GREATEST COMMON DIVISOR

Frank Tsai

April 14, 2024

Definition 0.1. The *greatest common divisor* (gcd) of two integers a and b, is an integer k such that

- $k \mid a$
- $k \mid b$
- $\forall k' \in \mathbb{Z}. (k' \mid a) \wedge (k' \mid b) \Rightarrow (k' \mid k)$

Remark 0.2. Note that Definition 0.1 allows nonunique gcds. In fact, if k is a gcd of a and b, then so is $-k$. This can be remedied by choosing the nonnegative one. We write $\gcd(a, b)$ for the nonnegative integer satisfying the conditions in Definition 0.1.

Remark 0.3. Although gcds is defined for integers, its computation can be done using just nonnegative integers (c.f., Lemmas 0.5 and 0.6).

Lemma 0.4 is the backbone lemma that enables us to device a recursive algorithm to compute gcds.

Lemma 0.4. *For any integers $a, b,$ and c,* $\gcd(a - cb, b) = \gcd(a, b)$.

Proof. Let $k = \gcd(a - cb, b)$. It follows by definition that $k \mid b$. Since $a - cb = dk$ for some integer d, we can express a as $a = dk + cb$. But since b is divisible by k, a is also divisible by k.

It remains to show that, for any integer k', if k' divides both a and b, then k' also divides k. To this end, it suffices to show that $k' \mid (a - cb)$ and that $k' \mid b$. The latter follows immediately by assumption. As for the former, since k' divides both a and b by assumption, it follows that k' divides $a - cb$. □

Lemma 0.5. *For all integers a and b,* $\gcd(a, b) = \gcd(b, a)$.

Proof. Exercise. □

Lemma 0.6. *For all integers a and b,* $\gcd(-a, b) = \gcd(a, b)$.

Proof. Exercise. □

Lemma 0.7. *For any integer a,* $\gcd(0, a) = a$.

Proof. Exercise. □

If we set $c := 1$ in Lemma 0.4, then we get $\forall a, b \in \mathbb{Z}. \gcd(a - b, b) = \gcd(a, b)$. This allows us to calculate the gcd of two integers as follows.

Example 0.8.

$$\begin{aligned}
\gcd(321, 123) &= \gcd(198, 123) && (1)\\
&= \gcd(75, 123) = \gcd(123, 75) && (2)\\
&= \gcd(48, 75) = \gcd(75, 48) && (3)\\
&= \gcd(27, 48) = \gcd(48, 27) && (4)\\
&= \gcd(21, 27) = \gcd(27, 21) && (5)\\
&= \gcd(6, 21) = \gcd(21, 6) && (6)\\
&= \gcd(15, 6) && (7)\\
&= \gcd(9, 6) && (8)\\
&= \gcd(3, 6) = \gcd(6, 3) && (9)\\
&= \gcd(3, 3) && (10)\\
&= \gcd(0, 3) = 3 && (11)
\end{aligned}$$

Instead of choosing a fixed c in each step, Euclid's algorithm chooses a more clever c. This choice is given by Euclid's division lemma.

Lemma 0.9 (Euclid's division lemma)**.** *Given two integers a and b, with $b \neq 0$, there are unique integers q and r such that*

- $a = bq + r$
- $0 \leq r < |b|$, *where $|b|$ is the absolute value of b*

Now, to compute $\gcd(a, b)$, we can choose $c := q$, where q is the unique integer such that $a = bq + r$. Then, $\gcd(a, b) = \gcd(a - qb, b)$. Note that $a - qb = r$, so we obtain a formula in terms of the remainder: $\gcd(a, b) = \gcd(r, b)$. Now, Example 0.8 can be computed as follows.

Example 0.10.

$$\begin{aligned}
\gcd(321, 123) &= \gcd(321 \bmod 123, 123) && (12)\\
&= \gcd(75, 123) = \gcd(123, 75) = \gcd(123 \bmod 75, 75) && (13)\\
&= \gcd(48, 75) = \gcd(75, 48) = \gcd(75 \bmod 48, 48) && (14)\\
&= \gcd(27, 48) = \gcd(48, 27) = \gcd(48 \bmod 27, 27) && (15)\\
&= \gcd(21, 27) = \gcd(27, 21) = \gcd(27 \bmod 21, 21) && (16)\\
&= \gcd(6, 21) = \gcd(21, 6) = \gcd(21 \bmod 6, 6) && (17)\\
&= \gcd(3, 6) = \gcd(6, 3) = \gcd(6 \bmod 3, 3) && (18)\\
&= \gcd(0, 3) = 3 && (19)
\end{aligned}$$

Theorem 0.11. *In each step of Euclid's algorithm computing $\gcd(a, b)$, both arguments can be expressed as a combination of a and b.*

Proof. Let n be the number of steps taken and a_n and b_n be the first and the second argument at step n, respectively. We need to show that $a_n = u_1 a + v_1 b$ and $b_n = u_2 a + v_2 b$ for some integers u_1, v_1, u_2, and v_2.

The base case is clear.

$$\gcd(a, b) = \gcd(1a + 0b, 0a + 1b).$$

In the induction step, let us assume without loss of generality that $b_n < a_n$. We can always swap them if it is not the case. By definition, $a_{n+1} = r$, where $r = a_n - b_n q$, and $b_{n+1} = b_n$. By the induction hypothesis, $b_n = u_2 a + v_2 b$, so clearly b_{n+1} can be expressed as a combination of a and b. As for a_{n+1}, we have $a_n = u_1 a + v_1 b$ by the induction hypothesis, so

$$a_{n+1} = a_n - b_n q = (u_1 a + v_1 b) - (v_2 a + v_2 b) q = (u_1 - v_2 q) a + (v_1 - v_2 q) b$$

$\square$

Corollary 0.12 (Bézout's lemma)**.** *If k is $\gcd(a, b)$, then $k = ua + vb$ for some integers u and v.*