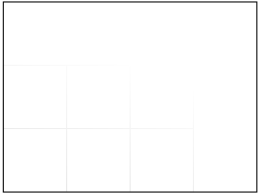
Sections 8.4 and 8.5: Greatest common divisors and the Fundamental Theorem of Arithmetic

CS1231S Discrete Structures

Wong Tin Lok

National University of Singapore

8 October 2020



Question

A rectangle of length 36 units and width 48 units is tiled using squares of length d units, where $d \in \mathbb{Z}$. What is the largest possible value of d?

Tell me your answer at `https://pollev.com/wtl/`.

Answer

$\gcd(36, 48) = 12$.

Introduction

What we saw

- base-b representation
- an algorithm for finding it, together with a proof that it always stops and gives the correct result
- uniqueness of base-b representation

> A mathematical understanding of this concept of correctness is useful beyond the field of program verification. It provides a way of thinking that can improve all aspects of writing programs and building systems.
>
> Leslie Lamport 2018

Theorem 8.3.13 (main theorem of last lecture)

For any $b \in \mathbb{Z}_{\geqslant 2}$ and any $n \in \mathbb{Z}^+$, there exist unique $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$ such that

$$n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0 \quad \text{and} \quad a_\ell \neq 0.$$

Now

- greatest common divisor
- the Euclidean Algorithm
- Fundamental Theorem of Arithmetic

Lamport 2011

Greatest common divisor

d is a divisor of n $\Leftrightarrow$ $d \mid n$
$\Leftrightarrow$ $n = dk$ for some $k \in \mathbb{Z}$.

Definition 8.4.1

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

(1) A *common divisor* of m and n is divisor of both m and n.

(2) The greatest common divisor of m and n is denoted $\gcd(m, n)$.

Example 8.4.2

(1) The positive divisors of 72 are $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$.

(2) The positive divisors of 63 are $1, 3, 7, 9, 21, 63$.

(3) So the positive common divisors of 72 and 63 are $1, 3, 9$.

(4) So $\gcd(72, 63) = 9$.

Exercise 8.4.3

Let $m, n \in \mathbb{Z}^+$. Show that $m \,\underline{\text{mod}}\, n = 0$ if and only if $\gcd(m, n) = n$.

Exercise 8.4.6

Let $m, p \in \mathbb{Z}^+$. Show that if p is prime, then either $\gcd(m, p) = 1$ or $p \mid m$.

(If $\gcd(m, p) = p$, then $m \,\underline{\text{mod}}\, p = 0$ by Exercise 8.4.3, and so $p \mid m$.)

Greatest common divisors — general properties

d is a divisor of n $\Leftrightarrow$ $d \mid n$
$\Leftrightarrow$ $n = dk$ for some $k \in \mathbb{Z}$.

Definition 8.4.1

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

(1) A *common divisor* of m and n is divisor of both m and n.

(2) The greatest common divisor of m and n is denoted $\gcd(m, n)$.

Lemma 8.1.9
Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $-d \mid n$ and $d \mid -n$ and $-d \mid -n$.

Proposition 8.1.10
Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $n \neq 0$, then $|d| \leqslant |n|$.

Remark 8.4.4

In view of Proposition 8.1.10, for all $m, n \in \mathbb{Z}$, if $m \neq 0$ or $n \neq 0$, then $\gcd(m, n)$ exists and is positive.

Question 8.4.5
$\gcd(0, 0)$ does not exist. Why? (What are the divisors of 0?)

Exercise 8.4.7

Let $m, n \in \mathbb{Z}$. Show that the common divisors of m and n are exactly the common divisors of $|m|$ and $|n|$, and hence $\gcd(m, n) = \gcd(|m|, |n|)$.

The Euclidean Algorithm

Algorithm 8.4.8

input $m, n \in \mathbb{Z}^+$ with $m \geqslant n > 0$

$x := m$

$y := n$

while $y \neq 0$ **do**

    $r := x \,\underline{\mathrm{mod}}\, y$

    $x := y$

    $y := r$

end do

output x

Definitions 8.1.16 and 8.1.17.

