Hammack Exercises - Chapter 7

FungusDesu

September 9st 2024

1 Preface

i dont really have anything to say

2 Non-Conditional Statements

Proposition 7.1α. *Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x + 5$ is odd.*

Proof. We first show that if x is even, then $3x + 5$ is odd. Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Thus $3x + 5 = 2(3k + 2) + 1$, which is odd by definition of an odd number.

Conversely, suppose to the contrapositive that x is odd. Then $x = 2l + 1$ for some $l \in \mathbb{Z}$. Thus $3x + 5 = 2(3l + 3)$, which is even by definition of an even number.

Proposition 7.2. *Suppose $x \in \mathbb{Z}$. Then x is odd if and only if $3x + 6$ is odd.*

Proof. We first show that if x is odd, then $3x+6$ is odd. Suppose x is odd. Then $x = 2k+1$ for some $k \in \mathbb{Z}$. Thus $3x + 6 = 2(3k + 4) + 1$, which is odd by definition of an odd number.

Conversely, suppose to the contrapositive that x is even. Then $x = 2l$ for some $l \in \mathbb{Z}$. Thus $3x + 6 = 2(3l + 3)$, which is even by definition of an even number.

Proposition 7.3. *Given an integer a, then $a^3 + a^2 + a$ is even if and only if a is even.*

Proof. We first show that if $a^3 + a^2 + a$ is even, then a is even. Suppose to the contrapositive that a is odd; we wish to show $a^3 + a^2 + a$ is odd, or $a(a^2 + a + 1)$ is odd. Since a is odd, we have $a^2 + a + 1$ is odd (the square of a is odd, the sum of two odd numbers is an even number, which becomes odd again when added by 1). The product of two odd numbers is odd itself, thus $a(a^2 + a + 1)$ is odd.

Conversely, suppose a is even. Regardless of the parity of $a^2 + a + 1$, their product will always be even. Thus the proof is completed.

Proposition 7.4. *Given an integer a, then $a^2 + 4a + 5$ is odd if and only if a is even.*

Proof. We first show that if $a^2 + 4a + 5$ is odd, then a is even. Suppose to the contrapositive that a is odd. Notice that a^2 is odd and $4a$ is even, thus their sum is an odd number (the sum of two numbers with opposite parity is an odd number). The sum of two odd numbers is an even number, thus $a^2 + 4a + 5$ is even.

Conversely, suppose a is even. By the same line of reasoning, we can deduce that $a^2 + 4a + 5$ is odd (a^2 is even, $4a$ is even, 5 is odd). The proof is completed.

Proposition 7.5. *An integer a is odd if and only if a^3 is odd.*

Proof. We first show that if a is odd, then a^3 is odd. Suppose a is odd. Then $a = 2x + 1$ for some $x \in \mathbb{Z}$. Thus $a^3 = 8x^3 + 12x^2 + 6x + 1 = 2(4x^3 + 6x^2 + 3x) + 1$. Because $4x^3 + 6x^2 + 3x \in \mathbb{Z}$, we have a^3 is odd by definition of an odd number.

Conversely, suppose to the contrapositive that a is even. Then $a = 2y$ for some $y \in \mathbb{Z}$. Thus $a^3 = 8y^3 = 2(4y^3)$. Because $4y^3 \in \mathbb{Z}$, we have a^3 is even by definition of an odd number. The proof is completed.

Proposition 7.6. *Suppose $x, y \in \mathbb{R}$. Then $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$.*

Proof. ($\Longleftarrow$) Suppose $y = x^2$ or $y = -x$; the equation is true if $x = y = 0$. We divide into the following two cases for non-zero x and y.

Case 1. If $y = x^2$, then

$$\begin{aligned} x^2 &= y \\ x^2y &= y^2 \\ x^3 + x^2y &= y^2 + x^3 \\ x^3 + x^2y &= y^2 + xy. \end{aligned}$$

Case 2. If $y = -x$, then

$$\begin{aligned} y &= -x \\ y(x^2 - y) &= -x(x^2 - y) \\ x^2y - y^2 &= -x^3 + xy \\ x^3 + x^2y &= y^2 + xy. \end{aligned}$$

The cases have shown that $x^3 + x^2y = y^2 + xy$ if $y = x^2$ or $y = -x$.

($\Longrightarrow$) Suppose $x^3 + x^2y = y^2 + xy$; this implies $(x + y)(x^2 - y) = 0$. For this equality to hold, either $x + y = 0$ or $x^2 - y = 0$. Thus $y = -x$ and $y = x^2$. The proof is completed.

