Division algorithms and Euclidean algorithms

Created by Mr. Francis Hung on 20081109 Last updated: August 31, 2021

I Division algorithm of numbers

Let a, b be two positive integers with $a > b$. There exists unique non-negative integers q and r such that $a = qb + r$, where $0 \le r < b$. (e.g. $47 = 5\times 9 + 2$)

Proof: Existence

Consider the sequence of integers: $a, a - b, a - 2b, a - 3b, \cdots, a - qb, \cdots$

It is a decreasing sequence of integers starting from a.

There is the least non-negative integer $r = a - qb \ge 0 > a - (q + 1)b \cdots (*)$

$\because 0 > a - (q + 1)b = a - qb - b$

$\therefore b > r$

So $0 \le r < b$ and $a = qb + r$.

Uniqueness

Suppose there is another set of non-negative integers (q_1, r_1) so that $a = q_1 b + r_1$; where $0 \le r_1 < b$.

$r_1 = a - q_1 b$

$0 \le r_1 < b \Rightarrow 0 \le a - q_1 b < b$

$\because r$ is the least non-negative integer such that $0 \le r < b$

$\therefore 0 \le r \le r_1 < b$

If $r \ne r_1$, then $0 \le r < r_1 < b \Rightarrow 0 \le a - qb < a - q_1 b < b$

$0 < qb - q_1 b$ and $a < q_1 b + b$

$q_1 < q$ and $a < (q_1 + 1)b$

$\therefore a < (q_1 + 1)b < (q + 1)b \Rightarrow -a > -(q_1 + 1)b > -(q + 1)b$

$a - a > a - (q_1 + 1)b > a - (q + 1)b$

$0 > a - (q_1 + 1)b > a - (q + 1)b$

By (*), $r = a - qb \ge 0 > a - (q_1 + 1)b > a - (q + 1)b$

$-qb > -(q_1 + 1)b > -(q + 1)b$

$q < q_1 + 1 < q + 1$, but $q_1 + 1$ cannot lie between two consecutive integers $\Rightarrow$ contradiction

$\therefore r = r_1 \Rightarrow q = q_1$

Let a, b be two positive integers, we can use synthetic division to find the H.C.F. and L.C.M..

e.g. To find the H.C.F. and L.C.M. of 5451 and 782.

$$\begin{array}{r|ll} 23 & 5451 & 782 \\ \hline 3 & 237 & 2\,|\,34 \\ \hline & 79 & 17 \\ & \text{prime} & \text{prime} \end{array}$$

$\therefore$ H.C.F. = 23

L.C.M. = $23\times 237\times 34 = 185334 = \dfrac{5451\times 782}{23}$

Note that (1) to determine whether a number n is a prime, divide n by all prime numbers $\le \sqrt{n}$.

(2) H.C.F. $\times$ L.C.M. = $a\times b$

(3) H.C.F. = Highest common factor = greatest common divisor = g.c.d. = (a, b)

(4) L.C.M. = least common multiplier (multiple)

II The Euclidean algorithms 輾轉相除法

We can use the Euclidean algorithm to find the H.C.F. of 5451 and 782.

Step 1 $5451 > 782$.

$5451 = 782\times 6 + 759$

Step 2 $782 > 759$

$782 = 759\times 1 + 23$

Step 3 $759 > 23$

$759 = 23\times 33 + 0$

$\therefore$ H.C.F. is 23 .

Exercise Find the H.C.F. of

(a) 462, 588; [ans. 42]

(b) 1518, 1932; [ans. 138]

(c) 7392, 6720, 8736. [ans. 672]

We can write in compact form as follows:

1	782	5451	6
	759	4692	
	23	759	33
	HCF	759	
		0	

Theorem To find the g.c.d.(a, b) using Euclidean algorithm.

If $a = b$, then $(a, b) = a$.

Otherwise suppose without loss of generality, $a > b$.

Consider $a \div b$, a = quotient $\times$ divisor + remainder

$$a = q_0 b + r_1, \qquad 0 \le r_1 < b$$
$$b = q_1 r_1 + r_2, \qquad 0 \le r_2 < r_1$$
$$r_1 = q_2 r_2 + r_3 \qquad 0 \le r_3 < r_2$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_{k-1} = q_k r_k + r_{k+1} \qquad 0 \le r_{k+1} < r_k$$

Since $0 \le r_{k+1} < r_k < r_{k-1} < \cdots < r_3 < r_2 < r_1 < b$ and b is a fixed number.

