Math 220 Fall 2021, Lecture 20: Number theory I

1. Number theory I

1.1. Division with remainder

Now comes the most fundamental theorem of number theory:

Theorem 1.1.1 (division with remainder theorem)**.** Let n be an integer. Let d be a positive integer. Then, there exist **unique** integers

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0, 1, \ldots, d-1\}$$

such that

$$n = qd + r.$$

We shall prove this soon. First, let us introduce some notations:

Definition 1.1.2. Let n be an integer. Let d be a positive integer. Let q and r be as in Theorem 1.1.1. Then:

- The number q is called the **quotient** of the division of n by d, and will be denoted by $n//d$.
- The number r is called the **remainder** of the division of n by d, and will be denoted by $n\%d$.
- The pair (q, r) is called the **quo-rem pair** of n and d.

For now, of course, we do not yet know that these q and r exist and are unique, so we should take care to speak of "**a** quotient", "**a** remainder" and "**a** quo-rem pair", never taking their existence and uniqueness for granted until we have proved it.

So Theorem 1.1.1 is saying that for any integer n and any positive integer d, there is a unique quo-rem pair of n and d. Let us now prove this.

Proof of Theorem 1.1.1. We need to prove two things: that a quo-rem pair of n and d exists, and that it is unique. Let me prove the uniqueness part first.

Proof of the uniqueness part: Fix an integer n and a positive integer d. We must show that there is **at most one** quo-rem pair (q, r) of n and d. In other words, we must show that there are no two distinct quo-rem pairs of n and d.

We prove this by contradiction. So we assume that (q_1, r_1) and (q_2, r_2) are two distinct quo-rem pairs of n and d, and we look for a contradiction.

Since (q_1, r_1) is a quo-rem pair of n and d, we have

$$q_1 \in \mathbb{Z} \qquad \text{and} \qquad r_1 \in \{0, 1, \ldots, d-1\} \qquad \text{and} \qquad n = q_1 d + r_1.$$

Since (q_2, r_2) is a quo-rem pair of n and d, we have

$$q_2 \in \mathbb{Z} \qquad \text{and} \qquad r_2 \in \{0, 1, \ldots, d-1\} \qquad \text{and} \qquad n = q_2 d + r_2.$$

Subtracting the equation $n = q_2 d + r_2$ from $n = q_1 d + r_1$, we obtain

$$0 = (q_1 d + r_1) - (q_2 d + r_2) = q_1 d + r_1 - q_2 d - r_2 = (q_1 - q_2)\, d + (r_1 - r_2)\,.$$

Thus,

$$-(r_1 - r_2) = (q_1 - q_2)\, d,$$

so that

$$(q_1 - q_2)\, d = -(r_1 - r_2) = r_2 - r_1.$$

This entails that $d \mid r_2 - r_1$. In other words, $r_2 - r_1$ is a multiple of d.

Now, however, r_1 and r_2 are in $\{0, 1, \ldots, d-1\}$. Hence, $r_2 - r_1 \in \underbrace{[-d+1,\ d-1]}_{\text{the interval from } -d+1 \text{ to } d-1}$.

(Formally speaking, this needs to be proved. But this is pretty doable: Combine

$$\underbrace{r_2}_{\leq d-1} - r_1 \leq d - 1 - \underbrace{r_1}_{\geq 0} \leq d-1 \qquad \text{and}$$

$$\underbrace{r_2}_{\geq 0} - r_1 \geq -\underbrace{r_1}_{\leq d-1} \geq -(d-1) = -d+1.$$

Thus, $r_2 - r_1 \in [-d+1,\ d-1]$.)

Hence, $|r_2 - r_1| \leq d - 1$ (formally speaking, this is because $|r_2 - r_1|$ is either $r_2 - r_1$ or $-(r_2 - r_1)$, but both of these numbers are $\leq d-1$).

However, if $r_2 - r_1$ was nonzero, then a proposition from Lecture 18 would yield that

$$|r_2 - r_1| \geq |d|$$

(since $r_2 - r_1$ is a multiple of d). Thus, we would have $|r_2 - r_1| \geq d > d - 1$. However, this would contradict $|r_2 - r_1| \leq d - 1$.

