Section 4.8

Sterling Jeppson

October 24, 2020

Problem 1

Find the value of z when the following algorithm is executed

$i := 2$
if $(i > 3 \mid\mid i \leq 0)$
  then $z := 1$
  else $z := 0$

Solution

Since $i = 2$, $i \not> 3$ and $i \not\leq 0$. Therefore the statement following **else** is executed. So after execution $z = 0$.

Problem 2

Find the value of z when the following algorithm is executed

$i := 3$
if $(i \leq 3 \mid\mid i > 6)$
  then $z := 2$
  else $z := 0$

Solution

Since the value of i is 3 before execution, the guard condition $i \leq 3 \mid\mid i > 6$ is true at the time it is evaluated. Hence the statement following **then** is executed, and so the value of z following execution is 2.

Problem 3

Consider the following algorithm segment

if $(x \cdot y > 0)$
  then do $y := 3 \cdot x$
    $x := x + 1$ **end do**
$z := x \cdot y$

Find the values of z if prior to execution x and y have the values given below.

(a) $x = 2$, $y = 3$

(b) $x = 1$, $y = 1$

Solution

(a) Since $x \cdot y = 2 \cdot 3 = 6 > 0$, the guard condition is true at the time it is evaluated. Hence the statements between **then do** and **end do** are executed. These statements give y a value of $3 \cdot x = 3 \cdot 2 = 6$ and x a value of $x + 1 = 2 + 1 = 3$. Now z will be assigned a value of $x \cdot y = 3 \cdot 6 = 18$.

(b) Since $x \cdot y = 1 \cdot 1 = 1 > 0$, the guard condition is true at the time it is evaluated. Hence the statements between **then do** and **end do** are executed. These statements give y a value of $3 \cdot x = 3 \cdot 1 = 3$ and x a value of $x + 1 = 1 + 1 = 2$. Now z will be assigned a value of $x \cdot y = 2 \cdot 3 = 6$.

Problem 4

Find the values of a after execution of the loop.

$a := 2$
for $i := 1$ **to** 2
  $a := \frac{a}{2} + \frac{1}{a}$
next i

Solution

At the start of execution $a = 2$. Now the for loop will execute 2 times. Each time it executes a will be reassigned according to $a := \frac{a}{2} + \frac{1}{a}$. The first time

$$a = \frac{2}{2} + \frac{1}{2} = \frac{3}{2}$$

Now $a = \frac{3}{2}$. Therefore after the second run of the for loop

$$a = \frac{3}{4} + \frac{2}{3} = \frac{9}{12} + \frac{8}{12} = \frac{17}{12}$$

Hence after the loop executes $a = \frac{17}{12}$.

Problem 5

Find the values of e after execution of the loop.

$e := 2$, $f := 2$
for $j := 1$ **to** 4
  $f := f \cdot j$
  $e := e + \frac{1}{f}$
next j

Solution

At the start of execution $e = 0$, $f = 2$, and $j = 1$. Now the for loop will be executed 4 times. After run 1 $f = 2$ and $e = \frac{1}{2}$. After run 2 $f = 4$ and $e = \frac{3}{4}$. After run 3 $f = 12$ and $e = \frac{10}{12}$. After run 4 $f = 48$ and $e = \frac{41}{48}$. Hence after the loop executes $e = \frac{41}{48}$.

Problem 6

Make a trace table to trace the action of algorithm 4.8.1 for input $a = 26$ and $d = 7$.

Solution

	0	**1**	**2**	**3**
a	26			
d	7			
r	26	19	12	5
q	0	1	2	3

Problem 7

Make a trace table to trace the action of algorithm 4.8.1 for input $a = 59$ and $d = 13$.

