MATH240 – Lecture 11

Enlai Li

February 8, 2023

1 Number theory ($\mathbb{Z}$)

1.1 Divisibility

We have seen that this is a reflexive and transitive relation

$$x \mid y \iff \exists k \in \mathbb{Z}, \text{ where } kx = y$$

Theorem:

1. If $a|b$, then $a|bc$ for every integer c
2. If $a|b$ and $a|c$, then $a|b \pm c$ for every integer c

proof 1.

$$\begin{aligned} a|b \Rightarrow & b = ka \\ \Rightarrow & bc = (kc)a \\ \Rightarrow & a|bc \end{aligned}$$

2.

$$\begin{aligned} a|banda|c \Rightarrow & b = ka \text{ and } c = la \\ \Rightarrow & b \pm c = (k \pm l)a \\ \Rightarrow & a|b \pm c \end{aligned}$$

1.1.1 Greatest common divisor

gcd of a and b is a number

$$d = gcd(a, b) \in \mathbb{Z}$$

such that

1. $d|a$ and $d|b$ (common divisor)
2. $c|a$ and $c|b \Rightarrow c \leq d$ (Greatest)

ex: a = 16, b = 24
positive divisor of 16: 1,2,4,8,16
positive divisor of 24: 1,2,3,4,6,8,12,24

Thid algorithm is very inefficient and requires "testing" all numbers $\leq a$ and $\leq b$. It takes $\log(n)$ digits to write in a computer memory

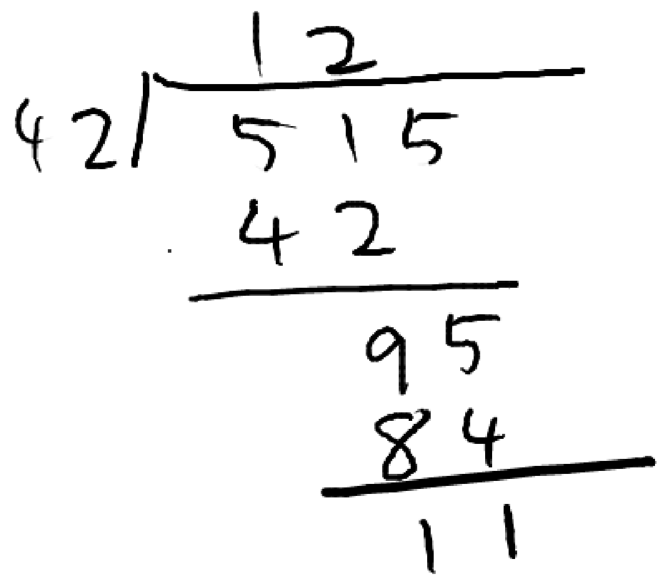
$$\Rightarrow \log(n) = \text{ size of input}$$

There are $\approx n$ numbers to test. It's an exponential in the size of n. (infeasible for a number with, say, 100 digits)

$$n = b^{\log_n(n)}$$

For the gcd problem, there is a much better algorithm (complexity log(n)). Found in $\approx$ 300 BC called **Euclid's algorithm**. It is based on the long division from elementary school . . . ex:

$$515 \div 42 = ?$$
$$515 = 12 \times 42 + 11$$



There is a method for finding number q (quotient) and r (remainder) such that

$$a = qb + r$$

Theorem: $\forall a, b \in \mathbb{Z}, b \neq 0$, there exists integers $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that

$$a = qb + r$$

and $0 \leq r < b$, moreover, those numbers q and r are unique
Proof 1: Existence

1. if $0 < b \leq a$ the use long division
2. If a < b and b > 0, add a multiple kb to a until $a + kb$ is $> b$. Then use case 1

$$a + kb = qb + r$$
$$\Rightarrow a = (q - k)b + r$$

3. If $b < 0$, apply case 1 or 2 with $-b$ instead of b ...

$$\Rightarrow a = q(-b) + r$$
$$a = (-q)b + r$$

Proof 2: Uniqueness
Suppose we have 2 solutions, show that those two solutions are the same. In our case, Assume:

$$a = q_1 b + r_1 0 \leq r_1 < |b|$$
$$\text{and } a = q_2 b + r_2 0 \leq r_2 < |b|$$

Goal: show that $q_1 = q_2$ and $r_1 = r_2$

$$a = q_1 b + r_1 = q_2 b + r_2$$
$$(q_1 - q_2)b = r_1 - r_2$$
$$\Rightarrow b | r_1 - r_1$$
$$|r_1 - r_2| \leq b - 1$$

r_1 and r_2 are both in the interval $[0, b-1]$, so the only way for b to divide this is:

$$r_1 - r_2 = 0$$
$$r_1 = r_2$$

$$(q_1 - q_2)b = 0$$
$$q_1 - q_2 = 0$$
$$q_1 = q_2$$

$\square$

Theorem: If $a = qb + r$, then

$$\gcd(a, b) = \gcd(b, r)$$

Typically, we would have $b < a$ and $r < b$ so it reduces the gcd problem to a smaller instance

