Further Proof and Number Theory

Prerequisites: Proof techniques (especially Mathematical Induction);
factors of whole numbers.

Maths Applications: Solving Diophantine equations.

Real-World Applications: Security systems.

Necessary and Sufficient Statements

Definition:

A statement A is **sufficient** for a statement B if $A \Rightarrow B$.

Definition:

A statement B is **necessary** for a statement A if $A \Rightarrow B$.

Example 1

In the conditional, ' If Iraq does not have WMDs, then Blair is a liar ', the sufficient statement is ' Iraq does not have WMDs ' and the necessary statement is ' Blair is a liar '.

Example 2

The biconditional ' $x = 3$ or $x = -3 \Leftrightarrow x^2 = 9$ ' is true.

Definition:

A is necessary and sufficient for B (or **B is necessary and sufficient for A**) if $A \Leftrightarrow B$.

Example 3

The biconditional '$x = 4$ or $x = -4 \Leftrightarrow x^2 = 16$', which is true, says that $x = 4$ or $x = -4$ is sufficient for $x^2 = 16$ and that $x = 4$ or $x = -4$ is necessary for $x^2 = 16$.

Further Examples of Proof and Counterexample

Example 4

Prove that if $n \in \mathbb{N}$ is divisible by 8, then n is also divisible by 4.

Suppose that 8 divides n. Then $\exists\ k \in \mathbb{N}$ s.t.

$$n = 8k$$

$$n = 4 \times 2k$$

As $k \in \mathbb{N}$, $2k \in \mathbb{N}$, so 4 divides n.

Example 5

Prove that the cube of an even integer plus the square of an odd integer is an odd integer.

Let p be an even integer and q an odd integer. Then $\exists\ m, n \in \mathbb{Z}$ s.t. $p = 2m$ and $q = 2n + 1$. So,

$$p^3 + q^2 = (2m)^3 + (2n + 1)^2$$

$$= 8m^3 + (4n^2 + 4n + 1)$$

$$= 2(4m^3 + 2n^2 + 2n) + 1$$

As $m, n \in \mathbb{Z}$, $4m^3 + 2n^2 + 2n \in \mathbb{Z}$, and so $p^3 + q^2$ is odd.

Example 6

Prove that a cubic polynomial P is divisible by $(x - a)$ if and only if $P(a) = 0$.

The statement involves the quantities $P(a)$ and $(x - a)$. To say that P is divisible by the linear factor is the same as saying that there exists a polynomial $Q(x)$ s.t. $P(x) = (x - a)\,Q(x)$ (it's a bit like saying that if an integer n is divisible by 3, then there exists an integer k s.t. $n = 3k$).

Consider the quantity $P(x) - P(a)$,

$$P(x) - P(a) = (Ax^3 + Bx^2 + Cx + D) - (Aa^3 + Ba^2 + Ca + D)$$

$$= A(x^3 - a^3) + B(x^2 - a^2) + C(x - a)$$

$$= (x - a)[A(x^2 + ax + a^2) + B(x + a) + C]$$

Taking $Q(x) = [A(x^2 + ax + a^2) + B(x + a) + C] + P(a)$, we can write,

$$P(x) = (x - a)\,Q(x) + P(a)$$

To prove ' a cubic polynomial P is divisible by $(x - a) \Rightarrow P(a) = 0$ ', the implicant can be written as $P(x) = (x - a)\,Q(x)$ and comparing this with the last equation shows that,

$$(x - a)\,Q(x) + P(a) = (x - a)\,Q(x)$$

$$P(a) = 0$$

To prove ' $P(a) = 0 \Rightarrow$ a cubic polynomial P is divisible by $(x - a)$ ', substituting $P(a) = 0$ into $P(x) = (x - a)\,Q(x) + P(a)$ shows that,

$$P(x) = (x - a)\,Q(x)$$

Hence, P is divisible by $(x - a)$.

Example 7

Prove that $6 + 7\sqrt{2}$ is irrational.

