Math 303
Proof Portfolio

Ellie Miranda

May 6, 2025

Theorem 1. *A positive integer is a multiple of 3 if and only if the sum of its digits is a multiple of 3.*

Proof. Let n be a positive integer that is a multiple of 3, and let s be the sum of its digits. Then, n can be written as $n = d_k 10^k + d_{k-1}10^{k-1} + ... + d_1 10^1 + d_0 10^0$, where the values d_i are integers between 0 and 9. Similarly, the sum of n's digits, s, is defined as $s = d_k + d_{k-1} + ... + d_1 + d_0$. Since $10^k \equiv 1^k \equiv 1 (\text{mod } 3)$, and n is a multiple of 3, we can reduce the equation mod 3 to get $n \equiv d_k + d_{k-1} + ... + d_1 + d_0$. Thus, $s \equiv n (\text{mod } 3)$. Further, because n is a multiple of 3, then $s \equiv n \equiv 0 (\text{mod } 3)$. Therefore, the sum of the digits of a positive integer n that is a multiple of 3 must also be a multiple of 3. In the other direction, if s, the sum of the digits of a positive integer n, is a multiple of 3, then $s \equiv 0 (\text{mod } 3)$. Since we already found that $s \equiv n (\text{mod } 3)$, we can say that $n \equiv 0 (\text{mod } 3)$ as well. Thus, n must also be a multiple of 3. Therefore, we can conclude that a positive integer is a multiple of 3 if and only if the sum of its digits is a multiple of 3. □

Theorem 2. *Let a, b, q, r be positive integers such that $a = bq + r$. Then $GCD(a, b) = GCD(b, r)$.*

Proof. Let $c = \text{GCD}(a, b)$. Then, by definition, $c|a$ and $c|b$. Next, since $a = bq + r$, we have $r = a - bq$. Then, since $c|a$ and $c|b$, we know that $c|(a - bq) \implies c|r$. So, we have that $c|b$ and $c|r$, which gives us $\text{GCD}(b, r) \geq c \implies \text{GCD}(b, r) \geq \text{GCD}(a, b)$. Similarly, let $d = \text{GCD}(b, r)$. Then, by definition, $d|b$ and $d|r$. Then, since $a = bq + r$, and $d|b$ and $d|r$, we know that $d|a$ as well. So, we have that $d|a$ and $d|b$, which gives us $\text{GCD}(a, b) \geq d \implies \text{GCD}(a, b) \geq \text{GCD}(b, r)$. Since $\text{GCD}(b, r) \geq \text{GCD}(a, b)$ and $\text{GCD}(a, b) \geq \text{GCD}(b, r)$, we have that $\text{GCD}(a, b) = \text{GCD}(b, r)$. □

Theorem 3. *Let $m_1, m_2, ..., m_k$ be a set of pairwise relatively prime positive integers, and let $a_1, a_2, ..., a_k \in \mathbb{Z}$. Then the system of congruences below has infinitely many integer solutions.*

$$x \equiv a_1 (mod\ m_1)$$

$$x \equiv a_2 (mod\ m_2)$$

$$...$$

$$x \equiv a_k (mod\ m_k)$$

Proof. We will prove this theorem by induction. For the base case, let $x \equiv a(\text{mod } m)$ and $x \equiv b(\text{mod } n)$, with $\text{GCD}(m, n) = 1$. Then, $x = a + mr = b + ns$, for $r, s \in \mathbb{Z}$, which gives us $mr - ns = b - a$. Since $\text{GCD}(m, n) = 1$, and $1 \mid (b - a)$, this Linear Diophantine Equation has solutions for $r, s \in \mathbb{Z}$. Then, we can find x to solve the system

$$x \equiv x_0$$

$$x \equiv x_0 (\text{mod } mn)$$

For the induction step, suppose that $k = n$, where the system of congruences $x \equiv a_1(\text{mod } m_1)$, $x \equiv a_2(\text{mod } m_2)$, ..., $x \equiv a_n(\text{mod } m_n)$ has infinitely many integer solutions. Then, there exists an x_0 in which $x = x_0 + my$, where $m = m_1 \cdot m_2 \cdot ... \cdot m_n$. Next, we say that $x \equiv a_{n+1}(\text{mod } m_{n+1})$. Then, we can substitute $x = x_0 + my$ into this equivalence so that $x_0 + my \equiv a_{n+1}(\text{mod } m_{n+1})$, which can be rearranged as $my \equiv a_{n+1}(\text{mod } m_{n+1}) - x_0$. Since m and m_{n+1} are relatively prime, due to the fact that $m_1, m_2, ..., m_k$ are pairwise relatively prime, there exists an integer solution for y. Thus, there are infinitely many solutions for x in the equation $x = x_0 + my$, where y is a solution. Therefore, by induction, the system of congruences has infinitely many solutions for any k. □

Theorem 4. *Every primitive Pythagorean triple contains exactly one number that is a multiple of 5.*

Proof. Consider the possibilities for $a^2, b^2, c^2 \pmod 5$.

