Solutions to J/STOW #4: Prime Numbers, Greatest Common Divisor, and Least Common Multiple

Zed Li

November 8, 2019

1. Prove that the fraction $\frac{4k+7}{7k+12}$ is reduced to lowest terms.

   Solution:

   Since $7(4k+7) - 4(7k+12) = 1$, Bézout's identity tells us that $4k+7$ and $7k+12$ are coprime, so $\frac{4k+7}{7k+12}$ is reduced to lowest terms.

2. Prove that the number of positive factors of positive integer n is less than $2\sqrt{n}$.

   Proof:

   Consider every positive factor d of n greater than $\sqrt{n}$. Let's say there are k of those. Then n/d is also a positive factor of n and $n/d < n/\sqrt{n} = \sqrt{n}$. So there are k positive factors of n less than $\sqrt{n}$, so $k < \sqrt{n}$. Then there are $2k < 2\sqrt{n}$ positive factors of n less than or greater than $\sqrt{n}$. If n is not a perfect square, $\sqrt{n}$ cannot be a factor of n, so there are $2k < 2\sqrt{n}$ positive factors of n in total. If n is a perfect square, then $\sqrt{n}$ is also a factor of n. Therefore, $k < \sqrt{n}$ means that $k \leq \sqrt{n} - 1$, so there are $2k + 1 = 2\sqrt{n} - 1 < 2\sqrt{n}$ positive factors of n. In conclusion, the number of positive factors of n is less than $2\sqrt{n}$.

3. Prove Bézout's general identity from the special identity. In other words, prove that there exist integers x, y such that $ax + by = \gcd(a, b)$ assuming we already know that there exist integers x, y such that $a'x + b'y = 1$ if a', b' are coprime.

   Proof:

   Let $a = a' \gcd(a, b)$ and $b = b' \gcd(a, b)$. Then $\gcd(a', b') = 1$, so there exist integers x, y such that $a'x + b'y = 1$. Therefore, $a'x \gcd(a, b) + b'y \gcd(a, b) = \gcd(a, b)$, i.e. $ax + by = \gcd(a, b)$.

4. Given that $a \mid bc$ for positive a, b, c, prove that: i) a is composite if $a > b, c$; ii) $\frac{bc}{a}$ is composite if $a < b, c$.

   Proof:

   i) If a is prime, then either $a \mid b$ or $a \mid c$, so $a \leq b$ or $a \leq c$, contradicting the fact that $a > b, c$. Hence, we must have a is composite.

ii) Let $\dfrac{bc}{a} = d$. Then $bc = ad$ so $d \mid bc$. Since $d = \dfrac{b}{a} \cdot c > c$ and $d = \dfrac{c}{a} \cdot b > b$, part i) tells us that d is composite, i.e. $\dfrac{bc}{a}$ is composite.

5. Given that $a + b \mid a^3 - b^3$ for positive integers a, b satisfying $a \neq b$ and $a + b$ is prime, prove that $a + b \mid ab$. *(SJAMMO 2019 Senior level Q1)*

   Proof:

   $a + b \mid a^3 - b^3 = (a - b)(a^2 + ab + b^2)$.

   But since $a - b, b - a < a + b$, meaning that $|a - b| < a + b$, and since $a \neq b$, we cannot have $a + b \mid a - b$.

   Since $a + b$ is prime, we must have $a + b \mid a^2 + ab + b^2$.

   Since $a^2 + ab + b^2 = (a + b)^2 - ab$, we get $a + b \mid ab$.

6. Prove that $2^{2^a} + 1$ and $2^{2^b} + 1$ are coprime for distinct non-negative a, b.

   Proof:

   WLOG (without loss of generality), assume that $a < b$. (The case for $b < a$ follows the same logic.) Then $a + 1 \leq b$ and hence $2^{a+1} \mid 2^b$. This means that

   $$2^{2^{a+1}} - 1 \mid 2^{2^b} - 1.$$

   Hence,

   $$\begin{aligned} \gcd\left(2^{2^{a+1}} - 1, 2^{2^b} + 1\right) &= \gcd\left(2^{2^{a+1}} - 1, \left(2^{2^b} - 1\right) + 2\right) \\ &= \gcd\left(2^{2^{a+1}} - 1, 2\right) \\ &= 1. \end{aligned}$$

   Now, $2^{2^a} + 1 \mid \left(2^{2^a} + 1\right)\left(2^{2^a} - 1\right) = 2^{2^{a+1}} - 1$, meaning that $\gcd\left(2^{2^a} + 1, 2^{2^b} + 1\right) = 1$.

