November 08, 2020

Algebra.

Recap: Elements of number theory. Euclid's algorithm and greatest common divisor.

All numbers used in this section are integers (possibly negative).

Theorem 1 (division representation).

Let a, b be integer numbers, with $b > 0$. Then a can be uniquely written in the form

$$a = bq + r, \quad q, r \in \mathbb{Z}, \qquad 0 \leq r < b$$

Note that we do not assume that a is positive.

Proof. Let us consider the smallest integer number m such that $a < mb$. Take $q = m - 1$; then $qb \leq a < (q + 1)b$, so if we define $r = a - qb$, then $0 \leq r < b$. This proves existence; uniqueness is left as an exercise.

The number r in that theorem is called **remainder** upon division of a by b.

Note: we didn't justify why such m exists, as it seems obvious. For those who want to insist on absolute mathematical rigor, we note that this can be justified using induction (in a).

Definition. A number $d \in \mathbb{Z}$ is a **divisor** (or a factor) of an integer a if $a = qd$ for some integer q. In this situation we also say that a is divisible by d and write $d|a$. (Note that both a and d could be negative.)

A number d is called a **common divisor** of integer numbers $a, b \in \mathbb{Z}$ if $d|a$ and $d|b$.

A set of all positive common divisors of the two numbers $a, b \in \mathbb{Z}$ is limited because these divisors can't be larger than the absolute value of the smaller of the two numbers. The greatest of the divisors, d, is called the **greatest common divisor** (gcd) and denoted $d = (a, b)$.

Definition. Two integers $a, b \in \mathbb{Z}$, are called **relatively prime** if they have no common divisors larger than 1, i. e. $(a, b) = 1$.

Theorem 2. Let a, b be integer numbers, and let r be the remainder upon division of a by b: $a = bq + r$. Then

$$(a, b) = (b, r).$$

Proof. Indeed, if d is a common divisor of $a, b \in \mathbb{Z}$, then $a = nd, b = md$ for some integers m, n. Therefore, $r = a - bq = nd - qmd = d(n - qm)$, so r is divisible by d; therefore, d is a common divisor of b, r.

Conversely, if d' is a common divisor of b and $r = a - bq$, then similar argument shows that d' is a common divisor of b and a.

Hence, set of common divisors of pair a, b is the same as set of common divisors of pair b, r. In particular, it shows that both pairs have the same gcd.

Corollary 1 (Euclid's algorithm). In order to find the greatest common divisor $d = (a, b)$, one proceeds iteratively performing successive divisions,

$$a = bq + r, (a, b) = (b, r)$$

$$b = rq_1 + r_1, (b, r) = (r, r_1),$$

$$r = r_1 q_2 + r_2, (r, r_1) = (r_1, r_2),$$

$$r_1 = r_2 q_3 + r_3, (r_1, r_2) = (r_2, r_3), \dots, r_{n-1} = r_n q_{n+1}$$

$$b > r_1 > r_2 > r_3 > \cdots r_n > 0 \Rightarrow \exists d \leq b, d = r_n = (a, b)$$

The last positive remainder, r_n, in the sequence $\{r_k\}$ is (a, b), the gcd of the numbers a and b. Indeed, the Eucleadean algorithm ensures that

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n = d$$

Examples.

a. $(385,105) = (105,70) = (70,35) = (35,0) = 35$
b. $(513,304) = (304,209) = (209,95) = (95,19) = (19,0) = 19$

Corollary 2 (Extended Euclid's algorithm).

Let a, b be integer numbers. Then a number n can be written in the form

$$n = xa + yb, x, y \in \mathbb{Z}$$

if and only if n is divisible by $d = (a, b)$.

Example. An integer number n can be written in the form $n = 9x + 21y$ if and only if n is a multiple of 3.

Proof. One direction is obvious: if $n = xa + yb$, and both a, b are divisible by d, then clearly n is also divisible by d.

To prove the opposite direction, it is enough to show that $d = (a, b)$ can be written as a combination of a, b.

To do that, recall Euclid's algorithm:

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n = d$$

Since $b = 0 * a + 1 * b,\ r_1 = a - q_1 b$, we see that both b, r_1 can be written as combination of a, b. But then $r_2 = b - q_2 r_1 = b - (a - q_1 b) = -a + (q_1 + 1)b$ is also a combination of a, b. More generally, if we already know that $r_{k-1} = x_{k-1}a + y_{k-1}b, r_k = x_k a + y_k b$, then

$$\begin{aligned} r_{k+1} = r_{k-1} - q_k r_k &= x_{k-1}a + y_{k-1}b - q_k(x_k a + y_k b) \\ &= (x_{k-1} - q_k x_k)a + (y_{k-1} - q_k x_k)b \end{aligned}$$

so it is again written as a combination of a, b. Thus, by induction, all r_i are linear combinations of a, b – including the last nonzero remainder, $d = (a, b)$.

Exercise. Find the representation $d = xa + yb$ for the pairs (385,105) and (513,304) considered in the above examples.

Continued fractions

A continued fraction is a presentation of a rational number in the form below:

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}}$$

To find such a representation, let us do repeated division with remainder:

$a = bq + r$, so $\frac{a}{b} = q + \frac{r}{b} = q + \frac{1}{b/r}$

Now repeat the same for $\frac{b}{r}$, and so on:

$\frac{b}{r} = q_1 + \frac{r_1}{r} = q_1 + \frac{1}{\frac{r}{r_1}}, \frac{r}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}, \ldots, \frac{r_{n-1}}{r_n} = q_{n+1}.$

You might notice that this is the same process as in the Euclid's algorithm: we get the next remainder r_{k+1} as the remainder upon division of r_{k-1} by r_k. (The main difference is that in Euclid's algorithm we discarded the quotients q_k, and here we use them.)

Exercise. Find the continued fraction representations for $\frac{385}{105}, \frac{513}{304}, \frac{105}{385}, \frac{304}{513}$.

Example. $\frac{105}{385} = \frac{1}{\frac{385}{105}} = \frac{1}{3+\frac{1}{\frac{105}{70}}} = \frac{1}{3+\frac{1}{1+\frac{1}{\frac{70}{35}}}} = \frac{1}{3+\frac{1}{1+\frac{1}{2}}}$.

You could even try finding continued fractions representation for irrational numbers, e.g.

$$\pi = 3 + 0.14115926\ldots = 3 + \frac{1}{7.062516\ldots} = 3 + \frac{1}{7 + 0.062516\ldots}$$
$$= 3 + \frac{1}{7 + \frac{1}{15.996\ldots}}$$

In this case, the sequence of quotients never ends, so we get an infinite expression. However, we can terminate at any moment to get an approximate value: for example,

$$\pi \approx 3 + \frac{1}{7} = \frac{22}{7}$$

It can be shown that these successive approximations get closer and closer to the actual number (to do it properly, you need to introduce the notion of limit). It can also be shown that the approximations obtained in this way are in some sense optimal: for example, $\frac{22}{7}$ is the best possible approximation to π among all fractions with denominator ≤ 7.