Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 11, 2023

Today's topics

- (Euclidean) Division Algorithm
- (Binary) linear Diophantine equation
- Greatest common divisor

(Euclidean) Division Algorithm

Now, we apply the (Euclidean) Division Algorithm to our example. (133, 85)

$$133 = (1)\cdot 85 + 48$$

$$85 = (1)\cdot 48 + 37$$

$$48 = (1)\cdot 37 + 11$$

$$37 = (3)\cdot 11 + 4$$

$$11 = (2)\cdot 4 + 3$$

$$4 = (1)\cdot 3 + 1$$

$$3 = (3)\cdot 1 + 0$$

$$\begin{aligned}
1 &= 4 + (-1)\cdot 3 \\
&= 4 + (-1)\cdot (11 - 2\cdot 4) \\
&= (-1)\cdot 11 + (3)\cdot 4 \\
&= (-1)\cdot 11 + (3)\cdot (37 - 3\cdot 11) \\
&= (3)\cdot 37 + (-10)\cdot 11 \\
&= (3)\cdot 37 + (-10)\cdot (48 - 1\cdot 37) \\
&= (-10)\cdot 48 + (13)\cdot 37 \\
&= (-10)\cdot 48 + (13)\cdot (85 - 1\cdot 48) \\
&= (13)\cdot 85 + (-23)\cdot 48 \\
&= (13)\cdot 85 + (-23)\cdot (133 - 1\cdot 85) \\
&= \underbrace{(-23)\cdot 133 + (36)\cdot 85}_{\text{a } \mathbb{Z}\text{-linear combination of 133 \& 85}}
\end{aligned}$$

Linear Diophantine equation

Linear Diophantine equation

two unknowns

Question (Binary linear Diophantine equation)

Given integers a, b, c, find integers x, y such that

$$a \cdot x + b \cdot y = c.$$

When c is the output of the division algorithm of (a, b), then we can use the (Euclidean) division algorithm to find a solution (x_0, y_0).

Some observations

$$a x_0 + b y_0 = c$$

1. By the ***2-out-of-3 principle*** of divisibility of integers, if the problem has a solution (x_0, y_0), then for any common divisor d of a and b, we must have $d \mid c$. has solution $\Rightarrow \forall d, \therefore d \mid c$
   Conversely, if c is not a multiple of common divisors of a and b, then the problem has no solution. $d \nmid c \Rightarrow$ has no solution!

2. If we can find a solution (x_0, y_0) to the Diophantine equation

$$a \cdot x + b \cdot y = c.$$

Then for any integer z, (zx_0, zy_0) is a solution of the Diophantine equation

$$a \cdot x + b \cdot y = zc.$$

$$a z x_0 + b z y_0 = zc$$

e.g.

$133x + 85y = 1$

$-23 \quad 36$

$133x + 85y = 5$

also has a solution:

$-23 \cdot 5 \quad 36 \cdot 5$

$-115 \quad 180$

Q: What is the positive integer s.t.

① It is a mutiple of common divisors of a & b

② It is as small as possible.

Greatest common divisor

e.g. a b

12, 30

common divisors are

1, 2, 3, 6

2 is a multiple of 1 & 2

and is as small as possible

A: the largest common divisor.

Q: Is this largest common divisor a multiple of other common divisors?

Greatest common divisor

Definition 2.1 (Greatest common divisor)

Let a, b be two integers (not all zero). Then a positive integer g is called a ***greatest common divisor*** of a and b if it satisfies the following two ***defining properties***:

1. $g \mid a$ and $g \mid b$, i.e. g is a common divisor of a and b; and
2. if d is any common divisor of a and b, then $d \mid g$.

$g' \mid g,\ g \mid g' \Rightarrow g' = g$

For a given pair (a, b), the greatest common divisor is unique, we use $\gcd(a, b)$ to denote it. In particular, we use $\gcd(a, b) = g$ to mean the greatest common divisor exists and equals to g.

Rmk: By 1 & 2, $\gcd(a,b)$ is the largest common divisor of a and b.

(Euclidean) division algorithm and greatest common divisor

Theorem 2.2

Let a, b be two positive integers. The output (namely, the last non-zero remainder r) of the (Euclidean) division algorithm of (a, b) is a greatest common divisor of a and b.