$\therefore$ $\{r_k\}$ is a decreasing sequence of integers and all are non-negative.

There is a <u>first</u> integer n such that $r_{n+1} = 0$

$$\begin{cases} a = q_0 b + r_1, \quad 0 < r_1 < b \cdots (1) \\ b = q_1 r_1 + r_2, \quad 0 < r_2 < r_1 \cdots (2) \\ r_1 = q_2 r_2 + r_3, \quad 0 < r_3 < r_2 \cdots (3) \\ \quad \cdots\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n, 0 < r_n < r_{n-1} \cdots (n) \\ r_{n-1} = q_n r_n + r_{n+1}, \quad r_{n+1} = 0 \ \cdots (n+1) \end{cases}$$

$\therefore$ $r_{n-1} = q_n r_n$

We can prove by induction that r_n divides r_{n-m} for $m = 1, 2, \cdots, n-1$.
From equation $(n + 1)$, $r_{n-1} = q_n r_n$, so r_n divides r_{n-1} .
From equation (n), $r_{n-2} = q_{n-1} r_{n-1} + r_n = q_{n-1}(q_n r_n) + r_n = (q_{n-1}q_n + 1)r_n$, so r_n divides r_{n-2} .
Suppose r_n divides r_{n-k} and r_{n-k+1} , i.e. $r_{n-k} = r_n s$ and $r_{n-k+1} = r_n t$, where s, t are integers.
$r_{n-(k+1)} = q_{n-k} r_{n-k} + r_{n-k+1} = q_{n-k} (r_n s) + r_n t = (q_{n-k} s + t) r_n$, r_n divides $r_{n-(k+1)}$.
By the principle of mathematical induction, r_n divides r_{n-m} for $m = 1, 2, \cdots, n-1$.
When $m = n - 1$, r_n divides r_1, which means equation (2): $b = q_1r_1 + r_2$ which is divisible by r_n .
Equation (1): $a = q_0b + r_1$, which is also divisible by r_n .
$\therefore$ r_n is a common factor of a and b $\cdots\cdots$ (*)

Let c (> 0) be any other common factor of a and b .
From equation (1): $r_1 = a - q_0b \Rightarrow c$ divides r_1 .
From equation (2): $r_2 = b - q_1r_1 \Rightarrow c$ divides r_2 .
Suppose c divides r_{k-2} and c divides r_{k-1} for some positive integer k, where $2 < k \le n$.
From equation (k): $r_k = r_{k-2} - q_{k-1}r_{k-1} \Rightarrow c$ divides r_k .
By MI, c divides r_m for all m, where $1 \le m \le n$.
In particular, c divides r_n $\cdots\cdots$ (**)

Combine (*) and (**), r_n is the H.C.F. of a and b .

Theorem If $(a, b) = r_n$, then there exist integers s, t such that $sa + tb = r_n$
We shall prove by M.I. that there exist integers s_m, t_m such that $s_ma + t_mb = r_m$ for $m = 1, 2, \cdots, n$.
Proof: From equation $(n+1)$: $r_{n-1} = q_n r_n$ $\cdots\cdots$ $(n+1')$
From equation (n): $r_n = r_{n-2} - q_{n-1} r_{n-1}$ $\cdots\cdots$ (n')
From equation $(n-1)$: $r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$ $\cdots\cdots$ $(n-1')$
$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$
From equation (3): $r_3 = r_1 - q_2 r_2$ $\cdots\cdots$ (3')
From equation (2): $r_2 = b - q_1 r_1$ $\cdots\cdots$ (2')
From equation (1): $r_1 = a - q_0 b$ $\cdots\cdots$ (1')
Sub. (1') into (2'): $r_2 = b - q_1(a - q_0 b) = -q_1a + (q_0q_1 + 1)b$ $\cdots\cdots$ (2'')
Sub. (1') & (2'') into (3'): $r_3 = a - q_0 b - q_2 [-q_1a + (q_0q_1 + 1)b] = (1 + q_1q_2)a - (q_0+q_0q_1q_2+q_2)b$
Suppose $s_{k-1}a + t_{k-1}b = r_{k-1}$ and $s_ka + t_kb = r_k$ for some positive integer $k - 1$ and k .
Sub. them into equation $(k+1')$: $r_{k+1} = r_{k-1} - q_k r_k = (s_{k-1}a + t_{k-1}b) - q_k (s_ka + t_kb)$
$r_{k+1} = (s_{k-1} - q_k s_k)a + (t_{k-1} - q_k t_k)b = s_{k+1} a + t_{k+1} b$
By M.I., there exist integers s_m, t_m such that $s_ma + t_mb = r_m$ for $m = 1, 2, \cdots, n$.
In particular, there exist integers s, t such that $sa + tb = r_n$.

