6.1200J/18.062J *Mathematics for Computer Science* Tuesday 5th March, 2024
Massachusetts Institute of Technology, Spring 2024
Z. Abel, B. Chapman, E. Demaine revised Tuesday 5th March, 2024

Lecture 08: Divisibility

1 Number Theory

Study of integers! One of oldest fields in math!

Quote from Hardy, 1940, *A Mathematician's Apology*: we can rejoice that "[number theory's] very remoteness from ordinary human activities should keep it gentle and clean", i.e., not usable in warfare.

But, ends up having tons of applications! secure encrypted communications, e-commerce, crucial in warfare, but that's besides the point

Lots of questions that are easy to state but hard to solve, like Goldbach's conjecture or the Twin Prime conjecture.

Speaking of Hardy, fun story with him and Ramanujan, $1729 = 1^3 + 12^3 = 9^3 + 10^3$. Not just a curiosity: precedes K3 surfaces (studied 30 years later), deep connections to string theory and quantum physics. Number theory connects to everything.

Including algorithms!!

2 Divisibility

Definition 1. *We'll say "a divides b" (equivalently, b is a multiple of a, b is divisible by a, a is a divisor of b), and we'll write $a \mid b$, iff there exists an integer k such that $ak = b$.*

E.g. $3 \mid 12$, $-5 \mid 100$, $n \mid n$, because $n \cdot 1 = n$. In particular, $0 \mid 0$ (!). Def is almost equivalent to saying that b/a is an integer, except for $0/0$ case.

Even just means "divisible by 2" i.e. "multiple of 2". Is 0 even? Story about Paris smog 1977? https://www.bbc.com/news/magazine-20559052

Some common divisibility facts:

- If $a \mid b$ and $b \mid c$ then $a \mid c$. (E.g., every multiple of 100 is also a multiple of 5.) If $ax = b$ and $by = c$ then $a(xy) = c$.
- If $a \mid b$ then $a \mid bc$. Just a restatement of the last one.
- If $a \mid b$ and $a \mid c$ then $a \mid b + c$. Just saying $xa + ya = (x + y)a$.
- If $a \mid b$ and $a \mid c$ then $a \mid sb + tc$ for all $s, t \in \mathbb{Z}$. Note: $sb + tc$ (for integers s, t) is known as an *integer linear combination* or ILC of b and c.

3 Die Hard

Film clip: Die Hard with a Vengence (Die Hard 3). Park in manhattan. Simon Gruber is forcing John (Bruce Willis) and Zeus (Samuel L. Jackson) to prevent bombs from going off. Bunch of kids playing in this park.

“You want to focus on the problem at hand?”

The problem: 3g jug and 5g jug, want to get exactly 4 gallons, just by pouring and *not guessing*. Who wants to try?

$$(0,0) \overset{\text{fill}}{\mapsto} (3,0) \overset{\text{pour}}{\mapsto} (0,3) \overset{\text{fill}}{\mapsto} (3,3) \overset{\text{pour}}{\mapsto} (1,5) \overset{\text{empty}}{\mapsto} (1,0) \overset{\text{pour}}{\mapsto} (0,1) \overset{\text{fill}}{\mapsto} (3,1) \overset{\text{pour}}{\mapsto} (0,4)$$

$$(0,0) \overset{\text{fill}}{\mapsto} (0,5) \overset{\text{pour}}{\mapsto} (3,2) \overset{\text{empty}}{\mapsto} (0,2) \overset{\text{pour}}{\mapsto} (2,0) \overset{\text{fill}}{\mapsto} (2,5) \overset{\text{pour}}{\mapsto} (3,4)$$

Little known sequel: Die Hard 9, Die even Harder! Now it’s jugs with capacity 6g and 9g, want to get 5g. How to prevent bomb?

Oh no, impossible! All amounts will be multiples of 3. Divisibility!

In fact, can prove more: given jugs with capacities a and b, all amounts will be *integer linear combinations* of a and b.

State machine: state is (x, y), where there are x gallons in the a gallon jug, and y in the b gallon jug. Start at $(0, 0)$. State (x, y) can transition to:

- Empty: $(0, y)$ or $(x, 0)$
- Fill: (a, y) or (x, b)
- Pour left to right: $(0, x + y)$ if $x + y \leq b$, or $(x + y - b, b)$ if $x + y > b$.
- Pour right to left: $(x + y, 0)$ if $x + y \leq a$, or $(a, x + y - a)$ if $x + y > a$.