In particular, since the (Euclidean) division algorithm always halts in finite steps, the greatest common divisor of any pairs of positive integers always exists.

Theorem 2.2

Let a, b be two positive integers. The output (namely, the last non-zero remainder r) of the (Euclidean) division algorithm of (a, b) is a greatest common divisor of a and b.

If we combine this theorem with our observations before, we see that: the Diophantine equation

$$a \cdot x + b \cdot y = c$$

has a solution (in $\mathbb{Z}$) if and only if c is a multiple of $\gcd(a, b)$.

Proof of the theorem

Let's start with a lemma.

Lemma 2.3

Let a, b be two positive integers. If there are integers q and r such that $a = qb + r$, then we have

$(r>0)$

$$\gcd(a, b) = g \iff \gcd(b, r) = g.$$

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

Lemma 2.3

Let a, b be two positive integers. If there are integers q and r such that $a = qb + r$, then we have

$$\gcd(a, b) = g \iff \gcd(b, r) = g.$$

Proof. ($\Rightarrow$) Suppose $\gcd(a, b) = g$, let's prove $\gcd(b, r) = g$ by verifying the two defining properties.

1. Since $\gcd(a, b) = g$, we have $g \mid a$ and $g \mid b$. Since $\underbrace{a}_{g} = \underbrace{qb}_{g} + \underline{r}$, by the 2-out-of-3 principle, we have $g \mid r$.
2. Let $d \mid b$ and $d \mid r$. Since $\underline{a} = \underbrace{qb}_{d} + \underbrace{r}_{d}$, by the 2-out-of-3 principle, we have $d \mid a$. Since $\gcd(a, b) = g$, we have $d \mid g$.

A very similar argument gives you ($\Leftarrow$). $\square$

Proof of the theorem

Let's assume $a \geqslant b$. The division algorithm gives us the following

$$\begin{aligned}
a &= q_1 b + r_1 && \text{(Step 1)}\\
b &= q_2 r_1 + r_2 && \text{(Step 2)}\\
&\vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r && \text{(Step } n-1\text{)}\\
r_{n-2} &= q_n r + 0 && \text{(Step } n\text{)}
\end{aligned}$$

↳ outputs

WTS: gcd(a,b) = r

Our lemma 2.3 tells us that

$$\begin{aligned}
\gcd(a, b) &= \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots \\
&= \gcd(r_{n-3}, r_{n-2}) = \gcd(r_{n-2}, r) = \underbrace{\gcd(r, 0)}_{\gcd(r,0) \text{ exists } \& = r} = r. \qquad \square
\end{aligned}$$

- - -

gcd(r_{n-2}, r) exists & = gcd(r, 0)

(Euclidean) division algorithm, backward

Note that, if we work the division algorithm backward, we have

$$
\begin{aligned}
r &= r_{n-3} + (-q_{n-1}) \cdot r_{n-2} \\
&= r_{n-3} + (-q_{n-1}) \cdot (r_{n-4} - q_{n-2} r_{n-3}) && \text{substitute in } r_{n-2} \\
&= (\cdots) \cdot r_{n-4} + (\cdots) \cdot r_{n-3} && \text{collect the coefficients} \\
&\ \ \vdots \\
&= x_0 \cdot a + y_0 \cdot b.
\end{aligned}
$$

Hence, the division algorithm gives us a solution (x_0, y_0) of the Diophantine equation $a \cdot x + b \cdot y = \gcd(a, b)$.

Theorem 2.4 (Bézout's identity)

Given non-zero integers a, b, there exist integers x_0, y_0 such that

$$a \cdot x_0 + b \cdot y_0 = \gcd(a, b).$$

Bézout's identity

Theorem 2.4 (Bézout's identity)

Given non-zero integers a, b, there exist integers x_0, y_0 such that

$$a \cdot x_0 + b \cdot y_0 = \gcd(a, b).$$

Proof. When a, b are both positive, the integers x_0, y_0 are obtained by working the division algorithm backward.

