Proof of Theorem

Clearly the smallest integer in $\mathbb{Z}_+$ of the form $a_1 m + b_1 n$, for $a_1, b_1 \in \mathbb{Z}$, does exist; and if $k|m$ and $k|n$ then $k | a_1 m + b_1 n$ for any $a_1, b_1 \in \mathbb{Z}$

If $g = a_0 m + b_0 n$ is the smallest such integer in $\mathbb{Z}_+$ we need to show $g | m$ and $g | n$

We show $g|m$. The proof that $g|n$ is similar.

By the Euclidean property

$$m = qg + r \quad \text{for } r, q \in \mathbb{Z} \text{ and } 0 \le r < g$$

So $r = m - qg = m - qa_0 m - qb_0 n = (1 - qa_0)m + (-qb_0)n$

If $r > 0$ this contradicts property 3 of g because $r < g$

So $r = 0$ and $m = qg$ and $g|m$. □

Least common multiple

If m, n are non zero integers, the least common multiple (lcm) l of m, n is a (strictly positive) integer such that

$$m | l, \quad n | l \quad \text{and} \quad l | p \text{ whenever } m|p \text{ and } n|p.$$

The lcm of m and n also exists. In fact, if g is the gcd of m and n and $m = m_1 g$, $n = n_1 g$ then

$$\text{lcm} = l = m_1 n_1 g.$$

How to find the gcd. using the Euclidean algorithm

Suppose $m, n \in \mathbb{Z} \setminus \{0\}$ with $|m| \leq |n|$

$$n = q_1 m + r_1 \qquad q_1, r_1 \in \mathbb{Z}, \quad 0 \leq r_1 < |m|$$

If $r_1 = 0$ then $m \mid n$ and gcd $= m$.

Otherwise

$$m = q_2 r_1 + r_2 \qquad q_2, r_2 \in \mathbb{Z}, \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$ then $r_1 \mid m \Rightarrow r_1 \mid n$

Otherwise define r_i for $0 \leq i \leq k$ $r_{i+1} < r_i$ $r_k = 0$

$$r_i = q_{i+2} r_{i+1} + r_{i+2} \qquad 0 \leq r_{i+2} < r_{i+1}$$
$$q_i, r_i \in \mathbb{Z} \ \forall i \leq k$$

Define $m = r_0$
$n = r_{-1}$ Using matrix notation.

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} q_{i+2} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix}$$

$$\begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$$

$$\cdots = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{k-1} \\ r_k = 0 \end{pmatrix}$$

$$= \begin{pmatrix} n_1 & v \\ m_1 & v \end{pmatrix} \begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix} = \begin{pmatrix} n_1 r_{k-1} \\ m_1 r_{k-1} \end{pmatrix} \qquad r_{k-1} \text{ is } \underline{\underline{\text{gcd}}}$$

$$\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} a & b \\ e & f \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix}$$

$r_{k-1} = am + bn \qquad 0 = em + fn.$

This gives a practical way to find the gcd of two integers.

Example

1) Find the gcd of 2088 and 319

By equations without matrices

$$2088 = \underbrace{6 \times 319}_{1914} + 174$$

$$319 = 174 + 145$$

$$174 = 145 + 29$$

$$145 = 5 \times 29 + 0$$

So 29 is the gcd.

$$29 = 174 - 145 = 174 - (319 - 174)$$

$$= 2 \times 174 - 319 = 2 \times (2088 - 6 \times 319) - 319$$

$$= 2 \times 2088 - 13 \times 319$$

$$319 = 2 \times 145 + 29 = 11 \times 29$$

$$2088 = 66 \times 29 + 6 \times 29 = 72 \times 29.$$

① gcd 2088, 319 (4)

Matrix method This is a shorthand

$$\left(\begin{array}{cc|c} 1 & 0 & 2088 \\ 0 & 1 & 319 \end{array}\right) \xrightarrow{R_1 - 6R_2} \left(\begin{array}{cc|c} 1 & -6 & 174 \\ 0 & 1 & 319 \end{array}\right) \xrightarrow{R_2 - R_1} \left(\begin{array}{cc|c} 1 & -6 & 174 \\ -1 & 7 & 145 \end{array}\right)$$