Invariant: $P(x, y) :=$ “x and y are integer linear combinations of a and b”.

Start state? $0 = 0a + 0b$.

Next show P is *preserved across transitions.* So assume $P(x, y)$ and $(x, y) \mapsto (x', y')$; must prove $P(x', y')$. From $P(x, y)$ we know $x = sa + tb$ and $y = ua + vb$ for integers s, t, u, v. Then x', y' are in $\{0, x, y, a, b, x + y, x + y - a, x + y - b\}$. Each of these is an i.l.c. of a and b! For example, $x + y = (s + u)a + (t + v)b$. $x + y - a = (s + u - 1)a + (t + v)b$. Rest are similar.

So P is true at start and is preserved across transitions. Done!

Explains why $6, 9$ can’t get to 5: every reachable amount has form $6s + 9t$, which must be divisible by 3.

4 Greatest Common Divisor

Definition 2. *A* common divisor *of integers a and b is an integer d such that $d \mid a$ and $d \mid b$.*

Definition 3. *The* greatest common divisor *of integers a, b, denoted* $\gcd(a, b)$*, is a non-negative common divisor g of a and b such that for every common divisor d of a and b, $d \mid g$.*

For example, $\gcd(6, 9) = 3$, $\gcd(5, 0) = 5$, $\gcd(0, 0) = 0$!

Note that $\gcd(a, b)$ is *usually* the greatest (in the usual $\geq$ sense) integer that divides both a and b, except for the $\gcd(0, 0)$ case.

Fast algorithm to compute $\gcd(a, b)$ *without factoring a and b*! [We don't have fast factoring algs in general.] Euclid's Algorithm, 300BC. One of the earliest known algorithms. Let's build up to it.

Lemma 1. *For every a,* $\gcd(a, 0) = |a|$.

Proof. Certainly $|a|$ is a common divisor of a and 0. For every common divisor d of a and 0, $d \mid a$. This also means $d \mid -a$, so $d \mid |a|$. □

Lemma 2. $\gcd(a, b) = \gcd(a, b - a)$.

Proof. Let d be a common divisor of a and b. This means $d \mid a$ and $d \mid b$, so $d \mid (b - a)$, i.e. d is also a common divisor of a and $b - a$. Similarly, if d is a common divisor of a and $b - a$, then d is also a divisor of $a + (b - a) = b$, i.e. d is a common divisor of a and b. The set of common divisors of a and b is the same as the set of common divisors of a and $b - a$, so the greatest common divisor (if extant) is also the same. □

This already gives an algorithm! Example:

$$\begin{aligned}\gcd(12, 41) = \gcd(12, 29) = \gcd(12, 17) = \gcd(12, 5) = \gcd(7, 5) = \gcd(2, 5)\\ = \gcd(2, 3) = \gcd(2, 1) = \gcd(1, 1) = \gcd(1, 0) = 1.\end{aligned}$$

Some obvious inefficiencies:

$$\gcd(1000002, 5) = \gcd(999997, 5) = \gcd(999992, 5) = \cdots = \gcd(7, 5) = \gcd(2, 5).$$

Can see pattern and jump straight to end, with *remainders*.

Theorem 3. *For all pairs of integers n, d with $d > 0$, there exists a* unique *pair of integers q, r where $n = qd + r$ and $0 \leq r < d$. The number $q = n \operatorname{div} d$ is the* quotient*, and $r = n \operatorname{rem} d$ is the* remainder*.*

Should jump straight from (x, y) to $(x \operatorname{rem} y, y)$.

Lemma 4. $\gcd(a, b) = \gcd(a, b \operatorname{rem} a)$.

Proof. Divide with remainder, $b = aq + r$. Then $\gcd(a, b) = \gcd(a, b - a) = \gcd(a, b - 2a) = \cdots = \gcd(a, b - qa)$ [hidden induction!]. Done! □

Note: this also means $\gcd(a, b) = \gcd(b, a \operatorname{rem} b)$ by symmetry of the definition.