Suppose that $6 + 7\sqrt{2}$ is rational. Then $\exists\ m, n \in \mathbb{Z}$ with $n \neq 0$ s.t.,

$$6 + 7\sqrt{2} = \frac{m}{n}$$

The idea is to reach a contradiction using $\sqrt{2}$. Let's try solving for $\sqrt{2}$,

$$7\sqrt{2} = \frac{m}{n} - 6$$

$$7\sqrt{2} = \frac{m - 6n}{n}$$

$$\sqrt{2} = \frac{m - 6n}{7n}$$

As $m, n \in \mathbb{Z}$ with $n \neq 0$, $\frac{m - 6n}{7n} \in \mathbb{Q}$. But this means that $\sqrt{2}$ would be rational too; this is the desired contradiction, so $6 + 7\sqrt{2}$ is irrational.

Example 8

Prove, or give a counterexample to, the statement ' For all natural numbers n, $(n + 1)(n + 2)$ is even '.

Experimenting with different values for n indicates that the statement is true (but an indication is not a proof). The idea is to consider 2 cases, one where n is even and the other when n is odd.

So first assume that n is even, i.e. assume $\exists\ k \in \mathbb{N}$ s.t. $n = 2k$. Then

$$(n + 1)(n + 2) = (2k + 1)(2k + 2)$$

$$= 2(2k + 1)(k + 1)$$

As $k \in \mathbb{N}$, $2k + 1, k + 1 \in \mathbb{N}$ and thus so is $(2k + 1)(k + 1)$. Hence, $(n + 1)(n + 2)$ is 2 times a natural number and so is even.

Now assume that n is odd, i.e. assume $\exists\ k \in \mathbb{N}$ s.t. $n = 2k + 1$. Then

$$(n + 1)(n + 2) = (2k + 2)(2k + 3)$$

$$= 2(k + 1)(2k + 3)$$

As $k \in \mathbb{N}$, $2k + 3$, $k + 1 \in \mathbb{N}$ and thus so is $(2k + 3)(k + 1)$. Hence, $(n + 1)(n + 2)$ is 2 times a natural number and so is even.

So, in conclusion, $(n + 1)(n + 2)$ is even $\forall\ n \in \mathbb{N}$.

Example 9

Prove, or give a counterexample to, the statement ' All prime numbers are odd '.

The number 2 provides a counterexample to the given statement.

Further Examples of Induction

Now that some more topics have been studied since the last time Mathematical Induction was covered, we now have a much more exotic collection of examples.

Finite Sums

Example 10

Prove that $\sum_{r=1}^{n} \frac{1}{r(r+1)} = \frac{n}{n+1}$, $\forall\ n \in \mathbb{N}$.

The P(n) statement can be written as,

$$P(n): \sum_{r=1}^{n} \frac{1}{r(r+1)} = \frac{n}{n+1}$$

The Base Case is $n = 1$. The LHS is $\frac{1}{2}$. The RHS is $\frac{1}{2}$. Hence, P(1) is true.

Assume that P(k) is true for some natural number k, i.e.,

$\sum_{r=1}^{k} \frac{1}{r(r+1)} = \frac{k}{k+1}$. The RTP statement is,

$$\sum_{r=1}^{k+1} \frac{1}{r(r+1)} = \frac{k+1}{k+2}$$

So,

$$\sum_{r=1}^{k+1} \frac{1}{r(r+1)} = \left(\sum_{r=1}^{k} \frac{1}{r(r+1)} \right) + \frac{1}{(k+1)(k+2)}$$

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}$$

$$= \frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)}$$

$$= \frac{k^2 + 2k + 1}{(k+1)(k+2)}$$

$$= \frac{(k+1)^2}{(k+1)(k+2)}$$

$$= \frac{k+1}{k+2}$$

Thus, P(k) true $\Rightarrow$ P($k+1$) true. So, P(1) is true and P(k) true $\Rightarrow$ P($k+1$) true imply, via the PMI, that P(n) is true ($\forall n \in \mathbb{N}$).

An important result regarding finite sums is the content of the following theorem (prove it by induction).

Theorem:

The sum of the squares of the first n natural numbers is,

$$\sum_{r=1}^{n} r^2 = \frac{1}{6} n(n+1)(2n+1)$$

Example 11

Show that for any natural number n, the sum of the cubes of the first n natural numbers is given by $\frac{1}{4} n^2 (n+1)^2$.

