MATH6222 week 6 lecture 16

Rui Qiu

2017-03-30

Given integers a, b, c, claim

$$ax + by = c$$

has a solution in integers if and only if $\gcd(a, b)|c$.

Proof:

($\Rightarrow$) Suppose $ax + by = c$ has a solution in integers, i.e. $\exists\ m, n \in \mathbb{Z}$ such that $am + bn = c$.

By definition, $\gcd(a, b)|a$ and $\gcd(a, b)|b$.

By properties of divisibility, $\gcd(a, b)|am + bn \implies \gcd(a, b)|c$, we are done.

($\Leftarrow$) Suppose $\gcd(a, b)|c$, then I must show $\exists\ m, n \in \mathbb{Z}$ such that $am + bn = c$.

First, suppose we already have mn, n such that $am + bn = \gcd(a, b)$.

Then I can get any other multiple of $\gcd(a, b)$ as follows:

If $c = k \gcd(a, b)$,

Let $m' = km, n' = kn$, then $am' + bn' = k(am + bn) = k \gcd(a, b)$.

Division Algorithm: Given integers $a > b$, there exists unique integers k, r such that

$$a = kb + r, 0 \leq r < b$$

Euclidean Algorithm: Given a, b, want output as $\gcd(a, b), m, n$ such that $am + bn = \gcd(a, b)$.

Set $a_1 := a, b_1 := b$. Use division to find k_1, r_1, such that

$$a_1 = k_1 b_1 + r_1, (0 \leq r_1 < b_1)$$

Now set $a_2 := b_1, b_2 := r_1$. Find k_2, r_2, such that

$$a_2 = k_2 b_2 + r_2, (0 \le r_2 < b_2)$$

Set $a_3 := b_2, b_3 := r_2$

$\cdots$

Eventually,

$$a_n = k_n b_n$$

Claim: when reminder is gone, we stop, and $\gcd(a, b) = b_n = r_{n-1}$.

Example: $a_1 = 343, b_1 = 154$

$$\begin{aligned} 343 &= 2 \times 154 + 35 \\ 154 &= 4 \times 35 + 14 \\ 35 &= 2 \times 14 + 7 \\ 14 &= 2 \times 7 \end{aligned}$$

So $\gcd(343, 154) = 7$.

Observe $\gcd(a_n, b_n) = b_n$. So it's enough to show $\gcd(a_i, b_i) = \gcd(a_{i+1}, b_{i+1})$, for each $i = 1, \ldots, n-1$. ($\Rightarrow \gcd(a_1, b_1) = \gcd(a_2, b_2) = \cdots = \gcd(a_n, b_n) = b_n$).

$$a_i = k_i b_i + r_i = k_i a_{i+1} + b_{i+1}$$

We are gonna prove $\gcd(a_i, b_i) \le \gcd(a_{i+1}, b_{i+1})$ and backward $\gcd(a_{i+1}, b_{i+1}) \ge \gcd(a_i, b_i)$.

- $\gcd(a_i, b_i) | r_i = b_{i+1}$, also $\gcd(a_i, b_i) | a_{i+1} = b_i$, therefore $\gcd(a_i, b_i) \le \gcd(a_{i+1}, b_{i+1})$
- $\gcd(a_{i+1}, b_{i+1}) | a_i$, also $\gcd(a_{i+1}, b_{i+1}) | b_i = a_{i+1}$, therefore $\gcd(a_{i+1}, b_{i+1}) \ge \gcd(a_i, b_i)$

Done.

Back to the example:

$$\begin{aligned} 35 &= 343 - 2 \times 154 \\ 14 &= 154 - 4 \times 35 \\ 7 &= 35 - 2 \times 14 \\ &= 9 \times 343 - 20 \times 154 \end{aligned}$$

1. Why is Number Theory hard? $\mathbb{Z}$ is not a "field" (cannot divide)
2. Think how fast this algorithm.