$x \,\underline{\mathrm{mod}}\, y$ is the remainder when x is divided by y, and $0 \leqslant x \,\underline{\mathrm{mod}}\, y < y$.

To find $\gcd(m, n)$, where $m \geqslant n > 0$:

$$\begin{array}{ccccc} x & & y & & r \\ \downarrow & & \downarrow & & \downarrow \\ m & \underline{\mathrm{mod}} & n & = & r_1 \\ n & \underline{\mathrm{mod}} & r_1 & = & r_2 \\ r_1 & \underline{\mathrm{mod}} & r_2 & = & r_3 \\ r_2 & \underline{\mathrm{mod}} & r_3 & = & r_4 \\ & & & \vdots & \\ r_{k-2} & \underline{\mathrm{mod}} & r_{k-1} & = & r_k \\ r_{k-1} & \underline{\mathrm{mod}} & r_k & = & 0 \\ \hline \end{array}$$

$$\therefore \quad \gcd(m, n) = r_k$$

Example 8.4.9. To find $\gcd(1076, 414)$:

$$\begin{array}{ccccc} x & & y & & r \\ \downarrow & & \downarrow & & \downarrow \\ 1076 & \underline{\mathrm{mod}} & 414 & = & 248 \\ 414 & \underline{\mathrm{mod}} & 248 & = & 166 \\ 248 & \underline{\mathrm{mod}} & 166 & = & 82 \\ 166 & \underline{\mathrm{mod}} & 82 & = & 2 \\ 82 & \underline{\mathrm{mod}} & 2 & = & 0 \\ \hline \end{array}$$

$$\therefore \quad \gcd(1076, 414) = 2$$

Why does the Euclidean Algorithm stop?

similar to base-b representation

Algorithm 8.4.8

```
input m, n ∈ ℤ⁺ with m ⩾ n > 0
x := m
y := n
while y ≠ 0 do
        r := x mod y
        x := y
        y := r
end do
output x
```

Definitions 8.1.16 and 8.1.17.
$x \bmod y$ is the remainder when x is divided by y, and $0 \leqslant x \bmod y < y$.

To find $\gcd(m, n)$, where $m \geqslant n > 0$:

$$
\begin{array}{cccc}
x & & y & r \\
\downarrow & & \downarrow & \downarrow \\
m & \bmod & n & = r_1 \\
n & \bmod & r_1 & = r_2 \\
r_1 & \bmod & r_2 & = r_3 \\
r_2 & \bmod & r_3 & = r_4 \\
 & & \vdots & \\
r_{k-2} & \bmod & r_{k-1} & = r_k \\
r_{k-1} & \bmod & r_k & = 0 \\
\hline
\therefore & \gcd(m, n) & = r_k &
\end{array}
$$

Note that each $r_i \geqslant 0$. So

$$
\begin{aligned}
n &> m \bmod n \\
&= r_1 > n \bmod r_1 \\
&= r_2 > r_1 \bmod r_2 \\
&= r_3 > r_2 \bmod r_3 \\
&\vdots
\end{aligned}
$$

Thus the **while** loop is executed at most n times.

In particular, the algorithm stops.

Note 8.4.10. We used the Well-Ordering Principle here to deduce that, since $\{n, r_1, r_2, r_3, \ldots\}$ is nonempty, it must have a smallest element.

Why is the Euclidean Algorithm correct?

Algorithm 8.4.8

input $m, n \in \mathbb{Z}^+$ with $m \geqslant n > 0$
$x := m$
$y := n$
while $y \neq 0$ **do**
  $r := x \,\underline{\text{mod}}\, y$
  $x := y$
  $y := r$
end do
output x

Definitions 8.1.16 and 8.1.17. $x \,\underline{\text{mod}}\, y$ is the remainder when x is divided by y, and $0 \leqslant x \,\underline{\text{mod}}\, y < y$.

Exercise 8.4.3. If $x \,\underline{\text{mod}}\, y = 0$, then $\gcd(x, y) = y$.