7. Prove that positive integers a, b, c are mutually coprime if and only if

   $$\operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) = [\operatorname{lcm}(a, b, c)]^2.$$

   Proof 1: (Cristian)

   If a, b, c are mutually coprime, then

   $$\begin{aligned} \operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) &= (ab)(bc)(ca) \\ &= (abc)^2 \\ &= [\operatorname{lcm}(a, b, c)]^2. \end{aligned}$$

   On the other hand, if

   $$\operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) = [\operatorname{lcm}(a, b, c)]^2,$$

let the prime factorizations of a, b, c be $p_1^{\alpha_1} p_2^{\alpha_2} \ldots$, $p_1^{\beta_1} p_2^{\beta_2} \ldots$, $p_1^{\gamma_1} p_2^{\gamma_2} \ldots$ where $p_1, p_2, \ldots$ are all prime numbers in ascending order and all exponents are non-negative integers. Then, for each integer $k \geq 1$, we have

$$\max(\alpha_k, \beta_k) + \max(\beta_k, \gamma_k) + \max(\gamma_k, \alpha_k) = 2\max(\alpha_k, \beta_k, \gamma_k).$$

WLOG, let $\alpha_k \geq \beta_k \geq \gamma_k$. Then

$$\begin{aligned} \alpha_k + \beta_k + \alpha_k &= 2\alpha_k \\ \beta_k &= 0. \end{aligned}$$

Since $\beta_k \geq \gamma_k$, we also have $\gamma_k = 0$. So $\min(\alpha_k, \beta_k) = \min(\beta_k, \gamma_k) = \min(\gamma_k, \alpha_k) = 0$ for all $k \geq 1$, i.e. a, b, c are mutually coprime.

Proof 2 (Zed):

If a, b, c are mutually coprime, then

$$\begin{aligned} \operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) &= (ab)(bc)(ca) \\ &= (abc)^2 \\ &= [\operatorname{lcm}(a, b, c)]^2. \end{aligned}$$

On the other hand, if

$$\operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) = [\operatorname{lcm}(a, b, c)]^2,$$

then

$$\begin{aligned} \frac{(ab)(bc)(ca)}{\gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(c, a)} &= [\operatorname{lcm}(\operatorname{lcm}(a, b), c)]^2 \\ \frac{a^2b^2c^2}{\gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(c, a)} &= \frac{[\operatorname{lcm}(a, b)]^2 c^2}{[\gcd(\operatorname{lcm}(a, b), c)]^2} \\ \frac{a^2b^2c^2}{\gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(c, a)} &= \frac{a^2b^2c^2}{[\gcd(a, b)]^2[\gcd(\operatorname{lcm}(a, b), c)]^2} \\ [\gcd(a, b)]^2[\gcd(\operatorname{lcm}(a, b), c)]^2 &= \gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(c, a) \\ \gcd(a, b) \cdot [\gcd(\operatorname{lcm}(a, b), c)]^2 &= \gcd(b, c) \cdot \gcd(c, a) \qquad (*) \end{aligned}$$

Now, since $\gcd(b, c) \mid b \mid \operatorname{lcm}(a, b)$ and $\gcd(b, c) \mid c$, we must have $\gcd(b, c) \mid \gcd(\operatorname{lcm}(a, b), c)$. Hence, $\gcd(\operatorname{lcm}(a, b), c) \geq \gcd(b, c)$. Similarly, $\gcd(\operatorname{lcm}(a, b), c) \geq \gcd(a, c)$. Therefore, $[\gcd(\operatorname{lcm}(a, b), c)]^2 \geq \gcd(b, c) \cdot \gcd(c, a)$. Plugging this into $(*)$ gives us $\gcd(a, b) \leq 1$, so we must have $\gcd(a, b) = 1$. Due to symmetry, we also have $\gcd(b, c) = \gcd(c, a) = 1$, so a, b, c are mutually coprime.