The P(n) statement can be written as,

$$P(n): \sum_{r=1}^{n} r^3 = \frac{1}{4} n^2 (n+1)^2$$

The Base Case is $n = 1$. The LHS is $1^3 = 1$. The RHS is $\frac{1}{4} \cdot 1^2 \cdot 2^2 = 1$. Hence, P(1) is true. Assume that P(k) is true for some natural number k, i.e., $\sum_{r=1}^{k} r^3 = \frac{1}{4} k^2 (k+1)^2$. The RTP statement is,

$$\sum_{r=1}^{k+1} r^3 = \frac{1}{4} (k+1)^2 (k+2)^2$$

So,

$$\sum_{r=1}^{k+1} r^3 = \left(\sum_{r=1}^{k} r^3 \right) + (k+1)^3$$

$$= \frac{1}{4} k^2 (k+1)^2 + (k+1)^3$$

There is a major temptation to expand the brackets here – don't. If it's possible to factorise expressions, do that instead of expanding brackets,

especially in examples of this sort where the answer (RHS of RTP statement) is written in fully factorised form. Factorising gives,

$$= \frac{1}{4}(k+1)^2[k^2+4(k+1)]$$

$$= \frac{1}{4}(k+1)^2(k^2+4k+4)$$

$$= \frac{1}{4}(k+1)^2(k+2)^2$$

Thus, P(k) true $\Rightarrow$ P($k+1$) true. So, P(1) is true and P(k) true $\Rightarrow$ P($k+1$) true imply, via the PMI, that P(n) is true ($\forall n \in \mathbb{N}$).

As an interesting point, note that the formula obtained in the above example is precisely the square of the expression for the sum of the first n natural numbers. This important enough to state as a theorem.

Theorem:

The sum of the cubes of the first n natural numbers is,

$$\sum_{r=1}^{n} r^3 = \frac{1}{4}n^2(n+1)^2 = \left(\sum_{r=1}^{n} r\right)^2$$

Note that $\left(\sum_{r=1}^{n} r\right)^2 \neq \sum_{r=1}^{n} r^2$. As an aside, there is a formula for the sum of the k^{th} powers of the first n natural numbers, but this general formula is much harder to prove.

Example 12

Prove that, for any natural number n, the sum of the first n terms of an arithmetic sequence is given by $\frac{n}{2}(2a+(n-1)d)$.

The statement P(n) can be expressed in terms of a finite sum, namely, $\sum_{r=1}^{n} u_r$, i.e.,

$$\text{P}(n): \sum_{r=1}^{n} (a + (r-1)d) = \frac{n}{2}(2a + (n-1)d)$$

where the notation from Unit 2 for arithmetic sequences has been used. The Base Case is $n = 1$. The LHS is $a + (1-1)d = a$. The RHS is $\frac{1}{2}(2a + (1-1)d) = a$. Hence, P(1) is true. Assume that P(k) is true for some natural number k, i.e., $\sum_{r=1}^{k} (a + (r-1)d) = \frac{k}{2}(2a + (k-1)d)$.

The RTP statement is,

$$\sum_{r=1}^{k+1} (a + (r-1)d) = \frac{k+1}{2}(2a + ((k+1)-1)d)$$

First note that the RHS of the RTP statement can be written as $\frac{(k+1)}{2}(2a + kd)$. So,

$$\sum_{r=1}^{k+1} (a + (r-1)d) = \left(\sum_{r=1}^{k} (a + (r-1)d)\right) + (a + (k+1) - 1)d)$$

$$= \frac{k}{2}(2a + (k-1)d) + (a + kd)$$

$$= ka + \frac{k}{2}(k-1)d + (a + kd)$$

$$= (k+1)a + \frac{k^2}{2}d - \frac{k}{2}d + kd$$

$$= (k+1)a + \frac{k^2}{2}d + \frac{k}{2}d$$

$$= (k + 1)a + \frac{k}{2}(k + 1)d$$

$$= \frac{(k + 1)}{2}(2a + kd)$$

Thus, P(k) true $\Rightarrow$ P($k + 1$) true. So, P(1) is true and P(k) true $\Rightarrow$ P($k + 1$) true imply, via the PMI, that P(n) is true ($\forall n \in \mathbb{N}$).