Conversely, if there exist integers s, t such that $sa + tb = r$, where r is the smallest positive integer, then r = g.c.d.(a, b). Note that s or t may be negative.

Proof: Let $M = \{sa + tb: s, t \in \mathbb{Z}\}$

$a > b \in M$

$\therefore M \neq \phi$

If $x = sa + tb \in M$

$-x = (-s)a + (-t)b \in M$

$\therefore$ M always has some positive integers.

Let $M_1 = \{x \in M: x > 0\}$

Then M_1 is bounded below by 0 .

There is the smallest positive integer $r \in M_1$.

Let $r = s_0a + t_0b$

Let d divides a and d divides b, then d divides $(s_0a + t_0b) = r$

Hence d divides r …… (*)

For any $x = sa + tb \in M$ ⋯ (1)

By division algorithm ($x \div r$), $x = qr + r_1$ ⋯ (2) where $0 \le r_1 < r$ ⋯ (3)

$x = sa + tb = q(s_0a + t_0b) + r_1$

$r_1 = (s - qs_0)a + (t - qt_0)b$

$\therefore r_1 \in M_1$

$\because$ By (3), $0 \le r_1 < r$ and r is the smallest positive integer.

$\therefore r_1 = 0$

By (2), $x = qr$

r divides x .

By (1), r divides $sa + tb \in M$

$a = 1a + 0b \in M$

$b = 0a + 1b \in M$

$\therefore$ r divides a and r divides b

r is the common factor of a and b …… (**)

By (*) and (**), r = g.c.d.(a, b).

In particular, if $sa + tb = 1$, then a and b are relatively prime. $(a, b) = 1$.

Example 1 Let d be the H.C.F. of 24543 and 17982.

(a) Find d .

(b) Find integers m and n such that $24543m + 17982n = d$.

(a) By Euclidean algorithm,

$24543 = 17982 + 6561$ …… (1)

$17982 = 2\times 6561 + 4860$ …… (2)

$6561 = 4860 + 1701$ …… (3)

$4860 = 2\times 1701 + 1458$ …… (4)

$1701 = 1458 + 243$ …… (5)

$1458 = 6\times 243$ …… (6)

$\therefore d = 243$

(b) From (5), $243 = 1701 - 1458$ …… (7)

From (4), $1458 = 4860 - 2\times 1701$ …… (8)

From (3), $1701 = 6561 - 4860$ … (9)

From (2), $4860 = 17982 - 2\times 6561$ …… (10)

From (1), $6561 = 24543 - 17982$ …… (11)

Sub. (11) into (10): $4860 = 17982 - 2\times(24543 - 17982)$

$4860 = 3\times 17982 - 2\times 24543$ …… (12)

Sub. (11) & (12) into (9): $1701 = 24543 - 17982 - (3\times 17982 - 2\times 24543)$

$1701 = 3\times 24543 - 4\times 17982$ …… (13)

Sub. (12) & (13) into (8): $1458 = 3\times 17982 - 2\times 24543 - 2\times(3\times 24543 - 4\times 17982)$

$1458 = 11\times 17982 - 8\times 24543$ …… (14)

Sub. (13) & (14) into (7): $243 = 3\times 24543 - 4\times 17982 - (11\times 17982 - 8\times 24543)$