Hence, $r_2 - r_1$ cannot be nonzero. In other words, $r_2 - r_1 = 0$, so that $r_2 = r_1$.

Next, we recall that

$$(q_1 - q_2)\, d = r_2 - r_1 = 0 \qquad (\text{since } r_2 = r_1)\,.$$

We can divide this equality by d (since $d \neq 0$). Thus, we obtain $q_1 - q_2 = 0$, so that $q_2 = q_1$.

Now, the pairs (q_2, r_2) and (q_1, r_1) are equal (since $q_2 = q_1$ and $r_2 = r_1$). This contradicts our assumption that these pairs are distinct! So we have proved the uniqueness part of the theorem.

Now, let us come to the existence part. It feels like we should induct on one of n and d, but induction on d does not work, and induction on n is hindered by the fact that n is an arbitrary integer (so there is no "smallest n" to use as a base case). However, we can surmount the second of these hurdles by first proving the theorem for $n \geq 0$. Thus, we shall prove the following lemma:

Lemma 1.1.3. Let $n \in \mathbb{N}$, and let d be a positive integer. Then, there exists a quo-rem pair of n and d.

Proof of Lemma 1.1.3. Fix d. We proceed by strong induction on n:

Induction step: Let $n \in \mathbb{N}$. Assume (as the induction hypothesis) that the lemma is proved for all nonnegative integers smaller than n instead of n. In other words, for each $k < n$, there exists a quo-rem pair of k and d. We must now prove that the lemma holds for n, i.e., that there exists a quo-rem pair of n and d.

If $n < d$, then we explicitly know such a pair: namely, $(0, n)$.

Otherwise, we have $n \geq d$, so that $n - d \in \mathbb{N}$. Thus, we can apply the induction hypothesis to $n - d$ instead of n. We conclude that there exists a quo-rem pair of $n - d$ and d. Let (q, r) be this pair. Then, we claim that $(q + 1, r)$ is a quo-rem pair of n and d. In fact, since (q, r) is a quo-rem pair of $n - d$ and d, we have

$$n - d = qd + r,$$

so that

$$n = (qd + r) + d = (q + 1)\, d + r,$$

which shows that $(q + 1, r)$ is a quo-rem pair of n and d. So we have shown that there exists a quo-rem pair of n and d, and thus our induction step is complete. So we have proved Lemma 1.1.3. □

Back to proving Theorem 1.1.1. We have shown that

- there is always **at most one** quo-rem pair of n and d, and
- there is **at least one** quo-rem pair of n and d if $n \in \mathbb{N}$.

What remains to be done is to prove that there is **at least one** quo-rem pair of n and d if $n < 0$.

One way to do so is to proceed similarly to the proof of Lemma 1.1.3, but using strong induction on $-n$.

Alternatively, it is easier to reduce the "negative n" case to the "nonnegative n" case (which we have already covered in Lemma 1.1.3): Namely, if n is negative, then $\underbrace{(1 - d)}_{\leq 0} \underbrace{n}_{<0}$ is nonnegative, so we can apply Lemma 1.1.3 to $(1 - d)\, n$ instead of n and conclude that there is a quo-rem pair of $(1 - d)\, n$ and n. Let (q, r) be this pair. Thus,

$$(1 - d)\, n = qd + r.$$

In other words,

$$n - dn = qd + r.$$

In other words,

$$n = dn + qd + r.$$

In other words,

$$n = (n+q)\,d + r.$$

This shows that $(n+q, r)$ is a quo-rem pair of n and d.

Thus, Theorem 1.1.1 is completely proved. □

Let us use this theorem to derive some basic facts about even and odd numbers. Recall:

Definition 1.1.4. **(a)** An integer n is said to be **even** if $2 \mid n$.

(b) An integer n is said to be **odd** if it is not even, i.e., if $2 \nmid n$.

We shall now show the following:

Proposition 1.1.5. Let n be an integer.

(a) The integer n is even if and only if there exists some $k \in \mathbb{Z}$ such that $n = 2k$.

(b) The integer n is odd if and only if there exists some $k \in \mathbb{Z}$ such that $n = 2k+1$.

Proof. **(a)** is a direct consequence of the definition of divisibility.

(b) is not!

