Fundamentals of Mathematics

Supplement 1

Spring, 2008

http://staffweb.ncnu.edu.tw/shieng

Example 1. For all integers m and n, if m and n are even, then $m+n$ is even.

Proof. Since m and n are even numbers, there exist integers m' and n' such that $m = 2m'$ and $n = 2n'$. Hence $m + n = 2m' + 2n' = 2(m' + n')$ is an even number.

Example 2. For all odd integers n, the number $n^2 - 1$ is divisible by 8.

Proof. Let n be an odd number. We divide the discussion into two cases: $n = 4k_1 + 1$ and $n = 4k_2 + 3$ for some integers k_1 and k_2.

- $n = 4k_1 + 1$: $n^2 - 1 = (4k_1 + 1)^2 - 1 = 16k_1^2 + 8k_1 + 1 - 1 = 8(2k_1^2 + k_1)$ is a multiple of 8.
- $n = 4k_2 + 3$: $n^2 - 1 = (4k_2 + 3)^2 - 1 = 16k_2^2 + 24k_2 + 9 - 1 = 8(2k_2^2 + 3k_2 + 1)$ is a multiple of 8.

Since both cases lead to the same conclusion, the claim is proved.

Example 3. For all integers n, if n^2 is even , then n is even.

Proof. We show its contraposition: If n is not even, then n^2 is not even. Let n be an odd number and assume $n = 2k + 1$. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ is an odd number. Therefore from contraposition, we get the assertion

Example 4. $\sqrt{2}$ is irrational.

Proof. Suppose $\sqrt{2}$ is rational. We will show contradiction happened. Since we assume $\sqrt{2}$ is rational, there exist integers m and n, having no common divisor other than 1, such that $\sqrt{2} = \frac{m}{n}$. Squaring both sides, we get $2 = \frac{m^2}{n^2}$. Thus, $2n^2 = m^2$. Hence 2 divides m^2, and subsequently, 2 divides m. Let $m = 2m_1$ where m_1 is an integer. Substitute m by $2m_1$ into $2n^2 = m^2$. We get $2n^2 = 4m_1^2$. Hence $2m_1^2 = n^2$. By the same argument, 2 divides n^2, and thus 2 divides n. Therefore 2 is a common divisor of m and n, which contradicts the assumption that m and n have no common divisor other than 1. Hence, $\sqrt{2}$ is irrational.

Example 5. For all integers a and p, if p is prime, then either p is a divisor of a, or a and p have no common factor greater than 1.

Proof. Let p be a prime. Assume a and p have common divisor greater than 1. Since p is a prime, the only positive factor of p other than 1 is p itself. Therefore the common divisor of a and p greater than 1 can only be p. Thus, we get the conclusion that p divides a.

Example 6. For all integers n, $n^2 - 1$ is either divisible by 8 or relatively prime to 8.

Proof. We divide n into two cases: $n = 2k$ and $n = 2k+1$. When $n = 2k$, $n^2 - 1$ is always an odd number, and thus, relatively prime to 8. When $n = 2k + 1$, from Example 2, we get the claim that $n^2 - 1$ is divisible by 8. Since all of the cases lead to the conclusion, the claim is proved.

Example 7. For all integers n, the following statements are equivalent:

(1) n is even;
(2) n^2 is even;
(3) n^k is even for all integers $k \geq 1$.

Proof. We use cyclic argument to establish their equivalence.

(1)⇒(3): The multiplication of two even numbers is again even. Hence if n is even, n^k for $k \geq 1$ are all even numbers.

(3)⇒(2): Setting $k = 2$ we get the implication.

(2)⇒(1): Has been proven in Example 3.

Example 8. Every finite, directed, and acyclic graph must have a source.

Proof. Note that a graph is acyclic iff it has no cycle, and a node is a source iff it has no incoming edges. Suppose there exists a counter example. That is, these is a finite, directed, and acyclic graph G that has no source. Then pick up any node in G, say n_1. Since there is no source in G, n_1 has an incoming edge. Trace back along this edge. There is a node n_2 that connects n_1. This process can continue, and we can eventually find an infinite sequence $n_1, n_2, \ldots, n_i, \ldots$ such that there is always an edge from n_{i+1} to n_i for each integer $i \geq 1$. However, G is a finite graph, and thus, some node must repeat infinite times on this sequence. Let p be such a node. There exist $n_s = n_t = p$ and $s < t$. This indicates a cycle starting from $n_t = p$ and ending at $n_s = p$, which contradicts the assumption that G is acyclic.

Example 9. There exists a number that is not rational.

Proof. We have shown that $\sqrt{2}$ is not rational in Example 4. Hence the existence is established.

Example 10. Given any seven integers $a_1, a_2, \ldots, a_7$, there always exist $1 \leq i \leq j \leq 7$ such that $a_i + a_{i+1} + \cdots + a_j$ is a multiple of 7.

Proof. We show this by using the pigeon hole principle. Let $S_k = a_1 + a_2 + \cdots + a_k$ for $1 \leq k \leq 7$. Without loss of generality, we can assume all S_k's for $1 \leq k \leq 7$ are not multiple of 7; otherwise, we can simply set $i = 1$ and $j = k$ and the claim is established. Hence the remainders of S_k's divided by 7 can only be $1, 2, 3, 4, 5$, or 6. However, there are seven S_k's but six remainders. By the pigeon hole principle, there exist $1 \leq u < v \leq 7$ such that the remainders of S_u and S_v are the same with respect to the divisor 7. Consequently, $S_v - S_u$ is a multiple of 7. Now let $i = u + 1$ and $j = v$, and accordingly, $a_i + a_{i+1} + \cdots + a_j$ is a multiple of 7.

Example 11. Given any integer n, there is an integer m with $m > n$.

Proof. Let n be any integer. Let $m = n + 1$, then clearly $m = n + 1 > n$.

Example 12. Given a natural number n, there is always a prime number p that is greater than n.

Proof. Let n be any natural number. Set $m = n! + 1$. We claim that any prime factor of m is larger than n. Let p be a prime factor of m. If p is less than or equal to n, $n!$ is a multiple of p. Then by the Euclidean algorithm, the greatest common divisor of p and m is 1. That is, p cannot divide m, a contradiction. Therefore, such p must be larger than n.