$243 = 11\times 24543 - 15\times 17982$; $m = 11$, $n = -15$

Method 2

$24543m + 17982n = d \Rightarrow 101\times243m + 74\times243n = 243$

$101m + 74n = 1$

$101 = 74 + 27 \cdots\cdots (1)$

$74 = 2\times27 + 20 \cdots\cdots (2)$

$27 = 20 + 7 \cdots\cdots (3)$

$20 = 2\times7 + 6 \cdots\cdots (4)$

$7 = 6 + 1 \cdots\cdots (5)$

From (5), $1 = 7 - 6 \cdots\cdots (6)$

From (4), $6 = 20 - 2\times7 \cdots\cdots (7)$

From (3), $7 = 27 - 20 \cdots\cdots (8)$

From (2), $20 = 74 - 2\times27 \cdots\cdots (9)$

From (1), $27 = 101 - 74 \cdots \cdots (10)$

Sub. (10) into (9): $20 = 74 - 2\times(101 - 74)$

$20 = 3\times74 - 2\times101 \cdots\cdots (11)$

Sub. (10) & (11) into (8): $7 = 101 - 74 - (3\times74 - 2\times101)$

$7 = 3\times101 - 4\times74 \cdots\cdots (12)$

Sub. (11) & (12) into (7): $6 = 3\times74 - 2\times101 - 2\times(3\times101 - 4\times74)$

$6 = 11\times74 - 8\times101 \cdots\cdots (13)$

Sub. (12) & (13) into (6): $1 = 3\times101 - 4\times74 - (11\times74 - 8\times101)$

$1 = 11\times101 - 15\times74$; $m = 11$, $n = -15$

Let F be a number field (e.g. rational number, real number, complex number.)

Define $F[x] = \{a_n x^n + \cdots + a_1 x + a_0 : a_r \in F, r = 0, 1, 2, \ldots, n\}$

If $f(x) \in F[x]$, then $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $n \in \mathbb{N} \cup \{0\}$.

If $a_n \neq 0$, define the degree of $f(x) = n$.
If $a_n = 0$, define the degree of $f(x) = -\infty$

The coefficient of x^r is a_r is a_r, $r = 0, 1, 2, \cdots, n$

The leading coefficient $= a_n$.
If $a_n = 1$, $f(x)$ is called a monic polynomial.

If $a_r \in \mathbb{Z}$ for $r = 0, 1, 2, \cdots, n$ and $a_n = 1$, $f(x)$ is called an integer monic polynomial.

The leading term $= a_n x^n$
Constant term $= a_0$
If $f(x) = a_0$, then $f(x)$ is called a constant polynomial.
Let $f(x), g(x) \in F[x]$.
$g(x)$ is a factor of $f(x)$ if there exist polynomial $h(x) \in F[x]$ such that $f(x) = g(x)\, h(x)$.
We say that $f(x)$ is divisible by $g(x)$ or $f(x)$ is a multiple of $g(x)$.

e.g. $x^2 - 2 \in \mathbb{Q}[x]$

$x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$

But $\left(x + \sqrt{2}\right) \notin \mathbb{Q}[x]$

$\therefore$ $\left(x + \sqrt{2}\right)$ is not a factor of $x^2 - 2$ over $\mathbb{Q}$.

On the other hand, for $x^2 - 2 \in \mathbb{R}[x]$
$\left(x + \sqrt{2}\right)$ is a factor of $x^2 - 2$ over $\mathbb{R}$.

Similarly $x^2 + 1 \in \mathbb{Q}[x]$ but $x + i \notin \mathbb{Q}[x]$, where $i = \sqrt{-1}$
$\therefore$ $x + i$ is not a factor of $x^2 + 1$ over $\mathbb{Q}$, nor a factor over $\mathbb{R}$.

In factor, for $x^2 + 1 \in \mathbb{C}[x]$, $x + i$ is a factor over $\mathbb{C}$.

$f(x) \in F[x]$ is said to be irreducible/ prime polynomial if it cannot be expressed as the product of two polynomials of positive degree in $F[x]$, otherwise it is reducible.

e.g. $2(x + 1)$ is irreducible over $\mathbb{Q}[x]$, $\mathbb{R}[x]$ or $\mathbb{C}[x]$.

$x^2 - 2$ is irreducible over $\mathbb{Q}[x]$ only.

$x^2 - 2$ is reducible over $\mathbb{R}[x]$ or $\mathbb{C}[x]$.