Solution

	0	**1**	**2**	**3**	**4**
a	59				
d	13				
r	59	46	33	20	7
q	0	1	2	3	4

Problem 8

The following algorithm segment makes change; given an amount of money A between 1¢ and 99¢, it determines a breakdown of A into quarters (q), dimes (d), nickels (n), and pennies (p).

$$q := A \; div \, 25$$
$$A := A \; mod \, 25$$
$$d := A \; div \, 10$$
$$A := A \; mod \, 10$$
$$n := A \; div \, 5$$
$$p := A \; mod \, 5$$

(a) Trace this algorithm segment for $A = 69$.
(b) Trace this algorithm segment for $A = 87$.

Solution

(a)

A	69	19	9	
q	2			
d		1		
n			1	
p				4

(b)

A	87	12	2	
q	3			
d		1		
n			0	
p				2

Problem 9 and Solution

Find the greatest common divisor of 27 and 72.

gcd(27, 72) = 9

Problem 10 and Solution

Find the greatest common divisor of 5 and 9.

gcd(5, 9) = 1

Problem 11 and Solution

Find the greatest common divisor of 7 and 21.

gcd(7, 21) = 7

Problem 12 and Solution

Find the greatest common divisor of 48 and 54.

gcd(48, 54) = 6

Problem 13 and Solution

Use the euclidean algorithm to hand-calculate the greatest common divisors of 1,188 and 385.

1,188 *mod* 385 = 33 and hence gcd(1,188, 385) = gcd(385, 33) by lemma 4.8.2.
385 *mod* 33 = 22 and hence gcd(385, 33) = gcd(33, 22) by lemma 4.8.2.
33 *mod* 22 = 11 and hence gcd(33, 22) = gcd(22, 11) by lemma 4.8.2.
22 *mod* 11 = 0 and hence gcd(22, 11) = gcd(11, 0) by lemma 4.8.2.
gcd(11, 0) = 11 by Lemma 4.8.1.
Hence gcd(1,188, 385) = 11.

Problem 14 and Solution

Use the euclidean algorithm to hand-calculate the greatest common divisors of 509 and 1,177.

1,177 *mod* 509 = 159 and hence gcd(1,188, 385) = gcd(509, 159) by lemma 4.8.2.
509 *mod* 159 = 32 and hence gcd(509, 159) = gcd(159, 32) by lemma 4.8.2.
159 *mod* 32 = 31 and hence gcd(159, 32) = gcd(32, 31) by lemma 4.8.2.
32 *mod* 31 = 1 and hence gcd(32, 31) = gcd(31, 1) by lemma 4.8.2.
32 *mod* 1 = 0 and hence gcd(32, 1) = gcd(1, 0) by lemma 4.8.2.
gcd(1, 0) = 1 by Lemma 4.8.1.
Hence gcd(1,177, 509) = 1.

Problem 15 and Solution

Use the euclidean algorithm to hand-calculate the greatest common divisors of 832 and 10,933.

10,933 *mod* 832 = 117 and hence gcd(10,933, 832) = gcd(832, 117) by lemma 4.8.2.
832 *mod* 117 = 13 and hence gcd(832, 117) = gcd(117, 13) by lemma 4.8.2.
117 *mod* 13 = 0 and hence gcd(117, 13) = gcd(13, 0) by lemma 4.8.2.
gcd(13, 0) = 13 by Lemma 4.8.1.
Hence gcd(10,933, 832) = 13.

Problem 16 and Solution

Use the euclidean algorithm to hand-calculate the greatest common divisors of 4,131 and 2,431.

4,131 *mod* 2,431 = 1,700 and hence gcd(4,131, 2,431) = gcd(2,431, 1,700) by lemma 4.8.2.
2,431 *mod* 1,700 = 731 and hence gcd(2,431, 1,700) = gcd(1,700, 731) by lemma 4.8.2.
1,700 *mod* 731 = 238 and hence gcd(1,700, 731) = gcd(731, 238) by lemma 4.8.2.
731 *mod* 238 = 17 and hence gcd(731, 238) = gcd(238, 17) by lemma 4.8.2.
238 *mod* 17 = 0 and hence gcd(238, 17) = gcd(17, 0) by lemma 4.8.2.
gcd(17, 0) = 17 by Lemma 4.8.1.
Hence gcd(4,131, 2,431) = 247.

