Numbers Made Dumber

Rohan Baijal
Vivek Kumar Singh
Yatharth Goswami

Week 1

05-04-2021

1.1 Natural Numbers and Integers

1.1.1 Natural Numbers

Definition 1. *The natural numbers are* $\mathbb{N} = \{1,\ 2,\ 3,\ \dots\ \}$.

Definition 2. *We say a divides n (or a is a divisor of n), and write* $a|n$*, if* $n = ab$*, where n, a, b are natural numbers.*

Ex 1.1. U sing the definition, prove that if $a|b$ and $b|c$, then $a|c$ (transitivity).

Definition 3. *A natural number p is prime if it has only 2 divisors: 1 and p*

1.1.2 Integers

Definition 4. *The integers are* $\mathbb{Z} = \{..., 3, 2, 1, 0, 1, 2, 3, ...\}$. *The fact that you can do subtraction lends more structure to* $\mathbb{Z}$ *over* $\mathbb{N}$.

1.1.3 Binary Notation

Definition 5. *Repeated division of* $n \in N$ *by* $b \in N$ *leads naturally to the b-ary representation of n.*
In general the b-ary representation of n is $a_k a_{k-1} \cdots a_1 a_0$ *if* $n = a_k b^k + a_{k1} b^{k1} + \cdots + a_1 b + a_0$ *where* $0 \leq b$. $It\ is\ well-defined\ and\ unique\ for\ n \geq 0$.

1.2 Divisors

Our starting-point is the *division* algorithm, which is as follows:

Theorem 1.2.1. *If a and b are integers with* $b > 0$*, then there is a unique pair of integers q and r such that*

$$a = qb + r \text{ and } 0 \leq r < b.$$

In Theorem 1, we call q the quotient and r the remainder. By dividing by b, so that

$$\frac{a}{b} = q + \frac{r}{b} \text{ and } 0 \leq \frac{r}{b} < 1$$

we see that q is the integer part of $\frac{a}{b}$. This makes it easy to calculate q, and then to find $r = a - qb$.

Proof. First we prove existence. Let

$$S = \{a - nb \mid n \in \mathbb{Z}\} = \{a, a \pm b, a \pm 2b, \dots\}.$$

This set of integers contains non-negative elements (take $n = -|a|$), so $S \cap \mathbb{N}$ is a non-empty subset of $\mathbb{N}$; by the well-ordering principle $S \cap \mathbb{N}$ has a least element, which has the form $r = a - qb \ \geq\ 0$ for some integer q. Thus $a = qb + r$ with $r \geq 0$. If $r \geq b$ then S contains a non-negative element $a - (q+1)b = r - b \ <\ r$; this contradicts the minimality of r, so we must have $r < b$.

We can now deal with the case $b < 0$: since $-b > 0$, Theorem 1 implies that there exist integers $q*$ and r such that $a = q^*(-b)+r$ and $0 \leq r < -b$, so putting $q = -q*$ we again have $a = qb+r$. Uniqueness is proved as before, so combining this with Theorem 1 we have:

Corollary 1.2.1.1. *If a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that*

$$a = qb + r \text{ and } 0 \leq r < |b|.$$

(Note that when $b < 0$ we have

$$\frac{a}{b} = q + \frac{r}{b} \text{ and } 0 \geq \frac{r}{b} > -1$$

so that in this case q is $\lceil \frac{a}{b} \rceil$, the least integer $i \geq a/b$.)

□

Definition 6. *If a and b are any integers, and $a = qb$ for some integer q, then we say that b divides a, or b is a factor of a, or a is a multiple of b. For instance, the factors of 6 are $\pm1, \pm2, \pm3$ and ±6. When b divides a we write $b|a$, and we use the notation $b \nmid a$ when b does not divide a. To avoid common misconceptions, we note that every integer divides 0 (since $0 = 0.b$ for all b), 1 divides every integer, and every integer divides itself.*

Corollary 1.2.1.2.

1. *$a|b$ and $b|a$ iff $a = \pm b$.*
2. *If c divides $a_1 \ldots, a_k$, then c divides $a_1u_1 \ldots, a_ku_k$ for all integers $u_1 \ldots u_k$.*

If $d|a$ and $d|b$ we say that d is a common divisor (or common factor) of a and b; for instance, 1 is a common divisor of any pair of integers a and b.The greatest common divisor (or highest common factor) of a and b is the unique integer d satisfying

1. $d|a$ and $d|b$ (d is a common divisor),
2. if $c|a$ and $c|b$ then $c \leq d$ (no common divisor exceeds d).

