Worksheet 3: Direct and Contrapositive Proofs, Division, GCD, Congruence

Problem 1. Prove that, if a is an integer such that $5 \mid 2a$, then $5 \mid a$.

Solution. Suppose $5 \mid 2a$. This means that $2a = 5k$ for some integer k, which means that $5k$ is even. Since 5 is odd, this means that k must be even, so there exists an integer ℓ such that $k = 2\ell$. Then $2a = 5k = 10\ell$, so $a = 5\ell$. This shows that $5 \mid a$.

Problem 2. Prove that $5n^2 + 3n + 7$ is odd for every integer n.

Solution. We uses cases. Suppose n is even so that $n = 2k$ for some integer k. Then

$$5n^2 + 3n + 7 = 5 \cdot 4k^2 + 3 \cdot 2k + 7 = 2(10k^2 + 3k + 3) + 1.$$

In other words, $5n^2 + 3n + 7 = 2q + 1$ for $q = 10k^2 + 3k + 3$, so $5n^2 + 3n + 7$ is odd. Next, suppose that n is odd so that $n = 2k + 1$ for some integer k. Then

$$5n^2 + 3n + 7 = 5 \cdot (4k^2 + 4k + 1) + 3 \cdot (2k + 1) + 7 = 2(10k^2 + 13k + 7) + 1$$

so $5n^2 + 3n + 7 = 2q + 1$ for $q = 10k^2 + 13k + 7$. Thus $5n^2 + 3n + 7$ is odd again.

Problem 3. Prove that every odd integer is the difference of two consecutive squares.

Solution. Every odd integer is of the form $2k + 1$, and $2k + 1 = (k + 1)^2 - k^2$.

Problem 4. Show that the square of any integer cannot be congruent to 2 modulo 3.

Solution. Let n be an integer. We use cases to show that n^2 cannot be congruent to 2 modulo 3. If $n \equiv 0 \bmod 3$, then $n^2 \equiv 0^2 = 0 \bmod 3$ (using the first proposition on page 132 in Ham18). Since $0 \not\equiv 2 \bmod 3$, we see that $n^2 \not\equiv 2 \bmod 3$. Next, if $n \equiv 1 \bmod 3$, then $n^2 \equiv 1^2 = 1 \bmod 3$, and since $1 \not\equiv 2 \bmod 3$, we again see that $n^2 \not\equiv 2 \bmod 3$. Finally, if $n \equiv 2 \bmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \bmod 3$. As in the previous case, see conclude that $n^2 \not\equiv 2 \bmod 3$.

Problem 5. For any integer n, show that either n, $n + 2$, or $n + 4$ must be divisible by 3.

Solution. We know that $n = 3q + r$ for $r \in \{0, 1, 2\}$. We split up into cases. If $r = 0$, then $n = 3q$ is divisible by 3. If $r = 1$, then $n + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$ is divisible by 3. Finally, if $r = 2$, then $n + 4 = (3q + 2) + 4 = 3q + 6 = 3(q + 2)$ is divisible by 3. Thus, in all cases, at least one of n, $n + 2$, and $n + 4$ is divisible by 3, so we are done.

Problem 6. Show that if n is an integer and n^2 is not divisible by 4, then n must be odd.

Solution. Let's prove this by contraposition. Suppose n is even. Then $n = 2k$ for some integer k, so $n^2 = (2k)^2 = 4k^2$ is divisible by 4.

Problem 7. Let $a, b \in \mathbb{Z}$ are both nonzero. Show that $\operatorname{lcm}(a, b)$ divides any common multiple of a and b.

Solution. Let $m = \operatorname{lcm}(a, b)$ and suppose n is a common multiple of a and b. By the division algorithm, there exist integers q and r such that $n = mq + r$ with $0 \leqslant r < m$. Observe that

$$r = n - mq$$

and since a, b are common factors of both n and m, they are also common factors of r. But m was supposed to be the *least* common multiple of a and b, so $0 \leqslant r < m$ implies that $r = 0$. Thus $n = mq$, which shows that $m \mid n$.

Problem 8. Suppose a and b are integers that are not both 0. Show that $\gcd(a, b) = \gcd(a - b, b)$.

Solution. Let us first show that $\gcd(a, b) \leqslant \gcd(a - b, b)$. Since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, there exist integers k_1 and k_2 such that $\gcd(a, b)k_1 = a$ and $\gcd(a, b)k_2 = b$. Then

$$a - b = \gcd(a, b)k_1 - \gcd(a, b)k_2 = \gcd(a, b)(k_1 - k_2)$$

so $\gcd(a, b) \mid a - b$. Thus $\gcd(a, b)$ divides both $a - b$ and b, and since $\gcd(a - b, b)$ is the largest common divisor of both $a - b$ and b, we must have $\gcd(a, b) \leqslant \gcd(a - b, b)$.