Problem 17

Make a trace table to trace the action of algorithm 4.8.2 for the input variables 1,001 and 871.

Solution

	0	**1**	**2**	**3**	**4**	**5**	**end**
A	1001						
B	871						
r	871	130	91	39	13	0	
b	871	130	91	39	13	0	
a	1001	871	130	91	39	13	
gcd							13

Problem 18

Make a trace table to trace the action of algorithm 4.8.2 for the input variables 5,895 and 1,232.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**end**
A	5895												
B	1232												
r	1232	967	265	172	93	79	14	9	5	4	1	0	
b	1232	967	265	172	93	79	14	9	5	4	1	0	
a	5895	1232	967	265	172	93	79	14	9	5	4	1	
gcd													1

Problem 19

Prove that for all positive integers a and b, $a \mid b$ if, and only if, $\gcd(a,\, b) = a$.

Theorem: For all positive integers a and b, $a \mid b \iff \gcd(a,\, b) = a$.

Proof. Let a and b be any positive integers such that $a \mid b$. It follows from that fact that $a = a \cdot 1$ that $a \mid a$. Since $a \mid a$ and $a \mid b$, a is a common divisor of a and b. Therefore we know that

$$a \leq \gcd(a, b)$$

From the definition of gcd we have that $\gcd(a,\, b) \mid a$. It follows from theorem 4.3.1 that

$$\gcd(a, b) \leq a$$

We now have that

$$\gcd(a, b) \leq a \leq \gcd(a, b)$$

Hence $a = \gcd(a,\, b)$.

Now let a and b be any positive integers such that $a = \gcd(a,\, b)$. It follows from the definition of gcd that $a \mid b$.

Since $a \mid b \implies [\gcd(a,\, b) = a]$ and $[\gcd(a,\, b) = a] \implies a \mid b$ we can conclude that $a \mid b \iff \gcd(a,\, b) = a$. □

Problem 20

(a) Prove that if a and b are integers, not both zero, and $d = \gcd(a,\, b)$, then a/d and b/d are integers with no common divisor that is greater than one.

(b) Write an algorithm that accepts the numerator and denominator of a fraction as input and produces as output the numerator and denominator of that fraction written in lowest terms.

Solution

Theorem: If a and b are integers, not both zero, and $d = \gcd(a,\, b)$, then a/d and b/d are integers with no common divisor that is greater than one.

Proof. Let a and b be any integers such that they are not both 0. Let d be an integer such that $d = \gcd(a,\, b)$. It follows from the definition of gcd that $d \mid a$ and $d \mid b$. It follows from the definition of divisibility that $a = dj$ and $b = dk$ for some integers j and k. Solving for j and k gives

$$j = \frac{a}{d} \quad \text{and} \quad k = \frac{b}{d}$$

It now follows that $\frac{a}{d}$ and $\frac{b}{d}$ are integers that are not both 0. Thus they must have a gcd. Suppose that $\gcd(\frac{a}{d}, \frac{b}{d}) = c$. Further, suppose that $c > 1$. It follows from the definition of gcd that

$$c \mid \frac{a}{b} \quad \text{and} \quad c \mid \frac{b}{d}$$

It follows from the definition of divisibility that there exist some integers p and q such that

$$\frac{a}{b} = cp \quad \text{and} \quad \frac{b}{d} = cq$$

Solving for p and q gives

$$p = \frac{a}{cd} \quad \text{and} \quad q = \frac{b}{cd}$$

It follows that since p and q are integers $cd \mid a$ and $cd \mid b$. Since the $\gcd(a, b) = d$ it must be that $cd \leq d$. Solving for c gives $c \leq 1$. However this is a contradiction as we supposed that $c > 1$. Thus the supposition is false and therefore $\frac{a}{d}$ and $\frac{b}{d}$ have no common divisor greater than 1. $\square$