Example:

$$\begin{aligned}
\gcd(1001, 777) &= \gcd(777, 1001 \operatorname{rem} 777) && = \gcd(777, 224) && [q = 1] \\
&= \gcd(224, 777 \operatorname{rem} 224) && = \gcd(224, 105) && [q = 3] \\
&= \gcd(105, 224 \operatorname{rem} 105) && = \gcd(105, 14) && [q = 2] \\
&= \gcd(14, 105 \operatorname{rem} 14) && = \gcd(14, 7) && [q = 7] \\
&= \gcd(7, 14 \operatorname{rem} 7) && = \gcd(7, 0) && [q = 2] \\
&= 7.
\end{aligned}$$

Definition 4 (Euclid's Algorithm)**.** *Start at (a, b) (let's assume $a \geq b \geq 0$). From each state (x, y), transition to $(y, x \operatorname{rem} y)$ as long as $y > 0$. When reaching a final state (x_f, y_f) where $y_f = 0$, the answer is $\gcd(a, b) = x_f$.*

Maintains the invariant $P(x, y) :=$ "$\gcd(x, y) = \gcd(a, b)$".

Partial correctness: Final states must have $y = 0$. When this happens, must have $\gcd(a, b) = \gcd(x, 0) = x$.

Termination: $x + y$ strictly decreases, because $x \operatorname{rem} y < x$ when $y \leq x$. So number of steps is at most $a + b$.

Actually, exponentially better: can prove $x \operatorname{rem} y < x/2$ when $y \leq x$, so $\operatorname{bitcount}(x) + \operatorname{bitcount}(y)$ strictly decreases! Number of steps is at most $\operatorname{bitcount}(a) + \operatorname{bitcount}(b)$.

(By the way, don't really need $a \geq b$ assumption. If $a < b$ then the next state is (b, a), and then we proceed as above. This adds at most 1 more step.)

5 Extended Euclidean Algorithm

Like the water jug game, every number reached by Euclidean algorithm is an ILC of a and b.

Example:

$$\begin{aligned}
1001 &= a \\
777 &= b \\
224 &= (1001) - 1(777) && = (a) - 1(b) && = a - b \\
105 &= (777) - 3(224) && = (b) - 3(a - b) && = -3a + 4b \\
14 &= (224) - 2(105) && = (a - b) - 2(-3a + 4b) && = 7a - 9b \\
7 &= (105) - 7(14) && = (-3a + 4b) - 7(7a - 9b) && = -52a + 67b.
\end{aligned}$$

This gives rise to the Extended Euclidean Algorithm, aka The Pulverizer. A version of this went by the name Kuṭṭaka [Sanskrit for *pulverization*]. Attributed to Āryabhaṭa, around 500CE.

Definition 5 (The Pulverizer)**.** *Start at* $(a, b, 1, 0, 0, 1)$ *(let's assume* $a \geq b \geq 0$*). From each state* (x, y, s, t, u, v)*, transition to* $(y, r, u, v, s - qu, t - qv)$ *as long as* $y > 0$*, where* $q = x \operatorname{div} y$ *and* $r = x \operatorname{rem} y$*. When reaching a final state* $(x_f, y_f, s_f, t_f, u_f, v_f)$ *where* $y_f = 0$*, the answer is* $\gcd(a, b) = x_f = as_f + bt_f$*.*

Maintains the following three invariants:

- $\gcd(x, y) = \gcd(a, b)$
- $x = as + bt$
- $y = au + bv$

First invariant is as above. Second follows from third. Third uses division theorem, whence $r = x - qy = (as + bt) - q(au + bv) = a(s - qu) + b(t - qv)$.

Theorem 5 (Bezout's Identity)**.** $\gcd(a, b)$ *can be written as an integer linear combination of* a *and* b*. In other words, there exist* s, t *such that* $\gcd(a, b) = as + bt$*.*

Corollary 6. *A number can be written as an ILC of* a, b *iff it is a multiple of* $\gcd(a, b)$*.*

Proof. Let $g = \gcd(a, b)$. Every ILC of a, b is divisible by g. Conversely, we know $g = sa + tb$ for some s, t by Bezout, so every multiple of g (say kg) can be written as $(ks)a + (kt)b$ and is therefore an ILC of a, b. □

Corollary 7. $\gcd(a, b)$ *is the smallest positive integer that can be written as a linear combination of* a *and* b*.*

Proof. Set $g = \gcd(a, b)$. The ILCs of a, b are precisely the multiples of g by the previous Lemma, and g is the smallest positive multiple of itself. □