- 3.8

The Euclidean Algorithm

P. Danziger

1 Greatest Common Divisor (gcd)

Definition 1 *Given two integers a and b, not both zero, the greatest common divisor of a and b, denoted $gcd(a, b)$, is the integer which satisfies the following two properties:*

1. $(gcd(a, b) \mid a) \wedge (gcd(a, b) \mid b)$.
2. $\forall a, b, d \in \mathbb{Z},\ (d \mid a \wedge d \mid b) \Rightarrow d \leq gcd(a, b)$.

Example 2

1. gcd(2,3) = 1, gcd(3,6) = 3, gcd(12, 16) = 4.
2. Find gcd(374,110).
   $374 = 2 \cdot 11 \cdot 17, \qquad 110 = 2 \cdot 5 \cdot 11.$
   Thus $\gcd(374,\ 110) = 2 \cdot 11 = 22$.
3. Find gcd(3743323,11012456).
   ??!

In the second example found the standard factored form of the two numbers, and used this to find the gcd. Is there an easier way?
YES: The Euclidean Algorithm.

Lemma 3 *The gcd of any integer with zero is itself.*

To Prove: $\forall a \in \mathbb{Z}^+,\ \gcd(a, 0) = a$.
Proof:
Let $a \in \mathbb{Z}^+$
Clearly $a \mid a$ and $a \mid 0$.
Also $\forall d \in \mathbb{Z}$, if $d \mid a$ then $d \leq a$. □

Lemma 4 *If an integer, d divides two integers a and b, then $d \mid b - a$.*
To Prove:
$\forall a, b, d \in \mathbb{Z}, (d \mid a \wedge d \mid b) \Rightarrow d \mid b - a$.

Proof:
Let $a, b, d \in \mathbb{Z}$, with $d \mid a$ and $d \mid b$.
$\Rightarrow \exists\, k, \ell \in \mathbb{Z}$ such that $a = k \cdot d$ and $b = \ell \cdot d$. (Definition of $\mid$)
Let $c = b - a$.
So $c = k \cdot d - \ell \cdot d = (k - \ell) \cdot d$ (Algebra)
But $(k - \ell) \in \mathbb{Z}$ (Closure of $\mathbb{Z}$ under $-$)
So $d \mid c$ (Definition of $\mid$) □

Lemma 5 $\forall a \in \mathbb{Z}, b \in \mathbb{Z}^+, q, r \in \mathbb{N},\ (a = b \cdot q + r) \Rightarrow gcd(a, b) = gcd(b, r)$

Proof:
Let $a \in \mathbb{Z}, b \in \mathbb{Z}^+, q, r \in \mathbb{N}$, with $a = b \cdot q + r$. (Such a q and r exist by the QRT.)
Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. (Definition of gcd)
Since $a = b \cdot q + r$ and d divides both a and b we must have that $d \mid r$ (Lemma 4)
Thus $d \mid b$ and $d \mid r$. It remains to show that d is the largest such integer.
We know that if $d \mid b$ and $d \mid r$ then $d \mid (bq + r)$.
Thus every common divisor of b and r is also a comon divisor of a and b.
But d is the largest common divisor of a and b (by definition of d), thus it must also be the largest divisor of b and r. □

Corollary 6 $\forall n \in \mathbb{Z}, m \in \mathbb{Z}^+,\ gcd(n, m) = gcd(m, n \bmod m)$.

2 The Euclidean Algorithm for finding $\gcd(a, b)$

Here is a *recursive* algorithm for finding gcd, usually known as the Euclidean Algorithm. A recursive algorithm is one which calls itself.

```
int gcd(a, b) {
    If a = b = 0, (no gcd) return ERROR.
    If a = b return a.
    If a = 0 return b.
    If b = 0 return a.
    If a > b return gcd(b, a mod b).
    Else return gcd(a, b mod a).
}
```

Example 7 *Trace the execution of the above algorithm in finding gcd(124, 3120)*

$a = 124$	$b = 3120$	$3120 \bmod 124 = 20$	return gcd(124, 20)
$a = 124$	$b = 20$	$124 \bmod 20 = 4$	return gcd(20, 4)
$a = 20$	$b = 4$	$20 \bmod 4 = 0$	return gcd(4, 0)
$a = 4$	$b = 0$	—	**return 4**

Example 8 *Trace the execution of the above algorithm in finding gcd(220, 124)*

$a = 124$	$b = 220$	$220 \bmod 124 = 96$	return gcd(124, 96)
$a = 124$	$b = 96$	$124 \bmod 96 = 28$	return gcd(96, 28)
$a = 96$	$b = 28$	$96 \bmod 28 = 12$	return gcd(28, 12)
$a = 28$	$b = 12$	$28 \bmod 12 = 4$	return gcd(12, 4)
$a = 12$	$b = 4$	$12 \bmod 4 = 0$	return gcd(4, 0)
$a = 4$	$b = 0$	—	**return 4**