MATH1050 Euclidean Algorithm

1. **Definition**.
   Let $m, n \in \mathbb{Z}$. Let $c \in \mathbb{Z}$. c is said to be a **common divisor of** *m, n if both of m, n are divisible by c.*

2. **Definition**.
   Let $m, n \in \mathbb{Z}$.

   (1) *Suppose m, n are not both zero. Let $g \in \mathbb{N}$. g is said to be a* **greatest common divisor of** *m, n if both of the following conditions are satisfied:*
   (1a) *g is a common divisor of m, n.*
   (1b) *For any $d \in \mathbb{Z}$, if d is a common divisor of m, n then $|d| \leq g$.*
   (2) *(Suppose $m = n = 0$.) We define the greatest common divisor of $0, 0$ is defined to be 0.*

   Remark. Two questions arise naturally:

   Existence question. Does each pair of integers, have at least one greatest common divisor?

   Uniqueness question. Does each pair of integers, have at most one greatest common divisor?

   If the answer to the existence question is *no*, our definition is something useless. Fortunately its answer is *yes*, but it will be take some effort (Lemma (2), Lemma (3) and Theorem (EAN) combined) to justify. The uniqueness question is settled immediately by Lemma (1).

3. **Lemma (1). (Uniqueness of greatest common divisor.)**
   Each pair of integers which are not both zero has at most one greatest common divisor.

   Proof of Lemma (1). Let $m, n \in \mathbb{Z}$. Without loss of generality, suppose $m \neq 0$. Let $g, g' \in \mathbb{N}$. Suppose each of g, g' is a greatest common divisor of m, n.

   By definition, each of g, g' is a common divisor of $m.n$.

   Since g is a greatest common divisor of m, n and g' is a common divisor of $m.n$, we have $g' = |g'| \leq g$. Similarly, we have $g = |g| \leq g'$. Therefore $g = g'$.

   Notation. From now on, for any $m, n \in \mathbb{Z}$, for any $g \in \mathbb{N}$, if g is a greatest common divisor of m, n then we write $\gcd(m, n)$.

   Remark. The importance of Lemma (1) is that it guarantees the uniqueness of greatest common divisor: it makes sense to use the article '*the*' when we write '*the* greatest common divisor of so-and-so'. and to write '$\gcd(m, n) = ...$'.

4. **Lemma (2)**.
   Let $b \in \mathbb{Z}$ and p be a prime number. The statements below hold:

   (1) *If b is divisible by p then $\gcd(b, p) = |p|$.*
   (2) *If b is not divisible by p then $\gcd(b, p) = 1$.*

   Proof of Lemma (2). Let $b \in \mathbb{Z}$ and p be a prime number. p is divisible by no integer other than $1, -1, |p|, -|p|$.

   (1) Suppose b is divisible by p. Then $1, -1, |p|, -|p|$ are the only common divisors of b, p. Therefore $\gcd(b, p) = |p|$.
   (2) Suppose b is not divisible by p. Then $1, -1$ are the only common divisors of b, p. Therefore $\gcd(b, p) = 1$.

5. **Lemma (3)**.
   Let $a, b \in \mathbb{Z}$. The statements below hold:

   (1) $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.
   (2) $\gcd(a, b) = \gcd(b, a)$.
   (3) $\gcd(a, a) = a$.
   (4) $\gcd(a, 1) = 1$.
   (5) $\gcd(a, 0) = a$.

   Proof of Lemma (3). Exercise.

   Remark. Lemma (2), Lemma (3) combine to tell us that we need only concern ourselves with the existence question of greatest common divisor for a pair of distinct positive integers both of which are not prime numbers. (Why?)

6. **Theorem (EAN). (Euclidean Algorithm for positive integers.)**

Let $a_0, a_1 \in \mathbb{N}\backslash\{0\}$. Suppose $a_0 > a_1$.

For each $j \in \mathbb{N}\backslash\{0,1\}$, if $a_{j-1} \neq 0$, then define $a_j \in \mathbb{N}$ to be the remainder obtained after dividing a_{j-2} by a_{j-1}; if $a_{j-1} = 0$, then define $a_j = 0$.

