Problem 1: prove that $d|n$ and $n|d$ implies $n = \pm d$

Pf: By def. we can rewrite that d divisble n ($d|n$) if $\exists c_1 \in \mathbb{Z}$ such that

$n = d \cdot c_1$

we can also rewrite n divisble d ($n|d$) if $\exists c_2 \in \mathbb{Z}$ such that

$d = n \cdot c_2$

we have $n = d \cdot c_1$, $d = n \cdot c_2 \Rightarrow n = n \cdot c_2 \cdot c_1$

$\Rightarrow 1 = c_1 \cdot c_2$, so $c_1 | 1$ or $c_2 | 1$

By fact from class $c_1 = \pm 1$ and $n = d \cdot c_1 \Rightarrow n = \pm d$

This show Either $n = d$ or $n = -d$. □

Problem 2: Prove that $x | (x^3 + x^2 + x + 1)$, then $x = \pm 1$.

Pf: since $x | x^3$, $x | x^2$, $x | x$, by the linearity $x | x^3 + x^2 + x$.

since $x | (x^3 + x^2 + x) + 1$ and $1 = x^3 + x^2 + x + 1 - (x^3 + x^2 + x)$

by the two out of three principle. $x | 1$, then $1 = c \cdot x$ for some $c \in \mathbb{Z}$

$\Rightarrow 1 = c \cdot x$ for some $c \in \mathbb{Z}$, but $|c| \geq 1$, $|x| \geq 1 \Rightarrow |x| = 1$, $x = \pm 1$ □

Problem 3. Compute the greatest common divisor of the following pair of integers.

a) gcd(200, 111): Let $a=200$, $b=111$

$200 = 1(111) + 89$
$111 = 1(89) + 22$
$89 = 4(22) + 1$
$22 = 22(1) + 0$

→ By them (Euclidean Algorithm) so the gcd(200, 111) = 1

b) gcd(289, -323): Based on A preperty of gcd: $gcd(a,b) = gcd(|a|,|b|)$

$gcd(289, -323) = gcd(289, 323)$. Let $a=323$, $b=289$

$323 = 1(289) + 34$
$289 = 8(34) + 17$
$34 = 2(17) + 0$

→ By them (Euclidean Algorithm) So gcd(289, -323) = 17

c) gcd(1800, 2100): Let $a=2100$, $b=1800$

$2100 = 1(1800) + 300$
$1800 = 6(300) + 0$

→ By them (Euclidean Algorithm) So gcd(1800, 2100) = 300.

Problem 4

(a) $192x - 231y = 29$

Change of variable $y = -z$, then $192x + 231z = 29$.

$231 = 1(192) + 39$
$192 = 4(39) + 36$
$39 = 1(36) + 3$
$36 = 12(3) + 0$.

The gcd(192, 231) = 3, but $3 \nmid 29$, so no solution for this.

b) $17x+19y=100$

Let $19=a$, $17=b$.

$19=1(17)+2$

$17=8(2)+1$

$2=2(1)+0$

Step 1:

The $\gcd(17,19)=1$, $1 \mid 100$. So we have solution

It's soluable.

step 2: we are doing linear combination

$1=17-8(2)$

$1=17-8(19-17)$

$1=(9)(17)+(-8)(19)$

$100=(900)(17)+(-800)19$

$x=900$ and $y=-800$ is the solution of $17x+19y=100$

Problem 5.

$\gcd(a,b)=\gcd(a,b+ak)$, $\forall k \in \mathbb{Z}$

I set $C=\gcd(a,b)$, $d=\gcd(a,b+ak)$

By the defination $C=\gcd(a,b)$ we get $C \mid a$ and $C \mid b$.

$C \mid a$ and $C \mid b \Longrightarrow C \mid b+ak$.

$d=\gcd(a,b+ak)$, by the defination, we get $d \mid a$ and $d \mid b+ak$

This $\Longrightarrow C \mid d$.

$d=\gcd(a,b+ak)$, then $d \mid a$ and $d \mid b+ak$.

By linearity, $d \mid (b+ka)-ka \Longrightarrow d \mid b$

we get $d \mid a$ and $d \mid b$.

So, $d=\gcd(a,b+ka)$ is common divisor of a and b

But $C=\gcd(a,b)$, C is the greater common divisor $\Longrightarrow d \mid C$

we now have $C \mid d$ and $d \mid C$, By the fact, we get

$C \mid d$ and $d \mid C \Longrightarrow C=+d$ ∎

Problem 6 Find all the solution to the equation

$16x + 12y = 200$

Step 1: check if the equation have solution.

