The Well-Ordering Principle for the Integers

Some proofs in mathematics use a property of the set of integers called the Well-Ordering Principle.

Definition of the Well-Ordering Principle for the Integers

Every non-empty set of integers
in which every element is greater than or equal to some fixed integer
has a least element.

More formally, specifying Condition (1) and Condition (2):

Let set S be a set of integers such that:

1) There is at least one integer element in S, and

2) There exists an integer L such that every element in set S is greater than or equal to L.

Then, by the Well-Ordering Principle, S has a least element m.

Note: The integer L (thought of a "Lower Bound" of integers in S) is most likely not in the set S.

And, the choices of which integer L might be is never unique:
many different integers can be chosen as L to serve as a lower bound for set S.
For example, if L = 2 works, then L = 1, L = 0, L = -1, etc., all will also work.

Example 1: Verify that the Well-Ordering Principle can be applied to set S,

where set S = { All integers x such that $24 = xy$ for some integer y } .

1) [Show that there is at least one integer element in set S.]

$24 = 12 \times 2 = xy$ where $x = 12$ and $y = 2$.
Thus, $x = 12$ is in set S, so there is at least one integer element in S, so S is a non-empty set.

2) [Show that there exists an integer L such that, for all x in S, $x \geq L$.]

By definition of S, every integer element in S is a divisor of 24.
The divisors of 24 range between –24 and +24 , so every divisor of 24 is greater than or equal to –25 . Thus, every element in set S is greater than or equal to –25 .

∴ Set S satisfies Condition (1) and Condition (2) of the Well-Ordering Principle of the Integers.
∴ By the Well-Ordering Principle of the Integers, set S has a least element , m .

Regarding the step of locating an integer L to serve as a "Lower Bound" of the elements in set S, sometimes the definition of S itself says, for instance, that set S is the set of all integers n, $n \geq 0$, such that n has such-and-such property. In that case, verifying the existence of a "Lower Bound" for the elements of S is accomplished just by saying, "By definition of set S, every integer in S is greater than or equal to 0."

A First Example of a Proof using the Well-Ordering Principle of the Integers

DEFINITION: Define the sequence $c_0, c_1, c_2, \ldots$ as follows:

$c_0 = 2$, $c_1 = 2$, $c_2 = 6$,

and $c_k = 3c_{(k-3)}$ for all integers $k \geq 3$.

TO PROVE: For every integer $n \geq 0$, c_n is even.

Proof: Suppose, by way of contradiction, that there exists an integer N such that: $N \geq 0$ and c_N is not even.

Let $S = \{$all integers t such that $t \geq 0$ and c_t is not even$\}$.

Since $N \geq 0$ and c_N is not even, N is in S and so S is not the empty set.

Also, every element of S is greater than or equal to zero. So, S satisfies the conditions of the Well-Ordering Principle of the integers.

By the Well Ordering Principle, S has a least element m.
∴ Since m is in set S, $m \geq 0$ and C_m is not even, by definition of set S.

INTERNAL LEMMA:
For all integers t, if $0 \leq t < m$, then
C_t is even.

Proof of Internal Lemma:
Let t be any integer.
Suppose $0 \leq t < m$.
∴ Since $t < m$ and m is the least element in Set S,
t is not in Set S.
Suppose BWOC that C_t is not even.
∴ t is in set S, by definition of set S,
but this contradicts the fact that t is not in set S,
∴ C_t is even, by proof-by-contradiction.
QED for the Internal Lemma.

Now, $C_0 = 2 = 2 \times 1$, ∴ C_0 is even and C_m is not even.
∴ $m \neq 0$, and since $m \geq 0$ also, $m \geq 1$.

$C_1 = 2 = 2 \times 1$. ∴ C_1 is even and C_m is not even.
∴ $m \neq 1$, and since $m \geq 1$ also, $m \geq 2$.
$C_2 = 6 = 3 \times 2$, ∴ C_2 is even and C_m is not even.
∴ $m \neq 2$, and since $m \geq 2$ also, $m \geq 3$.

Since $m \geq 3$, the formula in the Sequence Definition applies. ∴ $C_m = 3 \times C_{(m-3)}$, by that formula.
Since $m \geq 3$, $m - 3 \geq 0$.
∴ $0 \leq m - 3 < m$.
∴ By the Internal Lemma, $C_{(m-3)}$ is even.

