Proofs Involving Divisibility

July 15, 2009

Prove that $8|n^2-1$ for all odd integers n.

Proof Let n be an arbitrary odd integer. By definition of odd, $n = 2k+1$ for some $k \in \mathbb{Z}$. By substitution, we can say that $n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k$. By factoring, we obtain the product $4k(k+1) = 4[k(k+1)]$. Since the product of two consecutive integers is even, we can say that $4[k(k+1)] = 4(2z) = 8z$ for some $z \in \mathbb{Z}$. Since $n^2 - 1 = 8z$, we have proven that $8|n^2-1$ for all odd integers n as desired. ■

Prove that if $a|b$ and $b|c$, then $a|c$.

Proof Since $a|b$, then we can say that $b = ak$ for some $k \in \mathbb{Z}$. Since $b|c$, then we can say that $c = bm$ for some $m \in \mathbb{Z}$. By substitution, we can say that $c = (ak)m = a(km) = aj$ for some $j \in \mathbb{Z}$. Since $c = aj$, then we have proven $a|c$ as desired. ■

Prove that if $a|b$ and $b|c$, then $a|bx+cy$, where $x, y \in \mathbb{Z}$.

Proof Since $a|b$, then we can say that $b = ak$ for some $k \in \mathbb{Z}$. Since $b|c$, then we can say that $c = bm$ for some $m \in \mathbb{Z}$. By substitution, we can say that $bx + cy = (ak)x + (bm)y = akx + (ak)my = akx + akmy = a(kx + kmy)$. By letting $j = kx + kmy$, we see that $bx + cy = aj$ for some $j \in \mathbb{Z}$. Hence, we have proven that $a|bx + cy$ as desired. ■

Prove that $3|n^3 - n$ for all $n \in \mathbb{Z}$.

Proof We can factor $n^3 - n$ to obtain $n(n^2-1) = n(n-1)(n+1)$. If we rewrite this as $(n-1)n(n+1)$, then it is evident that we have the product of three consecutive integers. Obviously, one of these numbers must be divisible by 3. Thus, we can say that $n = 3m$ for some $m \in \mathbb{Z}$. By substitution, $(3m-1)3m(3m+1) = 3[(3m-1)m(3m+1)]$. By letting $z = (3m-1)m(3m+1)$, then we have that $n^3 - n = 3z$ for some $z \in \mathbb{Z}$. Therefore, $3|n^3 - n$ for all $n \in \mathbb{Z}$. ■

Prove that if $a|b$, then $a^n|b^n$.

Proof Since $a|b$, then we can say that $b = ak$ for some $k \in \mathbb{Z}$. By substitution, we obtain $b^n = (ak)^n = a^n k^n$. By letting $l = k^n$, we see that $b^n = a^n l$ for some $l \in \mathbb{Z}$. Hence, we have proven that $a^n|b^n$ as desired. ■

***Quotient-Remainder Theorem*: Let n and d be positive integers. Then there exists unique integers q and r such that $n = dq + r$ where $0 \leq r < d$ with r as the remainder, d as the divisor, and q as the quotient.**

Use the Quotient-Remainder Theorem with $d = 3$ to prove that the square of any integer has the form $3k$ or $3k + 1$ for some $k \in \mathbb{Z}$.

Proof

Let n, q, and r be non-negative integers. Using the Quotient-Remainder Theorem with $d = 3$ we see that $0 \leq r \leq 2$, implying that we have three possible cases.

Case 1: Suppose that $r = 0$. Then $n = 3q$ for some $q \in \mathbb{Z}^+$. By substitution, we see that $n^2 = (3q)^2 = 9q^2 = 3(3q^2)$. By letting $k = 3q^2$, we see that $n^2 = 3k$ for some $k \in \mathbb{Z}$ when $r = 0$.

Case 2: Suppose that $r = 1$. Then $n = 3q + 1$ for some $q \in \mathbb{Z}^+$. By substitution, we see that $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$. By letting $k = 3q^2 + 2q$, we see that $n^2 = 3k + 1$ for some $k \in \mathbb{Z}$ when $r = 1$.