Matrices

Example 13

Prove that, for $a, b \in \mathbb{R}$, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$, $\forall n \in \mathbb{N}$.

The P(n) statement can be written as,

$$\text{P}(n): \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$$

The Base Case is $n = 1$. The LHS is $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^1 = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. The RHS is $\begin{pmatrix} a^1 & 0 \\ 0 & b^1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Hence, P(1) is true. Assume that P(k) is true for some natural number k, i.e., $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^k = \begin{pmatrix} a^k & 0 \\ 0 & b^k \end{pmatrix}$. The RTP statement is,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{k+1} = \begin{pmatrix} a^{k+1} & 0 \\ 0 & b^{k+1} \end{pmatrix}$$

So,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{k+1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^k \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

$$= \begin{pmatrix} a^k & 0 \\ 0 & b^k \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Performing the simple matrix multiplication shows that

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{k+1} = \begin{pmatrix} a^{k+1} & 0 \\ 0 & b^{k+1} \end{pmatrix}$$

Thus, P(k) true $\Rightarrow$ P(k + 1) true. So, P(1) is true and P(k) true $\Rightarrow$ P(k + 1) true imply, via the PMI, that P(n) is true ($\forall\, n \in \mathbb{N}$).

Example 14

Show that $(A_1\, A_2\, \ldots\, A_n)^{-1} = A_n^{-1} \ldots A_2^{-1}\, A_1^{-1}$, for all natural numbers n greater than or equal to 2.

We have,

$$\text{P}(n): (A_1\, A_2\, \ldots\, A_n)^{-1} = A_n^{-1} \ldots A_2^{-1}\, A_1^{-1}$$

The Base Case is n = 2. The LHS is $(A_1\, A_2)^{-1}$. The RHS is $A_2^{-1}\, A_1^{-1}$. Hence, P(2) is true. Assume that P(k) is true for some natural number k, i.e., $(A_1\, A_2\, \ldots\, A_k)^{-1} = A_k^{-1} \ldots A_2^{-1}\, A_1^{-1}$. The RTP statement is,

$$(A_1\, A_2\, \ldots\, A_k\, A_{k+1})^{-1} = A_{k+1}^{-1}\, A_k^{-1} \ldots A_2^{-1}\, A_1^{-1}$$

So,

$$(A_1\, A_2\, \ldots\, A_k\, A_{k+1})^{-1} = \left((A_1\, A_2\, \ldots\, A_k)\, A_{k+1}\right)^{-1}$$

$$= A_{k+1}^{-1}\, (A_1\, A_2\, \ldots\, A_k)^{-1}$$

$$= A_{k+1}^{-1}\, \left(A_k^{-1} \ldots A_2^{-1}\, A_1^{-1}\right)$$

$$= A_{k+1}^{-1}\, A_k^{-1} \ldots A_2^{-1}\, A_1^{-1}$$

Thus, P(k) true $\Rightarrow$ P(k + 1) true. So, P(2) is true and P(k) true $\Rightarrow$ P(k + 1) true imply, via the PMI, that P(n) is true for all natural numbers greater than 1.

Differentiation

Induction examples involving differentiation can look scary, but if the notation for higher derivatives is remembered, they are easy.

Example 15

Prove that, for $a \in \mathbb{R}$, $\frac{d^n}{dx^n}(e^{ax}) = a^n e^{ax}$ $(\forall n \in \mathbb{N})$.