$$a \equiv 0(\text{mod } 5) \implies a^2 \equiv 0(\text{mod } 5)$$

$$a \equiv 1(\text{mod } 5) \implies a^2 \equiv 1(\text{mod } 5)$$

$$a \equiv 2(\text{mod } 5) \implies a^2 \equiv 4(\text{mod } 5)$$

$$a \equiv 3(\text{mod } 5) \implies a^2 \equiv 4(\text{mod } 5)$$

$$a \equiv 4(\text{mod } 5) \implies a^2 \equiv 1(\text{mod } 5)$$

Then, every perfect square is equivalent to either 0, 1, or 4 (mod 5). Next, we want to argue that one of $a, b, c \equiv 0(\text{mod } 5)$. If none are, then there are six cases:
Case 1: $a = b = 1, c = 1$,

$$a^2 + b^2 = c^2 \implies 1 + 1 \equiv 1(\text{mod } 5) \implies 2 \not\equiv 1(\text{mod } 5)$$

Case 2: $a = b = 1, c = 4$,

$$a^2 + b^2 = c^2 \implies 1 + 1 \equiv 4(\text{mod } 5) \implies 2 \not\equiv 1(\text{mod } 5)$$

Case 3: $a = b = 4, c = 1$,

$$a^2 + b^2 = c^2 \implies 4 + 4 \equiv 1 (\text{mod } 5) \implies 3 \not\equiv 1 (\text{mod } 5)$$

Case 4: $a = b = 4, c = 4$,

$$a^2 + b^2 = c^2 \implies 4 + 4 \equiv 4 (\text{mod } 5) \implies 3 \not\equiv 1 (\text{mod } 5)$$

Case 5: $a, b = 4, 1, c = 1$,

$$a^2 + b^2 = c^2 \implies 4 + 1 \equiv 1 (\text{mod } 5) \implies 0 \not\equiv 1 (\text{mod } 5)$$

Case 6: $a, b = 4, 1, c = 4$,

$$a^2 + b^2 = c^2 \implies 4 + 1 \equiv 4 (\text{mod } 5) \implies 0 \not\equiv 1 (\text{mod } 5)$$

In each of these cases we have reached a contradiction, so at least one of a, b, c is a multiple of 5. □

Theorem 5. *There are infinitely many rational points on the circle $x^2 + y^2 = 5$.*

Proof. First, note that (1,2) is a rational point on the circle $x^2 + y^2 = 5$. Then, the line $y = mx + (2 - m)$ intersects the circle at that point. If m is rational, then the point (x, y) at the intersection of the line and the circle must also be a rational point. Next, we can substitute the equation of the line into the equation of the circle to find x in terms of m.

$$x^2 + y^2 = 5 \implies x^2 + (mx + (2 - m))^2 = 5$$

$$\implies x^2 + m^2x^2 + 2mx(2 - m) + 4 - 4m + m^2 = 5$$

$$\implies (1 + m^2)x^2 + (4m - 2m^2)x + (m^2 - 4m - 1) = 0$$

$$\implies (x - 1)((1 + m^2)x - (m^2 - 4m - 1)) = 0$$

$$\implies x = 1 \quad \text{and} \quad x = \frac{m^2 - 4m - 1}{1 + m^2}$$

Then, substitute x back into the equation for the line to find y in terms of m.

$$y = mx + (2 - m)$$

$$\implies y = m(\frac{m^2 - 4m - 1}{1 + m^2}) + (2 - m)$$

$$\implies y = \frac{m^3 - 4m^2 - m}{1 + m^2} + \frac{2 + 2m^2 - m - m^3}{1 + m^2}$$

$$\implies y = \frac{-2m^2 - 2m + 2}{1 + m^2}$$

So, for any rational number m, the point $(\frac{m^2-4m-1}{1+m^2}, \frac{-2m^2-2m+2}{1+m^2})$ will be a rational point on the circle $x^2 + y^2 = 5$. □

Theorem 6. *If m and n are relatively prime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. To prove this statement, we need to show that there is a function that exists between two sets, S and T (where S has $\varphi(mn)$ elements and T has $\varphi(m)\varphi(n)$ elements) in which the function is a bijection. Since m and n are relatively prime, $\text{GCD}(mn) = 1$. Then, let

$$S = \{x \in \mathbb{Z}_{mn} : \text{GCD}(x, mn) = 1\}$$

$$T = \{(y, z) \in \mathbb{Z}_m \oplus \mathbb{Z}_n : \text{GCD}(y, m) = \text{GCD}(z, n) = 1\}$$

