Worksheet 4: Contradiction

Problem 1. Prove that $\sqrt{6}$ is irrational.

Solution. Suppose $\sqrt{6}$ is rational, ie, that $\sqrt{6} = a/b$ for some relatively prime integers a and b. Then $6 = a^2/b^2$, ie, $6b^2 = a^2$. This means that a^2 is even, so a must be even. But then $a = 2k$ for some k, so $6b^2 = a^2 = 4k^2$, which means that $3b^2 = 2k^2$. Thus $3b^2$ is even. Since 3 is odd, this means that b^2 must be even, which means that b must also be even. Thus 2 is a common divisor of a and b, contradicting our assumption that a and b are relatively prime.

Problem 2. Prove that there exist no integers a and b such that $21a + 30b = 1$.

Solution. If there did exist such integers, we would have $3(7a + 10b) = 1$, which means that $3 \mid 1$. This is clearly a contradiction.

Problem 3. Suppose a and b are integers such that $a^2 + b^2 \equiv 0 \bmod 4$. Show that a and b are not both odd.

Solution. We prove this by contraposition. Suppose it is not the case that a and b are not both odd, ie, that a and b are both odd. Then $a = 2k + 1$ and $b = 2\ell + 1$ for some integers k and ℓ, which means that

$$a^2 + b^2 = (2k+1)^2 + (2\ell+1)^2 = 4k^2 + 4k + 1 + 4\ell^2 + 4\ell + 1 \equiv 1 + 1 \equiv 2 \not\equiv 0 \bmod 4.$$

Problem 4. Show that, if n is composite, then there exists a divisor k of n such that $1 < k \leqslant \sqrt{n}$.

Solution. Suppose not, ie, that every divisor of n that's greater than 1 is greater than $\sqrt{n}$. Since n is composite, we know there exist integers a and b both greater than 1 such that $n = ab$. By our assumption, we know that $a, b > \sqrt{n}$. But then

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n$$

which is a contradiction.

Problem 5. Let $n \geqslant 2$ be an integer and let d be the smallest divisor of n which is larger than 1. Show that d must be prime.

Solution. Suppose for a contradiction that d is not prime. Then d has a divisor a where $1 < a < d$. Since $a \mid d$ and $d \mid n$, we must have $a \mid n$ as well. But then a is a divisor of n which is greater than 1 and smaller than d, contradicting our choice of d as the smallest divisor of n that's bigger than 1. Thus d must be prime.

Problem 6. Prove that the sum of a rational and an irrational is irrational.

Solution. Suppose x is rational and y is irrational, and suppose for a contradiction that $x + y$ is rational. Then $y = (x + y) - x$ is a difference of two rational numbers, so it would have to be rational. This is a contradiction.

Problem 7. If a and b are positive real numbers, show that $a + b \geqslant 2\sqrt{ab}$.

Solution. Suppose for a contradiction that $a + b < 2\sqrt{ab}$. Then $(a + b)^2 < 2ab$, ie, $a^2 + 2ab + b^2 < 2ab$, which means that $a^2 + b^2 < 0$. This is a contradiction, since $a^2, b^2 \geqslant 0$ and the sum of two non-negative numbers cannot be negative.

Problem 8. Suppose $x \in \mathbb{R}$ and $0 < x < 1$. Show that $\dfrac{1}{x(1-x)} \geqslant 4$.

Solution. Suppose for a contradiction that

$$\frac{1}{x(1-x)} < 4.$$

Clearing denominators, this means that $1 < 4x(1 - x)$. Then

$$0 < 4x - 4x^2 - 1 = -(4x^2 - 4x + 1) = -(2x - 1)^2.$$

But $(2x - 1)^2 \geqslant 0$, so $-(2x - 1)^2$ must be less than 0. This is a contradiction.

Problem 9. If a, b, c are integers such that $a^2 + b^2 = c^2$, show that either a or b must be even.

Solution. Suppose not, ie, that a and b are both odd. This means that a and b must both be congruent to 1 or 3 mod 4, but then in either case, a^2 and b^2 are both congruent to 1 mod 4. This means that $c^2 \equiv a^2 + b^2 \equiv 2 \bmod 4$. This cannot happen: if c is even, then it $c^2 \equiv 0 \bmod 4$, and if c is odd, then $c^2 \equiv 1 \bmod 4$. In no case can c^2 be congruent to 2 mod 4!

Problem 10. Prove that there exist no rational numbers x and y such that $x^2 + y^2 = 3$.