To find $\gcd(m, n)$, where $m \geqslant n > 0$:

$$
\begin{array}{cccc}
x & & y & r \\
\downarrow & & \downarrow & \downarrow \\
m & \underline{\text{mod}} & n & = r_1 \\
n & \underline{\text{mod}} & r_1 & = r_2 \\
r_1 & \underline{\text{mod}} & r_2 & = r_3 \\
r_2 & \underline{\text{mod}} & r_3 & = r_4 \\
 & & \vdots & \\
r_{k-2} & \underline{\text{mod}} & r_{k-1} & = r_k \\
r_{k-1} & \underline{\text{mod}} & r_k & = 0 \\
\hline
\therefore & \gcd(m, n) = r_k & &
\end{array}
$$

Same

- If $m \,\underline{\text{mod}}\, n = 0$, then $\gcd(m, n) = n$.
- Suppose $m \,\underline{\text{mod}}\, n \neq 0$. Let $r_1, r_2, \ldots, r_k$ be as generated on the left, where $k \in \mathbb{Z}^+$. Then Lemma 8.4.11 implies

$$
\begin{aligned}
\gcd(m, n) &= \gcd(n, r_1) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_2, r_3) \\
&\ \ \vdots \\
&= \gcd(r_{k-1}, r_k) \\
&= r_k
\end{aligned}
$$

because $r_{k-1} \,\underline{\text{mod}}\, r_k = 0$.

Lemma 8.4.11. If $x, y, r \in \mathbb{Z}$ such that $x \,\underline{\text{mod}}\, y = r$, then $\gcd(x, y) = \gcd(y, r)$.

The correctness of the Euclidean Algorithm

Lemma 8.1.14 (Closure Lemma)

Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

Proof of Lemma 8.4.11 below

1. Let $q = x \underline{\text{div}}\, y$.
2. Then $x = yq + r$ by the definition of div and mod.
3. $(\Rightarrow)$ If d is a common divisor of x and y, then d is a divisor of r by the Closure Lemma as $r = x - yq = 1 \cdot x + (-q)y$. $\Leftarrow$ $d|x$ and $d|y$
4. $(\Leftarrow)$ If d is a common divisor of y and r, then d is a divisor of x by the Closure Lemma as $x = yq + r = qy + 1 \cdot r$.
5. So the common divisors of x and y are the exactly the common divisors of y and r. $\hookrightarrow$ (by line 3 & 4)
6. Hence $\gcd(x, y) = \gcd(y, r)$. $\square$

$\hookrightarrow \{d \in \mathbb{Z} : d|x \wedge d|y\} = \{d \in \mathbb{Z} : d|y \wedge d|x\}$

need the both directions $(\Leftrightarrow)$

Lemma 8.4.11. If $x, y, r \in \mathbb{Z}$ such that $x \underline{\text{mod}}\, y = r$, then $\gcd(x, y) = \gcd(y, r)$.

The Extended Euclidean Algorithm

Theorem 8.5.2 (Bézout's Lemma)

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = \overbrace{ms + nt}^{\text{\textit{integer linear combination} of } m \text{ and } n}$.

Example 8.5.3

From the Euclidean Algorithm, we know $\gcd(1076, 414) = 2$ because

$$
\begin{array}{rcll}
1076 \,\underline{\text{mod}}\, 414 = 248 & \leftarrow -- & 248 = 1076 - 414 \times 2 & (1) \\
414 \,\underline{\text{mod}}\, 248 = 166 & \leftarrow -- & 166 = 414 - 248 \times 1 & (2) \\
248 \,\underline{\text{mod}}\, 166 = 82 & \leftarrow -- & 82 = 248 - 166 \times 1 & (3) \\
166 \,\underline{\text{mod}}\, 82 = 2 & \leftarrow -- & 2 = 166 - 82 \times 2 & (4) \\
82 \,\underline{\text{mod}}\, 2 = 0 & & &
\end{array}
$$

