

## 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?

### 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  $m, n$ .

[Hope to deduce:  $g = g'$ .]

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 also deduce that  $g = |g| \leq g'$ . Therefore  $g = g'$ .  $\square$

**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 ' $\gcd(m, n) = \dots$ '.

#### 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 these integers only:  $1, -1, p, -p$ .

(1) Suppose  $b$  is divisible by  $p$ .

Then the only common divisors of  $b, p$  are  $1, -1, p, -p$ .

The greatest of them is  $|p|$ .

So  $\gcd(b, p) = |p|$ .

(2) Suppose  $b$  is not divisible by  $p$ .

Then the only common divisors of  $b, p$  are  $1, -1$ .

The greatest of them is  $1$ .

So  $\gcd(b, p) = 1$ .

□

## 5. Lemma (3).

Let  $a, b \in \mathbb{Z}$ . The statements below hold:

$$(1) \quad \gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b).$$

$$(2) \quad \gcd(a, b) = \gcd(b, a).$$

$$(3) \quad \gcd(a, a) = a.$$

$$(4) \quad \gcd(a, 1) = 1.$$

$$(5) \quad \gcd(a, 0) = a.$$

**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  $a_0, a_1 \in \mathbb{N} \setminus \{0\}$ . Suppose  $a_0 > a_1$ .

For each  $j \in \mathbb{N} \setminus \{0, 1\}$ ,

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  $N \in \mathbb{N} \setminus \{0\}$  such that the following statements hold:

- (1)  $a_0 > a_1 > a_2 > \dots > a_N > 0$  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.

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

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

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  $\gcd(960, 825)$ :

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

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

$$\gcd(-960, 825) = \gcd(960, -825) = \gcd(-960, -825) = 15.$$

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

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

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

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

$$a_0 = \underline{2468008642}, a_1 = \underline{1357997531}$$

$$\begin{array}{rcl}
 2468008642 & = & 1 \cdot 1357997531 + 1110011111 \\
 a_0 & & q_1 \quad a_1 \quad a_2 \\
 1357997531 & = & 1 \cdot 1110011111 + 247986420 \\
 a_1 & & q_2 \quad a_2 \quad a_3 \\
 1110011111 & = & 4 \cdot 247986420 + 118065431 \\
 a_2 & & q_3 \quad a_3 \quad a_4 \\
 247986420 & = & 2 \cdot 118065431 + 11855558 \\
 a_3 & & q_4 \quad a_4 \quad a_5 \\
 118065431 & = & 9 \cdot 11855558 + 11365409 \\
 a_4 & & q_5 \quad a_5 \quad a_6 \\
 11855558 & = & 1 \cdot 11365409 + 490149 \\
 a_5 & & q_6 \quad a_6 \quad a_7 \\
 11365409 & = & 23 \cdot 490149 + 91982 \\
 a_6 & & q_7 \quad a_7 \quad a_8 \\
 490149 & = & 5 \cdot 91982 + 30239 \\
 a_7 & & q_8 \quad a_8 \quad a_9
 \end{array}$$

$$\begin{array}{rcl}
 91982 & = & 3 \cdot 30239 + 1265 \\
 a_8 & & q_9 \quad a_9 \quad a_{10} \\
 30239 & = & 23 \cdot 1265 + 1144 \\
 a_9 & & q_{10} \quad a_{10} \quad a_{11} \\
 1265 & = & 1 \cdot 1144 + 121 \\
 a_{10} & & q_{11} \quad a_{11} \quad a_{12} \\
 1144 & = & 9 \cdot 121 + 55 \\
 a_{11} & & q_{12} \quad a_{12} \quad a_{13} \\
 121 & = & 2 \cdot 55 + 11 \\
 a_{12} & & q_{13} \quad a_{13} \quad a_{14} \\
 55 & = & 5 \cdot 11 + 0 \\
 a_{13} & & q_{14} \quad a_{14} \quad a_{15} \\
 \hline
 & & & & \text{Stop.} \\
 a_{14} & & q_{15} \quad a_{15} \quad a_{16} \\
 & = & & & + \\
 a_{15} & & q_{16} \quad a_{16} \quad a_{17}
 \end{array}$$



Claim (x): Each of  $a_0, a_1$  is divisible by  $a_N$ .

---

Here  $N = \underline{14}$ .

$$a_{N-1} = q_N a_N$$

$$a_{N-2} = q_{N-1} a_{N-1} + a_N$$

$$a_{N-3} = q_{N-2} a_{N-2} + a_{N-1}$$

$$a_{N-4} = q_{N-3} a_{N-3} + a_{N-2}$$

⋮

$$a_4 = q_5 a_5 + a_6$$

$$a_3 = q_4 a_4 + a_5$$

$$a_2 = q_3 a_3 + a_4$$

$$a_1 = q_2 a_2 + a_3$$

$$a_0 = q_1 a_1 + a_2$$

$a_{N-1}$  is divisible by  $a_N$ .

