HOMEWORK - 0

SIDDHANT CHAUDHARY
BMC201953

Let a be a non-zero integer and let b be an integer. We carry out the following step by step development.

(i) Long Division. Carefully state the meaning of saying that we can do long division of b by a to get quotient q and remainder r. This is crucial to all that follows.

Solution: This means the following: given such integers a and b, there are integers q and r such that

$$b = aq + r$$

with $0 \leq r < |a|$. We want a to be non-zero, otherwise the condition on the size of the remainder won't make sense. This fact can be proven using the well-ordering principle on $\mathbb{Z}$.

(ii) Meaning of GCD. Define what it means for an integer d to be a *gcd* of a and b. Try to capture the notion of 'greatest' using only divisibility, not size. Defined this way, gcd(a, b) is *essentially* unique. Explain how.

Solution: Let a, b be two integers. We call an integer d a *greatest common divisor* of a and b if $d|a$ and $d|b$, and for every $k \in \mathbb{Z}$ such that $k|a$ and $k|b$, it is true that $k|d$. In simpler words, every common divisor of a and b also divides their greatest common divisor.

Now, we can show that given that a gcd of a, b exists, it is unique upto multiplication by units. In $\mathbb{Z}$, this reduces to the fact that the gcd of two numbers is unique upto sign. So suppose d_1 and d_2 are two candidates for gcd(a, b). So, this means that $d_1|a, b$ and $d_2|a, b$. But by our definition, this also means that $d_1|d_2$ and $d_2|d_1$. In $\mathbb{Z}$, this is possible if and only if $d_1 = \pm d_2$, and hence the gcd (if it exists) is unique upto sign.

(iii) Euclidean Algorithm. Use long division to prove existence of gcd(a, b) and to calculate it. Note that at this stage you do NOT know anything about primes, much less about prime factorization. See step **(vii)** below.

Solution: Suppose a, b are integers with $a \neq 0$ (the case when both integers are zero will be handled separately). So, by long division, there are integers q, r such that

$$b = aq + r$$

and $0 \leq r < |a|$. We show a key fact.

Lemma 0.1. *If a, b, q, r are as above, then*

$$\text{gcd}(a, b) = \text{gcd}(a, r)$$

provided atleast one of the above exists.

Date: September 2020.

Proof: Without loss of generality, suppose $d = \text{gcd}(a, b)$ exists. So, $d|a$ and $d|b$, and by the equation $r = b - aq$, it is clear that $d|r$. Now, suppose $k|a$ and $k|r$. Then, the equation $b = aq + r$ implies $k|b$, and hence we have that $k|d$. This shows that $d = \text{gcd}(a, r)$. On the other hand if we suppose that $\text{gcd}(a, r)$ exists, by similar arguments we can show that $\text{gcd}(a, b)$ is equal to $\text{gcd}(a, r)$. This completes the proof.

So, **Lemma** 0.1 shows that proving the existence of $\text{gcd}(a, b)$ is the same as proving the existence of $\text{gcd}(a, r)$. The benefit is that by going from (a, b) to (a, r), we have reduced the *size* of the argument.

So, consider the following chain of equations:

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\dots \\ r_n &= r_{n+1} q_{n+2} + r_{n+2} \end{aligned}$$

and we assume that $r_{n+2} = 0$. This assumption makes sense because for each i,

$$r_i > r_{i+1} \geq 0$$

because at each step, we are strictly reducing the size of the remainder. Now, we claim that r_{n+1}, which is the last non-zero remainder, is a gcd of a, b. To show this, observe that

$$\text{gcd}(r_n, r_{n+1}) = r_{n+1}$$

because $r_{n+1}|r_n$. Applying **Lemma** 0.1 repeatedly, we see that

$$r_{n+1} = \text{gcd}(r_{n+1}, r_n) = \text{gcd}(r_n, r_{n-1}) = \dots = \text{gcd}(r_1, a) = \text{gcd}(a, b)$$

and this is an algorithm to find the gcd of two numbers. This algorithm also proves the *existence* of a gcd, but the same can be also proven by using linear combinations.

Now, if both a and b are zero, then by definition, their gcd will be 0.

(iv) GCD as linear combination. Why can $\text{gcd}(a, b)$ be written in the form $xa + yb$ and how can we find such integers x and y? To what extent are x and y unique?