In general, we solve this problem for the positive integers $|a|, |b|$, producing integers x_0, y_0, then we have

$$a \cdot (\underline{\operatorname{sign}(a)x_0}) + b \cdot (\underline{\operatorname{sign}(b)y_0}) = \gcd(a, b),$$

where $\operatorname{sign}(\,\cdot\,)$ eats an integer and gives its signature, is a solution for our Diophantine equation. □

Summarizing

Summarizing

- Let a, b be two nonzero integers. The Diophantine equation

$$a \cdot x + b \cdot y = c$$

has a solution (in $\mathbb{Z}$) if and only if c is a multiple of $\gcd(a, b)$.

- If this is the case, the ***Bézout's identity*** gives a pair of integers (x_0, y_0) such that $ax_0 + by_0 = \gcd(a, b)$. Suppose $c = m \gcd(a, b)$. Then (mx_0, my_0) is a solution of our Diophantine equation.
- It remains to study what are ***all*** the solutions. Namely, to study the ***solution set***

$$\{(x, y) \in \mathbb{Z}^2 \mid a \cdot x + b \cdot y = c\}.$$

After Class Work

Terminology

Terminology

- ***Diophantine equation*** = equations in multiple unknowns and the interesting solutions are in a given set of numbers (e.g $\mathbb{Z}$).
- ***Linear*** = the expression only contains linear combinations of unknowns. Namely, no higher terms, no strange functions.

Example 2.5

- $x^2 + y^2 = 1$ is Diophantine equation but not a linear one.
- $18x - 27y + 39z = 4$ is a linear Diophantine equation with three unknowns.

Terminology

Given some objects $X, Y, \cdots, Z$, a ***linear combination*** of them is an ***expression*** of the form

$$aX + bY + \cdots + cZ,$$

where $a, b, \cdots, c$ are called the ***coefficients***. If all the coefficients are contained in a set S, then we say it is an S-***linear combination***.

Sometimes, we also call $Xa + Yb + \cdots + Zc$ a ***linear combination*** of the objects $X, Y, \cdots, Z$. The two definitions are equivalent as long as we are free to interchange the coefficient a and the object X.

Example 2.6

- X is a linear combination of X itself, while X^2 is not.
- $\frac{1}{2}X$ is not a $\mathbb{Z}$-linear combination of X since $\frac{1}{2}$ is not an integer.
- $(+2) \cdot 133 + (-3) \cdot 85$ is a $\mathbb{Z}$-linear combination of 133 and 85.
  The equation $(+2) \cdot 133 + (-3) \cdot 85 = 11$ should be read as the ***value*** of the linear combination $(+2) \cdot 133 + (-3) \cdot 85$ is 11, or the integer 11 ***can be expressed*** as the linear combination $(+2) \cdot 133 + (-3) \cdot 85$.
  It ***shouldn't*** read as "11 ***is*** the linear combination $(+2) \cdot 133 + (-3) \cdot 85$".

Remark. Distinguish an expression and a value.

Notations

When elements of a set are obtained as outputs of operations, we often use a shorthand notations to denote this set.

Example 2.7

- Let A, B be two sets. Then $A + B$ denotes the set of elements $a + b$, where $a \in A$, $b \in B$. Similarly, $AB := \{ab \mid a \in A, b \in b\}$.
- Let A be a set and x be an object (e.g. a number, an unknown, etc.). Then $A + x := \{a + x \mid a \in A\}$. Similarly, $Ax := \{ax \mid a \in A\}$.
- Given objects $x, y, \cdots, z$ and a set S, what does the notation $Sx + Sy + \cdots + Sz$ mean?

Exercise 2.1

Let a, b be two integers. Show that

1. $\gcd(a, b) = \gcd(|a|, |b|)$;
2. $\gcd(a, 0) = |a|$;
3. if $a \mid b$, then $\gcd(a, b) = |a|$;

Exercise 2.2 (substitution of $\mathbb{Z}$-linear combinations)

If an integer n can be expressed as a $\mathbb{Z}$-linear combination of the integers a and b, while the integer b can be expressed as a $\mathbb{Z}$-linear combination of the integers c and d, then n can be expressed as a $\mathbb{Z}$-linear combination of the integers a, c, and d.