$1 \times 2088 = 2088$

$1 \times 319 = 319$

$1 \times 2088 - 6 \times 319 = 174$

$-1 \times 2088 + 7 \times 319 = 145$

$$\xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 2 & -13 & 29 \\ -1 & 7 & 145 \end{array}\right) \xrightarrow{R_2 - 5R_1} \left(\begin{array}{cc|c} 2 & -13 & 29 \\ -11 & 72 & 0 \end{array}\right)$$

$2 \times 2088 - 13 \times 319 = 29$

$11 \times 2088 = 72 \times 319$ – this is the lcm

② Find the gcd of 2088 and 320.

$$\left(\begin{array}{cc|c} 1 & 0 & 2088 \\ 0 & 1 & 320 \end{array}\right) \xrightarrow{R_1 - 6R_2} \left(\begin{array}{cc|c} 1 & -6 & 168 \\ 0 & 1 & 320 \end{array}\right) \xrightarrow{R_2 - R_1} \left(\begin{array}{cc|c} 1 & -6 & 168 \\ -1 & 7 & 152 \end{array}\right)$$

$-2088 + 7 \times 320 = 152$

$2088 - 6 \times 320 = 168$

$$\xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} +2 & -13 & 16 \\ -1 & 7 & 152 \end{array}\right) \xrightarrow{R_2 - 9R_1} \left(\begin{array}{cc|c} 2 & -13 & 16 \\ -19 & 124 & 8 \end{array}\right) \xrightarrow{R_1 - 2R_2} \left(\begin{array}{cc|c} 40 & -261 & 0 \\ -19 & 124 & 8 \end{array}\right)$$

$\gcd = 8$ $\quad -19 \times 2088 + 124 \times 320 = 8$

$40 \times 2088 = 261 \times 320 \quad = \text{lcm}.$

③ Find the gcd of 2088 and 321

$$\left(\begin{array}{cc|c} 1 & 0 & 2088 \\ 0 & 1 & 321 \end{array}\right) \xrightarrow{R_1 - 6R_2} \left(\begin{array}{cc|c} 1 & -6 & 162 \\ 0 & 1 & 321 \end{array}\right) \xrightarrow{R_2 - R_1} \left(\begin{array}{cc|c} 1 & -6 & 162 \\ -1 & 7 & 159 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 2 & -13 & 3 \\ -1 & 7 & 159 \end{array}\right)$$

$$\xrightarrow{R_2 - 53R_1} \left(\begin{array}{cc|c} 2 & -13 & 3 \\ -107 & 696 & 0 \end{array}\right)$$

$\gcd = 3$ $\quad 2 \times 2088 - 13 \times 321 = 3$

$107 \times 2088 = 696 \times 321 = \text{lcm}.$

(4) Find the gcd of 2088 and 323

$$\left|\begin{array}{cc|c} 1 & 0 & 2088 \\ 0 & 1 & 323 \end{array}\right| \xrightarrow{R_1 - 6R_2} \left|\begin{array}{cc|c} 1 & -6 & 150 \\ 0 & 1 & 323 \end{array}\right| \xrightarrow{R_2 - 2R_1} \left|\begin{array}{cc|c} 1 & -6 & 150 \\ -2 & 13 & 23 \end{array}\right|$$

$$\xrightarrow{R_1 - 6R_2} \left|\begin{array}{cc|c} 13 & -84 & 12 \\ -2 & 13 & 23 \end{array}\right| \xrightarrow{R_2 - R_1} \left|\begin{array}{cc|c} 13 & -84 & 12 \\ -15 & 97 & 11 \end{array}\right| \xrightarrow{R_1 - R_2} \left|\begin{array}{cc|c} 28 & -181 & 1 \\ -15 & 97 & 11 \end{array}\right|$$

$$\xrightarrow{R_2 - 11R_1} \left|\begin{array}{cc|c} 28 & -181 & 1 \\ -323 & 2088 & 0 \end{array}\right|$$

$28 \times 2088 - 181 \times 323 = 1$

gcd = 1.