$$P(n): \frac{d^n}{dx^n}(e^{ax}) = a^n e^{ax}$$

The Base Case is $n = 1$. The LHS is $\frac{d}{dx}(e^{ax})$, which is clearly equal to $a e^{ax}$. The RHS is $a e^{ax}$. Hence, P(1) is true. Assume that P(k) is true for some natural number k, i.e., $\frac{d^k}{dx^k}(e^{ax}) = a^k e^{ax}$. The RTP statement is,

$$\frac{d^{k+1}}{dx^{k+1}}(e^{ax}) = a^{k+1} e^{ax}$$

So,

$$\frac{d^{k+1}}{dx^{k+1}}(e^{ax}) = \frac{d}{dx}\left(\frac{d^{k+1}}{dx^{k+1}}(e^{ax})\right)$$

$$= \frac{d}{dx}(a^k e^{ax})$$

$$= a^k \frac{d}{dx}(e^{ax})$$

$$= a^k (a e^{ax})$$

$$= a^{k+1} e^{ax}$$

$$\therefore \qquad \frac{d^{k+1}}{dx^{k+1}}\left(e^{ax}\right) = a^{k+1}e^{ax}$$

Thus, P(k) true $\Rightarrow$ P(k + 1) true. So, P(1) is true and P(k) true $\Rightarrow$ P(k + 1) true imply, via the PMI, that P(n) is true ($\forall n \in \mathbb{N}$).

Example 16

Prove that $\frac{d^{2n}}{dx^{2n}}(\sin x) = (-1)^n \sin x \quad (\forall n \in \mathbb{N})$.

$$\text{P}(n): \frac{d^{2n}}{dx^{2n}}(\sin x) = (-1)^n \sin x$$

Don't let the $2n$ be a distraction. The statement just says that even derivatives (2nd, 4th, 6th, etc.) of $\sin x$ are either $\sin x$ or $-\sin x$. The Base Case is $n = 1$. The LHS is $\frac{d^2}{dx^2}(\sin x) = \frac{d}{dx}(\cos x) = -\sin x$. The RHS is $-\sin x$. Hence, as equality holds, P(1) is true. Now assume that P(k) is true for some natural number k, i.e., $\frac{d^{2k}}{dx^{2k}}(\sin x) = (-1)^k \sin x$. The RTP statement is,

$$\frac{d^{2(k+1)}}{dx^{2(k+1)}}(\sin x) = (-1)^{k+1} \sin x$$

So,

$$\frac{d^{2(k+1)}}{dx^{2(k+1)}}(\sin x) = \frac{d^{2k+2}}{dx^{2k+2}}(\sin x)$$

Splitting up the derivative this time is less obvious, but remember that we want to use the inductive hypothesis.

$$\frac{d^{2(k+1)}}{dx^{2(k+1)}}(\sin x) = \frac{d^2}{dx^2}\left(\frac{d^{2k}}{dx^{2k}}(\sin x)\right)$$

$$= \frac{d^2}{dx^2}\left((-1)^k \sin x\right)$$

$$= (-1)^k \frac{d^2}{dx^2} (\sin x)$$

$$= (-1)^k . (-\sin x)$$

$$= (-1)^k . (-1) . \sin x$$

$$= (-1)^{k+1} \sin x$$

$$\therefore \quad \frac{d^{2(k+1)}}{dx^{2(k+1)}} (\sin x) = (-1)^{k+1} \sin x$$

Thus, P(k) true $\Rightarrow$ P(k + 1) true. So, P(1) is true and P(k) true $\Rightarrow$ P(k + 1) true imply, via the PMI, that P(n) is true ($\forall n \in \mathbb{N}$).

Inequalities

Example 17

Prove that $2^n > n^2$ ($\forall n \geq 5$).

$$P(n) : 2^n > n^2$$

The Base Case is $n = 5$. The LHS is 32, whereas the RHS is 25. As $32 > 25$, P(5) is true. Assume that P(k) is true for some natural number $k \geq 5$, i.e., $2^k > k^2$. The RTP statement is,

$$RTP : 2^{k+1} > (k + 1)^2$$

Note that $(k + 1)^2 = k^2 + 2k + 1$. Also, $k > 4 \Rightarrow 2k > 8$ and $k^2 > 4k$. So,

$$2^{k+1} = 2^k . 2$$

$$> k^2 . 2$$

$$= k^2 + k^2$$

$$> k^2 + 4k$$

$$= k^2 + 2k + 2k$$

$$> k^2 + 2k + 8$$

$$> k^2 + 2k + 1$$

$$= (k + 1)^2$$

$$\therefore \quad 2^{k+1} > (k + 1)^2$$

Thus, P(k) true $\Rightarrow$ P(k + 1) true. So, P(5) is true and P(k) true $\Rightarrow$ P(k + 1) true imply, via the PMI, that P(n) is true ($\forall\, n \geq 5$).