So let us prove part **(b)**. This is an "if and only if" statement, so we need to prove both directions

$$(n \text{ is odd}) \Longrightarrow (\text{there exists some } k \in \mathbb{Z} \text{ such that } n = 2k+1)$$

and

$$(n \text{ is odd}) \Longleftarrow (\text{there exists some } k \in \mathbb{Z} \text{ such that } n = 2k+1).$$

For brevity, I will call these two directions the "$\Longrightarrow$" and the "$\Longleftarrow$" directions.

Proof of the "$\Longrightarrow$" direction: Assume that n is odd. By Theorem 1.1.1, there is a quo-rem pair (q, r) for n and 2. Consider this (q, r). We have

$$q \in \mathbb{Z} \qquad \text{and} \qquad r \in \{0,1\} \qquad \text{and} \qquad n = 2q + r.$$

However, if we had $r = 0$, then we would get $n = 2q + \underbrace{r}_{=0} = 2q$, which would show that n is even; but this is impossible because n is odd. So we cannot have $r = 0$. Therefore, $r = 1$ (since $r \in \{0,1\}$). Thus, $n = 2q + \underbrace{r}_{=1} = 2q + 1$. Therefore, there exists some $k \in \mathbb{Z}$ such that $n = 2k+1$ (namely, $k = q$). This proves the "$\Longrightarrow$" direction.

Proof of the "$\Longleftarrow$" direction: Assume that there exists some $k \in \mathbb{Z}$ such that $n = 2k+1$. This shows that $(k, 1)$ is a quo-rem pair of n and 2.

We must prove that n is odd. Assume the contrary. Thus, n is even. In other words, $n = 2p$ for some integer p. Thus, $(p, 0)$ is a quo-rem pair of n and 2 (since $n = 2p = 2p + 0$).

Now we know that $(k, 1)$ and $(p, 0)$ are quo-rem pairs of n and 2. However, Theorem 1.1.1 tells us that the quo-rem pair of n and 2 is unique. So the two pairs $(k, 1)$ and $(p, 0)$ must be equal. But this is impossible, since $1 \neq 0$. So we get a contradiction, and we conclude that n is odd. This proves the "$\Longleftarrow$" direction.

Thus, Proposition 1.1.5 **(b)** is proved. □

Corollary 1.1.6. The sum of any two odd integers is even.

Proof. Let a and b be two odd integers. We must prove that $a + b$ is even.

Proposition 1.1.5 **(b)** shows that we can write a as $a = 2k + 1$ for some integer k (since a is odd).

Similarly, we can write b as $b = 2\ell + 1$ for some integer ℓ (since b is odd).

Using these k and ℓ, we now have

$$a + b = (2k + 1) + (2\ell + 1) = 2k + 2\ell + 2 = 2\underbrace{(k + \ell + 1)}_{\text{an integer}}.$$

This shows that $2 \mid a + b$, so that $a + b$ is even. □

Remark 1.1.7. This is a property specific to the number 2. It is not true that the sum of any two integers not divisible by 3 is divisible by 3.

Here are some properties of quotients and remainders:

Proposition 1.1.8. Let $n \in \mathbb{Z}$ and let d be a positive integer. Then:
(a) We have $n\%d \in \{0, 1, \ldots, d-1\}$ and $n\%d \equiv n \bmod d$.
(b) We have $d \mid n$ if and only if $n\%d = 0$.
(c) If $c \in \{0, 1, \ldots, d-1\}$ satisfies $c \equiv n \bmod d$, then $c = n\%d$.
(d) We have $n = (n//d)\, d + (n\%d)$.

Proof. **(d)** follows from the definition of quo-rem pairs (it is just the $n = qd + r$ equation).

(a) The definition of $n\%d$ yields $n\%d \in \{0, 1, \ldots, d-1\}$. Remains to show that $n\%d \equiv n \bmod d$.

Indeed, let (q, r) be the quo-rem pair of n and d. Then, $n\%d = r$ and $n = qd + r$. Now, $n = qd + r$ yields $n - r = qd$, which is divisible by d. So $d \mid n - r$; in other words, $n \equiv r \bmod d$. In other words, $r \equiv n \bmod d$. In other words, $n\%d \equiv n \bmod d$, since $r = n\%d$. So part **(a)** is proved.

Parts **(b)** and **(c)** will be proved next time. □