However, the case $a = b = 0$ has to be excluded: every integer divides 0 and is therefore a common divisor of a and b, so there is no greatest common divisor in this case. When it exists, we denote the greatest common divisor of a and b by $gcd(a, b)$, or simply (a, b). This definition extends in the obvious way to the greatest common divisor of any set of integers (not all 0).

Lemma 1.2.2. *If $a = qb + r$ then $gcd(a, b) = gcd(b, r)$.*

Proof. Any common divisor of b and r also divides $qb + r = a$; similarly, since $r = a - qb$, it follows that any common divisor of a and b also divides r. Thus the two pairs a, b and b, r have the same common divisors, so they have the same greatest common divisor. □

We now use the division algorithm (Theorem 1.2.1) to divide b into a, and write

$$a = q_1b + r_1 \text{ and } 0 \leq r_1 < b.$$

If $r1 = 0$ then $b|a$, so $d = b$ and we halt. If $r_1 \neq 0$ then we divide r_1 into b and write

$$b = q_2r_1 + r_2 \text{ and } 0 \leq r_2 < r_1.$$

Now Lemma 1.2.2 gives $gcd(a, b) = gcd(b, r_1)$, so if $r_2 = 0$ then $d = r_1$ and we halt. If $r_2 \neq 0$ we write

$$r_1 = q_3r_2 + r_3 \text{ and } 0 \leq r_3 < r_2.$$

and we continue in this way; since $b > r_1 > r_2 > ... \geq 0$, we must eventually get a remainder $r_n = 0$ (after at most b steps) at which point we stop. The last two steps will have the form

$$r_{n-3} = q_{n-1}r_{n-2} + r_{n-1} \text{ and } 0 \leq r_{n-1} < r_{n-2},$$

$$r_{n-2} = q_{n-1}r_{n-1} + r_n \text{ with } r_n = 0.$$

Theorem 1.2.3. *In the above calculation we have $d = r_{n-1}$ (the last non-zero remainder).*

Proof. By applying Lemma 1.2.2 to the successive equations for $a, b, r_1...., r_{n-3}$ we see that

$$d = gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{n-2}, r_{n-1}).$$

The last equation $r_{n-2} = q_n r_{n-1}$ shows that $r_{n-1}|r_{n-2}$, so $gcd(r_{n-2}, r_{n-1}) = r_{n-1}$ and hence $d = r_{n-1}$. □

1.3 Bezout's Identity

The following result uses Euclid's algorithm to give a simple expression for $d = gcd(a, b)$ in terms of a and b:

Theorem 1.3.1. *If a and b are integers (not both 0), then there exist integers u and v such that*

$$gcd(a, b) = au + bv.$$

Proof. We use the equations which arise when we apply Euclid's algorithm to calculate $d = gcd(a, b)$ as the last non-zero remainder r_{n-1}, The penultimate equation, in the form

$$r_{n-1} = r_{n-3} - q_{n-1}r_{n-2},$$

expresses d as a multiple of r_{n-3} plus a multiple of r_{n-2}. We then use the previous equation, in the form

$$r_{n-2} = r_{n-4} - q_{n-2}r_{n-3},$$

to eliminate r_{n-2} and express d as a multiple of r_{n-4} plus a multiple of r_{n-3}. We gradually work backwards through the equations in the algorithm, eliminating $r_{n-3}, \ldots$ in succession, until eventually we have expressed d as a multiple of a plus a multiple of b, that is, $d = au + bv$ for some integers u and v. □

Theorem 1.3.1 states that $gcd(a, b)$ can be written as a multiple of a plus a multiple of b; using this we shall describe the set of all integers which can be written in this form.

Theorem 1.3.2. *Let a and b be integers (not both 0) with greatest common divisor d. Then an integer c has the form $ax + by$ for some $x, y \in \mathbb{Z}$ if and only if c is a multiple of d. In particular, d is the least positive integer of the form $ax + by$ $(x, y \in \mathbb{Z})$.*

Proof. If $c = ax + by$ where $x, y \in \mathbb{Z}$, then since d divides a and b, implies that d divides c. Conversely, if $c = de$ for some integer e, then by writing $d = au + bv$ (as in Theorem 1.3.1) we get $c = aue + bve = ax + by$, where $x = ue$ and $y = ve$ are both integers. Thus the integers of the form $ax + by(x, y \in \mathbb{Z})$ are the multiples of d, and the least positive integer of this form is the least positive multiple of d, namely d itself. □

Two integers a and b are coprime (or relatively prime) if $gcd(a, b) = 1$. For example, 10 and 21 are coprime, but 10 and 12 are not. More generally, a set $a_1, a_2, \ldots$ of integers are coprime if $gcd(a_1, a_2, \ldots) = 1$, and they are mutually coprime if $gcd(a_i, a_j) = 1$ whenever $i \neq j$. If they are mutually coprime then they are coprime (since $gcd(a_1, a_2, ...)|gcd(a_i, a_j)$), but the converse is false: the integers 6, 10 and 15 are coprime but are not mutually coprime.