Then, there exists some $N \in \mathbb{N}\backslash\{0\}$ such that the following statements hold:

(1) *$a_0 > a_1 > a_2 > ... > a_N > 0$ and $a_j = 0$ whenever $j > N$.*

(2) *There exist some $s, t \in \mathbb{Z}$ such that $a_N = sa_0 + ta_1$.*

(3) *a_N is a common divisor of a_0, a_1.*

(4) *For any $d \in \mathbb{Z}$, if d is a common divisor of a_0, a_1 then $|d| \leq a_N$.*

(5) $\gcd(a_0, a_1) = a_N$.

Proof of Theorem (EAN). Postponed.

7. **Euclidean Algorithm.**

Given any two non-zero integers, we may apply the Euclidean Algorithm to determine their greatest common divisor. The theoretical justification is provided by Theorem (EAN). This method suggested by the theory is illustrated in the examples below:

1. We determine $\gcd(10000000011, 10101)$:

$$\begin{array}{rcrcrcr} 10000000011 & = & 990000 & \times & 10101 & + & 10011 \\ 10101 & = & 1 & \times & 10011 & + & 90 \\ 10011 & = & 111 & \times & 90 & + & 21 \\ 90 & = & 4 & \times & 21 & + & 6 \\ 21 & = & 3 & \times & 6 & + & 3 \\ 6 & = & 2 & \times & 3 & + & 0 \end{array}$$

By Theorem (EAN), we have $\gcd(10000000011, 10101) = 3$. From the definition, we also have

$$\gcd(-10000000011, 10101) = \gcd(10000000011, -10101) = \gcd(-10000000011, -10101) = 3.$$

2. We determine $\gcd(960, 825)$:

$$\begin{array}{rcrcrcr} 960 & = & 1 & \times & 825 & + & 135 \\ 825 & = & 6 & \times & 135 & + & 15 \\ 135 & = & 9 & \times & 15 & + & 0 \end{array}$$

By Theorem (EAN), we have $\gcd(960, 825) = 15$. From the definition, we also have

$$\gcd(-960, 825) = \gcd(960, -825) = \gcd(-960, -825) = 1.$$

3. We determine $\gcd(2468008642, 1357997531)$:

$$\begin{array}{rcrcrcr} 2468008642 & = & 1 & \times & 1357997531 & + & 1110011111 \\ 1357997531 & = & 1 & \times & 1110011111 & + & 247986420 \\ 1110011111 & = & 4 & \times & 247986420 & + & 118065431 \\ 247986420 & = & 2 & \times & 118065431 & + & 11855558 \\ 118065431 & = & 9 & \times & 11855558 & + & 11365409 \\ 11855558 & = & 1 & \times & 11365409 & + & 490149 \\ 11365409 & = & 23 & \times & 490149 & + & 91982 \\ 490149 & = & 5 & \times & 91982 & + & 30239 \\ 91982 & = & 3 & \times & 30239 & + & 1265 \\ 30239 & = & 23 & \times & 1265 & + & 1144 \\ 1265 & = & 1 & \times & 1144 & + & 121 \\ 1144 & = & 9 & \times & 121 & + & 55 \\ 121 & = & 2 & \times & 55 & + & 11 \\ 55 & = & 5 & \times & 11 & + & 0 \end{array}$$

By Theorem (EAN), we have $\gcd(2468008642, 1357997531) = 11$. From the definition, we also have

$$\begin{aligned} \gcd(-2468008642, 1357997531) &= \gcd(2468008642, -1357997531) \\ &= \gcd(-2468008642, -1357997531) = 11. \end{aligned}$$

8. **Proof of Theorem (EAN).**

Let $a_0, a_1 \in \mathbb{N}\backslash\{0\}$. Suppose $a_0 > a_1$.

For each $j \in \mathbb{N}\backslash\{0,1\}$, if $a_{j-1} \neq 0$, then define $a_j \in \mathbb{N}$ to be the remainder obtained after dividing a_{j-2} by a_{j-1}; if $a_{j-1} = 0$, then define $a_j = 0$.

(0) We apply proof-by-contradiction to argue that there exists some $M \in \mathbb{N}$ such that $a_M = 0$.

