# Number Theory:

## §3.4 Dividing:

- **Thm 3.4.1:**
  Let $a, b \in \mathbb{Z}$ w/ $b > 0$. $\exists\, q, r \in \mathbb{Z}$ s.t.

  $$a = bq + r \quad \text{and} \quad 0 \le r < b$$

  Moreover, there is only one such pair

- eg: $a = 26 \quad b = 8$
  Find $q$ & $r$.

- eg: $a = -26, \; b = 8$.
  Find $q$ & $r$.

Pf:

First we will show ~~that~~ $q$ & $r$ exist.

Put $B = \{ a - bk : k \in \mathbb{Z};\ a - bk \geq 0 \} \subseteq \mathbb{N}$

Show $B \neq \emptyset$

Let $r$ be the smallest element in $B$.

Note: 1) $r \geq 0$

2) $\exists\, q \in \mathbb{Z}$ s.t. $r = a - bq$

$\Rightarrow a = bq + r$

Show $r < b$. (by contradiction)

Finally, we will show that $q$ & $r$ are unique.

For the sake of contradiction assume

$$a = bq + r \qquad 0 \le r < b$$

$$a = bq' + r' \qquad 0 \le r' < b.$$

[redacted]

~~Def~~: Let $a, b \in \mathbb{Z}$ w/ $b > 0$. Let $q, r \in \mathbb{Z}$ be the unique pair satisfying

$$a = bq + r \quad \& \quad 0 \le r < b$$

Then we define

$$a \text{ div } b = q \qquad a \text{ mod } b = r.$$

~~eg~~:

$12 \text{ div } 4 =$ $\qquad$ $12 \text{ mod } 4 =$

$12 \text{ div } 5 =$ $\qquad$ $12 \text{ mod } 5 =$

$10 \text{ div } 3 =$ $\qquad$ $10 \text{ mod } 3 =$

$-33 \text{ div } 4 =$ $\qquad$ $-33 \text{ mod } 4 =$

**Prop. 34.6:** Let $a, b, n \in \mathbb{Z}$ w/ $n > 0$. Then

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

**Pf:**

($\Rightarrow$): $\not\Rightarrow$ $a \equiv b \pmod{n}$

There fore $a \bmod n = b \bmod n$

($\Leftarrow$): $\not\Leftarrow$ $a \bmod n = b \bmod n$

There fore $a \equiv b \pmod{n}$ ∎

## §35 G.C.D.

- Def: Let $a, b \in \mathbb{Z}$, we say that $d$ is a common divisor of $a$ & $b$ provided that $d \mid a$ & $d \mid b$.

- Def: Let $a, b \in \mathbb{Z}$. We say that $d$ is the greatest common divisor of $a$ and $b$ provided that
  1. $d \mid a$ & $d \mid b$.
  2. If $e$ is any other common divisor of $a$ & $b$ then $e \leq d$.

- Notation:
  $(a,b) :=$ greatest common divisor of $a$ & $b$.

- e.g. Compute $(10, 15)$.

Prop 3.3:

Let $a, b \in \mathbb{N}$ and let $c = a \bmod b$.

Then

$$(a,b) = (b,c)$$

Pf: $\because c = a \bmod b$. Then $\exists q \in \mathbb{Z}$ such that

$$a = bq + c$$

Let $d = (a,b)$ ; $e = (b,c)$

eg. Compute $(114, 9)$,

[redacted]

- Euclidean Algorithm.

Input: $a, b \in \mathbb{N}$.

Output: $(a, b)$.

1.) Put $c = a \bmod b$.

2.) If $c = 0$ then output $b$ and stop.

3.) Otherwise ($c \neq 0$) compute $(b, c)$ and output its value.

Note: This is an example of a recursive algorithm, that is an alg. defined in terms of itself.

- eg.: Compute $(63, 75) =$

• Prop 3.4:
The Euclidean algorithm correctly computes $(a,b)$ for any $a,b \in \mathbb{N}$.

– Pf: See pp. 263–264.

How fast?

• Prop 3.5:
Let $a,b \in \mathbb{Z}$ with $a \geq b > 0$. Then letting $c = a \bmod b$, $c < \frac{a}{2}$.

• Pf:
Case 1: $a < 2b$.

Case 2: $a \geq 2b$.

* Cor: The number of steps required for the Euclidean algorithm to compute $(a,b)$ is less or equal to $2\log_2(b)$.

Pf:

(The right way to think of gcd's).

- Thm 3.5.6: Let $a, b \in \mathbb{Z}$ not both 0. The smallest integer of the form $ax+by$ where $x, y \in \mathbb{Z}$ is $(a,b)$.

- Pf: Put $D = \{ax+by : x,y \in \mathbb{Z};\ ax+by > 0\} \subseteq \mathbb{N}$

Show $D \neq \emptyset$

Let $d \in D$ be the smallest element.

Claim: $d \mid a$,

Pf: (contradiction)

Claim: $d \mid b$.

Pf similar.

Claim: $e \mid a$ & $e \mid b \Rightarrow e \leq d$.

$\therefore \quad d = (a,b)$ ∎

eg Find $x, y \in \mathbb{Z}$ s.t.

$$431x + 29y = (431, 29).$$

Def:

Let $a, b \in \mathbb{Z}$ we say that $a$ and $b$ are relatively prime (or coprime) provided that $(a,b) = 1$.

- Cor 3B9:
  Let $a, b \in \mathbb{Z}$, $\exists\, x, y \in \mathbb{Z}$ s.t. $ax + by = 1$ iff $(a,b) = 1$.

- Pf:

- Prop 3B10:
  Let $a, b \in \mathbb{Z}$ and let $d = (a,b)$. If $e \mid a$ & $e \mid b$ then $e \mid d$.

- Pf: