Euclid's Algorithm

Discrete Mathematics 27100 Winter 2022

January 26, 2022

Corresponding sections in Margaret Fleck's "Building Blocks for Theoretical Computer Science": Sections 4.2,4.6,4.7 (the previous lecture and problem set 4 covered sections 4.1,4.3,4.4, and 4.5)
Corresponding material in Professor Kurtz's lecture notes: Lecture 3

1 Useful Facts About the Greatest Common Divisor

In this lecture, we prove two useful facts about the greatest common divisor. The first fact is that $Div(x) \cap Div(y) = Div(gcd(x, y))$ (as long as x and y are not both 0 or we define $gcd(0, 0) = 0$)

Theorem 1.1. *For all integers x, y such that x and y are not both 0, $Div(x) \cap Div(y) = Div(gcd(x, y))$*

Corollary 1.2. *For all integers x, y such that x and y are not both 0 and all integers d, $d \mid gcd(x, y)$ if and only if $d \mid x$ and $d \mid y$.*

As described in the lecture notes for the previous lecture, this fact can be shown by using the prime factorizations for x and y. In this lecture, we'll show it in a different way which does not rely on prime factorizations.

The second fact describes which integers can be written as a linear combination of two integers x and y.

Definition 1.3. *Given $x, y \in \mathbb{Z}$, we define the span of x, y to be $span\{x, y\} = \{ax + by : a, b \in \mathbb{Z}\}$*

Example 1.4. *$span\{9, 15\} = \{3n : n \in \mathbb{Z}\}$ (i.e. the set of all multiples of 3). For example, $3 = 2 * 9 - 15$ and $42 = 3 * 9 + 15$*

Theorem 1.5. *For all integers x, y such that x and y are not both 0, $span\{x, y\} = span\{gcd(x, y), 0\} = \{gcd(x, y)n : n \in \mathbb{Z}\}$*

Corollary 1.6 (Bézout's Identity). *For all integers x, y such that x and y are not both 0, $\exists a, b \in \mathbb{Z}(ax + by = gcd(x, y))$*

Example 1.7. *If $x = 18$ and $y = 42$ then $gcd(x, y) = 6$ and $y - 2x = 42 - 36 = 6$.*

Remark 1.8. *If we define $gcd(0, 0) = 0$ then these results are true when $x = y = 0$ as well.*

2 Basic Facts about Divisibility

Before stating and analyzing Euclid's algorithm, we need some basic facts about division and divisibility.

Proposition 2.1. *For all integers a, b, c, if $a \mid b$ and $b \mid c$ then $a \mid c$*

Proof. If $a \mid b$ and $b \mid c$ then $\exists y, z \in \mathbb{Z}(ax = b \wedge by = c)$. Now

$$a(xy) = (ax)y = by = c$$

so $a \mid c$, as needed. Note that this proof works because multiplication is associative. □

Proposition 2.2. *For all integers d, x, y, a, b, if $d \mid x$ and $d \mid y$ then $d \mid ax + by$*

Proof. If $d \mid x$ and $d \mid y$ then $\exists r, s \in \mathbb{Z}(rd = x \wedge sd = y)$. Now

$$ax + by = a(rd) + b(sd) = (ar)d + (bs)d = (ar + bs)d$$

so $d \mid ax + by$, as needed. Note that this proof works because of the distributive property of multiplication and the fact that multiplication is associative. □

Theorem 2.3 (The Division Theorem)**.** *For all integers n and all natural numbers d, there exists a unique pair of integers (q, r) such that*

1. $n = qd + r$
2. $0 \leq r \leq d - 1$

Proof. We first show that there exists an a pair of integers (q, r) such that $n = qd + r$ and $0 \leq r \leq d - 1$. Let $r = min\{x : x \geq 0, \exists q \in \mathbb{Z} : x = n - qd\}$. Because of the way r is defined, $\exists q \in \mathbb{Z}(r = n - qd)$. Rearranging this equation gives $n = qd + r$. Thus, we just need to show that $0 \leq r \leq d - 1$.

To show that $0 \leq r \leq d - 1$, assume that $r \geq d$. If so, then let $r' = r - d$. Now $r' < r$, $r' \geq 0$, and $r' = n - (q + 1)d$ so $r \neq min\{x : x \geq 0, \exists q \in \mathbb{Z}(x = n - qd)\}$, which is a contradiction. Thus, $0 \leq r \leq d - 1$, as needed.