H.C.F. (or gcd) of $f(x), g(x) \in F[x]$.
Let $d(x)$ be a monic polynomial in $F[x]$.
$d(x) = \gcd(f(x), g(x))$ if and only if the following are satisfied:
(1) $d(x)$ divides $f(x)$ and $d(x)$ divides $g(x)$.
(2) If $h(x) \in F[x]$ and if $h(x)$ divides $f(x)$, $h(x)$ divides $g(x)$, then $h(x)$ divides $d(x)$.

e.g. $f(x) = 2x$, $g(x) = 4x(x - 1)$
HCF $= x$ (not $2x$)

e.g. $f(x) = x^2 + 1$, $g(x) = x - i$ over $\mathbb{R}$.

There is no H.C.F. because $g(x) \notin \mathbb{R}[x]$.

Let F be the field (either $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$), f(x), g(x) $\in$ F[x] and g(x) $\neq 0$

then there exist unique q(x), r(x) $\in$ F[x] such that f(x) = g(x)q(x) + r(x), where deg r(x) < deg g(x).

Proof: <u>Existence</u>

If f(x) $\equiv 0$ or deg f(x) < deg g(x), then f(x) = 0 g(x) + f(x), done.

Otherwise use induction on deg f(x).

Step 1 If deg f(x) = 0

$f(x) = a_0 \neq 0$

$\because$ deg f(x) $\geq$ deg g(x) = 0

$\therefore$ g(x) = $c \neq 0$

$f(x) = a_0 = \left(\frac{a_0}{c}\right)c + 0$, done.

Step 2 Suppose it is true for <u>all</u> polynomial $\in$ F[x] of degree less than (but not equal to) k.

Let $f(x) = a_k x^k + \cdots + a_1 x + a_0$, where $a_k \neq 0$

and $g(x) = b_m x^m + \cdots + b_1 x + b_0$, where $b_m \neq 0$, $k, m \in \mathbb{N}$, $k \geq m$

Let $f_1(x) = f(x) - \frac{a_k}{b_m} x^{k-m} g(x) = a_k x^k + \cdots + a_1 x + a_0 - (a_k x^k + \text{other lower terms})$

= polynomial of degree < k

By induction assumption, $f_1(x) = q_1(x)g(x) + r(x)$, deg r($x$) < deg g($x$).

$\therefore q_1(x)\, g(x) + r(x) = f(x) - \frac{a_k}{b_m} x^{k-m} g(x)$

$f(x) = \left[q_1(x) + \frac{a_k}{b_m} x^{k-m}\right] g(x) + r(x) = Q(x)\, g(x) + r(x)$, where $Q(x) = q_1(x) + \frac{a_k}{b_m} x^{k-m}$.

By the principle of mathematical induction, the existence is true for all $k \in \mathbb{N}$.

<u>Uniqueness</u>

Suppose $f(x) = q_1(x)g(x) + r_1(x) \equiv q_2(x)g(x) + r_2(x)$

where $r_1(x) \equiv 0$ or deg $r_1(x)$ < deg g(x), $r_2(x) \equiv 0$ or deg $r_2(x)$ < deg g(x)

Rearrange the terms: $[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x)$ …… (*)

If $r_1(x) \neq r_2(x)$, deg $g(x) \leq \deg[(q_1(x) - q_2(x))g(x)] = \deg[r_2(x) - r_1(x)]$

$\leq \max[\deg r_1(x), \deg r_2(x)]$

$< \deg g(x)$, which is a contradiction.

$\therefore r_1(x) \equiv r_2(x)$; after substitution into (*), $q_1(x) \equiv q_2(x)$

By division algorithm, let $f(x)$, $g(x) \in F[x] \setminus \{0\}$, then there exists a positive integer $n \in \mathbb{N}$ such that

$f(x) = q_0(x)\, g(x) + r_0(x)$, $\deg r_0(x) < \deg g(x)$

$g(x) = q_1(x)\, r_0(x) + r_1(x)$, $\deg r_1(x) < \deg r_0(x)$

$r_0(x) = q_2(x)\, r_1(x) + r_2(x)$, $\deg r_2(x) < \deg r_1(x)$

…………………………………………………

$r_{n-2}(x) = q_n(x) r_{n-1}(x) + r_n(x)$, $\deg r_n(x) < \deg r_{n-1}(x)$

$r_{n-1}(x) = q_{n+1}(x)\, r_n(x)$

In this case, $r_n(x) = \text{HCF}(f(x), g(x))$.