Proposition 7.7. *Suppose $x, y \in \mathbb{R}$. Then $(x + y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.*

Proof. ($\Longrightarrow$) Suppose $(x + y)^2 = x^2 + y^2$ for some $x, y \in \mathbb{R}$. Then $x^2 + 2xy + y^2 = x^2 + y^2$ implies $xy = 0$. The equation holds if and only if $x = 0$ or $y = 0$.

($\Longleftarrow$) Suppose $x = 0$. Then $(x + y)^2 = x^2 + y^2$ implies $y^2 = y^2$. The same line of reasoning applies when $y = 0$. Thus the proof is completed.

Proposition 7.8. *Suppose $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{10}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.*

Proof. ($\Longrightarrow$) Suppose $a \equiv b \pmod{10}$ for some $a, b \in \mathbb{Z}$. Then $10 \mid (a - b)$. Thus there exists x such that $a - b = 10x$; because $10x = 2 \cdot 5x = 5 \cdot 2x$, we have $2 \mid (a - b)$ and $5 \mid (a - b)$ consequently. Therefore $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.

($\Longleftarrow$) Suppose $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$. Then there exists m, n such that

$$(a - b) = 2m = 5n. \tag{1}$$

Thus $5 \mid 2m$, which implies $5 \mid m$ by Proposition 4.8. As such, there exists $x \in \mathbb{Z}$ such that $m = 5x$. Substituting it into (1) yields $(a - b) = 10x$. We have shown that $10 \mid (a - b)$, and consequently $a \equiv b \pmod{10}$. The proof is completed.

Proposition 7.9. *Suppose $a \in \mathbb{Z}$. Prove that $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.*

Proof. ($\Longrightarrow$) Suppose $14 \mid a$. Then $a = 14x$ for some $x \in \mathbb{Z}$. Note that $a = 14x = 7 \cdot (2x) = 2 \cdot (7x)$; thus $7 \mid a$ and $2 \mid a$.

($\Longleftarrow$) Suppose $7 \mid a$ and $2 \mid a$. Then there exists $m, n \in \mathbb{Z}$ such that

$$a = 7m = 2n. \tag{2}$$

Thus $7 \mid 2n$ implies $2n = 7x$ for some $x \in \mathbb{Z}$. The left hand side is an even number, so the right hand side must be as well. Thus x is a multiple of 2, so $\frac{x}{2} \in \mathbb{Z}$. Let $k = \frac{x}{2}$; we have $n = 7k$. Substituting this into (2), we get $a = 14k$. Thus $14 \mid a$. The proof is completed.

Proposition 7.10. *If $a \in \mathbb{Z}$, then $a^3 \equiv a \pmod 3$.*

Proof. Consider the expression $a^3 - a$ for some integer a. We can rewrite it into $(a-1)a(a+1)$, which is the product of three consecutive integers. Note that no matter what three numbers we pick, there will always be a multiple of 3. Thus their product will also be, and we are done.

Proposition 7.11. *Suppose $a, b \in \mathbb{Z}$. Prove that $(a-3)b^2$ is even if and only if a is odd or b is even.*

Proof. ($\Longrightarrow$) Suppose to the contrapositive that a is even and b is odd. Then there exist $m, n \in \mathbb{Z}$ such that $a = 2m$ and $b = 2n+1$. Thus $(a-3)b^2 = (2m-3)(2n+1)^2 = 2(4mn^2 + 4mn + m - 6n^2 - 6n - 2) + 1$, which is odd.

($\Longleftarrow$) Suppose that a is odd or b is even. We divide into the following two cases:

Case 1. If a is odd, then $a = 2m+1$ for some $m \in \mathbb{Z}$. Thus $(a-3)b^2 = (2m-2)b^2 = 2(m-1)b^2$, which is even.

Case 2. If b is even, then $b = 2n$ for some $n \in \mathbb{Z}$. Thus $(a-3)b^2 = 4n^2(a-3)$, which is even.

The proof is completed.

Proposition 7.12. *There exists a positive real number x for which $x^2 < \sqrt{x}$.*

Proof. Consider $x = \frac{1}{4}$. Note that $x^2 = \frac{1}{16} < \sqrt{x} = \frac{1}{2}$. Thus $x = \frac{1}{4}$ is a positive real number that satisfies $x^2 < \sqrt{x}$.

Proposition 7.13. *Suppose $a, b \in \mathbb{Z}$. If $a+b$ is odd, then $a^2 + b^2$ is odd.*

Proof. Suppose $(a+b)$ is odd. Then $(a+b)^2 = a^2+b^2+2ab$ is also odd. Note that a sum of two integers is odd if and only if the integers have opposite parity (Reason: Let m, n be any integer. Then $2m+2n = 2(m+n)$ is even, $2m+1+2n+1 = 2(m+n+1)$ is even, but $2m+2n+1 = 2(m+n)+1$ is odd. The converse can be proven by reversing this line of reasoning). $2ab$ is even, thus a^2+b^2 must be odd, and we are done.