Let $a=16, b=12$ $\quad \gcd(16,12) = 4$

$16 = 1(12) + 4$

$12 = 3(4) + 0$

$4 \mid 200$ and we have solution

Step 2: linear combination.

$4 = (16 - 12)$

$200 = (16)(50) + (-50)(12) \Rightarrow x_0 = 50, \; y_0 = -50$ is one solution

Step 3: Consider the homogenous part $16x + 12y = 0$

By prop 4, the general solution are:

$$x = n \cdot \frac{\operatorname{lcm}(a,b)}{a} \qquad y = -n \cdot \frac{\operatorname{lcm}(a,b)}{b}$$

$$= n \cdot \frac{\operatorname{lcm}(16,12)}{16} \qquad = -n \cdot \frac{\operatorname{lcm}(16,12)}{12}$$

$$x = n \cdot \frac{48}{16} = 3n \; \forall n \in \mathbb{Z} \qquad y = -n \cdot \frac{48}{12} = -4n \; \forall n \in \mathbb{Z}$$

$$\operatorname{lcm}(16,12) = \frac{16 \cdot 12}{\gcd(16,12)} = \frac{16 \cdot 12}{4} = 48$$

Step 4: By prop 5, The General solution to $ax + by = c$

$x = 50 + 3n$, $y = -50 - 4n$, $\forall n \in \mathbb{Z}$ is the General solution of $16x + 12y = 200$.

Problem 7. Let a, b be non zero integers. Show $\text{lcm}(a,b)/a$ and $a/\gcd(a,b)$ are coprime.

Pf: By Def, two integer a and b are called coprime if $\gcd(a,b)=1$.

So we have two integer $\frac{\text{lcm}(a,b)}{a}$ and $\frac{a}{\gcd(a,b)}$

use the product formula of GCD and Lcm, I rewrite.

$$\frac{\text{lcm}(a,b)}{a} \Rightarrow \frac{1}{a} \cdot \frac{a \cdot b}{\gcd(a,b)} \Rightarrow \frac{b}{\gcd(a,b)}$$

Show that coprime.

$$\gcd\left(\frac{b}{\gcd(a,b)}, \frac{a}{\gcd(a,b)}\right) = 1$$

I use the scaling property:

Scaling property:
Let $a, b, c \in \mathbb{Z}$, and $c > 0$
then $\gcd(ac, bc) = c \cdot \gcd(a,b)$

$$\gcd\left(\frac{b}{\gcd(a,b)}, \frac{a}{\gcd(a,b)}\right) = 1$$

$$\Rightarrow \gcd(b,a) \cdot \frac{1}{\gcd(a,b)} = 1$$

$$1 = 1.$$

Since LHS = RHS, Finish prove ▨

problem 8. Let a, b, n be three integer
Assume $\gcd(a,b)=1$, $a \mid n$ and $b \mid n$. show $ab \mid n$.

Lemma (Euclid's lemma) If $a, b, c \in \mathbb{Z}$ such that $a \mid b \cdot c$, and if $\gcd(a,b)=1$, then $a \mid c$.

Pf: Since $a \mid n$ and $b \mid n$, we can have $a \cdot c_1 = n$
$b \cdot c_2 = n$

$a \cdot c_1 = n$
$b \cdot c_2 = n$ for some $c_1, c_2 \in \mathbb{Z}$, which $a \cdot c_1 = n = b \cdot c_2$.

By Euclid's lemma: $a \mid c_2 \Longrightarrow ab \mid b \cdot c_2 \Rightarrow ab \mid n$ ▨

Another Proof:

By fact, $\exists\, x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 1$. we first time n both side $\Longrightarrow$ we get $a(n)(x_0) + b(n)(y_0) = n$.

Because we have $a \mid n$, $b \mid n$. so we can write $n = a \cdot c_1$, $n = b \cdot c_2$

$\Rightarrow a(n)(x_0) + b(n)(y_0) = n$

$\Rightarrow a(b \cdot c_2)(x_0) + b(a \cdot c_1)(y_0) = n$

$\Rightarrow ab \cdot (c_2 x_0 + c_1 y_0) = n$

By def. we know ab divisible n. $\Rightarrow ab \mid n$ ▨