Proof: We shall prove that $r_{n-i}(x)$ is a multiple of $r_n(x)$ by MI on i.

$i = 0$, $r_n(x)$ is a multiple of itself.

$i = 1$, $r_{n-1}(x) = q_{n+1}(x) r_n(x)$, which is a multiple of $r_n(x)$.

Suppose $r_{n-i}(x) = t(x) r_n(x)$, for some $t(x) \in F[x]$, and

suppose $r_{n-i+1}(x) = u(x) r_n(x)$, for some $u(x) \in F[x]$, where $i \geq 1$.

Now $r_{n-(i+1)} = q_{n-i+1}(x) r_{n-i}(x) + r_{n-i+1}(x)$, $\deg r_{n-i+1}(x) < \deg r_{n-i}(x)$

$= q_{n-i+1}(x) t(x) r_n(x) + u(x) r_n(x)$

$= [q_{n-i+1}(x) t(x) + u(x)] r_n(x)$

$\therefore$ $r_{n-(i+1)}$ is a multiple of $r_n(x)$.

By MI, $r_{n-i}(x)$ is a multiple of $r_n(x)$ for $i = 0, 1, 2, \dots, n$

In particular, $i = n - 1$, $r_1(x)$ is a multiple of $r_n(x)$.

$i = n$, $r_0(x)$ is a multiple of $r_n(x)$.

So $g(x) = q_1(x)\, r_0(x) + r_1(x)$, which is a multiple of $r_n(x)$.

Also, $f(x) = q_0(x)\, g(x) + r_0(x)$, which is a multiple of $r_n(x)$.

$\therefore$ $r_n(x)$ is a common factor of $g(x)$ and $f(x)$.

Now suppose $d(x) \in F[x] \setminus \{0\}$ such that $d(x)$ divides both $g(x)$ and $f(x)$.

Then $d(x)$ divides $[u(x)g(x) + v(x)f(x)]$ for all $u(x)$, $v(x) \in F[x]$

Claim $r_j(x) = m_j(x)\, f(x) + n_j(x)\, g(x)$, $j = 0, 1, 2, \dots, n$ for some $m_j(x)$, $n_j(x) \in F[x]$

Induction on j.

$j = 0$, $r_0(x) = f(x) - g(x) q_0(x)$ $\therefore$ It is true for $j = 0$.

$j = 1$, $r_1(x) = g(x) - r_0(x) q_1(x) = g(x) - [f(x) - g(x) q_0(x)] q_1(x)$

$= -q_1(x) f(x) + [1 + q_0(x) q_1(x)] g(x)$, $\therefore$ It is also true for $j = 1$.

Suppose $r_j(x) = m_j(x)\, f(x) + n_j(x)\, g(x)$, for $j < k \leq n$.

$\because$ $r_{k-2}(x) = q_k(x) r_{k-1}(x) + r_k(x)$

$\therefore$ $r_k(x) = r_{k-2}(x) - r_{k-1}(x) q_k(x)$

$r_k(x) = m_{k-2}(x)\, f(x) + n_{k-2}(x)\, g(x) - [m_{k-1}(x)\, f(x) + n_{k-1}(x)\, g(x)] q_k(x)$, by induction assumption.

$r_k(x) = [m_{k-2}(x) - m_{k-1}(x) q_k(x)]\, f(x) + [n_{k-2}(x) - n_{k-1}(x)\, q_k(x)] g(x)$

$\therefore$ It is also true for $j = k$.

By M.I., it is true for all $j = 0, 1, 2, \cdots, n$.

When $j = n$, $r_n(x) = u_n(x)\, f(x) + v(x) g(x)$

$\therefore$ $d(x)$ divides $r_n(x)$.

$r_n(x)$ is the gcd of $f(x)$ and $g(x)$ over F.

Example 2 1989 Sample Paper 1 Q7

Let $P(x) = 2x^5 + x^3 + 3x^2 + 1$ and $Q(x) = x^3 + x + 1$.

(a) Show that $P(x)$ and $Q(x)$ are relatively prime.

(b) Find two polynomial $S(x)$ and $T(x)$ such that $P(x)\ S(x) + Q(x)\ T(x) \equiv 1$.