Proposition 7.14. *Suppose $a \in \mathbb{Z}$. Then $a^2 \mid a$ if and only if $a \in \{-1, 0, 1\}$.*

Proof. ($\Longrightarrow$) Suppose $a^2 \mid a$. Then there exists k such that $a = a^2 k$. We divide into two cases as follows:

Case 1. If $a = 0$, then the equation $a = a^2 k$ is true.

Case 2. If $a \neq 0$, then $a = a^2 k$ implies $1 = ak$. The equality holds if and only if $a = 1$ and $k = 1$, or $a = -1$ and $k = -1$.

The cases have shown that if $a^2 \mid a$, then $a \in \{-1, 0, 1\}$.

($\Longleftarrow$) Suppose $a \in A = \{-1, 0, 1\}$. We can easily see that all elements of A all satisfy $a^2 \mid a$ ($1 \mid -1, 0 \mid 0, 1 \mid 1$). The proof is complete.

Proposition 7.15. *Suppose $a, b \in \mathbb{Z}$. Prove that $a + b$ is even if and only if a and b have the same parity.*

Proof. ($\Longrightarrow$) Suppose to the contrapositive that a and b have the opposite parity. Without loss of generality, suppose a is odd and b and even; thus $a = 2m+1$ and $b = 2n$ for some $m, n \in \mathbb{Z}$. Then $a+b = 2m+1+2n = 2(m+n)+1$, which is odd.

($\Longleftarrow$) Suppose a and b have the same parity. If a and b are both odd, then there exist $m, n \in \mathbb{Z}$ such that $a = 2m+1$ and $b = 2n+1$; thus $a + b = 2(m+n+1)$, which is even. If a and b are both even, then there exist $m, n \in \mathbb{Z}$ such that $a = 2m$ and $b = 2n$; thus $a+b = 2(m+n)$, which is even. The proof is thus completed.

Proposition 7.16. *Suppose $a, b \in \mathbb{Z}$. If ab is odd, then $a^2 + b^2$ is even.*

Proof. Note that if ab is odd, then a and b must also be odd themselves (Suppose to the contrapositive that a or b is even; then ab must also be even because there is a multiple of two due to a or b being even.). Therefore, there exist $m, n \in \mathbb{Z}$ such that $a = 2m+1$ and $b = 2n+1$. Thus

$$a^2 + b^2 = (2m+1)^2 + (2n+1)^2 = 2(2m^2 + 2n^2 + 2m + 2n + 1).$$

The proof is complete.

Proposition 7.17. *There is a prime number between 90 and 100.*

Proof. Observe 97.

Proposition 7.18. *There is a set X for which $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$.*

Proof. Observe $X = \mathbb{N} \cup \{\mathbb{N}\}$.

Proposition 7.19. *If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 1$.*

Proof. Consider a geometric progression with common ratio $q = 2$. The sum of the first $n+1$ terms is

$$2^0 + 2^1 + 2^2 + \cdots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

Proposition 7.20. *There exists an $n \in \mathbb{N}$ for which $11 \mid (2^n - 1)$*

Proof. Consider $n = 10$. Note that $2^10 - 1 = 1023 = 11 \cdot 93$. Thus $n = 10$ is a possible value of n for which $11 \mid (2^n - 1)$.

Proposition 7.21. *Every real solution of $x^3 + x + 3 = 0$ is irrational.*

Proof. Suppose to the contrary that there exists a rational solution of $x^3 + x + 3 = 0$. Let that solution be $x_0 = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$. Let this fraction be irreducible; that is, $\gcd(p, q) = 1$. Substituting this into the original equation, we get:

$$\begin{aligned}
\frac{p^3}{q^3} + \frac{p}{q} + 3 &= 0 \\
\frac{p^3 + pq^2}{q^3} + 3 &= 0 \\
\frac{p(p^2 + q^2)}{q^3} &= -3 \\
p^3 + pq^2 + 3q^3 &= 0
\end{aligned}$$

We divide into three cases as follows depending on the parity of p and q. The case where p and q are both even will not be considered since it contradicts the fact that p and q are coprime.

Case 1. Consider odd p and q. Note that p^3 is odd, pq^2 is odd and $3q^3$ is odd. The sum of three odd numbers is odd, which contradicts with the fact that $p^3 + pq^2 + 3q^3 = 0$.