Algorithm to reduce fractions to their lowest terms

$a := |N|$, $b := |D|$
if $a < b$ **then**
  $temp := a$
  $a := b$
  $b := temp$
end if
r := b
while $b \neq 0$ **do**
  $r := a \ mod \ b$
  $a := b$
  $b := r$
end while
$gcd := a$
$N := N/gcd$
$D := D/gcd$

Problem 21

Complete the proof of Lemma 4.8.2 by providing the following: If a and b are any integers with $b \neq 0$ and q and r are any integers such that

$$a = bq + r$$

then

$$\gcd(b, r) \leq \gcd(a, b)$$

Solution

Proof. Let a and b be integers with $b \neq 0$ and let $c = \gcd(b, r)$. Then $c \mid b$ and $c \mid r$, and so, by definition of divisibility, $b = nc$ and $r = mc$ for some integers n and m. Now substitute into the equation

$$a = bq + r$$

to obtain

$$a = (nc)q + mc = c(nq + m)$$

But $nq + m$ is an integer and so by definition $c \mid a$. We also know that $c \mid b$. Thus c is a common divisor of a and b. It follows from property 2 of gcd that that $c \leq \gcd(a, b)$. Thus $\gcd(b, r) \leq \gcd(a, b)$. □

Problem 22

(a) Prove that if a and d are positive integers and q and r are integers such that $a = dq + r$ and $0 < r < d$, then

$$a = d(-(q + 1)) + (d - r) \quad \text{and} \quad 0 < d - r < d$$

(b) Indicate how to modify algorithm 4.8.1 to allow for the input a to be negative.

Solution

(a) *Theorem*: If a and d are positive integers and q and r are integers such that $a = dq + r$ and $0 < r < d$, then

$$a = d(-(q + 1)) + (d - r) \quad \text{and} \quad 0 < d - r < d$$

Proof. Let a and d be positive integers and let q and r be any integers such that $a = dq + r$.

$$\begin{aligned} a &= dq + r \\ -a &= -dq - r \\ -a &= -dq + (-d + d) - r \\ -a &= (-dq - d) + (d - r) \\ -a &= d(-(q + 1)) + (d - r) \end{aligned}$$

Now suppose that $0 < r < d$

$$\begin{aligned} 0 &< r < d \\ -d &< r - d < 0 \\ d &> d - r > 0 \\ 0 &< d - r < d \end{aligned}$$

□

(b) When running algorithm 4.8.1, if the input a is negative, take the absolute value of a and run the algorithm as normal. At the end simply set $q := -(q+1)$ and set $r := d - r$.

Problem 23

(a) Prove that if a, d, q, and r are integers such that $a = dq + r$ and $0 \le r < d$, then

$$q = \left\lfloor \frac{a}{d} \right\rfloor \quad \text{and} \quad r = a - \left\lfloor \frac{a}{d} \right\rfloor \cdot d$$

(b) In a computer language with a built in floor function, *div* and *mod* can be calculated as follows:

$$a\ div\ d = \left\lfloor \frac{a}{d} \right\rfloor \quad \text{and} \quad a\ mod\ d = a - \left\lfloor \frac{a}{d} \right\rfloor \cdot d$$

Rewrite the steps of Algorithm 4.8.2 for a computer language with a built-in floor function but without *div* and *mod*.

