Quiz 1

The following shows the implementation of the Euclidean Algorithm for $(36, 21)$

1) $36 = 1 \cdot 21 + 15$

2) $21 = 1 \cdot 15 + 6$

3) $15 = 2 \cdot 6 + 3$

4) $6 = 2 \cdot 3 + \underline{\underline{0}}$ Halt!

Question: Using above to find an integer solution of

$$36x + 21y = 3$$

Solution to Quiz 1 :

1) $36 = 1 \cdot 21 + 15$

2) $21 = 1 \cdot 15 + 6$

3) $15 = 2 \cdot 6 + 3$

4) $6 = 2 \cdot 3 + \underline{\underline{0}}$ Halt!

$$
\begin{aligned}
3 &\overset{(3)}{=} 15 - 2 \cdot 6 \\
&\overset{(2)}{=} 15 - 2 \cdot (21 - 1 \cdot 15) \\
&= -2 \cdot 21 + 3 \cdot 15 \\
&\overset{(1)}{=} -2 \cdot 21 + 3 \cdot (36 - 1 \cdot 21) \\
&= 3 \cdot 36 - 5 \cdot 21
\end{aligned}
$$

This gives an integer solution

$$
\begin{cases} x = 3 \\ y = -5 \end{cases}.
$$

Situation $ax + by = R$,

where a, b are positive integers, and

R is the last non-zero remainder

in the Euclidean Algorithm for (a, b).

We are able to find an integer solution under this situation.

a set of numbers

Terminology: An S-linear combination of a and b is an expression

$$s \cdot a + t \cdot b \quad (s, t \in S)$$

We say R can be written as an S-linear combination of a and b if there are $s, t \in S$ such that $s \cdot a + t \cdot b = R$.

Proof. Carry out the Euclidean Algorithm as follows:

$$
\begin{array}{lll|l}
0) & a = q_0 \cdot b + r_1 & \Rightarrow & r_1 \text{ is a } \mathbb{Z}\text{-linear combination of } a \,\&\, b \\
1) & b = q_1 \cdot r_1 + r_2 & \Rightarrow & r_2 \text{ is a } \mathbb{Z}\text{-linear combination of } b \,\&\, r_1 \\
 & \cdots \quad \cdots & & \cdots \quad \cdots \\
t) & r_{t-1} = q_t \cdot r_t + R & \Rightarrow & R \text{ is a } \mathbb{Z}\text{-linear combination of } r_{t-1} \,\&\, r_t \\
 & r_t = q_{t+1} R + \underline{0}. & &
\end{array}
$$

Applying the following lemma to , then we prove that R is a $\mathbb{Z}$-linear combination of a & b by induction. $\boxtimes$

Lemma: If α is a $\mathbb{Z}$-linear combination of a & b,
β is a $\mathbb{Z}$-linear combination of b & α,
then β is a $\mathbb{Z}$-linear combination of a & b.

Summarize so far:

We can use Euclidean Algorithm to find any integer solution of

$$ax + by = R,$$

where a, b are positive integers, and

R is the last non-zero remainder

in the Euclidean Algorithm for (a, b).

Extensions:

1) Negative a or b

E.g. $a > 0$ & $b < 0$

If x_0 & y_0 form an integer solution of $|a|x + |b|y = R$,

then x_0 & $-y_0$ form an integer solution of $ax + by = R$.

2) Replace R by a multiple c of it.

E.g. $c = m \cdot R$

If x_0 & y_0 form an integer solution of $ax + by = R$,

then $m \cdot x_0$ & $m \cdot y_0$ form an integer solution of $ax + by = c$.

Ex: What if one of a & b is zero?

General Questions $\qquad ax + by = c$

Q1: Is there any INTEGER solution? ✓p

Q2: If there is, find ONE such a solution. ✓p

Q3: Find ALL integer solutions.

Def. Let a and b be two integers.

The greatest common divisor of a and b is a natural number $g \in \mathbb{N}$ satisfying the following properties:

i) g is a common divisor of a and b, i.e. $g \mid a$ & $g \mid b$

ii) If d is a common divisor of a and b, then $d \mid g$

Notation: $GCD(a, b)$.

Rmk The properties i) & ii) together are called the defining property or the universal property of the notion "the greatest common divisor of a and b".

Prop (uniqueness of GCD)

There is at most ONE natural number $g \in \mathbb{N}$ satisfying i) & ii).

Proof: Suppose g_1 & g_2 are GCD of a and b.

By i), we have $g_1 | a$, $g_1 | b$, $g_2 | a$, $g_2 | b$

By ii), we have $g_1 | g_2$ and $g_2 | g_1$.

By ~~reflexive~~ property of $|$, $g_1 = g_2$.

antisymmetric

$\boxtimes$

Prop: Let a & b be positive integers, say $a \geq b$. Carry out the Euclidean Algorithm for (a, b). Then the last non-zero remainder is $GCD(a, b)$.

Pf:

0) $a = q_0 \cdot b + r_1$

1) $b = q_1 \cdot r_1 + r_2$

$\cdots \qquad \cdots$

t) $r_{t-1} = q_t \cdot r_t + R$

$r_t = q_{t+1} R + 0$.

To show R satisfies i) & ii)

i) $R \mid a$, $R \mid b$

$R \mid r_t$

By t) & 2-out-of-3,

$R \mid r_{t-1}$

In general,

if $R \mid r_i$, r_{i+1}, then by $r_{i-1} = q_i \cdot r_i + r_{i+1}$ & 2-out-of-3

we have $R \mid r_{i-1}$

ii) If $d \mid a$ & $d \mid b$, then $d \mid R$.

By $a = q_0 \cdot b + r_1$ & 2-out-of-3, $d \mid r_1$.

In general,

if $R \mid r_{i-1}, r_i$, then by $r_{i-1} = q_i \cdot r_i + r_{i+1}$ & 2-out-of-3

we have $d \mid r_{i+1}$

In particular, $d \mid R$.

Pf the uniqueness. $GCD(a, b) = R$.

Ex: How to compute $GCD(a, b)$

when $a, b \in \mathbb{Z}$.

Theorem.

Let a, b & c be integers. The equation $ax + by = c$ has an integer solution iff c is a multiple of $GCD(a, b)$

Pf: If case follows from Euclidean Algorithm.

Only If case:

Assume $\cancel{GCD(a, b) \nmid c \text{ and}}$ (x_0, y_0) is an integer solution of $ax + by = c$.

Then $a x_0 + b y_0 = c$.

Since $GCD(a, b) \mid a, b$, by 2-out-of-3,

$GCD(a, b) \mid c$.

General Questions

$$ax + by = c$$

Q1: Is there any INTEGER solution?

Q2: If there is, find ONE such a solution.

Q3: Find ALL integer solutions.

Some after-class reading suggestions:

- Today's topic are the GCD and the solvability of the linear Diophantine equation $ax + by = c$. Refer pp. 30–33 in the textbook.
- I encourage you to read the rest of Chapter 1 preparing for our next meeting.