Solution (a)

$2x^2 - 1$	$2x^5 + x^3 + 3x^2 + 1$	$x^3 + x + 1$	$x - 1$
	$2x^5 + 2x^3 + 2x^2$	$x^3 + x^2 + 2x$	
	$-x^3 + x^2 + 1$	$-x^2 - x + 1$	
	$-x^3 - x - 1$	$-x^2 - x - 2$	
	$x^2 + x + 2$	3	

$\therefore$ $P(x)$ and $Q(x)$ are relatively prime.

(b) From (a), $3 = Q(x) - (x^2 + x + 2)(x - 1)$

$= Q(x) - [P(x) - Q(x)\ (2x^2 - 1)](x - 1)$

$= Q(x)\ (2x^3 - 2x^2 - x + 2) + P(x)(1 - x)$

$\therefore\ S(x) = \frac{1}{3}\left(2x^3 - 2x^2 - x + 2\right)$; $T(x) = \frac{1}{3}(1 - x)$

Example 3 HKU O Level 1959 Paper 1 Q6 (a)

(a) Find the H.C.F. of $x^4 - 21x + 8$ and $8x^4 - 21x^3 + 1$.

(b) Find the values of the constants a, b, a', b' so that

$(ax + b)\ (x^4 - 21x + 8) + (a'x + b')\ (8x^4 - 21x^3 + 1) \equiv x^2 - 3x + 1$

(a)

x	$x^4 - 21x + 8$		$8x^4 - 21x^3 + 1$	8
	$x^4 - 8x^2 + 3x$		$8x^4 - 168x + 64$	
8	$8x^2 - 24x + 8$	-21	$-21x^3 + 168x - 63$	
	$x^2 - 3x + 1$		$x^3 - 8x + 3$	$x + 3$
			$x^3 - 8x + 3$	
			0	

$\therefore$ HCF $= x^2 - 3x + 1$

(b) We have already found out the H.C.F. is $x^2 - 3x + 1$. By division,

$x^4 - 21x + 8 = (x^2 - 3x + 1)(x^2 + 3x + 8)$; $8x^4 - 21x^3 + 1 = (x^2 - 3x + 1)(8x^2 + 3x + 1)$

So $(ax + b)\ (x^2 + 3x + 8) + (a'x + b')\ (8x^2 + 3x + 1) \equiv 1$

Using Euclidean Algorithm again,

$8x^2 + 3x + 1 = 8(x^2 + 3x + 8) - 21(x + 3)$ ...... (1)

$x^2 + 3x + 8 = (x + 3)x + 8$ ...... (2)

x(1) + 21(2): $21(x^2 + 3x + 8) + x(8x^2 + 3x + 1) = 8x(x^2 + 3x + 8) + 168$

$(21 - 8x)(x^2 + 3x + 8) + x(8x^2 + 3x + 1) = 168$

$\left(\frac{1}{8} - \frac{1}{21}x\right)\left(x^2 + 3x + 8\right) + \left(\frac{1}{168}x + 0\right)\left(8x^2 + 3x + 1\right) \equiv 1$

1986 Paper 1 Q8

Let f(x) and $g(x)$ be two non-zero polynomials. A polynomial $d(x)$ is said to be a Greatest Common Divisor (G.C.D.) of f(x) and $g(x)$ if $d(x)$ divides each of them and every common divisor of them also divides $d(x)$.

(a) Let $d_1(x)$ and $d_2(x)$ be two non-zero polynomials which divides each other.
Show that $d_1(x) = kd_2(x)$ for some non-zero constant k.

(b) Let A be the set of non-zero polynomials $p(x)$, where $p(x) = m(x)$ f(x) + $n(x)g(x)$ for some polynomials $m(x)$ and $n(x)$.

(i) Show that if a polynomial $s(x)$ divides both f(x) and $g(x)$, then it divides every $p(x)$ in A.

(ii) Let $p(x)$ be in A. Show that when f(x) is divided by $p(x)$, then the remainder $r(x)$ is either zero or a polynomial in A.

(iii) Let $d_1(x)$ be in A with deg $d_1(x) \le$ deg $p(x)$ for all $p(x)$ in A. Show that $d_1(x)$ is a G.C.D. of f(x) and $g(x)$.

(c) Show that if $d(x)$ is a G.C.D. of f(x) and $g(x)$, then there exist polynomials $m_0(x)$ and $n_0(x)$ such that $d(x) = m_0(x)$ f(x) + $n_0(x)$ $g(x)$.