Next, define the function $f : S \to T$ as

$$f(x) = (x \pmod m, x \pmod n)$$

First, we must show that the function is well-defined. Since $\text{GCD}(x, mn) = 1$, that means that $\text{GCD}(x, m) = 1$ and $\text{GCD}(x, n) = 1$. Next, we can define that $y \equiv x(\text{mod } m)$ and $z \equiv x(\text{mod } n)$. So, $\text{GCD}(y, m) = \text{GCD}(z, n) = 1$, which means that f is well-defined.
Next, we must show that the function is one-to-one. If $f(x_1) = f(x_2)$, then

$$f(x_1) = (x_1 \pmod m, x_1 \pmod n) \text{ and } f(x_2) = (x_2 \pmod m, x_2 \pmod n)$$

$$\implies x_1 = x_2(\text{mod } m) \text{ and } x_1 = x_2(\text{mod } n)$$

Then, since $\text{GCD}(m, n{=}1)$, $x_1 = x_2(\text{mod } mn)$. Thus, f is a one-to-one function.
Lastly, we must show that the function is onto. If $(x, y) \in T$, then $x \in \mathbb{Z}_m$ and $y \in \mathbb{Z}_n$, with $\text{GCD}(x, m) = 1$ and $\text{GCD}(y, n) = 1$. Then, by the definition of surjection, there exists an a in $\mathbb{Z}_{mn}$ so that $a \equiv x(\text{mod } m)$ and $a \equiv y(\text{mod } n)$. Next, we can determine that $\text{GCD}(a, m) = 1$ and $\text{GCD}(a, n) = 1$. Since m and n are relatively prime, then $\text{GCD}(a, mn) = 1$, so $a \in S$. Thus, $f(a) = (x, y)$, and so we have shown f is onto.
So, since we have shown that f is well-defined, one-to-one, and onto, we have proven that f is a bijection between the sets S and T. Thus, since a bijection exists between these two sets, the sets must be the same size. Therefore, $\varphi(mn) = \varphi(m)\varphi(n)$. □

Theorem 7. *Prove the rule that states that if p is a prime number that is congruent to 7 modulo 8, then $(\frac{2}{p}) = 1$.*

Proof. Suppose p is a prime number that is congruent to 7 (mod 8). We will show that $(\frac{2}{p}) = 1$. Since $p \equiv 7(\text{mod } 8)$, we can write $p = 8k + 7$, for some integer k. Then,

$$p = 8k + 7 \implies \frac{p-7}{2} = 4k \implies \frac{p-1}{2} = 4k + 3$$

Next, according to Gauss's Criterion, for any odd prime p and integer a that is not a multiple of p we have $(\frac{a}{p}) = (-1)^{\mu(a,p)}$ where $\mu(a, p)$ is the number of integers in the set $\{\ a, 2a, 3a, ..., \frac{p-1}{2}a\}$ whose least positive residues mod p are greater than $\frac{p}{2}$. In this case, $(\frac{2}{p}) = (-1)^{\mu(2,p)}$ where $\mu(2, p)$ is the number of integers in the set $\{\ 2, 4, 6, ..., 2(4k + 3)\}$ =

$\{ 2, 4, 6, ..., 8k+6\}$ whose least positive residues mod p are greater than $\frac{p}{2}$. So, this set has $4k+3$ elements. When reduced mod p, the number of integers that are greater than $\frac{p}{2}$ is even. Then, we have that $(\frac{2}{p}) = (-1)^{\mu(2,p)} = (-1)^{even} = 1$. Thus, $(\frac{2}{p}) = 1$ when $p \equiv 7 (\text{mod } 8)$. □

Theorem 8. *The elliptic curve $y^2 = x^3 + x^2 + 4$ has infinitely many rational points.*

Proof. We will prove that there are infinitely many rational points on the curve $y^2 = x^3 + x^2 + 4$ by showing that one point on the curve, when repeatedly added to itself, generates an infinite number of distinct rational points. Let $P = (0, 2)$ be a rational point on the curve. We can compute $2P$ by first finding the slope of the tangent line at P. To find the slope of the tangent line, we differentiate both sides of the equation of the curve to get $\frac{d}{dx}(y^2) = \frac{d}{dx}(x^3 + x^2 + 4) \implies \frac{dy}{dx} = \frac{3x^2+2x}{2y}$. Then, substituting in the x- and y-values, we get $\frac{3(0)^2+2(0)}{2(2)} = \frac{0}{4} = 0$ So, the equation for the tangent line is $y = 2$. Substituting this into the equation of the curve, we can find the coordinates of the third point of intersection by

$$2^2 = x^3 + x^2 + 4 \implies 0 = x^3 + x^2 \implies 0 = x^2(x+1) \implies x = 0, x = -1$$

So, we have the point (-1,2), which when reflected over the x-axis, is $(-1, -2) = 2P$. We can further calculate $3P$ and $4P$ using the same method to get $3P = (16, -66)$ and $4P = (\frac{17}{16}, \frac{161}{64})$. Each of these points have unique rational coordinates, and each new multiple of P gives a new, more complex point without any signs of repeating or returning to the identity. So, we have that P has infinite order. Since the group of rational points on an elliptic curve forms an abelian group under addition, and we have found one point of infinite order, we know that the group is infinite. Thus, the elliptic curve $y^2 = x^3 + x^2 + 4$ has infinitely many rational points. □