Prime numbers

Recall that an integer n is prime (or prime number if $n \neq 0, \pm 1$ and the only divisors of n are $\pm n$ and ± 1.

Examples 2 is prime. 3 is prime. $4 = 2 \times 2$ is not prime.

The Fundamental Theorem of Arithmetic

If $n \in \mathbb{Z}_+$, $n > 1$ then there are $k \in \mathbb{Z}_+$ and primes $1 < p_1 < \dots < p_k$ and $m_i \in \mathbb{Z}_+$ such that

$$n = \prod_{i=1}^{k} p_i^{m_i}$$

The k and the p_i and m_i are unique given n.

Also A consequence of this is that any integer n, $n \neq 0, \pm 1$, is divisible by at least one prime p_1. and is divisible by p_i, $1 \leq i \leq k$, and by $\pm \prod_{i=1}^{k} p_i^{t_i}$ for $0 \leq t_i \leq m_i$ and by nothing else

So n is prime $\iff n = p_1$. This makes it easier to check whether numbers are prime.

If n is not prime then $p_1^2 \leq n$ where p_1 is the smallest positive prime division. So to check whether $n \in \mathbb{Z}^+ \setminus \{1\}$ is prime we only need to check whether n is divisible by k, for any prime k with $k^2 \leq n$.

Example Is 323 prime? $324 = 18^2$ So the primes divides 323 (if 323 is not prime) must include at least one prime ≤ 17 2, 3, 5, 11 do not divide 323

$7 \nmid 323$ $323 = 46 \times 7 + 1$

$13 \nmid 323$ $323 = 14 \times 13 + 11$

But $323 = 17 \times 19$ So 323 is not prime!

~~2, 3, 5, 11 do not divide 327~~

Is 327 prime?

No. $327 = 3 \times 109$

$327 = 46 \times 7 + 5$

$327 = 18 \times 13 + 2$

$327 = 19 \times 17 + 4$

~~$19^2 > 327$~~

So 327 is prime!

However 331 is prime. 2, 3, 5, 7, 11, 13, 17 do not divide 331

Sieve of Eratosthenes

This is the oldest known method for finding prime numbers

Write down the natural nubers ≥ 2 in ascending order.

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, ...

(27)

Cross out those divisible by 2, then by 3, 5, 7, 11, 13, 17, 19.. after 2, then 3, 5, 7, 11...

The prime nos ≤ 100 are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,

53, 59, 61, 67, 71, 73, 79, 83, 89, 93, 97...

Then

101, 103, 107, 113, 119, 127, 131, 137, 139, 149, 151, 157

163, 167, 173...

Primes are important building blocks.

A consequence of the FTA $n = \prod_{i=1}^{r} p_i^{k_i}$ is formulae for the GCD and LCM using prime factorisation

If $m = \prod_{i=1}^{r} p_i^{k_i}$ and $n = \prod_{i=1}^{r} p_i^{l_i}$ with $k_i, l_i \in \mathbb{N}$.

then $\gcd(m,n)$ is $\prod_{i=1}^{r} p_i^{\min(k_i, l_i)}$

$\operatorname{lcm}(m,n) = \prod_{i=1}^{r} p_i^{\max(k_i, l_i)}$

Examples Using previously worked examples

$2088 = 2^3 \times 3^2 \times 29$

$319 = 11 \times 29$

$320 = 2^6 \times 5$

$321 = 3 \times 107$.

$323 = 17 \times 19$

$\gcd(2088, 319) = 29$

$\gcd(2088, 320) = 2^3 = 8$

$\gcd(2088, 321) = 3$

$\operatorname{lcm}(2088, 319) = 11 \times 2088$

$\operatorname{lcm}(320, 2088) = 2^3 \times 5 \times 2088$

$\operatorname{lcm}(321, 2088) = 107 \times 2088$

Proof of FTA The proof has two parts: existence of prime factorisation and uniqueness of prime factorisation.

Existence uses $m < n$ if $mk = n$ for $m, k \in \mathbb{Z}_+$ both > 1

Proof is by induction on $n \in \mathbb{Z}_+$.