Then  $a_{N-2}$  is divisible by  $a_N$ . (Why?)

Then  $a_{N-3}$  is divisible by  $a_N$ . (Why?)

Then  $a_{N-4}$  is divisible by  $a_N$ . (Why?)

⋮

Then  $a_4$  is divisible by  $a_N$ . (Why?)

Then  $a_3$  is divisible by  $a_N$ . (Why?)

Then  $a_2$  is divisible by  $a_N$ . (Why?)

Then  $a_1$  is divisible by  $a_N$ . (Why?)

Then  $a_0$  is divisible by  $a_N$ . (Why?)

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

Here  $N = \underline{14}$ .

$$a_{N-1} = q_N a_N$$

$$a_{N-2} = q_{N-1} a_{N-1} + a_N$$

$$a_{N-3} = q_{N-2} a_{N-2} + a_{N-1}$$

$$a_{N-4} = q_{N-3} a_{N-3} + a_{N-2}$$

⋮

$$a_4 = q_5 a_5 + a_6$$

$$a_3 = q_4 a_4 + a_5$$

$$a_2 = q_3 a_3 + a_4$$

$$a_1 = q_2 a_2 + a_3$$

$$a_0 = q_1 a_1 + a_2$$

$$\begin{aligned}
 a_N &= 1 \cdot a_{N-2} - q_{N-1} a_{N-1} \\
 &= 1 \cdot a_{N-2} - q_{N-1} (a_{N-3} - q_{N-2} a_{N-2}) \\
 &= -q_{N-1} a_{N-3} + (1 + q_{N-1} q_{N-2}) a_{N-2} \\
 &= -q_{N-1} a_{N-3} + (1 + q_{N-1} q_{N-2}) (a_{N-4} - q_{N-3} a_{N-3}) \\
 &= (1 + q_{N-1} q_{N-2}) a_{N-4} \\
 &\quad - [q_{N-1} + (1 + q_{N-1} q_{N-2}) q_{N-3}] a_{N-3} \\
 &\quad \vdots \\
 &= sa_0 + ta_1,
 \end{aligned}$$

in which each of  $s, t$  is a sum of products of integers with  $q_1, q_2, \dots, q_{N-1}$ .  
So  $s, t$  are integers as well.

Claim (8):  $a_N = \gcd(a_0, a_1)$ .

- Each of  $a_0, a_1$  is divisible by  $a_N$ .  
Then  $a_N$  is a common divisor of  $a_0, a_1$ .
- We verify that for any  $d \in \mathbb{Z}$ , if  $d$  is a common divisor of  $a_0, a_1$ ,  
then  $|d| \leq a_N$ .

\* 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  $a_N = sa_0 + ta_1 = ss'd + tt'd = (ss' + tt')d$ .

Note that  $a_N > 0$ . Then  $ss' + tt' \neq 0$ .

Then  $a_N = |a_N| = |ss' + tt'| \cdot |d| \geq 1 \cdot |d| = |d|$ .

- It follows that  $a_N = \gcd(a_0, a_1)$ .

## 8. Proof of Theorem (EAN).

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

For each  $j \in \mathbb{N} \setminus \{0, 1\}$ , 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

$$a_M = 0.$$

Idea of argument:  
Repeated application of Division Algorithm gives:

$$\left. \begin{array}{l} a_0 = q_1 a_1 + a_2 \\ a_1 = q_2 a_2 + a_3 \\ a_2 = q_3 a_3 + a_4 \\ a_3 = q_4 a_4 + a_5 \\ \vdots \end{array} \right\} \text{ in which:}$$

$$a_0 > a_1 > a_2 > a_3 > \dots$$

Ask: Will this ever 'stop'?

Answer:  
 $a_0 > a_1$ . Then  $a_1 \leq a_0 - 1$ .  
 $a_1 > a_2$ . Then  $a_2 \leq a_1 - 1 \leq a_0 - 2$ .  
 $a_2 > a_3$ . Then  $a_3 \leq a_2 - 1 \leq a_1 - 2 \leq a_0 - 3$ .  
 $a_3 > a_4$ . Then  $a_4 \leq a_3 - 1 \leq a_2 - 2 \leq a_1 - 3 \leq a_0 - 4$ .  
 $\vdots$   
Hence  $a_{a_0} \leq a_{a_0-1} - 1 \leq a_{a_0-2} - 2 \leq \dots \leq a_0 - a_0 = 0$ .