∴ Since $c_{(m-3)}$ is even, there exists an integer k such that $c_{(m-3)} = 2k$.

Recall that $c_m = 3 \times c_{(m-3)}$,

∴ $c_m = 3 \times (2k)$

∴ $c_m = 2 \cdot (3k)$ and $3k$ is an integer.

∴ c_m is even, which contradicts the fact that c_m is not even.

∴ For every integer $n \geq 0$, c_n is even, by proof-by-contradiction.

A Second Example of a proof Using the Well-Ordering Principle:

Sequence (d_n) is defined as follows: $d_1 = \frac{9}{10}$, $d_2 = \frac{10}{11}$, and, for all integers $k \geq 3$, $d_k = d_{(k-1)} \times d_{(k-2)}$.

To Prove: For all integers $n \geq 1$, $d_n < 1$.

Proof: [By proof-by-contradiction]

Suppose, by way of contradiction, that there exists an integer index $T \geq 1$ such that $d_T \not< 1$; that is, $d_T \geq 1$.

Let set S = {all integer indicies $n \geq 1$ such that $d_n \geq 1$}

By definition of T, $d_T \geq 1$ and $T \geq 1$.

∴ By definition of Set S, $T \in S$, and so S is non-empty.

∴ Condition (1) of the Well-Ordering Principle is satisfied.

By definition of Set S, every integer n in Set S is greater than or equal to 1. [So, set S has a Lower Bound $L = 1$]

∴ Condition (2) of the Well-Ordering Principle is satisfied.

∴ By the Well-Ordering Principle, the set S has a least element, which we will call m.

INTERNAL LEMMA: For all integers t,
if $1 \leq t < m$, then $d_t < 1$.

Proof of the INTERNAL LEMMA:

Let t be any integer.
Suppose that $1 \leq t < m$. [WE NTS: $d_t < 1$]
Since $t < m$ and m is the least element of Set S,
t is NOT IN Set S.
Suppose, BWOC, that $d_t \geq 1$ [ie. $d_t \not< 1$].

Since $t \geq 1$ and $d_t \geq 1$, d_t is in Set S, by definition of Set S, which contradicts the fact that t is NOT IN Set S.
$\therefore d_t < 1$, by Proof-by-contradiction.
[QED for the INTERNAL LEMMA]

Recall that,
Since m is in Set Set, $d_m \geq 1$ and $m \geq 1$.
NOW, $d_1 = \frac{9}{10}$, so $d_1 < 1$ and $d_m \geq 1$, so $m \neq 1$.
Since $m \geq 1$ and $m \neq 1$, $\underline{m \geq 2}$.
Also, $d_2 = \frac{10}{11}$, so $d_2 < 1$ and $d_m \geq 1$, so $m \neq 2$.
Since $m \geq 2$ and $m \neq 2$, $\underline{m \geq 3}$.
Since $m \geq 3$, $m - 2 \geq 1$. $\therefore 1 \leq m - 2 < m$.
$\therefore$ By the Internal Lemma, $\underline{d_{(m-2)} < 1}$.

Since $m \geq 3$, $m - 1 \geq 2 \geq 1$. $\therefore 1 \leq m - 1 < m$.
By the Internal Lemma, $\underline{d_{(m-1)} < 1}$.

Since $m \geq 3$, the formula in the Sequence Definition applies to d_m.

$\therefore d_m = d_{(m-1)} \times d_{(m-2)}$, by the formula.

Since $d_{(m-1)} < 1$, $d_{(m-1)} \times d_{(m-2)} < 1 \cdot d_{(m-2)}$.

$\therefore d_{(m-1)} \times d_{(m-2)} < d_{(m-2)} < 1$.

$\therefore$ By Transitivity of Inequality,

$$d_{(m-1)} \times d_{(m-2)} < 1$$

Recall that $d_m = d_{(m-1)} \times d_{(m-2)}$.

$\therefore d_m < 1$, by substitution, but this contradicts the fact that $d_m \geq 1$.

$\therefore$ For all integers $n \geq 1$, $d_n < 1$,

by proof-by-contradiction.

QED.

On the following two pages are two proofs of Theorem 4.3.4, which states that every integer which is greater than 1 is divisible by some prime number. We will need to apply the following theorem.

The following theorem is useful when a proof deals with integers which are not prime numbers.