If True for $n = 1$ (trivially) and for $n = 2$ - because 2 is prime.

Assume true for all $m \in n. \in \mathbb{Z}_+$, $n \geq 2$

Consider $n+1$. If $n+1$ is prime then line.

If not then $n+1 = mk$ for $1 < m, k < n+1$

So $m, k \in n$ and each has a prime factorisation.

Hence so does $n+1$.

So by induction, prime factorisation exists for all $n \in \mathbb{Z}_+$, $n \geq 2$.

Uniqueness 2 has unique prime factorisation because any positive prime apart from 2 is > 2 and cannot divide 2.

Suppose prime factorisation holds for m $\forall$ $2 \leq m \in n$ $m \in \mathbb{Z}_+$.

Consider $n+1$. Suppose $n+1 = \prod_{k=1}^{r} p_k^{k_i} = \prod_{i=1}^{s} q_i^{l_i} = q_1 \times n'$ are 2 prime factorisations

p_1 is prime claim $p_1 = q_i$ for some i. If $p_1 \mid q_1 \times n'$ either $p_1 \mid q_1$ or $p_1 \nmid q_1$ (because q_1 is prime)

If $p_1 \nmid q_1$ then $\gcd(p_1, q_1) = 1$ and

$a p_1 + b q_1 = 1$ for $a, b \in \mathbb{Z}_+$

So $a p_1 n' + b q_1 n' = n'$

$n' = a p_1 n' + b_1 (q_1 n') = a p_1 n' + b_1 (n+1)$

$p_1 \mid a p_1 n'$ and $p_1 \mid n+1 \Rightarrow p_1 \mid n'$.

Unique prime factorisation of $n' \Rightarrow p_1 = q_i$ for some $i > 1$.

Renumbering we can assume $p_1 = q_1$

Then unique prime factorisation of n'

$\Rightarrow n+1$ also has unique prime factorisation □

Infinitely many primes

One of the oldest and most famous theorems in mathematics is

Theorem There are infinitely many prime numbers.

This theorem appears in Euclid and is proved by contradiction.

Proof Suppose there are only finitely many prime numbers:

Call them $p_1, \ldots p_n$. All of them > 1.

Put $N = \prod_{i=1}^{n} p_i$ Then $p_i \mid N$ for all i, $1 \le i \le n$. So $p_i \nmid N+1$

for any $1 \le i \le n$. So no number apart from $\pm 1, \pm(N+1)$ divides $N+1$ and $N+1$ is prime! ↯ Contradiction.

Examples

(1) Find the gcd and lcm of 63 and 45 using prime factorisation

$63 = 3^2 \times 7 \quad 45 = 3^2 \times 5$.

$\text{gcd} = 3^2 = 9$

$\text{lcm} = 3^2 \times 7 \times 5 = 63 \times 5 = 45 \times 7 = 315$

Using Euclidean algorithm

$$\left(\begin{array}{cc|c} 1 & 0 & 63 \\ 0 & 1 & 45 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 1 & -1 & 18 \\ 0 & 1 & 45 \end{array}\right) \longrightarrow \left(\begin{array}{cc|c} 1 & -1 & 18 \\ -2 & 3 & 9 \end{array}\right)$$

$$\xrightarrow{R_1 - 2R_2} \left(\begin{array}{cc|c} 5 & -7 & 0 \\ -2 & 3 & 9 \end{array}\right)$$

$9 = \text{gcd} \quad 5 \times 63 - 7 \times 45 = 0$

$\text{lcm} = 5 \times 63 = 7 \times 45 = 315$

(2) gcd and lcm of 365 and 237.