Solution

Theorem: If a, d, q, and r are integers such that $a = dq + r$ and $0 \le r < d$, then

$$q = \left\lfloor \frac{a}{d} \right\rfloor \quad \text{and} \quad r = a - \left\lfloor \frac{a}{d} \right\rfloor \cdot d$$

Proof. Let a, d, q, and r be integers such that $a = dq + r$ and $0 \le r < d$.

$$\begin{aligned} a &= dq + r \\ \frac{a}{d} &= q + \frac{r}{d} \quad (1) \\ \frac{a}{d} &> q + \frac{r}{d} - \frac{r}{d} \\ \frac{a}{d} &> q \quad (2) \end{aligned}$$

Since $r < d$ it follows that $\frac{r}{d} < 1$. Now with equation (1) we have

$$\frac{a}{d} = q + \frac{r}{d} < q + 1$$

It follows that

$$\frac{a}{d} < q + 1 \quad (3)$$

Now by combining inequalities (2) and (3) we obtain

$$q < \frac{a}{d} < q + 1$$

$$q \le \frac{a}{d} < q + 1$$

It now follows from the definition of floor that

$$q = \left\lfloor \frac{a}{d} \right\rfloor$$

To prove part two simply substitute our newly discovered expression for q into the equation $a = dq + r$.

$$\begin{aligned} a &= dq + r \\ a &= d \cdot \left\lfloor \frac{a}{d} \right\rfloor + r \\ r &= a - \left\lfloor \frac{a}{d} \right\rfloor \cdot d \end{aligned}$$

□

Euclidean algorithm without use of *div* or *mod*

$a := A$, $b := B$, $r := B$
while $b \neq 0$ **do**
  $r := a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b$
  $a := b$
  $b := r$
end while
$gcd := a$

Problem 24

An alternative to the Euclidean algorithm uses subtraction rather than division to compute greatest common divisors. It is based on the following lemma:

Lemma. $a \geq b > 0 \implies gcd(a,\, b) = gcd(b,\, a - b)$.

(a) Prove Lemma 4.8.3.

(b) Trace the execution of Algorithm 4.8.3 for $A = 630$ and $B = 336$.

(c) Trace the execution of algorithm 4.8.3 for $A = 768$ and $B = 358$.

Solution

Lemma. $a \geq b > 0 \implies gcd(a,\, b) = gcd(b,\, a - b)$.

Proof. Let a, and b be any integers such that $a \geq b > 0$. It follows that since a and b are integers not both 0 there exists an integer $c = \gcd(a,\, b)$. It follows that $c \mid a$ and $c \mid b$. Then, by definition, there exist integers k and j such that

$$a = ck \quad \text{and} \quad b = cj$$

By substitution,

$$a - b = ck - cj$$
$$a - b = c(k - j)$$

It follows from the fact that $k - j$ is an integer that $c \mid (a - b)$. We already know that $c \mid b$ and so it follows that c is a common divisor of b and $a - b$. Now from property 2 of the definition of gcd it follows that $c \leq \gcd(b,\ a - b)$. By substitution

$$\gcd(a, b) \leq \gcd(b, a - b) \quad (1)$$

Since b and $a - b$ are integers not both 0 there exists an integer $e = \gcd(b, a - b)$ It follows that $e \mid b$ and $e \mid a - b$. Then, by definition, there exist integers m and n such that

$$b = em \quad \text{and} \quad a - b = en$$

By substitution,

$$a - b = en$$
$$a - em = en$$
$$a = en + em$$
$$a = e(n + m)$$

It follows from the fact that $n + m$ is an integer that $e \mid a$. We already know that $e \mid b$ and so it follows that e is a common divisor of b and a. Now from property 2 of the definition of gcd it follows that $e \leq \gcd(a,\ b)$. By substitution,

$$\gcd(b, a - b) \leq \gcd(a, b) \quad (2)$$

It now follows from inequalities (1) and (2) that

$$\gcd(a, b) = \gcd(b, a - b)$$ □

Trace table for algorithm 4.8.3 with $A = 630$, $B = 336$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**end**
A	630										
B	336										
a	630	294	294	252	210	168	126	84	42	0	
b	336	336	42	42	42	42	42	42	42	42	
gcd											42