Corollary 1.3.2.1. *Two integers a and b are coprime if and only if there exist integers x and y such that*

$$ax + by = 1$$

Corollary 1.3.2.2. *If $gcd(a, b) = d$ then*

$$gcd(ma, mb) = md$$

for every integer $m > 0$ and

$$gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Corollary 1.3.2.3. *Let a and b be coprime integers.*

1. *If $a|c$ and $b|c$ then $ab|c$*
2. *If $a|bc$ then $a|c$.*

Proof.

1. We have $ax + by = 1$, $c = ae$ and $c = bf$ for some integers x, y, e *and* f Then $c = cax + cby = (bf)ax + (ae)by = ab(fx + ey)$, so $ab|c$.
2. As in (1), $c = cax + cby$. Since $a|bc$ and $a|a$, it implies that $a|(cax + cby) = c$.

□

1.4 Least common multiples

If a and b are integers, then a common multiple of a and b is an integer l satistfying

1. $a|l$ and $b|l$ (so l is a common multiple), and
2. if $a|c$ and $b|c$, with $c > 0$, then $l \leq c$ (so no positive common multiple is less than l).

We usually denote l by $lcm(a, b)$, or simply $[a, b]$.

Theorem 1.4.1. *Let a and b be positive integers, with $d = gcd(a, b)$ and $l = lcm(a, b)$. Then*

$$dl = ab$$

(Since $gcd(a, b) = gcd(|a|, |b|)$ and $lcm(a, b) = lcm(|a|, |b|)$, it is no great restriction to assume $a, b > 0$.)

Proof. Let $e = \frac{a}{d}$ and $f = \dfrac{b}{d}$, and consider

$$\frac{ab}{d} = \frac{de \cdot df}{d} = def$$

Clearly this is positive, so we can show that it is equal to l by showing that it satisfies conditions (1) and (2) of the definition of $lcm(a, b)$. First,

$$def = (de)f = af \text{ and } def = (df)e = be;$$

thus $a|def$ and $b|def$, so (1) is satisfied. Second, suppose $a|c$ and $b|c$, with $c > 0$; we need to show that $def \leq c$. We know that there exists integers u and v such that $d = au + bv$. Now

$$\frac{c}{def} = \frac{cd}{de \cdot df} = \frac{cd}{ab} = \frac{c(au + bv)}{ab} = \left(\frac{c}{b}\right)u + \left(\frac{c}{a}\right)v$$

is an integer, since a and b are factors of c; thus $def|c$ and hence we have $def \leq c$, as required.

□

1.5 Linear Diophantine Equations

Theorem 1.5.1. *Let a, b and c be integers, with a and b not both 0, and let $d = gcd(a,b)$. Then the equation $ax + by = c$ has an integer solution x, y if and only if c is a multiple of d, in which case there are infinitely many solutions. These are the pairs*

$$x = x_0 + \frac{bn}{d}, y = y_0 - \frac{an}{d}(n \in \mathbb{Z})$$

where x_0, y_0 is any particular solution.

Proof. The fact that there is a solution if and only if $d|c$ is merely a restatement of Theorem(??). For the second part of the theorem, let x_0, y_0 be a particular solution, so

$$ax_0 + by_0 = c.$$

If we put

$$ax + by = a(x_0 + \frac{bn}{d}) + b(y_0 + \frac{an}{d}) = ax_o + by_o = c,$$

so x, y is also a solution. (Note that x and y are integers since d divides band a respectively.) This gives us infinitely many solutions, for different integers n. To show that these are the only solutions, let x, y be any integer solution, so $ax + by = c$. Since $ax + by = c = ax_0 + by_0$ we have

$$a(x - x_0) + b(y - y_0) = 0,$$

so dividing by d we get

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0).$$

Now a and b are not both 0, and we can suppose that $b \neq 0$ (if not, interchange the roles of a and b in what follows). Since b/d divides each side of above equation, and is coprime to a/d by Corollary (??), it divides $x - x_0$ by Corollary (??). Thus $x - x_0 = bn/d$ for some integer n, so

$$x = x_0 + \frac{bn}{d}.$$

Substituting back for $x - x_0$ we get

$$-\frac{b}{d}(y - y_0) = \frac{a}{d}(x - x_0) = \frac{a}{d}.\frac{bn}{d},$$

so dividing b/d (which is non-zero) we have

$$y = y_0 - \frac{an}{d}.$$

□