Solution. Suppose there exist rational numbers x and y such that $x^2 + y^2 = 3$. Writing them over a common denominator, we have $x = a/c$ and $y = b/c$ for integers a, b and c which have no common factor greater than 1 (*). Then $(a/c)^2 + (b/c)^2 = 3$ implies that

$$a^2 + b^2 = 3c^2.$$

Note that, if x is not divisible by 3, then we must have $x \equiv \pm 1 \bmod 3$, and in either case we have $x^2 \equiv 1 \bmod 3$. This means that a and b must both be divisible by 3 (otherwise, the left hand side of the above equation would have to be congruent to either 1 or 2 but the right hand side is clearly congruent to 0). Thus $a = 3a'$ and $b = 3b'$ for some integers a', b', so the above equation can be rewritten

$$9a'^2 + 9b'^2 = 3c^2$$

which means that

$$3(a'^2 + b'^2) = c^2$$

which implies that c must be divisible by 3. In other words, 3 is a common factor of a, b and c, contradicting our choice that a, b, c share no common factor greater than 1.

Note. Felix and Esa asked in class about why (*) above is valid. Let's prove this! In other words, for every $x, y \in \mathbb{Q}$, we want to show there exist integers $a, b, c \in \mathbb{Z}$ such that $x = a/c$ and $y = b/c$ and there are no factors in common among all three of a, b, c.

I can think of at least two arguments. The first argument only uses things you've read about, but it's slightly sophisticated from a logical standpoint. The second argument is more straightforward from a logical standpoint, but it makes use of Bézout's theorem (which you haven't read about yet).

Argument 1. Consider the set

$$S = \{c \in \mathbb{N} : \text{there exist } a, b \in \mathbb{Z} \text{ such that } x = a/c \text{ and } y = b/c\}.$$

Let me first claim that S is nonempty. Since x and y are rational, there exist integers a', b', r, s such that $x = a'/r$ and $y = b'/s$, where $r, s > 0$. Then $rs \in S$, since we can write $x = a's/rs$ and $y = b'r/rs$. Thus S is a nonempty subset of $\mathbb{N}$.

Now, by the well-ordering principle, S must have a least element c. Since $c \in S$, there exist integers $a, b \in \mathbb{Z}$ such that $x = a/c$ and $y = b/c$. I now claim that $\gcd(a, b, c) = 1$. Suppose for a contradiction that there exists an integer $d > 1$ which is a common factor of a, b, c. Then $a/d, b/d$, and c/d are all integers, and we have $x = a/c = (a/d)/(c/d)$ and $y = b/c = (b/d)/(c/d)$, which shows that $c/d \in S$. But $d > 1$, so $c/d < c$, and c was supposed to be the least element of S. This contradiction completes argument 1.

Argument 2. Since x, y are rational, there exist integers a', b', r, s such that $x = a'/r$ and $y = b'/s$, where $\gcd(a', r) = 1$ and $\gcd(b', s) = 1$. Let $c = \text{lcm}(r, s)$ and let $a = a'c/r$ and $b = b'c/s$. Note that a and b are integers since c is divisible by both r and s. Moreover,

$$\frac{a}{c} = \frac{a'c/r}{c} = \frac{a'}{r} = x \text{ and } \frac{b}{c} = \frac{b'c/s}{c} = \frac{b'}{s} = y.$$

Let us now show that $\gcd(a, b, c) = 1$. Suppose for a contradiction that some integer $d > 1$ is a common factor of a, b, c. Then $a/d, b/d$, and c/d are all integers, and

$$x = \frac{a}{c} = \frac{a/d}{c/d} \text{ and } y = \frac{b}{d} = \frac{b/d}{c/d}$$

so by claim A below, we see that c/d must be a common multiple of r and s. Since $d > 1$, we have $c/d < c = \text{lcm}(r, s)$, contradicting the definition of least common multiples. Thus we will be done once we prove the following.

Claim A. If there exist integers a, b, c such that $x = a/c$ and $y = b/c$, then c must be a common multiple of r and s.

Proof of claim A. Note that

$$x = \frac{a'}{r} = \frac{a}{c} \implies a'c = ra$$

and similarly

$$y = \frac{b'}{s} = \frac{b}{c} \implies b'c = sb.$$

Then $r \mid a'c$ and $\gcd(a', r) = 1$, so $r \mid c$ using claim B below. Similarly, $s \mid b'c$ and $\gcd(b', s) = 1$, so $s \mid c$ again by claim B below. Thus c is a common multiple of r and s, and this proves claim A.

Claim B. If d, e, f are integers such that $d \mid ef$ and $\gcd(d, e) = 1$, then $d \mid f$.

Proof of claim B. This is the lemma that Harry told us about on Discord. I don't know a proof of this that avoids Bézout's theorem, but here's the quick proof using Bézout's theorem. Since $\gcd(d, e) = 1$, there exist integers u and v such that $du + ev = 1$. Then $f = f \cdot 1 = f(du + ev) = dfu + efv$. Clearly $d \mid dfu$, and $d \mid efv$ by our assumption that $d \mid ef$. Thus $d \mid (dfu + efv) = f$. This proves claim B, and also completes argument 1.