Next, we show that $\gcd(a - b, b) \leqslant \gcd(a, b)$. Since $\gcd(a - b, b) \mid a - b$ and $\gcd(a - b, b) \mid b$, there exist integers ℓ_1 and ℓ_2 such that $\gcd(a - b, b)\ell_1 = a - b$ and $\gcd(a - b, b)\ell_2 = b$. Then

$$a = (a - b) + b = \gcd(a - b, b)\ell_1 + \gcd(a - b, b)\ell_2 = \gcd(a - b, b)(\ell_1 - \ell_2)$$

so $\gcd(a - b, b) \mid a$. Thus $\gcd(a - b, b) \mid a$ and $\gcd(a - b, b) \mid b$, so $\gcd(a - b, b) \leqslant \gcd(a, b)$.

Since $\gcd(a - b, b) \leqslant \gcd(a, b)$ and $\gcd(a, b) \leqslant \gcd(a - b, b)$, we conclude that $\gcd(a - b, b) = \gcd(a, b)$.

Problem 9. For positive integers a and b, prove that $\gcd(a,b)\operatorname{lcm}(a,b) = ab$.

Solution. Here is a solution that only uses definitions and the result of problem 7 above, courtesy of a friend of Harry's. Observe that

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

and we know that $b/\gcd(a,b)$ and $a/\gcd(a,b)$ are both integers since $\gcd(a,b)$ divides both a and b, so $ab/\gcd(a,b)$ is a positive common multiple of a and b. By definition of least common multiples, it follows that

$$\operatorname{lcm}(a,b) \leqslant \frac{ab}{\gcd(a,b)},$$

which means that $\operatorname{lcm}(a,b)\gcd(a,b) \leqslant ab$.

Next, observe that $ab/\operatorname{lcm}(a,b)$ is an integer by problem 7 above. Moreover,

$$\frac{ab}{\operatorname{lcm}(a,b)} = \frac{a}{\operatorname{lcm}(a,b)/b} = \frac{b}{\operatorname{lcm}(a,b)/a}$$

being an integer means that $ab/\operatorname{lcm}(a,b)$ is a common divisor of a and b. By definition of greatest common divisors, this means that

$$\frac{ab}{\operatorname{lcm}(a,b)} \leqslant \gcd(a,b)$$

which means that $ab \leqslant \operatorname{lcm}(a,b)\gcd(a,b)$. We've thus shown inequalities both ways, so we must have $ab = \gcd(a,b)\operatorname{lcm}(a,b)$.

Alternatively, here's a different solution that makes use of Bézout's theorem. Let $d = \gcd(a,b)$ and $m = ab/d$. Since d is a common divisor of a and b, we have $a = dr$ and $b = ds$ for some integers r and s. Then $m = ab/d = drb/d = rb$ and $m = ab/d = ads/d = as$, which shows that m is a common multiple of a and b.

Suppose c is any positive common multiple of a and b. Then $c = au = bv$ for some integers u and v. By Bézout's theorem, exist integers x and y such that $d = ax + by$, and

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy \in \mathbb{Z},$$

so $m \mid c$. This implies that $m \leqslant c$. Thus m is the least common multiple. In other words,

$$\operatorname{lcm}(a,b) = m = \frac{ab}{d} = \frac{ab}{\gcd(a,b)}$$

which shows that

$$\gcd(a,b)\operatorname{lcm}(a,b) = ab.$$

Problem 10. Let n be a positive integer. Show that, if a and b are integers such that $a \equiv b \bmod n$, then $\gcd(a,n) = \gcd(b,n)$.

Solution. Since $a \equiv b \bmod n$, we know that there exists an integer k such that $a - b = nk$.

Let us first show that $\gcd(a,n) \leqslant \gcd(b,n)$. Note that $\gcd(a,n) \mid a$ and $\gcd(a,n) \mid n$, so there exist integers k_1 and k_2 such that $\gcd(a,n)k_1 = a$ and $\gcd(a,n)k_2 = n$. Since $b = a - nk$, we see that

$$b = a - nk = \gcd(a,n)k_1 - \gcd(a,n)k_2k = \gcd(a,n)(k_1 - k_2k)$$

so $\gcd(a,n) \mid b$. Thus $\gcd(a,n)$ divides both b and n. Since $\gcd(b,n)$ is the largest integer which divides both b and n, we see that $\gcd(a,n) \leqslant \gcd(b,n)$.

We then show that $\gcd(b,n) \leqslant \gcd(a,n)$. This proof is completely analogous to the previous paragraph and is omitted, but you should make sure you can fill in the details yourself.

Thus $\gcd(a,n) \leqslant \gcd(b,n)$ and $\gcd(b,n) \leqslant \gcd(a,n)$, which means that $\gcd(a,n) = \gcd(b,n)$.