MATH 135 Fall 2020: Extra Practice 6

Warm-Up Exercises

WE01. What is the remainder when -98 is divided by 7?

$-98 \div 7 = -14$, so the remainder is 0.

WE02. Calculate $\gcd(10, -65)$.

We have $10 = 2 \cdot 5$ and $-65 = -1 \cdot 5 \cdot 13$, so the GCD is 5.

WE03. Let $a, b, c \in \mathbb{Z}$. Consider the implication S: If $\gcd(a, b) = 1$ and $c \mid (a + b)$, then $\gcd(b, c) = 1$. Fill in the blanks to complete a proof of S.

(a) Since $\gcd(a, b) = 1$, by $\boxed{\text{Bézout's Lemma}}$, there exist integers x and y such that $ax + by = 1$.

(b) Since $c \mid (a + b)$, by $\boxed{\text{definition}}$, there exists an integer k such that $a + b = ck$.

(c) Substituting $a = ck - b$ into the first equation, we get $1 = (ck - b)x + by = b(-x + y) + c(kx)$.

(d) Since 1 is a common divisor of b and c and $-x + y$ and kx are integers, $\gcd(b, c) = 1$ by $\boxed{\text{the GCD Characterization Theorem}}$.

WE04. Disprove: For all integers a, b, and c, if $a \mid (bc)$, then $a \mid b$ or $a \mid c$.

Proof. We prove the negation, there are integers a, b, and c where $a \mid bc$, $a \nmid b$, and $a \nmid c$.

Let $a = 15$, $b = 5$, and $c = 3$. Clearly, $a \nmid b$ and $a \nmid c$. However, $bc = 15$, and $15 \mid 15$. $\square$

Recommended Problems

RP01.

(a) Use the Extended Euclidean Algorithm to find three integers x, y and $d = \gcd(1112, 768)$ such that $1112x + 768y = d$.

Solution. Apply the EEA with $x = 1112$ and $y = 768$.

x	y	r	q
1	0	1112	
0	1	768	
1	-1	344	1
-2	3	80	2
9	-13	24	4
-29	42	8	3
96	-139	0	3

Therefore, we have that $d = \gcd(1112, 768) = 8$, and that

$$1112(-29) + 768(42) = 8$$

That is, our solution is when $x = -29$ and $y = 42$. $\square$

(b) Determine integers s and t such that $768s - 1112t = \gcd(768, -1112)$.

Solution. Since the GCD is invariant under sign changes, we immediately know that $\gcd(768, -1112) = 8$. We also have that $1112(-29) + 768(42) = 8$. But this is the same as saying $768(42) - 1112(29) = 8$, so $s = 42$ and $t = 29$. □

RP02. Prove that for all $a \in \mathbb{Z}$, $\gcd(9a + 4, 2a + 1) = 1$.

Proof. Let a be an integer. We must show that $9a + 4$ and $2a + 1$ are coprime. Recall the Coprimeness Characterization Theorem: it suffices to find integers a and b such that $(9a + 4)a + (2a + 1)b = 1$.

Choose $a = -2$ and $b = 9$. Then,

$$\begin{aligned}(9a + 4)a + (2a + 1)b &= -2(9a + 4)a + 9(2a + 1)\\ &= -18a - 8 + 18a + 9\\ &= 1\end{aligned}$$

as desired. Therefore, $\gcd(9a + 4, 2a + 1) = 1$. □

RP03. Let $\gcd(x, y) = d$ for integers x and y. Express $\gcd(18x + 3y, 3x)$ in terms of d and prove that you are correct.

Proof. Let x and y be integers with GCD d.

We may apply GCD With Remainders to reduce $g = \gcd(18x+3y, 3x)$. We have $18x+3y = 6(3x) + 3y$, so $g = \gcd(3x, 3y)$.

Now, $x \mid d$ and $y \mid d$, so we can find integers m and n where $x = dm$ and $y = dn$. Multiplying through by 3, we have $3x = (3d)m$ and $3y = (3d)n$. It follows that $3d \mid 3x$ and $3d \mid 3y$, that is, $3d$ is a common divisor of $3x$ and $3y$.

By Bézout's Lemma, there are integers s and t where $xs + yt = d$. Again multiplying through by 3, we have $(3x)s + (3y)t = 3d$.

Therefore, by the GCD Characterization Theorem, $\gcd(3x, 3y) = 3d$. □

RP04. Let $a, b \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$, then $\gcd(2a + b, a + 2b) \in \{1, 3\}$.

Proof. Let a and b be coprime integers.

Applying GCD WR, we have that $2a + b = 2(a + 2b) - 3b$, so $\gcd(2a + b, a + 2b) = \gcd(a + 2b, -3b)$. The properties of GCD state this is equivalent to $\gcd(3b, a + 2b)$.