Solution: We claim that $\text{gcd}(a, b)$ can *always* be written as a $\mathbb{Z}$-linear combination of a, b, and we can show this using the algorithm described in **(iii).** We have the equations

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\dots \\ r_n &= r_{n+1} q_{n+2} \end{aligned}$$

and we showed that $r_{n+1} = \text{gcd}(a, b)$. Observe that

$$r_1 = b - aq_1$$

i.e r_1 is a $\mathbb{Z}$-linear combination of a, b. Inductively, suppose r_i is a linear comination of a, b for every $1 \leq i \leq k$ for some $k < n + 1$. Then, observe that

$$r_{k+1} = r_{k-1} - r_k q_{k+1}$$

and since both r_{k-1}, r_{k+1} are $\mathbb{Z}$-linear combinations of a, b, it follows that r_{k+1} is also a $\mathbb{Z}$-linear combination of a, b. This shows that r_{n+1} is a $\mathbb{Z}$-linear combination of (a, b), and hence

$$\text{gcd}(a, b) = ax + by$$

for some $x, y \in \mathbb{Z}$. Observe that the division algorithm also gives us possible values for x, y.

Now, suppose

$$ax_1 + by_1 = ax_2 + by_2$$

for some integers x_1, y_1, x_2, y_2. Then,

$$a(x_1 - x_2) = b(y_2 - y_1)$$

Dividing both sides by gcd(a, b), we see that

$$\frac{a}{\text{gcd}(a,b)}(x_1 - x_2) = \frac{b}{\text{gcd}(a,b)}(y_2 - y_1)$$

Now, it can be shown that for any $a, b \in \mathbb{Z}$ atleast one of which is non-zero,

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

So, we get that

$$\frac{b}{\text{gcd}(a,b)}|(x_1 - x_2)$$

and that

$$\frac{a}{\text{gcd}(a,b)}|(y_2 - y_1)$$

where we have used the fundamental fact (which is not hard to prove) that if $c|ab$ and gcd$(c, a) = 1$, then $c|b$. So, it follows that

$$x_2 = x_1 - t\frac{b}{\text{gcd}(a,b)}$$

and that

$$y_2 = y_1 + t\frac{a}{\text{gcd}(a,b)}$$

for some integers $t \in \mathbb{Z}$. So, if a solution x_1, y_1 is already known, all other solutions are given by a parametric formula.

(v) Two ways to think of a prime number. Suppose p is an integer other than $0, \pm 1$. Show the equivalence: 'p has no factors other than $\pm p$ and ± 1' $\iff$ 'if $p|ab$ then $p|a$ or $p|b$'. Under these conditions we call p a prime number.

Solution: First, we will show the given equivalence. So, suppose p has no factors other than $\pm p$ and ± 1. Then, suppose $p|ab$ for some $a, b \in \mathbb{Z}$. Then, if $p|a$, we are done. So, suppose $p \nmid a$. We know that gcd(p, a) exists. Moreover, because of the assumption that $p \nmid a$, it must be true that

$$\text{gcd}(p, a) = 1$$

because the only factors of p are ± 1 and $\pm p$. So, there are integers $x, y \in \mathbb{Z}$ such that

$$px + ay = 1$$

and hence

$$bpx + bay = b$$

Now, by our assumption, $p|ab$, so the above equation implies $p|b$.

Conversely, suppose p is an integer such that $p|ab$ implies $p|a$ or $p|b$. Let d be a factor of p, so that

$$p = dk$$

for some $k \in \mathbb{Z}$. Hence, $p|dk$, so that $p|d$ or $p|k$. Without loss of generality, suppose $p|d$, so that $d = pk'$ for some $k' \in \mathbb{Z}$. So, we have

$$p = pk'k$$

and hence

$$p(k'k - 1) = 0$$

implying that $k'k = 1$, and hence $k = \pm 1$, which means that $d = \pm p$. Similarly, if we assume that $p|k$, then we will obtain $d = \pm 1$ and $k = \pm p$, so the only factors of p are ± 1 and $\pm p$.

(vi) Existence of prime factorization. Why can each non-zero integer n other than ± 1 be written as a finite product of prime numbers?

Solution: We can assume that only positive integers are being considered, as a factorization for a negative integer can be obtained from its additive inverse. The existence of a factorization can be proven using induction. For the base case, we have $n = 2$. We know that if d is a factor of 2, then $|d| \leq 2$. So, the only possible non-zero values of d are $\pm 1, \pm 2$, and hence it follows that 2 is prime in $\mathbb{Z}$. For the inductive case, suppose all $2 \leq k \leq m$ have a prime factorisation. Consider the integer $m + 1$. If $m + 1$ is a prime, then we are done, because the factorisation is

$$m + 1 = m + 1$$

So suppose $m + 1$ is not a prime. Then, we have that

$$m + 1 = ab$$

where a, b are positive integers such that $a, b > 1$. Clearly, we have that $a < m+1$ and $b < m + 1$, so by the inductive hypothesis,

$$a = p_1 p_2 ... p_s$$
$$b = q_1 q_2 ... q_t$$

for some $s, t \in \mathbb{N}$ where each p_i, q_j is a prime in $\mathbb{Z}$. So, we see that

$$m + 1 = p_1 p_2 ... p_s q_1 q_2 ... q_t$$

and hence $m + 1$ also can be written as a product of primes. This completes the proof.