Trace table for algorithm 4.8.3 with $A = 768$, $B = 348$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**end**
A	768													
B	348													
a	768	420	72	72	72	72	72	12	12	12	12	12	0	
b	348	348	348	276	204	132	60	60	48	36	24	12	12	
gcd														12

Problem 25 and Solution

Find the following values

(a) $\operatorname{lcm}(12,\, 18) = \operatorname{lcm}(2^2 \cdot 3,\, 2 \cdot 3^2) = 2^2 \cdot 3^2$

(b) $\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\, 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5$

(c) $\operatorname{lcm}(2800,\, 6125) = \operatorname{lcm}(2^4 \cdot 5^2 \cdot 7,\, 5^3 \cdot 7^2) = 2^4 \cdot 5^3 \cdot 7^2$

Problem 26

Prove that for all positive integers a and b, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if, and only if, $a = b$.

Theorem. *$\forall\ a,\ b \in \mathbb{Z}^+,\ gcd(a,\ b) = lcm(a,\ b) \iff a = b.$*

Proof. Let a and b be any integers positive integers. First we will derive that

$$\gcd(a, b) = \operatorname{lcm}(a, b) \implies a = b$$

Assume that $\gcd(a,\ b) = \operatorname{lcm}(a,\ b)$. It follows from the definition of gcd that

$$\gcd(a, b) \mid a \quad \text{and} \quad \gcd(a, b) \mid b$$

It now follows from theorem 4.3.1 that

$$\gcd(a, b) \leq a \quad \text{and} \quad \gcd(a, b) \leq b \qquad (1)$$

From the assumption that $\gcd(a,\ b) = \operatorname{lcm}(a,\ b)$ we have

$$a \mid \gcd(a, b) \quad \text{and} \quad b \mid \gcd(a, b)$$

It now follows from theorem 4.3.1 that

$$a \leq \gcd(a, b) \quad \text{and} \quad b \leq \gcd(a, b) \qquad (2)$$

Now by combining the inequalities in (1) and (2) we obtain

$$\gcd(a, b) \leq a \leq \gcd(a, b) \quad \text{and} \quad \gcd(a, b) \leq b \leq \gcd(a, b)$$

Hence $a = \gcd(a, b)$ and $b = \gcd(a, b)$ and so $a = b$.

Now we will derive that

$$a = b \implies \gcd(a, b) = \operatorname{lcm}(a, b)$$

Assume that $a = b$. It follows that

$$\gcd(a, b) = \gcd(a, a) \quad \text{and} \quad \operatorname{lcm}(a, b) = \operatorname{lcm}(a, a)$$

Now let $c = \gcd(a,\, a)$. By definition $c \mid a$. It follows from theorem 4.3.1 that $c \leq a$. Since $a \mid a$ it follows from definition of gcd that $a \leq c$. We have that $c \leq a$ and $a \leq c$ and hence

$$a = c = \gcd(a, b) \qquad (3)$$

Now let $e = \operatorname{lcm}(a,\, a)$. By definition $a \mid e$. It follows from theorem 4.3.1 that $a \leq e$. Since $a \mid a$ it follows from definition of lcm that $e \leq a$. We have that $a \leq e$ and $e \leq a$ and hence

$$a = e = \operatorname{lcm}(a, b) \qquad (4)$$

Finally from the transitive property of equality on a in equation (3) and (4) we have that

$$\gcd(a, b) = \operatorname{lcm}(a, b)$$

□

Problem 27

Prove that for all positive integers a and b, $a \mid b$ if, and only if, $\operatorname{lcm}(a,\, b) = b$.

