Math 2001. Lecture 24. Midterm 2: April 1 03.16. 2022.

Last time:

- proving equivalences of multiple statements

- existence proofs

e.g. For any $a, b \in \mathbb{Z}_{>0}$, $\exists\, k, l \in \mathbb{Z}$ s.t. $\gcd(a,b) = ak + bl$.

We proved: the smallest positive integer, d, in the set

$D = \{ax+by : x,y \in \mathbb{Z}\}$, must divide a and divide b.

Today:

- finishing the proof, and the Euclidean algorithm,

- Constructive vs. nonconstructive proofs

1. Finishing the example.

Need: $\forall a, b \in \mathbb{Z}_{>0}$, $\exists k, l$. s.t. $\gcd(a,b) = ak + bl$.

Showed: $d := \min\{ax + by : x, y \in \mathbb{Z}, ax+by > 0\}$ divides both a and b.

To finish the proof, it suffices to show that $\gcd(a,b) = d$.

(1) "$d \le \gcd$": Since $d \mid a$ and $d \mid b$, we have d is a common divisor of a and b, (c.d.)

therefore $d \le \gcd(a,b)$.

(2) "$\gcd \le d$": We have $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$, so

$\gcd(a,b) \mid ax + by \quad \forall x, y \in \mathbb{Z}$.

therefore $\gcd(a,b) \mid d$ since d is of the form $ax+by$ for some $x, y \in \mathbb{Z}$.

Thus we have $\gcd(a,b) \le d$.

By (1) and (2), we have $\gcd(a,b) = d$. so we are done.

Take-away: The gcd of two pos. int. equals the smallest positive integral lin. comb. of those two integers. ($\gcd(a,b) = ak + bl$)

Aside*: The Euclidean algorithm (for getting "k" and "l".)

Examples: $a = 43$, $b = 13$.

$$43 = 13 \cdot 3 + 4$$
$$13 = 4 \cdot 3 + 1$$
the gcd
$$4 = 4 \cdot 1 + \boxed{0}$$
halt when 0 appears

$a = 210$, $b = 45$.

$$210 = 45 \cdot 4 + 30$$
$$45 = 30 \cdot 1 + 15$$
the gcd.
$$30 = 15 \cdot 2 + \boxed{0}$$
halt at 0

General algorithm: WLOG, assume $a > b$. Starting with $(x_0, y_0) = (a, b)$, keep dividing x_i by y_i and setting $(x_{i+1}, y_{i+1}) = (y_i$, the remainder r in $x_i = y_i \cdot q + r)$ until $r = \boxed{0}$.

Fact: The last nonzero "r" is the gcd.

The algorithm can also help us find "k" and "ℓ":

$a = 210$, $b = 45$.

$210 = 45 \cdot 4 + 30$

$45 = 30 \cdot 1 + 15$

$30 = 15 \cdot 2 + \boxed{0}$

$$\gcd(a,b) = 15 = 45 - 30 \cdot 1$$

$$= 45 - (210 - 45 \cdot 4)$$

$$= -210 + 45 \cdot 5$$

$$= (-1) \cdot 210 + 5 \cdot 45. \checkmark$$

Ex: Try the Euclidean algorithm and find k, ℓ for $a = 270$ and $b = 192$.

2. Constructive vs. nonconstructive proofs

Recall: $((x)^a)^b = x^{ab}$

We'll prove the following prop. in two ways.

Prop: There exist irrational numbers x, y s.t. x^y is rational.

Pf 1 (constructive): Take $x = \sqrt{2}$ and $y = \log_2 9$. We know x is irrational.

We claim that $\underbrace{y \text{ is also irrational}}_{(a)}$ and $\underbrace{x^y \text{ is rational}}_{(b)}$, so we'd be done.

✓ (b): $x^y = \sqrt{2}^{\log_2 9} = \sqrt{2}^{\log_2(3^2)} = (\sqrt{2})^{(2\log_2 3)} = \left((\sqrt{2})^2\right)^{\log_2 3} = 2^{(\log_2 3)} = 3 \in \mathbb{Q}$.

✓ (a): We prove y is irr. by contradiction: Suppose $y = \log_2 9$ is rational. Then

$\log_2 9 = \frac{m}{n}$ for some $m, n \in \mathbb{Z}_{>0}$. Thus, we have $(2)^{m/n} = 9$. so

$2^m = (2^{m/n})^n = 9^n$. This is impossible since 2^m is even while 9^n is odd. $\square$

Pf 2 (non-constructive): Consider $x = \sqrt{2}$, $y = \sqrt{2}$, so that $x^y = \sqrt{2}^{\sqrt{2}}$ and $x, y \notin \mathbb{Q}$.

If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, we are done.

If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, then we may take $x' = \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ and $y' = \sqrt{2} \notin \mathbb{Q}$,

and we have
$$(x')^{y'} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2 \in \mathbb{Q},$$

and we are again done. $\square$

Next time: more proof examples