(vii) Uniqueness of prime factorization. In what way is an expression of n as a product of primes unique? Formulate this carefully and prove it.

Solution: First, suppose n is a non-zero integer. From **(vi)**, we know that n can be written as a product of primes. We show that this factorisation is unique (in some sense). Suppose

$$n = p_1 p_2 p_3 ... p_s = q_1 q_2 q_3 ... q_t$$

where each p_i, q_j is a prime. This means that

$$p_1 | q_1 q_2 .... q_t$$

Because p_1 is a prime, this means that p_1 divides atleast one of $q_1, ..., q_t$. Without loss of generality, suppose $p_1 | q_1$. But, recall that q_1 is a prime number, and hence the only possible values for p_1 are $\pm q_1$ (because p_1 cannot be ± 1). Hence, the equation reduces to

$$(\pm q_1)p_2...p_s = q_1 q_2...q_t$$

and since $\mathbb{Z}$ has the cancellation property, we have

$$\pm p_2...p_s = (\pm p_2)...p_s = q_2...q_t$$

Then, we can keep repeating this argument finitely many times, and conclude that $s = t$, and that $p_i = \pm q_j$ for some $1 \leq j \leq s$ for every $1 \leq i \leq s$. So, if we combine equal primes and write n as a product of prime powers, we see that

$$n = \pm p_1^{a_1}...p_k^{a_k}$$

where each p_i is a positive prime, each $a_k \geq 0$ and $0 \leq k \leq s$. Hence, it follows that the factorisation of n as a product of primes is unique upto sign.

(viii) Chinese Remainder Theorem. Suppose gcd$(a, b) = 1$. Prove that given any integer r and any integer s, there exists an integer n such that $a|n - r$ and $b|n - s$. How does one explicitly find such n? To what extent is it unique?

Solution: Because gcd$(a, b) = 1$, we have

$$ax + by = 1$$

for some $x, y \in Z$. Put

$$n = sax + rby$$

Observe that

$$n - r = sax + r(by - 1) = sax + r(-ax)$$

so that $a|n - r$. Similarly,

$$n - s = s(ax - 1) + rby = s(-by) + rby$$

and hence $b|n - s$. So, the required integer n has been found.

To explicity compute n, we just need to solve the diophantine equation $ax+by = 1$, which can be easily done using the long division method.

Finally, suppose n_1, n_2 are integers such that

$$a|n_1 - r$$
$$a|n_2 - r$$
$$b|n_1 - s$$
$$b|n_2 - s$$

This means that $a|n_1 - n_2$ and $b|n_1 - n_2$, so that $n_1 - n_2$ is a common multiple of a, b. Now we know that gcd$(a, b) = 1$, and hence lcm$(a, b) = ab$ (this can be proven easily). So, we see that $ab|n_1 - n_2$, so that

$$n_2 = n_1 + tab$$

for some integer $t \in \mathbb{Z}$. Hence, if one such integer n_1 is found, all others can be written as a parametric formula.

(ix) Example. Carry out parts **(iii)** and **(iv)** for $(a, b) = ($your roll number of form $201xxx, 2017)$. Then do part **(viii)** for $(r, s) = (20, 19)$.

Solution: By roll number is

$$201953$$

The procedure in **(iii)** will be carried out as follows.

$$\begin{aligned}
201953 &= 2017 \cdot 100 + 253 \\
2017 &= 253 \cdot 7 + 246 \\
253 &= 246 \cdot 1 + 7 \\
246 &= 7 \cdot 35 + 1 \\
7 &= 1 \cdot 7 + 0
\end{aligned}$$

So, it follows that

$$\gcd(201953, 2017) = 1$$

(iv) will be carried out as follows.

$$\begin{aligned}
253 &= 201953 - 2017 \cdot 100 \\
246 &= 2017 - 253 \cdot 7 = 201953 \cdot (-7) + 2017 \cdot 701 \\
7 &= 253 - 246 = 201953 \cdot 8 + 2017 \cdot (-801) \\
1 &= 246 - 7 \cdot 35 = 201953 \cdot (-287) + 2017 \cdot 28736
\end{aligned}$$

Finally, we carry out part **(viii)** for $(r, s) = (20, 19)$, i.e we solve the system of congruences

$$\begin{aligned}
x &\equiv 20 \pmod{201953} \\
x &\equiv 19 \pmod{2017}
\end{aligned}$$

As highlighted in **(viii)**, one solution is

$$x = 19 \cdot 201953 \cdot (-287) + 20 \cdot 2017 \cdot 28736 = 57960531$$

and any other solution is of the form

$$x = 57960531 + 407339201t$$

for $t \in \mathbb{Z}$.