Hence $\gcd(1076, 414) = 2$

$$
\begin{aligned}
&= 166 - 82 \times 2 && \text{by (4);} \\
&= 166 - (248 - 166 \times 1) \times 2 = 248 \times (-2) + 166 \times 3 && \text{by (3);} \\
&= 248 \times (-2) + (414 - 248 \times 1) \times 3 = 414 \times 3 + 248 \times (-5) && \text{by (2);} \\
&= 414 \times 3 - (1076 - 414 \times 2) \times 5 = 1076 \times (-5) + 414 \times 13 && \text{by (1).}
\end{aligned}
$$

The Extended Euclidean Algorithm — negative numbers

Theorem 8.5.2 (Bézout's Lemma)

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = \overbrace{ms + nt}^{\substack{\textit{integer linear} \\ \textit{combination} \\ \text{of } m \text{ and } n}}$.

Exercise 8.4.7

Let $m, n \in \mathbb{Z}$. Then $\gcd(m, n) = \gcd(|m|, |n|)$.

Remark 8.5.4

Let $m, n \in \mathbb{Z}^+$. If $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = ms + nt$, then by Exercise 8.4.7,

- $\gcd(-m, n) = \gcd(m, n) = ms + nt = (-m)(-s) + nt$;
- $\gcd(m, -n) = \gcd(m, n) = ms + nt = ms + (-n)(-t)$; and
- $\gcd(-m, -n) = \gcd(m, n) = ms + nt = (-m)(-s) + (-n)(-t)$.

Primality

Theorem 8.5.2 (Bézout's Lemma)

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = \overbrace{ms + nt}^{\text{integer linear combination of } m \text{ and } n}$.

Theorem 8.5.5 (Euclid's Lemma)

Let $m, n, p \in \mathbb{Z}^+$. If p is prime and $p \mid mn$, then $\overset{A}{p \mid m}$ or $\overset{B}{p \mid n}$.

$\sim A \to B$

Proof

1. Suppose p is prime and $p \mid mn$.
2. Suppose $p \nmid m$.
3. Then $\gcd(m, p) = 1$ by Exercise 8.4.6.
4. Apply Bézout's Lemma to find $s, t \in \mathbb{Z}$ such that $1 = \gcd(m, p) = ms + pt$.
5. Multiplying through by n gives $n = nms + npt = s(mn) + (nt)p$.
6. Since $p \mid mn$ by assumption and $p \mid p$, the Closure Lemma implies $p \mid n$. □

Let $m, p \in \mathbb{Z}^+$. If p is prime, then either $\gcd(m, p) = 1$ or $p \mid m$.

Lemma 8.1.14. Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

Corollary 8.5.6

Let $n, m_0, m_1, \ldots, m_n, p \in \mathbb{Z}^+$. If p is prime and $p \mid m_0 m_1 \ldots m_n$, then $p \mid m_i$ for some $i \in \{0, 1, \ldots, n\}$.

Prime factorization

Definition 8.5.7

A *prime factorization* of an integer n is a way of writing n as a product of primes.

Example 8.5.8

(1) A prime factorization of 100 is $2 \times 2 \times 5 \times 5 = 2^2 5^2$.

(2) A prime factorization of 641 is 641.

Theorem 8.5.9 (Fundamental Theorem of Arithmetic; Prime Factorization Theorem)

Every integer $n \geqslant 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.

Remark 8.5.10

(1) The uniqueness part of the theorem above becomes false if we omit the "nondecreasing order" requirement, because 2×5 and 5×2 are different prime factorizations of 10.

(2) The uniqueness part of the theorem above becomes false if we allowed 1 to be "prime", because then 2×5 and $1 \times 2 \times 5$ would be different "prime factorizations" of 10 in which the "prime factors" are arranged in nondecreasing order.

The existence of prime factorizations

Lemma 8.2.4. An integer n is composite iff n has a divisor such that $1 < d < n$.

Definition 8.5.7

A *prime factorization* of an integer n is a way of writing n as a product of primes.