The GCD of $3b$ and $a + 2b$ must divide both $3b$ and $a + 2b$. The positive divisors of $3b$ are 1, 3, and any positive divisor $d \geq 2$ of b. We show that no such divisors of b also divide $a + 2b$.

Suppose for a contradiction that an integer $d \geq 2$ divides both b and $a + 2b$. Then, by DIC, $d \mid ((a + 2b) - 2(b))$, that is, $d \mid a$. This means that d is a common divisor of a and b. However, a and b are coprime, meaning $d = 1$. This is a contradiction since $1 \not\geq 2$. Therefore, no positive divisor of b, other than 1, also divides $a + 2b$.

It follows that $\gcd(2a + b, a + 2b)$ can only be 1 or 3, as desired. □

RP05. Prove that for all integers a, b and k, if $b \neq 0$, then $\gcd(a, b) \leq \gcd(ak, b)$.

Proof. Let a, b, and k be integers where b is non-zero. Also, let $d = \gcd(a, b)$ and $g = \gcd(ak, b)$. We must show $d \leq g$.

We will apply the GCD from Prime Factorization. For convenience, we define p_n to be the n^{th} prime. First, by UPF, we are guaranteed to be able to write $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, and $k = p_1^{\kappa_1} p_2^{\kappa_2} \cdots p_n^{\kappa_n}$, with non-negative α_i, β_i, and κ_i. Notice that we may write ak as a product of primes: $p_1^{\alpha_1+\kappa_1} p_2^{\alpha_2+\kappa_2} \cdots p_n^{\alpha_n+\kappa_n}$.

Now, by GCD PF, we have $d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$, where $\delta_i = \min(\{\alpha_i, \beta_i\})$ for all integers $1 \leq i \leq k$. Likewise, we have $g = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$, where $\gamma_i = \min(\{\alpha_i + \kappa_i, \beta_i\})$.

We will show that $\delta_i \leq \gamma_i$ for all i, from which it follows $d \leq g$. Let i be arbitrary.

If $\alpha_i \leq \beta_i \leq \alpha_i + \kappa_i$, then we have $\delta_i = \alpha_i$ and $\gamma_i = \beta_i$. It follows that $\delta_i \leq \gamma_i$. Otherwise, $\beta_i \leq \alpha_i \leq \alpha_i + \kappa_i$, so $\delta_i = \beta_i$ and $\kappa_i = \alpha_i$. We again have $\delta_i \leq \gamma_i$.

Therefore, since every exponent in the prime factorization of d is less than or equal to the coresponding exponent in the prime factorization of g, it must be the case that $d \leq g$. $\square$

RP06. Prove that for all integers a, b and c: if $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

Proof. Let a, b, and c be integers such that a and b divide c, and a and b are coprime.

Then, there exist integers m and n such that $am = c$ and $bn = c$. Also, by the CCT, there exist integers s and t such that $as + bt = 1$.

Then, $cas + cbt = c$, so $(bn)as + (am)bt = c$. It follows that $ab(ns + bt) = c$, so $ab \mid c$. $\square$

RP07. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $c \mid a$, then $\gcd(b, c) = 1$.

Proof. Let a, b, and c be integers such that $\gcd(a, b) = 1$ and $c \mid a$.

Then, $nc = a$ for some integer n and, by Bézout's Lemma, $as + bt = 1$. Substituting, $(nc)a + bt = bt + c(na) = 1$ for integers t and na, so by the CCT, $\gcd(b, c) = 1$. $\square$

RP08. Let a and b be integers. Prove that if $\gcd(a, b) = 1$, then $\gcd(a^m, b^n) = 1$ for all $m, n \in \mathbb{N}$. You may use the result which is proved in Example 14 in the notes.

Proof. Recall that Example 14 proved that for all integers a, b, and natural numbers n, if $\gcd(a, b) = 1$, then $\gcd(a, b^n) = 1$. Therefore, it suffices to let $c = b^n$ and prove that $\gcd(a, c) = 1$ implies $\gcd(a^m, c) = 1$.

In fact, we may simplify the problem further. If we show that the arguments of the GCD are commutative, then we may again use the result from Example 14. Let x and y be coprime integers, that is, $\gcd(x, y) = 1$. By Bézout's Lemma, there exist s and t such that $xs + yt = 1$. Equivalently, $yt + xs = 1$, and by the CCT, $\gcd(y, x) = 1$.

Then, $\gcd(a, c) = \gcd(c, a) = 1$. By Example 14, $\gcd(c, a^m) = 1$, that is, $\gcd(a^m, c) = \gcd(a^m, b^n) = 1$, as desired. $\square$

RP09. Suppose a, b and n are integers. Prove that $n \mid \gcd(a,n) \cdot \gcd(b,n)$ if and only if $n \mid ab$. (sooshi, CS Discord)

Proof. Let a, b, and n be integers. Then, let $d = \gcd(a,n)$ and $c = \gcd(b,n)$. We prove both implications.