Case 2. Consider odd p and even q. Note that p^3 is odd, pq^2 is even and $3q^3$ is even. The sum of two even numbers and an odd number is odd, contradicting with the fact that $p^3 + pq^2 + 3q^3 = 0$.

Case 3. Consider even p and odd q. Note that p^3 is even, pq^2 is even and $3q^3$ is odd. Similar to Case 2, this is a contradiction.

In every possible case, we come into a contradiction. The proof is thus completed.

Proposition 7.22. *If $n \in \mathbb{Z}$, then $4 \mid n^2$ or $4 \mid (n^2 - 1)$.*

Proof. This is proven in Proposition 5.28. The proof is thus completed.

Proposition 7.23. *Suppose a, b and c are integers. If $a \mid b$ and $a \mid (b^2 - c)$, then $a \mid c$.*

Proof. Suppose $a \mid b$ and $a \mid (b^2 - c)$; then there exists $k \in \mathbb{Z}$ such that $b = ak$. Thus $b^2 = a(ak^2)$, which implies $a \mid b^2$. Therefore $a \mid b^2$ and $a \mid (b^2 - c)$ imply $a \mid c$ by Proposition 4.6. The proof is completed.

Proposition 7.24. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$*

Proof. Proposition 5.28 tells that indeed $4 \nmid (a^2 - 3)$.

Proposition 7.25. *If $p > 1$ is an integer and $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$, then p is prime.*

Proof. Suppose to the contrapositive that p is not prime, where $p \in \mathbb{Z}$ and $p > 1$. Then $p = ab$ for some integer a, b. Observe that at least one of a or b must be less than or equal $\sqrt{p}$. Thus p must have at least one divisor n such that $2 \leq n \leq \sqrt{p}$, and we are done.

Proposition 7.26. *The product of any n consecutive positive integers is divisible by $n!$.*

Proof. Let k be the starting number in a sequence of n consecutive positive integers. The product of every number from that sequence is $k(k+1)(k+2)\cdots(k+n-1)$. Thus we wish to prove the following:

$$\frac{k(k+1)(k+2)\cdots(k+n-1)}{n!} \in \mathbb{Z}.$$

Note that the fraction can be reduced into the following:

$$\frac{k(k+1)(k+2)\cdots(k+n-1)}{n!} = \frac{(k+n-1)!}{n!(k-1)!} = \binom{k+n-1}{n}.$$

By the definition of $\binom{a}{b}$ for some natural a, b, we have $\binom{k+n-1}{n}$ is always a natural number. The proof is thus completed.

Proposition 7.27. *Suppose $a, b \in \mathbb{Z}$. If $a^2 + b^2$ is a perfect square, then a and b are not both odd.*

Proof. Suppose to the contrapositive that both a and b are odd. Then $a = 2m+1$ and $b = 2n+1$ for some $m, n \in \mathbb{Z}$. Then $a^2 + b^2 = 4(m^2+m+n^2+n)+2$. Suppose for the sake of contradiction that this is a perfect square. Then there exists $k \in \mathbb{Z}$ such that $4(m^2+m+n^2+n) = k^2 - 2$. The left hand side is a multiple of 4, so the right hand must also be. But only $4 \mid k^2$ or $4 \mid (k^2-1)$ is true (proven in Proposition 5.28), thus the right hand side cannot be a multiple of 4. This is a contradiction, therefore $4(m^2+m+n^2+n)+2$ must not be a perfect square. The proof is completed.

Proposition 7.28. *If $a, b \in \mathbb{N}$, there exist unique integers q, r for which $a = bq + r$, and $0 \leq r < b$.*

Proof. Form the set A for which

$$A = \{a - bq : q \in \mathbb{Z}, a - bq \geq 0\} \subseteq \mathbb{N}_0.$$

Let r be the smallest element of A. Since $r \in A$, we have $r = a - bq$ implies $a = bq + r$. We know that $r \geq 0$ because $r \in A \subseteq \mathbb{N}_0$. Additionally, it must be true that $r < b$. Suppose to the contrary that $r \geq b$, then the non-negative number $r - b = a - bq - b = a - b(q+1)$ would be an element of A and smaller than r. This contradicts the fact that r is the smallest element of A, thus $r < b$. We have established the existence of $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

To show there exist unique pair of integers (q, r) that satisfy such property, we assume there is a second pair that also does. Let (q', r') be such pair of integers. Thus $a = bq' + r' = bq + r$. This implies $b(q' - q) = r - r'$, which means $r - r'$ is a multiple of b. Note that $0 \leq r \leq b - 1$ and $-b + 1 \leq -r' \leq 0$, thus $-b + 1 \leq r - r' \leq b - 1$, implying the only multiple of b in the range of $r - r'$ is 0. Thus $r - r' = 0$ implies $r = r'$, and consequently $q' = q$. The uniqueness of q, r has been established, the proof is thus completed.