To show that (q, r) is the unique pair of integers such that $n = qd + r$ and $0 \leq r \leq d - 1$, assume that (q', r') is another pair of integers such that $n = q'd + r'$ and $0 \leq r' \leq d - 1$. Without loss of generality, we may assume that $r' \geq r$. Now observe that

1. $r' = n - q'd$ and $r = n - qd$ so $r' - r = qd - q'd = (q - q')d$ is divisible by d.
2. $0 \leq r' - r \leq d - 1$

The only way that $r' - r$ can be both divisible by d and between 0 and $d - 1$ is if $r' - r = 0$. Thus, $r' = r$. We now have that $q' = \frac{n-r'}{d} = \frac{n-r}{d} = q$, as needed. □

3 Euclid's Algorithm

Euclid's algorithm for finding the greatest common denominator works as follows:

Input: Natural numbers x, y.
Initialization: Set $a = max\{x, y\}$ and set $b = min\{x, y\}$
Iterative step: While $b > 0$:

1. Divide a by b and let r be the remainder.

2. Set $a = b$ and set $b = r$.

Output: When $b = 0$, output a.

Example 3.1. *If $x = 55$ and $y = 40$ then we take the following steps:*

1. *If we divide 55 by 40 then we get a remainder of 15 so after the first iteration we have $a = 40$ and $b = 15$*

2. *If we divide 40 by 15 then we get a remainder of 10 so after the second iteration we have $a = 15$ and $b = 10$*

3. *If we divide 15 by 10 then we get a remainder of 5 so after the third iteration we have $a = 10$ and $b = 5$*

4. *If we divide 10 by 5 then we get a remainder of 0 so after the fourth iteration we have $a = 5$ and $b = 0$*

5. *We now stop and output $gcd(55, 40) = 5$*

If we extend Euclid's algorithm by keeping track of how a and b can be expressed in terms of x and y, we can also find integers a, b such that $ax + by = gcd(x, y)$.

Example 3.2. *If $x = 98$ and $y = 21$ then we take the following steps:*

1. *If we divide 98 by 21 then the answer is 4 with a remainder of 14. Thus, after the first iteration we have $a = 21$ and $b = 14$. Note that $a = y$ and $b = x - 4y$*

2. *If we divide 21 by 14 then the answer is 1 with a remainder of 7. Thus, after the second iteration we have $a = 14$ and $b = 7$. Note that $a = x - 4y$ and $b = y - (x - 4y) = 5y - x$*

3. *If we divide 14 by 7 then the answer is 2 with a remainder of 0. Thus, after the third iteration we have $a = 7$ and $b = 0$. Note that $a = 5y - x$ and $b = (x - 4y) - 2(5y - x) = 3x - 14y$*

4. *We now stop and output $gcd(98, 21) = 7$ and that $5y - x = 105 - 98 = 7$.*

3.1 Proof of the Properties of the Greatest Common Divisor via Euclid's Algorithm

Theorem 3.3. *For all integers x, y such that x and y are not both 0,*

1. $Div(x) \cap Div(y) = Div(gcd(x, y))$
2. $span\{x, y\} = span\{gcd(x, y), 0\} = \{gcd(x, y)n : n \in \mathbb{Z}\}$

Proof. The key idea is that $Div(x) \cap Div(y)$, $gcd(x, y)$, and $span\{x, y\}$ remain invariant as we run Euclid's algorithm

Lemma 3.4. *For all integers x,y, and k,*

1. $Div(x + ky) \cap Div(y) = Div(x) \cap Div(y)$
2. $span\{x + ky, y\} = span\{x, y\}$

Proof. To prove this, we need to prove the following four statements:

1. If $d \mid x + ky$ and $d \mid y$ then $d \mid x$.
2. If $d \mid x$ and $d \mid y$ then $d \mid x + ky$.
3. If $n \in span\{x + ky, y\}$ then $n \in span\{x, y\}$.
4. If $n \in span\{x, y\}$ then $n \in span\{x + ky, y\}$.

We can prove these statements as follows:

1. For the first statement, observe that $x = (x + ky) - ky$. Thus, by Proposition 2.2, if $d \mid x + ky$ and $d \mid y$ then $d \mid (x + ky) - ky = x$.
2. For the second statement, by Proposition 2.2, if $d \mid x$ and $d \mid y$ then $d \mid x + ky$.
3. For the third statement, if $n \in span\{x + ky, y\}$ then $\exists a, b \in \mathbb{Z}(n = a(x + ky) + by)$. Now $n = a(x + ky) + by = ax + (b + ak)y$ so $n \in span\{x, y\}$.
4. For the fourth statement, if $n \in span\{x, y\}$ then $\exists a, b \in \mathbb{Z}(n = ax + by)$. Now $n = ax + by = a(x + ky) + (b - ak)y$ so $n \in span\{x + ky, y\}$

□

Since $Div(x) \cap Div(y)$, $gcd(x, y)$, and $span\{x, y\}$ remain invariant as we run Euclid's algorithm, if a is the output of Euclid's algorithm then we must have that

1. $Div(x) \cap Div(y) = Div(a) \cap Div(0) = Div(a)$
2. $gcd(x, y) = gcd(a, 0) = a$
3. $span\{x, y\} = span\{a, 0\} = \{an : n \in \mathbb{Z}\}$

□

Remark 3.5. *This proof can be made more rigorous by turning it into a proof by induction. We will cover proofs by induction next lecture.*