- Suppose it were true that there was no such $M \in \mathbb{N}$.
  Then for any $j \in \mathbb{N}$, $a_j \neq 0$.
  Whenever $j \geq 2$, a_j would be the remainder obtained after dividing a_{j-2} by a_{j-1}. Therefore $0 < a_j < a_{j-1}$.
  It would follow (from mathematical induction) that $\{a_k\}_{k=0}^{\infty}$ was a strictly decreasing infinite sequence of positive integers.
  Now $a_1 \leq a_0 - 1$, $a_2 \leq a_1 - 1 \leq a_0 - 2$, ..., $a_{a_0} \leq a_0 - a_0 = 0$. Then $a_{a_0} = 0$. Contradiction arises.
  Hence, in the first place, there exists some $M \in \mathbb{N}$ such that $a_M = 0$.

Define $S = \{j \in \mathbb{N} : a_j = 0\}$. We have $M \in S$. Then $S \neq \emptyset$.
By the Well-ordering Principle for integers, S has a least element, which we denote by ν.
Note that $a_0 \neq 0$. Then $\nu \neq 0$. Define $N = \nu - 1$.

(1) From the argument above, $a_0, a_1, a_2, \cdots, a_N$ is a strictly decreasing finite sequence of positive integers.
By definition of N, $a_k = 0$ whenever $k > N$.

(2) By definition, there exist some $q_1, q_2, \cdots q_N \in \mathbb{N}$ such that

$$\begin{array}{lllllll} a_0 & = & q_1 & \times & a_1 & + & a_2, \\ a_1 & = & q_2 & \times & a_2 & + & a_3, \\ & \vdots & & & & & \\ a_{N-3} & = & q_{N-2} & \times & a_{N-2} & + & a_{N-1}, \\ a_{N-2} & = & q_{N-1} & \times & a_{N-1} & + & a_N, \\ a_{N-1} & = & q_N & \times & a_N & + & 0. \end{array}$$

We have $a_N = 1 \cdot a_{N-2} - q_{N-1}a_{N-1}$. Here $1, -q_{N-1} \in \mathbb{Z}$. Then

$$a_N = a_{N-2} - q_{N-1}(a_{N-3} - q_{N-2}a_{N-2}) = -q_{N-1}a_{N-3} + (1 + q_{N-1}q_{N-2})a_{N-2}.$$

Here $-q_{N-1}, 1 + q_{N-1}q_{N-2} \in \mathbb{Z}$.
Repeating this argument finitely many times, we deduce that there exist some $s, t \in \mathbb{Z}$ such that $a_N = sa_0 + ta_1$.

(3) a_{N-1} is divisible by a_N.
Since $a_{N-2} = q_{N-1}a_{N-1} + a_N$, a_{N-2} is divisible by a_N. (Why?)
Since $a_{N-3} = q_{N-2}a_{N-2} + a_{N-1}$, a_{N-3} is divisible by a_N. (Why?)
Repeating this argument for finitely many times, we deduce that a_0, a_1 are both divisible by a_N.

(4) Pick any $d \in \mathbb{Z}$. Suppose d is a common divisor of a_0, a_1.
Then there exist some $s', t' \in \mathbb{Z}$ such that $a_0 = s'd$ and $a_1 = t'd$.
Now $a_N = sa_0 + ta_1 = (ss' + tt')d$.
Note that $ss' + tt' \in \mathbb{Z}$. Since $a_N > 0$, we have $ss' + tt' \neq 0$.
Then $a_N = |a_N| = |ss' + tt'||d| \geq |d|$.

(5) The result follows from (3) and (4) combined.

9. **Theorem (4). (Bézout's Identity.)**

Let $m, n \in \mathbb{Z}$. There exist some $s, t \in \mathbb{Z}$ such that $sm + tn = \gcd(m, n)$.

Proof of Theorem (4). A very tedious exercise. (Apply Lemma (3) to help reduce the number of cases. Repeatedly apply Theorem (EAN).)

10. **Lemma (5).**

Let $m, n \in \mathbb{Z}$. Let $c \in \mathbb{Z}$. c is a common divisor of m, n iff $\gcd(m, n)$ is divisible by c.

Proof of Lemma (5). Let $m, n \in \mathbb{Z}$. Let $c \in \mathbb{Z}$.

- ['⇒-part'.]
  Suppose c is a common divisor of $m.n$.
  Then, by definition of divisibility, there exist some $h, k \in \mathbb{Z}$ such that $m = hc$ and $n = kc$.
  By Bézout's Identity, there exist some $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = sm + tn$.
  Then $\gcd(m, n) = sm + tn = s \cdot hc + t \cdot kc = (sh + tk)c$.
  Since $s, t, h, k \in \mathbb{Z}$, we have $sh + ck \in \mathbb{Z}$.
  Therefore $\gcd(m, n)$ is divisible by c.