By prime factorisation: $365 = 5 \times 73$ (1, prime) $\quad 237 = 3 \times 79$ (prime)

$\text{gcd} = 1 \quad \text{lcm} = 365 \times 237 = 3 \times 5 \times 73 \times 79 = 86505$

By Euclidean algorithm

$$\left(\begin{array}{cc|c} 1 & 0 & 365 \\ 0 & 1 & 237 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 1 & -1 & 128 \\ 0 & 1 & 237 \end{array}\right) \longrightarrow \left(\begin{array}{cc|c} 1 & -1 & 128 \\ -1 & 2 & 109 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 2 & -3 & 19 \\ -1 & 2 & 109 \end{array}\right)$$

$$\longrightarrow \left(\begin{array}{cc|c} 2 & -3 & 19 \\ -11 & 17 & 14 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 13 & -20 & 5 \\ -11 & 17 & 14 \end{array}\right) \xrightarrow{R_2 - 2R_1} \left(\begin{array}{cc|c} 13 & -20 & 5 \\ -37 & 57 & 4 \end{array}\right)$$

$$\xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 50 & -77 & 1 \\ -37 & 57 & 4 \end{array}\right) \longrightarrow \left(\begin{array}{cc|c} 50 & -77 & 1 \\ -237 & 365 & 0 \end{array}\right)$$

(3) gcd & lcm of 196 & 64 $\quad 196 = 2^2 \times 49 = 2^2 \times 7^2 \quad 64 = 2^6$

$\text{gcd} = 2^2 = 4 \quad \text{lcm} = 2^6 \times 7^2 = 3136$

$= 64 \times 49$

Euclidean

(3) Euclidean algorithm

$$\left(\begin{array}{cc|c} 1 & 0 & 196 \\ 0 & 1 & 64 \end{array}\right) \xrightarrow{R_1 - 3R_2} \left(\begin{array}{cc|c} 1 & -3 & 4 \\ 0 & 1 & 64 \end{array}\right) \xrightarrow{R_2 - 16R_1} \left(\begin{array}{cc|c} 1 & -3 & 4 \\ -16 & 49 & 0 \end{array}\right)$$

$\gcd = 4 \qquad \text{lcm} = 16 \times 196 = 49 \times 64$

Rules for dividing by 2, 3, 5, 9, 11.

There are quick rules for deciding whether a number is divisible by 2, 5, 3, 9, 11.

A natural number is divisible by 2 $\iff$ the last digit is even (0, 2, 4, 6, 8)

This is because if $a_i \in \{0, 1, \dots 9\}$ then ~~$a_n a_{n-1} \dots a_0$~~

$$a_n a_{n-1} \dots a_0 = 10 \times a_n a_{n-1} \dots a_1 + a_0 = 2 \times 5 \times a_n \dots a_1 + a_0$$

Similarly a natural number is divisible by 5 $\iff$ the last digit is 0 or 5.

What about 3?

$$3 \mid a_n \dots a_0 \iff 3 \mid a_n + \dots + a_0$$

Why $a_n \dots a_0 = \sum_{i=0}^{n} a_i 10^i = \sum_{i=0}^{n} a_i + \sum_{i=1}^{n} a_i (10^i - 1)$

$10 - 1 = 9 = 3 \times 3$

$10^2 - 1 = (10-1) \times (10+1) = 9 \times 11 = 3 \times 3 \times 11$

Similarly $10^i - 1 = (10-1)(1 + \dots + 10^{i-1}) = 3 \times 3 \times (1 + \dots + 10^{i-1})$

So $a_n \dots a_0$ is divisible by 3 $\iff 3 \mid \sum_{i=0}^{n} a_i$

Similarly $9 \mid a_n \cdots a_0 \iff 9 \mid \sum_{i=0}^{n} a_i$

What about 11.?

$10^0 - 1 = 0 \quad 11 \mid 0 \qquad 10^1 + 1 = 11 \quad 11 \mid 11$

$10^2 - 1 = (10-1)(10+1) = 9 \times 11 \qquad 11 \mid 10^2 - 1$

$\forall i, \quad 11 \mid 10^{2i} - 1 \quad$ and $\quad 11 \mid 10^{2i+1} + 1)$

because $10^{2i} - 1 = \underbrace{(10^2 - 1)}_{9 \times 11}(1 + \cdots + 10^{2(i-1)})$

$$10^{2i+1} + 1 = (10+1)(10^{2i} - 10^{2i-1} + 10^{2(i-1)} - \cdots - 10 + 1)$$

There are similar rules for divisibility by any non-zero integer. See Problem sheet 4 for a rule about divisibility by 13.