Example 18

Show that $(n + 1)! > n^3$ ($\forall\, n > 3$).

$$P(n) : (n + 1)! > n^3$$

The Base Case is $n = 4$. The LHS is 120, whereas the RHS is 64. As $120 > 64$, P(4) is true. Assume that P(k) is true for some natural number $k \geq 5$, i.e., $(k + 1)! > k^3$. The RTP statement is,

$$RTP : (k + 2)! > (k + 1)^3$$

Note that $(k + 1)^3 = k^3 + 3k^2 + 3k + 1$. Also, $k > 3 \Rightarrow k + 2 > 5$, $k^2 > 3k$ and $k^3 > 3k^2$. So,

$$(k + 2)! = (k + 2).(k + 1)!$$

$$> (k + 2).k^3$$

$$> 5k^3$$

$$= k^3 + 4k^3$$

$$> k^3 + 12k^2$$

$$= k^3 + 3k^2 + 9k^2$$

$$> k^3 + 3k^2 + 27k$$

$$= k^3 + 3k^2 + 3k + 24k$$

$$> k^3 + 3k^2 + 3k + 72$$

$$> k^3 + 3k^2 + 3k + 1$$

$$= (k + 1)^3$$

$$\therefore \quad (k + 2)! > (k + 1)^3$$

Thus, P(k) true $\Rightarrow$ P($k + 1$) true. So, P(4) is true and P(k) true $\Rightarrow$ P($k + 1$) true imply, via the PMI, that P(n) is true ($\forall n > 3$).

Divisibility

Example 19

Prove that $6^n + 4$ is divisible by 5 ($\forall n \in \mathbb{N}$).

$$P(n) : \exists r \in \mathbb{N} \text{ s.t. } 6^n + 4 = 5r$$

The Base Case is $n = 1$. The LHS is 10, as is the RHS. Hence, P(1) is true. Assume that P(k) is true for some natural number k, i.e., $6^k + 4 = 5r$. The RTP statement is,

$$\text{RTP} : \exists s \in \mathbb{N} \text{ s.t. } 6^{k+1} + 4 = 5s$$

So,

$$6^{k+1} + 4 = 6^k . 6 + 4$$

$$= (5r - 4) . 6 + 4$$

$$= 30r - 24 + 4$$

$$= 30r - 20$$

$$= 5(6r - 4)$$

As $r \in \mathbb{N}$, $6r - 4 \in \mathbb{N}$, and so $6^{k+1} + 4$ is divisible by 5. So, P(k) true $\Rightarrow$ P($k + 1$) true. So, P(1) is true and P(k) true $\Rightarrow$ P($k + 1$) true imply, via the PMI, that P(n) is true $\forall n \in \mathbb{N}$.

Example 20

Prove that $7^{2n} - 48n - 1$ is divisible by 576 ($\forall n \in \mathbb{N}$).

$$P(n) : \exists r \in \mathbb{N} \text{ s.t. } 7^{2n} - 48n - 1 = 576r$$

The Base Case is $n = 1$. Substituting this value of n into the given expression yields $49 - 48 - 1 = 0$, which is clearly divisible by 576. Hence, P(1) is true. Assume that P(k) is true for some natural number k, i.e., $7^{2k} - 48k - 1 = 576r$. The RTP statement is,

$$RTP : \exists s \in \mathbb{N} \text{ s.t. } 7^{2(k+1)} - 48(k + 1) - 1 = 576s$$

So,

$$\begin{aligned} & 7^{2(k+1)} - 48(k + 1) - 1 \\ = \; & 7^{2k+2} - 48(k + 1) - 1 \\ = \; & 7^{2k} \cdot 7^2 - 48(k + 1) - 1 \\ = \; & (576r + 48k + 1) \cdot 49 - 48k - 49 \\ = \; & 576(49r) + 49 \cdot 48k + 49 - 48k - 49 \\ = \; & 576(49r) + 2\,304k \\ = \; & 576(49r + 4k) \end{aligned}$$

As $k, r \in \mathbb{N}$, $49r + 4k \in \mathbb{N}$, and so $7^{2(k+1)} - 48(k + 1) - 1$ is divisible by 576. So, P(k) true $\Rightarrow$ P($k + 1$) true. Together with P(1) is true, this implies, via the PMI, that P(n) is true $\forall n \in \mathbb{N}$.