- ['⇐-part'.]
  Suppose $\gcd(m,n)$ is divisible by c.
  By definition, $\gcd(m,n)$ is a common divisor of m,n. Then m is divisible by $\gcd(m,n)$. Therefore m is divisible by c. (Why?)
  Similarly, we deduce that n is divisible by c.
  Hence c is a common divisor of m,n.

11. **Theorem (6). (Alternative definition of greatest common divisor.)**
  Let $m,n \in \mathbb{Z}$. Let $g \in \mathbb{N}$. The statements (†), (‡) are logically equivalent:

  (†) $g = \gcd(m,n)$.

  (‡) *g is a common divisor of m,n and g is divisible by every common divisor of m,n.*

  Proof of Theorem (6). Exercise. (Apply Lemma (5).)

12. **Euclid's Lemma.**
  Let $a,b \in \mathbb{Z}$ and p be a prime number. Suppose ab is divisible by p. Then at least one of a,b is divisible by p.

  Proof of Euclid's Lemma. Let $a,b \in \mathbb{Z}$ and p be a prime number. Suppose ab is divisible by p.

  [We want to deduce: at least one of a,b is divisible by p.] b is divisible by p or b is not divisible by p.

  - (Case 1). Suppose b is divisible by p. Then at least one of a,b, namely, b is divisible by p.
  - (Case 2). Suppose b is not divisible by p. We verify that a is divisible by p:
    Since b is not divisible by p, $\gcd(b,p) = 1$.
    There exist some $s,t \in \mathbb{Z}$ such that $sb + tp = \gcd(b,p)$.
    Then $a = a \cdot 1 = a\gcd(b,p) = a(sb+tp) = sab + atp$.
    Since ab is divisible by p, there exists some $k \in \mathbb{Z}$ such that $ab = kp$.
    Now $a = sab + atp = skp + atp = (sk + at)p$.
    Since $s,t,k,a \in \mathbb{Z}$, we have $sk + at \in \mathbb{Z}$. Then a is divisible by p.
    Therefore one of a,b, namely, a, is divisible by p.

  Hence, in any case, at least one of a,b is divisible by p.

  Corollary to Euclid's Lemma. (Generalization of Euclid's Lemma.)

  Let p be a prime number. Let $n \in \mathbb{N}\backslash\{0,1\}$. Let $a_1, a_2, \cdots, a_n \in \mathbb{Z}$. Suppose $a_1a_2 \cdot ... \cdot a_n$ is divisible by p. Then at least one of $a_1, a_2, \cdots, a_n$ is divisible by p.

13. **Theorem (7). (A characterization of prime numbers.)**
  Let $p \in \mathbb{Z}\backslash\{-1,0,1\}$. The statements (†), (‡) are logically equivalent:

  (†) *p is a prime number.*

  (‡) *For any $a,b \in \mathbb{Z}$, if ab is divisible by p then at least one of a,b is divisible by p.*

  Proof of Theorem (7). Exercise.

14. **Fundamental Theorem of Arithmetic.**
  Let $n \in [\![2,+\infty)$. The statements below hold:

  (1) *n is a prime number or a product of several prime numbers.*

  (2) *Let $p_1, p_2, \cdots, p_s$, $q_1, q_2, \cdots, q_t$ be prime numbers. Suppose $0 < p_1 \leq p_2 \leq \cdots \leq p_s$ and $0 < q_1 \leq q_2 \leq \cdots \leq q_t$. Further suppose $n = p_1p_2 \cdot ... \cdot p_s$ and $n = q_1q_2 \cdot ... \cdot q_t$. Then $s = t$ and $p_1 = q_1$, $p_2 = q_2$, ... , $p_s = q_s$.*

  Proof. Exercise in mathematical induction. (You need Euclid's Lemma at some stage.)

  Remark. The statement of this result can be 'condensed' as:

  > *Let $n \in [\![2,+\infty)$. There is a factorization of n as a product of positive prime numbers, uniquely determined up to the ordering of the prime factors.*

15. **Appendix.**
  As an exercise, check the formal definitions for '**common multiple**', '**lowest common multiple**', and '**relatively prime**' are, and their basic properties.

  Something resembling all the above will appear in *polynomials over fields*. You will see why it is the case in your *abstract algebra* course.