Case 3: Suppose that $r = 2$. Then $n = 3q + 2$ for some $q \in \mathbb{Z}^+$. By substitution, we see that $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1$. By letting $k = 3q^2 + 4q + 1$, we see that $n^2 = 3k + 1$ for some $k \in \mathbb{Z}$ when $r = 2$.

By the three cases, we have proven that the square of any integer has the form $3k$ or $3k + 1$. ■

Use the Quotient-Remainder Theorem with $d = 3$ to prove that the product of two consecutive integers has the form $3k$ or $3k + 2$ for some $k \in \mathbb{Z}$.

Proof

Let n, q, and r be non-negative integers. Using the Quotient-Remainder Theorem with $d = 3$ we see that $0 \leq r \leq 2$, implying that we have three possible cases.

Case 1: Suppose that $r = 0$. Then $n = 3q$ for some $q \in \mathbb{Z}^+$. By substitution, we see that $n(n + 1) = 3q(3q + 1) = 9q^2 + 3q = 3(3q^2 + q)$. By letting $k = 3q^2 + q$, we see that $n(n + 1) = 3k$ for some $k \in \mathbb{Z}$ when $r = 0$.

Case 2: Suppose that $r = 1$. Then $n = 3q + 1$ for some $q \in \mathbb{Z}^+$. By substitution, we see that $n(n + 1) = (3q + 1)(3q + 2) = 9q^2 + 6q + 3q + 2 = 9q^2 + 9q + 2 = 3(3q^2 + 3q) + 2$. By letting $k = 3q^2 + 3q$, we see that $n(n + 1) = 3k + 2$ for some $k \in \mathbb{Z}$ when $r = 1$.

Case 3: Suppose that $r = 2$. Then $n = 3q + 2$ for some $q \in \mathbb{Z}^+$. By substitution, we see that $n(n + 1) = (3q + 2)(3q + 3) = 9q^2 + 9q + 6q + 6 = 9q^2 + 15q + 6 = 3(3q^2 + 5q + 2)$. By letting $k = 3q^2 + 5q + 2$, we see that $n(n + 1) = 3k$ for some $k \in \mathbb{Z}$ when $r = 2$.

By the three cases, we have proven that the product of two consecutive integers has the form $3k$ or $3k + 2$. ■

Let x be an integer. Prove that $x^2 - 2$ is not divisible by 4.

Proof

By the Quotient-Remiander Theorem, $x^2 - 2 = 4q + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < 4$. If $x^2 - 2$ is not divisible by 4, then $r \neq 0$, implying that for some $z \in \mathbb{Z}$, $x^2 - 2$ has the form $4q + 1$, $4q + 2$, or $4q + 3$. To show this, we must consider two cases, one with x being even, and the other with x being odd.

Case 1: Suppose that x is even. By definition of even, we can say that $x = 2p$ for some $p \in \mathbb{Z}$. By substitution, we see that $x^2 - 2 = (2p)^2 - 2 = 4p^2 - 2 = 4p^2 - 4 + 2 = 4(p^2 - 1) + 2$. By letting $q = p^2 - 1$, we see that $x^2 - 2 = 4q + 2$ for some $q \in \mathbb{Z}$ when x is odd.

Case 2: Suppose that x is odd. By definition of even, we can say that $x = 2p + 1$ for some $p \in \mathbb{Z}$. By substitution, we see that $x^2 - 2 = (2p + 1)^2 - 2 = 4p^2 + 4p + 1 - 2 = 4p^2 + 4p - 1 = 4p^2 + 4p - 4 + 3 = 4(p^2 + p - 1) + 3$. By letting $q = p^2 + p - 1$, we see that $x^2 - 2 = 4q + 3$ for some $q \in \mathbb{Z}$ when x is even.

In either case, we see that $x^2 - 2 \neq 4q$ for any $x \in \mathbb{Z}$. Hence, we have proven that $x^2 - 2$ is not divisible by 4. ■