Linear Combination vs Common Divisor

Theorem: gcd(a,b) = spc(a,b)

For example, the *greatest* common divisor of 52 and 44 is 4.
And 4 is a linear combination of 52 and 44:

$$6 \cdot 52 + (-7) \cdot 44 = 4$$

Furthermore, no linear combination of 52 and 44 is equal to a smaller positive integer.

To prove the theorem, we will prove:

gcd(a,b) <= spc(a,b)

gcd(a,b) | spc(a,b)

spc(a,b) <= gcd(a,b)

spc(a,b) is a common divisor of a and b

GCD <= SPC

3. If $d \mid a$ and $d \mid b$, then $d \mid sa + tb$ for all s and t.

Proof of (3)

$d \mid a \Rightarrow a = dk_1$

$d \mid b \Rightarrow b = dk_2$

$sa + tb = sdk_1 + tdk_2 = d(sk_1 + tk_2)$

$\Rightarrow d \mid (sa+tb)$

GCD | SPC

Let $d = \gcd(a,b)$. By definition, $d \mid a$ and $d \mid b$.

Let $f = spc(a,b) = sa+tb$

By (3), $d \mid f$. This implies $d \le f$. That is $\gcd(a,b) \le spc(a,b)$.

SPC <= GCD

We will prove that spc(a,b) is actually a common divisor of a and b.

First, show that spc(a,b) | a.

1. Suppose, by way of contradiction, that spc(a,b) does not divide a.
2. Then, by the Division Theorem,
3. $a = q \times spc(a,b) + r$ and $spc(a,b) > r > 0$
4. Let $spc(a,b) = sa + tb$.
5. So $r = a - q \times spc(a,b) = a - q \times (sa + tb) = (1\text{-}qs)a + qtb$.
6. Thus r is an integer linear combination of a and b, and spc(a,b) > r.
7. This contradicts the definition of spc(a,b), and so r must be zero.

Similarly, spa(a,b) | b.

So, spc(a,b) is a common divisor of a and b, thus by definition spc(a,b) <= gcd(a,b).

Extended GCD Algorithm

How can we write gcd(a,b) as an integer linear combination?

This can be done by extending the Euclidean's algorithm.

Example: $a = 259$, $b=70$

$259 = 3 \cdot 70 + 49$ $\qquad$ $49 = a - 3b$

$70 = 1 \cdot 49 + 21$ $\qquad$ $21 = 70 - 49$

$21 = b - (a-3b) = -a+4b$

$49 = 2 \cdot 21 + 7$ $\qquad$ $7 = 49 - 2 \cdot 21$

$7 = (a-3b) - 2(-a+4b) = \underline{3a - 11b}$

$21 = 7 \cdot 3 + 0$ $\qquad$ done, gcd = 7

Extended GCD Algorithm

Example: $a = 899$, $b=493$

$899 = 1 \cdot 493 + 406$ so $406 = a - b$

$493 = 1 \cdot 406 + 87$ so $87 = 493 - 406$

$= b - (a-b) = -a + 2b$

$406 = 4 \cdot 87 + 58$ so $58 = 406 - 4 \cdot 87$

$= (a-b) - 4(-a+2b) = 5a - 9b$

$87 = 1 \cdot 58 + 29$ so $29 = 87 - 1 \cdot 58$

$= (-a+2b) - (5a-9b) = \underline{-6a + 11b}$

$58 = 2 \cdot 29 + 0$ done, gcd = 29

Application of the Theorem

Theorem: gcd(a,b) = spc(a,b)

Why is this theorem useful?

(1) we can now "write down" gcd(a,b) as some concrete equation,

(i.e. gcd(a,b) = sa+tb for some integers s and t),

and this allows us to reason about gcd(a,b) much easier.

(2) If we can find integers s and t so that sa+tb=c,

then we can conclude that gcd(a,b) <= c.

In particular, if c=1, then we can conclude that gcd(a,b)=1.

Prime Divisibility

Theorem: $\gcd(a,b) = \operatorname{spc}(a,b)$

Lemma: p prime and $p \mid a \cdot b$ implies $p \mid a$ or $p \mid b$.

pf: say p does not divide a. so $\gcd(p,a)=1$.

So by the **Theorem**, there exist s and t such that

$$sa + tp = 1$$

$$\underbrace{(sa)b}_{p \mid ab} + \underbrace{(tp)b}_{p \mid p} = b$$

Hence $p \mid b$

Cor : If p is prime, and $p \mid a_1 \cdot a_2 \cdots a_m$ then $p \mid a_i$ for some i.