Proposition 7.29. *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Suppose $a \mid bc$ and $\gcd(a, b) = 1$. By Proposition 7.1, then there exist $m, n \in \mathbb{Z}$ such that $\gcd(a, b) = am + bn = 1$. Note that $amc + bnc = c$. We have amc is a multiple of a; because $a \mid bc$, we can see bc is a multiple of a, and thus so is bnc. The sum of two multiples of a is itself a multiple of a, thus $a \mid c$.

Proposition 7.30. *Suppose $a, b, p \in \mathbb{Z}$ and p is prime. Prove that if $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. Suppose $p \mid ab$. We divide into two cases as follows, depending on the divisibility of p on a:

Case 1. If $p \mid a$, then we are done.

Case 2. If $p \nmid a$, then that implies $\gcd(a, p) = 1$. This is because $\gcd(a, p) \mid p$, but because p is prime, $\gcd(a, p)$ can only evaluate to 1 or p; the latter happens if and only if $p \mid a$. Since $p \mid ab$ and $\gcd(a, p) = 1$, by Proposition 7.29, we have $p \mid b$.

This completes the proof.

Proposition 7.31. *If* $n \in \mathbb{Z}$*, then* $\gcd(n, n+1) = 1$.

Proof. By Proposition 5.29.1, we have $\gcd(n, n+1) = \gcd(n+1-n, n) = \gcd(1, n)$, which evaluates to 1.

Proposition 7.32. *If* $n \in \mathbb{Z}$*, then* $\gcd(n, n+2) \in \{1, 2\}$.

Proof. By Proposition 5.29.1, we have $\gcd(n, n+2) = \gcd(n+2-n, n) = \gcd(n, 2)$. If n is even, then $\gcd(n, 2)$ evaluates to 2; otherwise, $\gcd(n, 2)$ evaluates to 1. Thus $\gcd(n, n+2) \in \{1, 2\}$, as desired.

Proposition 7.33. *If* $n \in \mathbb{Z}$*, then* $\gcd(2n+1, 4n^2+1) = 1$.

Proof. By Proposition 5.29.1, for any integer n, we have:

$$\begin{aligned}\gcd(2n+1, 4n^2+1) &= \gcd(4n^2+1-4n^2-2n, 2n+1) = \gcd(1-2n, 2n+1) \\ &= \gcd(1-2n+2n+1, 2n+1) = \gcd(2, 2n+1).\end{aligned}$$

Note that $2n+1$ is odd. Thus $\gcd(2, 2n+1) = 1$, and we are done.

Proposition 7.34. *If* $\gcd(a, c) = \gcd(b, c) = 1$*, then* $\gcd(ab, c) = 1$.

Proof. Suppose to the contrary that $\gcd(ab, c) \neq 1$. Let p be a prime number such that $p \mid \gcd(ab, c)$. It follows that $p \mid ab$ and $p \mid c$. Thus $p \mid a$ and $p \mid c$, or $p \mid b$ and $p \mid c$ by Proposition 7.30. But this contradicts the fact that $\gcd(a, c) = \gcd(b, c) = 1$. Thus we have a contradiction.

Proposition 7.35. *Suppose* $a, b \in \mathbb{N}$*. Then* $a = \gcd(a, b)$ *if and only if* $a \mid b$.

Proof. ($\implies$) Suppose $a = \gcd(a, b)$. Thus there exists $x \in \mathbb{Z}$ such that $b = \gcd(a, b)x = ax$. Therefore $a \mid b$.

($\impliedby$) Suppose $a \mid b$. Since a divides b, every divisor of a will also divide b, where a itself is the largest among them. Thus $\gcd(a, b) = a$. This completes the proof.

Proposition 7.36. *Suppose* $a, b \in \mathbb{N}$*. Then* $a = \operatorname{lcm}(a, b)$ *if and only if* $b \mid a$

Proof. ($\implies$) Suppose $a = \operatorname{lcm}(a, b)$. Thus there exists $x \in \mathbb{Z}$ such that $\operatorname{lcm}(a, b) = a = bx$. Therefore $b \mid a$. ($\impliedby$) Suppose $b \mid a$. Since b divides a, every multiple of a will also be divided by b, where a is the lowest among them. Thus $\operatorname{lcm}(a, b) = a$. This completes the proof.