Theorem (The Non-Prime Integer Greater Than One Theorem):

For every integer n, if $n > 1$ and n is not a prime number,

then there exist integers r and s such that $1 < r < n$ and $1 < s < n$ and $n = rs$.

Proof: Let n be any integer.

Suppose that $n > 1$ and n is not a prime number.

Since n is not prime, there exist positive integers r and s such that $n = rs$ and $r \neq 1$ and $s \neq 1$.

$\therefore r > 1$ and $s > 1$, since they are positive integers not equal to 1.

$\therefore rs > r$ and $rs > s$, by rules of algebra.

$\therefore n > r$ and $n > s$, by substitution (recall that $n = rs$).

$\therefore 1 < r < n$ and $1 < s < n$ and $n = rs$. **QED**

Theorem 4.3.4 : For every integer $n > 1$, n is divisible by some prime number.

[This proof illustrates one way to use the Well-Ordering Principle of the Integers to prove a theorem. Following this proof, another proof of this theorem is presented which illustrates a second way to use the Well-Ordering Principle to prove a theorem.]

Proof # 1 :

Suppose, by way of contradiction, that there exists an integer N such that $N > 1$ and N is not divisible by any prime number.

Let S = { all positive integers n such that that $n > 1$ and n is not divisible by any prime number. }

[Here, the least element m will be the first integer greater than 1 which is not divisible by a prime number.]

Since $N > 1$ and N is not divisible by any prime number, $N \in S$, so S is not the empty set.

By definition of set S, every element of S is greater than 1, so 1 is a "Lower Bound" integer for set S.

$\therefore$ S satisfies the conditions of the Well-Ordering Principle of the Integers..

$\therefore$ By the Well-Ordering Principle of the Integers, S has a least element, m.

Since m is divisible by m (that is, m is its own divisor) and since m is not divisible by any prime number, m is not a prime number. Also, $m > 1$.

Thus, since $m > 1$ and m is not a prime number, there exist integers r and s such that $1 < r < m$ and $1 < s < m$ and $m = rs$. Thus, $r \mid m$.

Since $r < m$, r is not in the set S.

Since $1 < r$ and r is not in the set S, there exists a prime p such that $p \mid r$, by definition of S.

Since $p \mid r$ and $r \mid m$, $p \mid m$ by transitivity of divisibility.

Since p is a prime number, m is divisible by the prime number p, which contradicts the fact that m is not divisible by any prime number.

Therefore, for every integer $n > 1$, n is divisible by some prime number, by proof-by-contradiction. **Q E D**

Theorem 4.3.4 : For every integer $n > 1$, n is divisible by some prime number p.

Proof # 2 :

Let n be any integer such that $n > 1$. [NTS: There exists a prime number p such that $p \mid n$.]

Let $S = \{$ all integers t such that that $t > 1$ and $t \mid n.\}$

[Here, the least element m will be the first divisor of n which is greater than 1. It will be a prime number.]

Since $n > 1$ and $n \mid n$, n is an element of set S, by definition of set S. Thus, S is not the empty set.

Also, by definition of S, every element of S is greater than 1, so 1 is a "Lower Bound" integer for set S.

$\therefore$ S satisfies the conditions of the Well-Ordering Principle of the Integers..

$\therefore$ By the Well-Ordering Principle of the Integers, S has a least element, m. [NTS: m is a prime number]

$\therefore m > 1$ and $m \mid n$.

Suppose, by way of contradiction, that m is not a prime number.

By definition of S, $m > 1$. Thus, m is a non-prime integer greater than one.

Thus, since $m > 1$ and m is not a prime number, there exist integers r and s such that

$1 < r < m$ and $1 < s < m$ and $m = rs$. Thus, $r \mid m$.

Since $r < m$ and m is the least element in S, r is not an element in the set S.

Since $1 < r$ and r is not an element in the set S, we conclude that $r \nmid n$.

Since $r \mid m$ and $m \mid n$, $r \mid n$ by transitivity of divisibility.

Therefore, $r \mid n$ and $r \nmid n$, which is a contradiction.

$\therefore$ m is a prime number, by proof-by-contradiction.

Recall that $m \mid n$.

$\therefore$ n is divisible by the prime number m. Let $p = m$. $\therefore p$ is a prime number and $p \mid n$.

$\therefore$ n is divisible by some prime number p.

Therefore, for every integer $n > 1$, n is divisible by some prime number p, by Direct Proof. **Q E D**