Fundamental Theorem of Arithmetic

Every integer, $n>1$, has a *unique* factorization into primes:

$$p_0 \le p_1 \le \cdots \le p_k$$

$$p_0\, p_1 \cdots p_k = n$$

Example:

$61394323221 = 3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$

Unique Factorization

Theorem: There is a unique factorization.

proof: suppose, by contradiction,

that there are numbers with two different factorization.

By the well-ordering principle, we choose the smallest such $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

Since n is smallest, we must have that $p_i \neq q_j$ all i,j

(Otherwise, we can obtain a smaller counterexample.)

contradiction!

Since $p_1 | n = q_1 \cdot q_2 \cdots q_m$, so by Cor., $p_1 | q_i$ for some i.

Since both $p_1 = q_i$ are prime numbers, we must have $p_1 = q_i$.

Application of the Theorem

Theorem: $\gcd(a,b) = \mathrm{spc}(a,b)$

Lemma. If $\gcd(a,b)=1$ and $\gcd(a,c)=1$, then $\gcd(a,bc)=1$.

By the **Theorem**, there exist s,t,u,v such that

$$sa + tb = 1$$
$$ua + vc = 1$$

Multiplying, we have $(sa + tb)(ua + vc) = 1$

$\Rightarrow saua + savc + tbua + tbvc = 1$

$\Rightarrow (sau + svc + tbu)a + (tv)bc = 1$

By the **Theorem**, since $\mathrm{spc}(a,bc)=1$, we have $\gcd(a,bc)=1$

Two Jug Puzzle

For two jugs with capacity A gallons and B gallons,
is it possible to fill up one jug with exactly c gallons
of waters

This question is not so easy to answer without number theory.

General Solution

Invariant:

Suppose that we have water jugs with capacities B and L.

Then the amount of water in each jug is always an integer linear combination of B and L.

Theorem: gcd(a,b) = spc(a,b)

Corollary: Every linear combination of a and b is a multiple of gcd(a, b).

Corollary: The amount of water in each jug is a multiple of gcd(a,b).

General Solution

Corollary: The amount of water in each jug is a multiple of gcd(a,b).

Given jug of 3 and jug of 9, is it possible to have exactly 4 gallons in one jug?

NO, because gcd(3,9)=3, and 4 is not a multiple of 3.

Given jug of 21 and jug of 26, is it possible to have exactly 3 gallons in one jug?

gcd(21,26)=1, and 3 is a multiple of 1,
so this possibility has not been ruled out yet.

Theorem. Given water jugs of capacity a and b,
it is possible to have exactly k gallons in one jug
if and only if k is a multiple of gcd(a,b).

General Solution

Theorem. Given water jugs of capacity a and b,
it is possible to have exactly k gallons in one jug
if and only if k is a multiple of gcd(a,b).

Given jug of 21 and jug of 26, is it possible to have exactly 3 gallons in one jug?

$$\gcd(21,26) = 1$$

$$\Rightarrow 5\times21 - 4\times26 = 1$$

$$\Rightarrow 15\times21 - 12\times26 = 3$$

Repeat 15 times:

1. Fill the 21-gallon jug.
2. Pour all the water in the 21-gallon jug into the 26-gallon jug.
   Whenever the 26-gallon jug becomes full, empty it out.

General Solution

$$15 \times 21 - 12 \times 26 = 3$$

Repeat 15 times:

1. Fill the 21-gallon jug.
2. Pour all the water in the 21-gallon jug into the 26-gallon jug.

   Whenever the 26-gallon jug becomes full, empty it out.

1. There must be exactly 3 gallons left after this process.
2. Totally we have filled 15x21 gallons.
3. We pour out some multiple t of 26 gallons.
4. The 26 gallon jug can only hold somewhere between 0 and 26.
5. So t must be equal to 12.
6. And there are exactly 3 gallons left.

General Solution

Given two jugs with capacity A and B with $A < B$, the target is C.

If $\gcd(A,B)$ does not divide C, then it is impossible.

Otherwise, compute $C = sA + tB$.

Repeat s times:

1. Fill the A-gallon jug.
2. Pour all the water in the A-gallon jug into the B-gallon jug.

   Whenever the B-gallon jug becomes full, empty it out.

The B-gallon jug will be emptied exactly t times.

After that, there will be exactly C gallons in the B-gallon jug.