Proof:

$$\text{Let } x = gcd(a, b)$$
$$y = gcd(b, v)$$

Goal: prove $x = y$
We will prove this by proving

1. $x \leq y$
2. $y \leq x$

1.

$$x = gcd(a, b) \Rightarrow x|a \text{ and } x|b$$
$$\text{Since } a = qb + r, \text{ then } r = a - qb$$
$$\text{But } x|a \text{ and } x|qb \Rightarrow x|r$$
$$\Rightarrow x \text{ is a common divisor of b and r}$$
$$\Rightarrow x \leq y$$

2.

$$y = gcd(b, r) \Rightarrow y|b \text{ and } y|r$$
$$\Rightarrow y|qb + r$$
$$\Rightarrow y|a \text{ (y is a common divisor of a and b)}$$
$$\Rightarrow y \leq x$$

Corollary Euclid's algorithm:
To find $gcd(a, b)$, assume $a > b\ldots$
Find (with long division) r such that

$$a = qb + r$$

then find $gcd(b, r)$ (with the same method)
ex: find $gcd(515, 42)$

We stop when we find a remainder of 0, because $gcd(x, 0) = |x|$

$$515 = 12 \times 42 + 11$$
$$\Rightarrow gcd(515, 42) = gcd(42, 11)$$
$$\text{Then } 42 = 3 \times 11 + 9$$
$$11 = 1 \times 9 + 2$$
$$9 = 4 \times 2 + 1$$
$$2 + 2 \times 1 + \boxed{0} \text{ (Stop)}$$

Conclusion:

$$\begin{aligned} gcd(515,42) &= gcd(42,11) \\ &= gcd(11,9) \\ &= gcd(9,2) \\ &= gcd(2,1) \\ &= gcd(\boxed{1},0) \end{aligned}$$

Theorem Bezout:
Let $d = gcd(a,b)$, then there exists $s,t \in \mathbb{Z}$ such that

$$\boxed{d = sa + tb}$$

We roll back the steps of Euclid's algorithm

ex:

$$a = 515 \quad b = 42 \quad d = 1$$

$$9 = 4 \times 2 + \boxed{1} \Rightarrow 1 = 9 - 4 \times 2$$

$$11 = 1 \times 9 + \boxed{2} \Rightarrow 2 = 11 - 1 \times 9$$

$$\begin{aligned} \Rightarrow 1 &= 9 - 4 \times (11 - 1 \times 9) \\ &= 5 \times 9 - 4 \times 11 \end{aligned}$$

Then

$$\begin{aligned} 9 &= 42 - 3 \times 11 \\ \Rightarrow 1 &= 5 \times (42 - 3 \times 11) - 4 \times 11 \\ &= 5 \times 42 - 15 \times 11 - 4 \times 11 \\ &= 5 \times 42 - 19 \times 11 \end{aligned}$$

Then

$$11 = 515 - 12 \times 42$$

$$\Rightarrow 1 = 5 \times 42 - 19(515 - 12 \times 42) - 19 \times 515 + 233 \times 42$$

Proof of Bezout algorithm:
Let

$$r_0 = a_1 \quad r_1 = b$$

Then Euclid's algorithm runs as :

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \end{aligned}$$

We prove by induction on n that we can always find $t_n, S_n \in \mathbb{Z}$ (including the gcd, which is one of those remainders r_n) such that

$$r_n = s_n a + t_n b$$

There are two basic cases here:

n=0: $r_0 = a = 1 \times a + 0 \times b$ so $s_0 = 1, t_0 = 0$

n=1: $r_1 = b = 0 \times a + 1 \times b$ so $s_1 = 0, t_1 = 1$

Induction step Asumme that:

$$\begin{aligned} r_{n-1} &= s_{n-1}a + t_{n-1}b \\ r_n &= s_n a + t_n b \end{aligned}$$

We want to prove it for r_{n+1}, but

$$\begin{aligned} r_{n-1} &= q_n r_n + r_{n+1} \\ \Rightarrow r_{n+1} &= r_{n-1} - q_n r_n \\ &= (s_{n-1}a + t_{n-1}b) - q_n(s_n a + t_n b) \\ &= \underbrace{(s_{n-1} - q_n s_n)}_{s_{n+1}} a + \underbrace{(t_{n-1} - q_n t_n)}_{t_{n+1}} b \end{aligned}$$

Conclusion Since $d = r_n$ for some n, then

$$d = s_n a + t_n b$$

□