($\Leftarrow$) Suppose that $n \mid dc$. Recall that by definition, $d \mid a$ and $c \mid b$. Then, we may write $dn = a$ and $cm = b$ for some integers n and m. Multiplying together, $dc(mn) = ab$, that is, since mn is an integer, $dc \mid ab$. By the transitivity of divisibility, $n \mid dc$ and $dc \mid ab$ imply $n \mid ab$, as desired.

($\Rightarrow$) Suppose that $n \mid ab$. We apply Bézout's Lemma to rewrite $d = as+nt$ and $c = bx+ny$ with integers s, t, x, and y. Multiplying together gives $dc = absx + asny + bxnt + n^2ty$. This factors to $dc = (ab)(sx) + n(asy + bxt + nty)$. Since we have both $n \mid ab$ and $n \mid n$, by DIC, $n \mid (ab)(sx) + n(asy + bxt + nty)$. However, this is just $n \mid dc$.

Therefore, since both implications hold, $n \mid dc$ if and only if $n \mid ab$. □

RP10. How many positive divisors does 33480 have?

Solution. We may apply prime factorization to get $33480 = 2^3 \cdot 3^3 \cdot 5 \cdot 31$. Then, by DFPF, we have that any positive divisor $d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 31^\delta$ for integers $0 \leq \alpha \leq 3$, $0 \leq \beta \leq 3$, $0 \leq \gamma \leq 1$, and $0 \leq \delta \leq 1$.

That is, there are 4 choices for each of α and β, and 2 choices for γ and δ. Multiplying out, we have $4 \cdot 4 \cdot 2 \cdot 2 = 64$ positive divisors. □

RP11. Prove that for all integers a and b, if $9a^2 = b^4$ where $a, b \in \mathbb{Z}$, then 3 is a common divisor of a and b.

Proof. Let a and b be integers such that $9a^2 = b^4$. Without loss of generality, let both a and b be positive (if $a = b = 0$, then, trivially, $3 \mid a$ and $3 \mid b$).

By UFT, $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ for k distinct primes p_i and non-negative integers α_i. Likewise, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ for non-negative integers β_i. Since 3 is prime, there is an n where $p_n = 3$.

It follows that $9a^2$ has $2 + 2\alpha_n$ factors of 3 and that b^4 has $4\beta_n$ factors. Since $9a^2 = b^4$, by UFT, $2 + 2\alpha_n = 4\beta_n$.

We have that $4\beta_n = 2 + 2\alpha_n \geq 2$, so $\beta_n \geq 1$, which means $3 \mid b$.

However, if $\beta_n \geq 1$, then $2 + 2\alpha_n = 4\beta_n \geq 4$, which means $\alpha_n \geq 1$. That is, $3 \mid a$.

Therefore, 3 is a common divisor of a and b. □

RP12. Let $n \in \mathbb{N}$. Prove that if p is prime and $p \leq n$, then p does not divide $n! + 1$.

Proof. Let n be a natural number, and p be a prime number.

Since $n!$ is defined as the product of all positive integers up to n and $p \leq n$, p clearly divides n. Therefore, $n! = kp$ for some integer k. Then, k is the product of all positive integers up to n *except* p. Since p is prime, $k \nmid p$.

Then, we have $n! + 1 = p(k + \frac{1}{p})$, so $p \mid (n! + 1)$ only if $k + \frac{1}{p}$ is an integer, which it clearly is not (since $p \geq 2$). Therefore, $p \nmid (n! + 1)$. □

Challenges

C01. Prove that for any integer $a \neq 1$ and $n \in \mathbb{N}$, $\gcd\left(\frac{a^n-1}{a-1}, a-1\right) = \gcd(n, a-1)$.

C02. Let n be a positive integer for which $\gcd(n, n+1) < \gcd(n, n+2) < \cdots < \gcd(n, n+20)$. Prove that $\gcd(n, n+20) < \gcd(n, n+21)$.

C03. Let a and b be nonnegative integers. Prove that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

C04. An integer n is *perfect* if the sum of all of its positive divisors (including 1 and itself) is $2n$.

(a) Is 6 a perfect number? Give reasons for your answer.

(b) Is 7 a perfect number? Give reasons for your answer.

(c) Prove the following statement: If k is a positive integer and $2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is perfect.

C05. Let $a, b \in \mathbb{Z}$. Prove that $\gcd(a^n, b^n) = \gcd(a, b)^n$ for all $n \in \mathbb{N}$.