MATH 271: Proof Portfolio

Micah Sherry

December 9, 2024

Sample Direct Proof (problem 7.34)

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

Proof. Assume $\gcd(a,c) = \gcd(b,c) = 1$, So, $\exists w,x,y,z \in \mathbb{Z}$ such that $1 = aw + cx$ and $1 = by + cz$ (by proposition 7.1 page 152). Let d denote the $\gcd(ab,c)$, therefore $d|c$ and $d|ab$. So, $\exists m,n$ such that $c = dm$ and $ab = dn$. Consider,

$$\begin{aligned}
1 &= aw + cx \\
b &= abw + cby && \text{(multiplying both sides by } b.\text{)} \\
&= dnw + dmby && \text{(substituting } c \text{ for } dm \text{ and } ab \text{ for } dn.\text{)} \\
&= d(nw + mby) && \text{(let } k \text{ denote } nw + mby.\text{)}
\end{aligned}$$

Therefore $b = dk$. Now consider,

$$\begin{aligned}
1 &= by + cz \\
&= dky + dmz && \text{(substituting } c \text{ for } dm\text{, and } b \text{ for } dk\text{)} \\
&= d(ky + mz) \\
&= dj && \text{(letting } j \text{ denote } ky + mz\text{)}
\end{aligned}$$

This implies that $d|1$, therefore, d=1 (because 1 only has divisors -1, and 1; and $1 > -1$). Therefore the $\gcd(ab,c) = 1$, so the proposition holds. □

Sample Indirect Proof (problem 5.10)

Suppose $x,y,z \in \mathbb{Z}$ and $x \neq 0$, If $x \nmid yz$ then $x \nmid y$ and $x \nmid z$

Proof. Consider the contrapositive: if $x \mid y$ or $x \mid z$ then $x \mid yz$. Without loss of generality let x divide y. So, $\exists k \in \mathbb{Z}$ such that $y = xk$

$$\begin{aligned}
yz &= (xk)z \\
yz &= x(kz)
\end{aligned}$$

Let n denote kz, Then yz can be expressed as $yz = xn$ and n is an integer. So, x divides yz (by definition of divisibility). Thus the contrapositive holds and so does the original statement.

□

Sample Proof by Cases (problem 7.22)

If $n \in \mathbb{Z}$ then $4|n^2$ or $4|(n^2-1)$

Proof. Let $n \in Z$ be given, notice there are two cases for n: odd and even.

Case 1: n is odd. So, $\exists k \in \mathbb{Z}$ such that $n = 2k+1$. Consider,

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

So 4 divides $n^2 - 1$ when n is odd.

Case 2: n is even. So, $\exists k \in \mathbb{Z}$ such that $n = 2k$. Consider,

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4(k^2). \end{aligned}$$

So, 4 divides n^2 when n is even. Since 4 divides n^2 or $n^2 - 1$, the proposition holds.

□

Sample Proof by Contradiction (problem 6.8)

Suppose $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$ then a or b is even

Proof. Assume for the sake of contradiction that $a^2 + b^2 = c^2$, and a and b are odd. Then $\exists k, n \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2n+1$. So,

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2k+1)^2 + (2k+1)^2 \\ &= 4k^2 + 4k + 1 + 4n^2 + 4n + 1 \\ &= 4(k^2 + n^2 + k + n) + 2. \end{aligned}$$

let $m = k^2 + n^2 + k + n$ Therefore c^2 = 4m+2.

Case 1: c is even. Then $c = 2j$ for some $j \in \mathbb{Z}$. Then $c^2 = 4j^2$. This is a contradiction because we have established that c^2 is of the form $4m+2$

Case 2: c is odd. Then $c = 2j+1$ for some $j \in \mathbb{Z}$. Then $c^2 = 4j^2 + 4j + 1 = 4(j^2 + j) + 1$. This is a contradiction because we have established that $c^2$is of the form $4m+2$.

Since both cases for c leads to a contradiction the original statement holds. □

Sample Disproof (problem 9.2)

For every natural number n, the integer $2n^2 - 4n + 31$ is prime.

Proof. consider the counterexample $n = 31$, then

$$\begin{aligned} 2n^2 - 4n + 31 &= 2(31)^2 - 4(31) + 31 \\ &= 31(2(31) - 4 + 1) \\ &= 31(59). \end{aligned}$$

Therefore $2n^2 - 4n + 31$ is not prime for all n (because it is divisible by 31 and 59). Thus the proposition is false. □

Sample Induction Proof (problem 10.26)

Concerning the Fibonacci sequence, prove that $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$.

Proof. **Base Case:** Consider the base case $n = 1$.

$$\sum_{i=1}^{1} F_i^2 = F_1^2 = 1 \text{ and } F_1 F_2 = 1 * 1 = 1$$

therefore the base case holds.

Induction Hypothesis: Assume $\sum_{i=1}^{k} F_i^2 = F_k F_{k+1}$ is true for some k.

Inductive step: Now consider the case when $n = k + 1$.

$$\begin{aligned}
\sum_{i=1}^{k+1} F_i^2 &= \sum_{i=1}^{k} F_i^2 + F_{k+1}^2 \\
&= F_k F_{k+1} + F_{k+1}^2 && \text{(by the induction hypothesis)} \\
&= F_{k+1}(F_k + F_{k+1}) && \text{(by factoring)} \\
&= F_{k+1}(F_{k+2}) && \text{(by definition of the Fibonacci sequence)}
\end{aligned}$$

Since the base case holds and $S_k \implies S_{k+1}$ by the principle of mathematical induction, the statement is true $\forall n \in \mathbb{N}$ $\square$