GREATEST COMMON DIVISORS

Below is a nice result on common divisors that is useful in future proofs while, at the same time, has never seemed that obvious to me.

Theorem: Let $a,b\in\mathbb{Z}$ with $a,b\neq 0$. Then there exist unique elements *r* and *s* such that the greatest common divisor of *a* and *b* can be written as,

$$\gcd(a,b)=ar+bs$$

Proof: Let $S=\{am+bn\,|\,m,n\in\mathbb{Z}\text{ and }am+bn>0\}$. Clearly, $S\neq\varnothing$ since if $a,b>0$, then $a\cdot 1+b\cdot 1>0$ and $a\cdot 1+b\cdot 1\in S$. On the other hand, if one or both of *a* and *b* is negative, say for example that $a<0$ and $b>0$, $a\cdot(-1)+b\cdot 1>0$ and $a\cdot(-1)+b\cdot 1\in S$. The other possible combinations of one or both of *a* and *b* being negative can be handled similarly.

Since *S* is a subset of the positive integers, there is going to be a smallest element in *S* which we can represent as $d=ar+bs$ for some $r,s\in\mathbb{Z}$. Our claim now is that $d=\gcd(a,b)$, the greatest common divisor of *a* and *b*. First, we will show that *d* divides both *a* and *b*. Now, we know that in general, if we divide *d* into *a*, then we will get a result that looks like $a=d\cdot q+t$ where $0\leq t<d$. If $t>0$, then $a=d\cdot q+t\Rightarrow t=a-d\cdot q\Rightarrow t=a-(ar+bs)q=a-arq-bsq=a(1-rq)+b(-sq)\in S$. However, since $t<d$, this contradicts our choice of *d* as the smallest element in *S*. Hence, we must have $t=0$ and *d* divides *a*. An identical argument can now be used to show that *d* divides *b*.

To show that *d* is the greatest common divisor of *a* and *b*, suppose that there exists $f\in\mathbb{Z}$ such that *f* divides both *a* and *b*, and $f>d$. Since *f* divides *a*, there is an integer *q* such that $a=fq$, and since *f* divides *b*, there is an integer *z* such that $b=fz$. Hence, $d=ar+bs=(fq)r+(fz)s=f(qr+zs)$. From this last expression it follows that *f* divides *d*. But this is a contradiction since $f>d$. Therefore, $d=ar+bs=\gcd(a,b)$.

□

Corollary: If $f>0$ is a common divisor of *a* and *b*, and if we can write $f=am+bn$ for some $m,n\in\mathbb{Z}$, then $f=\gcd(a,b)$.

Proof: Let $d=\gcd(a,b)$. Then by our theorem above, *d* is the smallest positive element in $S=\{am+bn\,|\,m,n\in\mathbb{Z}\text{ and }am+bn>0\}$. If $f>0$ is also a common divisor of *a* and *b*, then clearly $f\leq d=\gcd(a,b)$. But on the other hand, if we can write *f* in the form $f=am+bn$ for some $m,n\in\mathbb{Z}$, then $\cup S=\{am+bn\,|\,m,n\in\mathbb{Z}\text{ and }am+bn>0\}$, and, hence, $f\geq d$. It now easily follows that $f=d$. □

We'll now illustrate a procedure called the *Euclidean Algorithm* for finding the greatest common divisor of two positive integers. In particular, let's find $\gcd(945, 2415)$. We'll start by writing 2415 in the form (dividend) = (divisor)(quotient) + (remainder) where the dividend is 2415 and the divisor is 945. This gives us,

$$2415 = 945 \cdot 2 + 525$$

We now repeat the process by, this time, using 945 as our dividend and 525 as the divisor.

$$945 = 525 \cdot 1 + 420$$

An if we continue this same pattern, then eventually we will arrive at a remainder of 0.

$$525 = 420 \cdot 1 + 105$$
$$420 = 105 \cdot 4 + 0$$

The claim now is that $105 = \gcd(945, 2415)$. To verify this, we can start by working backwards from our last equation.

$$420 = 105 \cdot 4 + 0$$
$$525 = (105 \cdot 4) \cdot 1 + 105$$
$$945 = [(105 \cdot 4) \cdot 1 + 105] \cdot 1 + (105 \cdot 4)$$
$$2415 = ([(105 \cdot 4) \cdot 1 + 105] \cdot 1 + (105 \cdot 4)) \cdot 2 + [(105 \cdot 4) \cdot 1 + 105]$$

Since we can rewrite this last equation as ,

$$2415 = 105([(1 \cdot 4) \cdot 1 + 1] \cdot 1 + (1 \cdot 4)) \cdot 2 + [(1 \cdot 4) \cdot 1 + 1] = 105 \cdot 23$$

And since we can rewrite the next to last equation as,

$$945 = 105 \cdot [(1 \cdot 4) \cdot 1 + 11] \cdot 1 + (1 \cdot 4) = 105 \cdot 9,$$

It is clear that 105 is a divisor of both 2145 and 945. But on the other hand, we can also work backwards to obtain,

$$105 = 525 + (-1) \cdot 420$$
$$105 = 525 + (-1) \cdot [945 + (-1) \cdot 525] = 2 \cdot 525 + (-1) \cdot 945$$
$$105 = 2 \cdot [2415 + (-2) \cdot 945] + (-1) \cdot 945 = 2 \cdot 2415 + (-5) \cdot 945 > 0$$

Thus, since 105 is a common divisor of 2145 and 945 and since $105 = 2 \cdot 2415 + (-5) \cdot 945$, it follows from our corollary above that $105 = \gcd(945, 2415)$.

□