Number Theory

The Division Algorithm

Theorem (**Division Algorithm**):

Given $a, b \in \mathbb{N}$, $\exists!\ q$ (**quotient**), r (**remainder**) $\in \mathbb{N}$ satisfying,

$$a = bq + r \qquad (0 \leq r < b)$$

Definition:

The **greatest common divisor** (aka **highest common factor**) of 2 natural numbers a and b, denoted GCD(a, b) is the biggest natural number that exactly divides those 2 numbers.

Theorem:

When $a = bq + r$, GCD(a, b) = GCD(b, r).

The Euclidean Algorithm and the HCF

The Division Algorithm and repeated use of the above give the following.

Theorem (**Euclidean Algorithm**):

A repeated use of the Division Algorithm for the integers a and b,

$$a = b\,q_1 + r_1 \quad (0 \leq r_1 < b)$$

$$b = r_1\,q_2 + r_2 \quad (0 \leq r_2 < r_1)$$

$$r_1 = r_2\,q_3 + r_3 \quad (0 \leq r_3 < r_2)$$

$$\vdots$$

$$r_{k-2} = r_{k-1}\,q_k$$

then gives GCD(a, b) = r_{k-1}.

Example 21

Find the GCD of 203 and 8 using the Euclidean Algorithm.

$$203 = 8 \,.\, 25 + 3 \quad \Rightarrow \quad GCD(203, 8) = GCD(8, 3)$$

$$8 = 3 \,.\, 2 + 2 \quad \Rightarrow \quad GCD(8, 3) = GCD(3, 2)$$

$$3 = 2 \,.\, 1 + 1 \quad \Rightarrow \quad GCD(3, 2) = GCD(2, 1)$$

$$2 = 1 \,.\, 2 \quad \Rightarrow \quad GCD(2, 1) = 1$$

Hence, stringing the equalities for the GCDs together shows that GCD(203, 8) = 1.

Theorem (**Bézout's Lemma**):

For any pair of non-zero integers a and b, the Euclidean Algorithm can be used to write GCD(a, b) as,

$$GCD(a, b) = ax + by$$

where $x, y \in \mathbb{Z}$.

Example 22

Write GCD(30, 42) in the form $30x + 42y$, stating the values of the integers x and y.

The Euclidean Algorithm gives,

$$42 = 30 \,.\, 1 + 12 \quad \Rightarrow \quad GCD(42, 30) = GCD(30, 12)$$

$$30 = 12 \,.\, 2 + 6 \quad \Rightarrow \quad GCD(30, 12) = GCD(12, 6)$$

$$12 = 6 \,.\, 2 \quad \Rightarrow \quad GCD(12, 6) = 6$$

Hence, GCD(42, 30) = 6. Solving for the remainders,

$$42 = 30 \,.\, 1 + 12 \quad \Rightarrow \quad 12 = 42 - 30 \,.\, 1$$

$$30 = 12 \,.\, 2 + 6 \quad \Rightarrow \quad 6 = 30 - 12 \,.\, 2$$

$$12 = 6 \,.\, 2 \quad \Rightarrow \quad 0 = 12 - 6 \,.\, 2$$

and working backwards gives,

$$\begin{aligned} 6 &= 30 - 12 \,.\, 2 \\ &= 30 - (42 - 30 \,.\, 1) \,.\, 2 \\ &= 30 - 42 \,.\, 2 + 30 \,.\, 2 \end{aligned}$$

i.e.,

$$6 = 30 \,.\, 3 - 42 \,.\, 2$$

with $x = 3$ and $y = -2$.

Definition:

2 integers a and b are **coprime** (aka **relatively prime**) if GCD$(a, b) = 1$.

Example 23

Determine whether or not 4 and 7 are coprime.