Define  $S = \{j \in \mathbb{N} : a_j = 0\}$ .

Note that  $a_{a_0} = 0$ . (Why?)

Then  $S \neq \emptyset$ .

By the Well-ordering Principle for Integers,  $S$  has a least element, say  $\nu$ .

Take  $N = \nu - 1$ . Then  $a_0 > a_1 > a_2 > \dots > a_N > a_\nu = 0$ .

(1) From the argument above,  $a_0, a_1, a_2, \dots, a_N$  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  $q_1, q_2, \dots, q_N \in \mathbf{N}$  such that

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

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

Repeating this argument finitely many times, we deduce that there exist some  $s, t \in \mathbf{Z}$  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.

Needed: { Lemma (3).  
Statement (2) of 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  $c \in \mathbb{Z}$ .

• [' $\Rightarrow$ -part'.]

Suppose  $c$  is a common divisor of  $m, n$ .

Then there exist some  $h, k \in \mathbb{Z}$  such that  $m = hc$  and  $n = kc$ .

By Theorem (4),

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

Then  $\gcd(m, n) = sm + tn = s \cdot hc + t \cdot kc = (sh + tk)c$ .

Since  $h, k, s, t \in \mathbb{Z}$ , we have  $sh + tk \in \mathbb{Z}$ .

Therefore  $\gcd(m, n)$  is divisible by  $c$ .

• [' $\Leftarrow$ -part'.] Exercise. (Apply some basic properties of divisibility.)

Ask: How to relate  $\gcd(m, n)$  with  $m, n$  through an equality?

Hope: Name some appropriate  $r \in \mathbb{Z}$  which satisfies  $\gcd(m, n) = rc$ !

11. **Theorem (6).** (Alternative definition of greatest common divisor.)

Let  $m, n \in \mathbb{Z}$ . Let  $g \in \mathbb{N}$ .

The statements  $(\dagger)$ ,  $(\ddagger)$  are logically equivalent:

$(\dagger)$   $g = \gcd(m, n)$ .

$(\ddagger)$   $g$  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  $p$ . [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  $p$ . [Hope to deduce:  $a$  is divisible by  $p$ .]

By Lemma (2), since  $p$  is a prime number,  
we have  $\gcd(b, p) = 1$ .

By Theorem (4), there exist some  $s, t \in \mathbb{Z}$   
such that  $\gcd(b, p) = sb + tp$ .

So  $1 = \gcd(b, p) = sb + tp$ .

Then  $a \cdot 1 = a \cdot \gcd(b, p) = a \cdot (sb + tp) = s \cdot ab + at \cdot p$ .

Since  $ab$  is divisible by  $p$ ,

there exists some  $k \in \mathbb{Z}$  such that  $ab = kp$ .

Then  $a = s \cdot kp + at \cdot p = (sk + at) p$ .

Since  $s, k, a, t \in \mathbb{Z}$ , we have  $sk + at \in \mathbb{Z}$ . Therefore  $a$  is divisible by  $p$ .

...  $\square$

## **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  $p$ .*

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

*Let  $p$  be a prime number.*

*Let  $n \in \mathbb{N} \setminus \{0, 1\}$ . Let  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ .*

*Suppose  $a_1 a_2 \cdot \dots \cdot a_n$  is divisible by  $p$ .*

*Then at least one of  $a_1, a_2, \dots, a_n$  is divisible by  $p$ .*

## 13. **Theorem (7). (A characterization of prime numbers.)**

*Let  $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ . The statements  $(\dagger)$ ,  $(\ddagger)$  are logically equivalent:*

*$(\dagger)$   $p$  is a prime number.*

*$(\ddagger)$  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  $n \in \llbracket 2, +\infty \rrbracket$ . The statements below hold:

- (1)  $n$  is a prime number or a product of several prime numbers.
- (2) Let  $p_1, p_2, \dots, p_s, q_1, q_2, \dots, q_t$  be prime numbers. Suppose  $0 < p_1 \leq p_2 \leq \dots \leq p_s$  and  $0 < q_1 \leq q_2 \leq \dots \leq q_t$ . Further suppose  $n = p_1 p_2 \cdot \dots \cdot p_s$  and  $n = q_1 q_2 \cdot \dots \cdot q_t$ . Then  $s = t$  and  $p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$ .

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

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

Let  $n \in \llbracket 2, +\infty \rrbracket$ . There is a factorization of  $n$  as a product of positive prime numbers, uniquely determined up to the ordering of the prime factors.

Illustration :  $1050 = 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 = 2 \cdot 5 \cdot 7 \cdot 3 \cdot 5 = 7 \cdot 3 \cdot 5 \cdot 2 \cdot 5 = \dots$

## 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.