Theorem. *$\forall a, b \in \mathbb{Z}^+,\ a \mid b \iff lcm(a,\ b) = b$.*

Proof. Let a and b be any positive integers. First we will derive that

$$a \mid b \implies \operatorname{lcm}(a, b) = b$$

Assume that $a \mid b$ and let q be an integer such that $q = \operatorname{lcm}(a, b)$. Then $b \mid q$ and so by theorem 4.3.1 $b \leq q$. We know that $a \mid b$ and $b \mid b$ and thus $b \geq q$. We now have that $b \leq q$ and $b \geq q$ and hence

$$b = q = \operatorname{lcm}(a, b)$$

It is now necessary to derive that

$$\operatorname{lcm}(a, b) = b \implies a \mid b$$

Assume that $\operatorname{lcm}(a, b) =$ b. It follows that $b \mid b$ and $a \mid b$. □

Problem 28

Prove that for all integers a, and b, $\gcd(a, b) \mid \operatorname{lcm}(a, b)$.

Theorem. *$\forall a, b \in \mathbb{Z}$, gcd(a, b) $\mid$ lcm(a, b).*

Proof. Let a and b be any integers. By definition $\gcd(a, b) \mid a$ and by definition $a \mid \operatorname{lcm}(a, b)$. It now follows from the transitivity of divisibility that

$$\gcd(a, b) \mid \operatorname{lcm}(a, b)$$

□

Problem 29

Prove that for all positive integers a and b, $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.

Theorem. $\forall a, b \in \mathbb{Z}^+$, *gcd(a, b)·lcm(a, b) = ab.*

Proof. Let a and b be any positive integers. It follows from the definition of gcd that $\gcd(a,b) \mid a$ and so $a = \gcd(a,b) \cdot k$, for some integer k. Multiply both sides by b to obtain $ab = \gcd(a,b) \cdot kb$. Thus

$$kb = \frac{ab}{\gcd(a,b)}$$

Since k is an integer this implies that b is a multiple of $\frac{ab}{\gcd(a,b)}$. Also by definition of gcd $\gcd(a,b) \mid b$ and so $b = \gcd(a,b) \cdot j$, for some integer j. Multiply both sides by a to obtain $ab = \gcd(a,b) \cdot ja$. Thus

$$ja = \frac{ab}{\gcd(a,b)}$$

Since j is an integer this implies that a is a multiple of $\frac{ab}{\gcd(a,b)}$. Since a and b are both multiples of $\frac{ab}{\gcd(a,b)}$ it must be that $\operatorname{lcm}(a,b) \leq \frac{ab}{\gcd(a,b)}$. Multiply both sides by $\gcd(a,b)$ to obtain

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) \leq ab \qquad (1)$$

It follows from the definition of lcm that $a \mid \operatorname{lcm}(a,b)$ and $b \mid \operatorname{lcm}(a,b)$. Thus $\operatorname{lcm}(a,b) = aq$ and $\operatorname{lcm}(a,b) = bp$ for some integers q and p.

$$\begin{aligned} \operatorname{lcm}(a,b) &= aq \\ b \cdot \operatorname{lcm}(a,b) &= aqb \\ \frac{ab}{\operatorname{lcm}(a,b)} \cdot q &= b \end{aligned}$$

It follows from the definition of divides that $\frac{ab}{\operatorname{lcm}(a,b)} \mid a$.

$$\begin{aligned} \operatorname{lcm}(a,b) &= bp \\ a \cdot \operatorname{lcm}(a,b) &= bpa \\ \frac{ab}{\operatorname{lcm}(a,b)} \cdot p &= a \end{aligned}$$

It follows from the definition of divides that $\frac{ab}{\operatorname{lcm}(a,b)} \mid b$. Since a and b are both divided by $\frac{ab}{\operatorname{lcm}(a,b)}$ it must be that $\gcd(a,b) \geq \frac{ab}{\operatorname{lcm}(a,b)}$. Multiply both sides by $\operatorname{lcm}(a,b)$ to obtain

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) \geq ab \qquad (2)$$

Combining inequalities (1) and (2) gives

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) \leq ab \leq \operatorname{lcm}(a,b) \cdot \gcd(a,b)$$

Hence it must be that $\operatorname{lcm}(a,b) \cdot \gcd(a,b) = ab$ $\square$