Working out the GCD gives,

$$7 = 4 \,.\, 1 + 3$$

$$4 = 3 \,.\, 1 + 1$$

$$3 = 1 \,.\, 3$$

Hence, as GCD$(4, 7) = 1$, 4 and 7 are coprime.

Example 24

Show that 12 and 16 are not relatively prime.

Working out the GCD gives,

$$16 = 12 . 1 + 4$$

$$12 = 4 . 3$$

So, as GCD(12,16) $\neq$ 1 (as it equals 4), 12 and 16 are not relatively prime.

Definition:

A **linear Diophantine equation** is an equation of the form,

$$ax + by = c \qquad (a, b, c, x, y \in \mathbb{Z})$$

Theorem:

A linear Diophantine equation has a solution provided that GCD(a, b) divides c.

Example 25

Show that the Diophantine equation $3x + 6y = 5$ has no solutions.

As GCD(3, 6) = 3 and 3 does not divide 5, the given equation has no solutions.

Theorem:

If a linear Diophantine equation has a solution, then it has infinitely many solutions.

Theorem:

If (x, y) is a solution to the Diophantine equation $ax + by = c$, then ($x + b$, $y - a$) is also a solution to $ax + by = c$.

Example 26

Find all solutions to the Diophantine equation $30x - 42y = 66$.

From Example 22, GCD(42, 30) = 6 = 30 . 3 − 42 . 2. As 6 divides 66, solutions to the given Diophantine equation exist.

As,

$$6 \,.\, 11 = 30 \,.\, 33 - 42 \,.\, 22$$

$x = 33$ and $y = -22$ are solutions to the given equation. All other solutions are of the form $x = 33 + 42n$ and $y = -22 + 30n$.

Number Bases

Theorem:

Any number A may be written uniquely in base n as,

$$A = \sum_{i=0}^{k} r_{k-i}\ n^{k-i} \equiv \left(r_k\ r_{k-1}\ \ldots\ r_2\ r_1\ r_0\right)_n$$

by dividing A, and all subsequent quotients, by n and obtaining the remainders (until a zero quotient is reached).

Changing a number to base 10 is quite easy.

Example 27

Write $(2031)_5$ in base 10.

$$(2031)_5 = 2 \,.\, 5^3 + 0 \,.\, 5^2 + 3 \,.\, 5^1 + 1 \,.\, 5^0$$

$$= 2 \,.\, 125 + 0 + 15 + 1$$

$$= (266)_{10}$$

Changing a base 10 number to another base requires use of the previous theorem.

Example 28

Change $(8469)_{10}$ to base 7.

$$8\,469 \div 7 = 1\,209 \text{ remainder } 6$$

$$1\,209 \div 7 = 172 \text{ remainder } 5$$

$$172 \div 7 = 24 \text{ remainder } 4$$

$$24 \div 7 = 3 \text{ remainder } 3$$

$$3 \div 7 = 0 \text{ remainder } 3$$

Hence, according to the above theorem, $(8469)_{10} = (33456)_{17}$.

For number bases bigger than 10, we need to invent new symbols for the bigger numbers. For example, in base 13, A stands for 11, B for 12 and C for 13.

Example 29

Convert $(8A69)_{12}$ to base 5.

We convert $(8A69)_{12}$ to base 10, then change that to base 5. Performing the first conversion gives,

$$(8A69)_{12} = 8 \cdot 12^3 + 11 \cdot 12^2 + 6 \cdot 12^1 + 9 \cdot 12^0$$

$$= 8 \cdot 1\,728 + 11 \cdot 144 + 6 \cdot 12 + 9 \cdot 1$$

$$= (15489)_{10}$$

Next, change this base 10 number into base 5,

$$15\,489 \div 5 = 3\,097 \text{ remainder } 4$$

$$3\,097 \div 5 = 619 \text{ remainder } 2$$

$$619 \div 5 = 123 \text{ remainder } 4$$

$$123 \div 5 = 24 \text{ remainder } 3$$

$$24 \div 5 = 4 \text{ remainder } 4$$

$$4 \div 5 = 0 \text{ remainder } 4$$

Hence, $(8A69)_{12} = (443424)_5$.