d = \gcd(a,b)$ then $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$.
2. (GCDCT - GCD Characterization Theorem) If $d > 0$, $d \mid a$, $d \mid b$ and $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$, then $d = \gcd(a,b)$.

Ex: $6 > 0$, $6 \mid 30$, $6 \mid 42$ and

$$30(3) + 42(-2) = 6$$

GCDCT $\Rightarrow \gcd(30, 42) = 6$

Q: Prove if $a, b, x, y \in \mathbb{Z}$ are s.t. $\gcd(a,b) \neq 0$ and $ax + by = \gcd(a,b)$ then $\gcd(x,y) = 1$

Pf: Since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ we divide by $\gcd(a,b) \neq 0$ to see that

$$\underbrace{\left(\frac{a}{\gcd(a,b)}\right)}_{\text{"}x\text{"}=} \underbrace{x}_{\text{"}a\text{"}=} + \underbrace{\left(\frac{b}{\gcd(a,b)}\right)}_{\text{"}y\text{"}=} \underbrace{y}_{\text{"}b\text{"}=} = 1$$

Since $1 \mid x$, $1 \mid y$, $1 > 0$, GCDCT $\Rightarrow \gcd(x,y) = 1$.

$\blacksquare$

Euclid's Lemma (PAD Primes and Divisibility)

If p is a prime and $p|ab$ then $p|a$ or $p|b$.

Pf: Suppose p is prime, $p|ab$ and $p\nmid a$. Since $p\nmid a$, $\gcd(p,a)=1$. By Bézout's Lemma, $\exists x,y\in\mathbb{Z}$ s.t.

$p|ab$ so $\exists k\in\mathbb{Z}$ s.t. $ab=pk$

$$px+ay=1$$
$$pbx+aby=b$$
$$pbx+pky=b$$
$$p\underbrace{(bx+ky)}_{\in\mathbb{Z}.}=b \Rightarrow p|b$$

L19P4

Prove or disprove the following:

1. If $n \in \mathbb{N}$ then $\gcd(n, n+1) = 1$.
2. Let $a, b, c \in \mathbb{Z}$. If $\exists\ x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$ then $\gcd(a, b) \mid c$.
3. Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) \mid c$ then $\exists\ x, y \in \mathbb{Z}$ such that $ax^2 + by^2 = c$.

1. $n+1 = n(1)+1$ TRUE

GCDWR $\Rightarrow$ $\gcd(n+1, n) = \gcd(n, 1) = 1$

2. $\gcd(a,b) \mid a$ TRUE

$\gcd(a,b) \mid b$

DIC $\Rightarrow$ $\gcd(a,b) \mid ax^2+by^2 = c$. ✓

3.