Proof of the existence part of the Fundamental Theorem of Arithmetic

1.1. For each $n \in \mathbb{Z}_{\geqslant 2}$, let $P(n)$ be the proposition "n has a prime factorization".

1.2. (Base step) 2 is a prime factorization of 2 because 2 is prime. So $P(2)$ is true.

1.3. (Induction step) 1.3.1. Let $k \in \mathbb{Z}_{\geqslant 2}$ such that $P(2), P(3), \ldots, P(k)$ are true.

1.3.2. If $k+1$ is prime, then $k+1$ is a prime factorization of $k+1$.

1.3.3. So suppose $k+1$ is not prime. Then $k+1$ is composite.

1.3.4. Use Lemma 8.2.4 to find $d \mid k+1$ such that $1 < d < k+1$.

1.3.5. Use the definition of divisibility to find $e \in \mathbb{Z}$ such that $k+1 = de$.

1.3.6. Since $d < k+1 = de$, dividing through by d gives $1 < e$.

1.3.7. Since $1 < d$, multiplying through by e gives $e < de = k+1$.

1.3.8. Combining lines 1.3.6 and 1.3.7 gives $1 < e < k+1$. trying to make e in the correct range

1.3.9. So both d and e have prime factorizations by the induction hypothesis.

1.3.10. This implies $k+1$ has a prime factorization, because $k+1 = de$.

1.3.11. So $P(k+1)$ is true.

1.4. Thus $\forall n \in \mathbb{Z}_{\geqslant 2}\ P(n)$ is true by Strong MI. $\square$

The uniqueness of prime factorizations

2.1. Suppose $n \in \mathbb{Z}_{\geqslant 2}$ with two different prime factorizations:

$$p_0 p_1 \ldots p_k = n = q_0 q_1 \ldots q_\ell. \tag{$*$}$$

2.2. Now we cancel all the primes that are common to both sides of $(*)$.

2.3. We know that some primes are left on both sides because otherwise the two prime factorizations in $(*)$ are the same when arranged in nondecreasing order.

2.4. Let the result of the cancellation in line 2.2 be

$$p'_0 p'_1 \ldots p'_{k'} = q'_0 q'_1 \ldots q'_{\ell'}. \tag{$\dagger$}$$

2.5. No prime appears on both sides of $(\dagger)$ since we cancelled out all of them.

2.6. We see from $(\dagger)$ that $p'_0 \mid q'_0 q'_1 \ldots q'_{\ell'}$.

2.7. Use Corollary 8.5.6 to find $i \in \{0, 1, \ldots, \ell'\}$ such that $p'_0 \mid q'_i$.

2.8. Since q'_i is prime, its only positive divisors are 1 and q'_i. So $p'_0 = q'_i$ as $p'_0 \neq 1$.

2.9. Line 2.5 and line 2.8 contradict each other. $\square$

Corollary 8.5.6. Let $n, m_0, m_1, \ldots, m_n, p \in \mathbb{Z}^+$. If p is prime and $p \mid m_0 m_1 \ldots m_n$, then $p \mid m_i$ for some $i \in \{0, 1, \ldots, n\}$.

Summary

Algorithm 8.4.8 (Euclidean Algorithm)

input $m, n \in \mathbb{Z}^+$ with $m \geqslant n > 0$
$x := m$
$y := n$
while $y \neq 0$ **do**
    $r := x \,\underline{\mathrm{mod}}\, y$
    $x := y$
    $y := r$
end do
output x

> [T]he proof, although not 'difficult', requires a certain amount of preface and might be found tedious by an unmathematical reader. — G.H. Hardy

Theorem 8.5.2 (Bézout's Lemma)

For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(m, n) = ms + nt$.

Theorem 8.5.5 (Euclid's Lemma)

Let $m, n, p \in \mathbb{Z}^+$. If p is prime and $p \mid mn$, then $p \mid m$ or $p \mid n$.

Theorem 8.5.9 (Fundamental Theorem of Arithmetic; Prime Factorization Theorem)

Every integer $n \geqslant 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.

Next

modular arithmetic