(a) $d_1(x) = p(x)d_2(x)$

$d_2(x) = q(x)d_1(x)$

deg $d_1(x)$ = deg $p(x)$ + deg $d_2(x) \ge$ deg $d_2(x)$

deg $d_2(x)$ = deg $q(x)$ + deg $d_2(x) \ge$ deg $d_1(x)$

$\therefore$ deg $d_1(x)$ = deg $d_2(x)$ and deg $p(x) = 0 =$ deg $q(x)$

$\Rightarrow p(x) = k_1$, $q(x) = k_2 \ne 0$

$\therefore$ $d_1(x) = kd_2(x)$ for some non-zero constant k.

(b) $A = \{p(x) \ne 0$: $p(x) = m(x)$ f(x) + $n(x)g(x)$ for some polynomials $m(x)$ and $n(x)\}$

(i) If a polynomial $s(x)$ divides both f(x) and $g(x)$, then f(x) = $s(x)u(x)$, $g(x) = s(x)v(x)$.

For every $p(x)$ in A, $p(x) = m(x)$ f(x) + $n(x)g(x) = m(x)s(x)u(x) + n(x)s(x)v(x)$

$p(x) = [m(x)\ u(x) + n(x)\ v(x)]\ s(x)$

$\therefore$ $s(x)$ divides $p(x)$.

(ii) When f(x) is divided by $p(x)$, let f(x) = $p(x)\ Q(x) + r(x)$

The remainder $r(x)$ is either zero or degree of $r(x)$ < degree of f(x)

If $r(x)$ is a non-zero polynomial, then degree of $r(x)$ < degree of f(x)

f(x) = $[m(x)$ f(x) + $n(x)g(x)]\ Q(x) + r(x)$

$r(x) = [1 - m(x)Q(x)]$f(x) $- n(x)Q(x)g(x)$

$\therefore$ $r(x) \in A$

$\therefore$ The remainder $r(x)$ is either zero or a polynomial in A.

(iii) Let $d_1(x)$ be in A with deg $d_1(x) \le$ deg $p(x)$ for all $p(x)$ in A.

Let $d_1(x) = m_1(x)$ f(x) + $n_1(x)g(x)$

Consider f(x) $\div d_1(x)$. f(x) = $q(x)\ d_1(x) + r(x)$, where deg $r(x)$ < deg $d_1(x)$

By the result of (b) (ii), $r(x) \equiv 0$ or $r(x) \in A$.

Given that deg $d_1(x) \le$ deg $p(x)$ for all $p(x)$ in A.

If $r(x) \in A$, then deg $d_1(x) \le$ deg $r(x)$, which contradict that deg $r(x)$ < deg $d_1(x)$

$\therefore r(x) \equiv 0$

$f(x) = q(x)\, d_1(x)$, so $d_1(x)$ divides $f(x)$.

Similarly consider $g(x) \div d_1(x)$. It is easy to show that the remainder is zero and $d_1(x)$ divides $g(x)$.

$\therefore d_1(x)$ is a common factor of $f(x)$ and $g(x)$ … (1)

Let $s(x)$ be a common factor of $f(x)$ and $g(x)$.

By the result of (b) (i), $s(x)$ divides every polynomial $p(x)$ in A.

In particular, $d_1(x) = m_1(x)f(x) + n_1(x)g(x) \in A$

So $s(x)$ divides $d_1(x)$ ⋯⋯ (2)

Combining (1) & (2), $d_1(x)$ is the G.C.D. of $f(x)$ and $g(x)$.

(c) By (b) $d_1(x) = m_1(x)\, f(x) + n_1(x)g(x)$ is a G.C.D. of $f(x)$ and $g(x)$.

Let $d(x)$ be a G.C.D. of $f(x)$ and $g(x)$.

By (a), $d(x)$ and $d_1(x)$ divides each other.

So $d(x) = kd_1(x)$ for some non-zero constant k.

$d(x) = k[m_1(x) f(x) + n_1(x)g(x)]$

$d(x) = km_1(x) f(x) + kn_1(x)g(x)$

$d(x) = m_0(x) f(x) + n_0(x)g(x)$, where $m_0(x) = km_1(x)$ and $n_0(x) = kn_1(x)$.