In conclusion, positive integers a, b, c are mutually coprime if and only if

$$\operatorname{lcm}(a, b) \cdot \operatorname{lcm}(b, c) \cdot \operatorname{lcm}(c, a) = [\operatorname{lcm}(a, b, c)]^2.$$

8. The Fibonacci sequence F_n is defined such that $F_0 = 0, F_1 = 1$ and $F_{k+2} = F_{k+1} + F_k$ for $k \geq 0$.

   (a) Prove that F_k and F_{k+1} are coprime for all $k \geq 0$.

   (b) Prove that $F_m \mid F_n$ if and only if $m \mid n$.

   Proof:

   (a) We prove this by induction. Obviously, $\gcd(F_0, F_1) = \gcd(0, 1) = 1$. Assume $\gcd(F_k, F_{k+1}) = 1$ for some $k \geq 0$. Then $\gcd(F_{k+1}, F_{k+2}) = \gcd(F_{k+1}, F_{k+1}+F_k) = \gcd(F_{k+1}, F_k) = 1$, hence completing the proof for $\gcd(F_k, F_{k+1}) = 1$ for all $k \geq 0$.

   (b) The case for $m = 1$ is obvious since $F_1 \mid F_n$ and $1 \mid n$ for all n.
   Now, let $m > 1$ since $m \neq 0$. Obviously, $F_m \mid F_0 = 0$. Now we need to prove that $F_m \mid F_{qm}$ while $F_m \nmid F_{qm-r}$ ($q \geq 1$, $0 < r < m$). We prove this by induction on q.
   Note that $F_m \nmid F_{m-r}$ for $0 < r < m$ since in that case $0 < F_{m-r} < F_m$.
   For the base case, we have $F_m \mid F_0 = 0$ when $q = 0$.
   Assume that for some $q \geq 0$, we have that $F_m \mid F_{qm}$. Consider the sequences $a_k = (F_k F_{qm+1} \bmod F_m)$ and $b_k = (F_k \bmod F_m)$ for $k \geq 0$.
   Note that the sequence a_k satisfies $a_0 = 0$, $a_1 = (F_{qm+1} \bmod F_m)$, and

$$\begin{aligned} a_{k+2} &= (F_{k+2} F_{qm+1} \bmod F_m) \\ &= \big((F_{k+1} + F_k) F_{qm+1} \bmod F_m\big) \\ &= \big((a_{k+1} + a_k) \bmod F_m\big) \end{aligned}$$

   for $k \geq 0$; on the other hand, sequence b_k satisfies $b_{qm} = (F_{qm} \bmod F_m) = 0$, $b_{qm+1} = (F_{qm+1} \bmod F_m)$, and

$$\begin{aligned} b_{k+2} &= (F_{k+2} \bmod F_m) \\ &= \big((F_{k+1} + F_k) \bmod F_m\big) \\ &= \big((b_{k+1} + b_k) \bmod F_m\big) \end{aligned}$$

   for $k \geq 0$. Now, since $a_0 = b_{qm}$, $a_1 = b_{qm+1}$, and the recursive definitions for the sequences a_k and b_k are the same, we conclude that $a_k = b_{qm+k}$ for all $k \geq 0$.
   Hence, we have

$$(F_{(q+1)m} \bmod F_m) = b_{qm+m} = a_m = (F_m F_{qm+1} \bmod F_m) = 0,$$

   i.e. $F_m \mid F_{(q+1)m}$. Furthermore, for $0 < r < m$, note that $F_m \mid F_{qm}$ and $\gcd(F_{qm}, F_{qm+1}) = 1$ (from part a) result in $\gcd(F_m, F_{qm+1}) = 1$, so $F_m \nmid F_{m-r}$ tells us that $F_m \nmid F_{m-r} F_{qm+1}$. Hence,

$$(F_{(q+1)m-r} \bmod F_m) = b_{qm+m-r} = a_{m-r} = (F_{m-r} F_{qm+1} \bmod F_m) \neq 0,$$

   i.e. $F_m \nmid F_{(q+1)m-r}$ for $0 < r < m$.
   By induction, $F_m \mid F_{qm}$ while $F_m \nmid F_{qm-r}$ ($q \geq 1$, $0 < r < m$).
   In conclusion, $F_m \mid F_n$ if and only if $m \mid n$.