Homework

Prop: if $a, b \in \mathbb{Z}$, and a and b are not both zero, then $\gcd(a,b) = \gcd(a+3b, b)$

Recall: the $\gcd(a,b)$ is the integer d such that

① d is a common divisor, that is, $d|a$ and $d|b$

② if $c|a$ and $c|b$, $d \geq c$.

$a=6 \quad b=9$

$\gcd(6,9)=3$

$a+3b = 6+3\cdot 9 = 33$

$\gcd(a+3b, b)$

$= \gcd(33, 9) = 3$

If you want to prove d is the gcd of a, b, just show:

→ ① show $d|a$ and $d|b$

→ ② show if $c|a$ and $c|b$ then $d \geq c$.

Proof Suppose $a, b \in \mathbb{Z}$ and a, b not both zero. Let $d = \gcd(a,b)$.

Then $d|a$ and $d|b$, by definition of gcd.

Notice $a = dx$ and $b = dy$ for some $x, y \in \mathbb{Z}$, by definition of divides.

So $a + 3b = dx + 3(dy)$

$= d(x + 3$

$= d(x+3y)$

note $x+3y \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under $+$, $\cdot$

so $d \mid a+3b$, by definition of divides.

Since $d \mid b$ was given, we have that d is a common divisor of $a+3b, b$.

Now suppose c is a common divisor of $a+3b, b$,

so $c \mid a+3b$ and $c \mid b$.

so $a+3b = cp$, $p \in \mathbb{Z}$ and $b = cq$, $q \in \mathbb{Z}$. by the definition of divides.

comment: want to show $c|a$ and $c|b$

Consider $a = a+3b-3b$

$$a = cp - 3(cq)$$
$$a = c(p-3q)$$

Note $p-3q \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under $+$, $\cdot$.

Thus $c \mid a$, by definition of divides.

Since c is a common divisor of a and b and d is the greatest common divisor of a and b, it follows that $d \geq c$.

Therefore $d = \gcd(a+3b, b)$, by the defn of gcd.

Useful fact you can ~~[illegible]~~ use in proofs:

NT2.1 Suppose $a, b \in \mathbb{Z}$, not both zero.

then there exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a,b) = ax + by$$

"$\gcd(a,b)$ is a linear combination of a and b"

Proof by contradiction

Prop. If $a, b \in \mathbb{Z}$ then $a^2 - 4b \neq 2$.

what if the proposition was false? what would go wrong?

$a = 2$
$b = 4$

$a^2 - 4b =$

$2^2 - 4 \cdot 4 = 4 - 16 = -12$
$\neq 2$

$a = 4$
$b = 8$

$4^2 - 4 \cdot 8 = 16 - 32$
$= -16 \neq 2$

$a = 2$
$b = 1$

$2^2 - 4 \cdot 1 = 4 - 4 = 0 \neq 2$

Proof Suppose $a, b \in \mathbb{Z}$ and $a^2 - 4b = 2$.

then $a^2 = 2 + 4b$

$a^2 = 2(1 + 2b)$

let $c = 1 + 2b$, note $c \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under $+, \cdot$.

thus $a^2 = 2c$ is even, by definition of even.

Thus since a^2 is even, a must be even (proved in class/homework)

So $a = 2d$, $d \in \mathbb{Z}$, by defn of even.

substituting, we find

$$(2d)^2 - 4b = 2$$

$$4d^2 - 4b = 2$$

divide by 2:

$$2d^2 - 2b = 1$$

$$2(d^2 - b) = 1$$

Note $d^2 - b \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under $\overset{\text{subtraction}}{-}$, $\overset{\text{multiplication}}{\cdot}$

Thus $\overbrace{\text{1 is even}}^{C}$ by definition of even.

$\sim C$

But we know 1 is not even.

Contradiction!

Thus if $a, b \in \mathbb{Z}$ then $a^2 - 4b \neq 2$. $\square$

Overall, we did the following:

Proposition: P

Proof (contradiction). Suppose $\sim P$,

⋮

Thus $C \wedge \sim C$

contradiction.

Therefore P $\square$

<u>Prop.</u> $\overbrace{\sqrt{2} \text{ is irrational.}}^{P}$

<u>Proof (contradiction)</u> Suppose $\sqrt{2}$ is rational.

Thus $\sqrt{2} = \frac{p}{q}$, $p, q \in \mathbb{Z}$ and $q \neq 0$, by the definition of rational number. Without less of generality, $\frac{p}{q}$ is in lowest terms

(p, q have no common factors besides 1)

goal: reach a contradiction

by rules of algebra,

$$(\sqrt{2})^2 = \left(\frac{p}{q}\right)^2$$

$$2 = \frac{p^2}{q^2}$$

$$2q^2 = p^2$$

Note $q^2 \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication.

$$\frac{3}{6} = \frac{1}{2}$$

$$\frac{3}{6} = \frac{4}{8} = \frac{6}{12}$$

etc.

Thus p^2 is even, by definition of even.

Thus p is even (proved in class)

So $p = 2x$, $x \in \mathbb{Z}$, by definition of even.

Substitute to get

$$2q^2 = (2x)^2$$

$$\frac{2q^2}{2} = \frac{4x^2}{2}$$

$$q^2 = 2x^2$$

$x^2 \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under multiplication.

So q^2 is even by definition of even.

So q is also even.

Thus since p, q are both even they are both divisible by 2.

Thus p, q have a

common factor of 2.

Contradiction (we said p, q had no common factors).

Thus $\sqrt{2}$ is irrational.

$\boxed{\checkmark}$