Math 221 Winter 2023, Lecture 8: Elementary number theory

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wd`

3. Elementary number theory

3.3. Division with remainder

3.3.1. The theorem

What comes next is the most fundamental theorem of number theory:

Theorem 3.3.1 (division-with-remainder theorem)**.** Let n be an integer. Let d be a positive integer. Then, there exists a **unique** pair (q, r) of integers

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

such that

$$n = qd + r.$$

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

Definition 3.3.2. Let n be an integer. Let d be a positive integer. Let (q, r) be the pair whose existence and uniqueness is claimed in Theorem 3.3.1. 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 (because we haven't proved the theorem yet). Thus, we will 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.

Example 3.3.3. What are $8//5$ and $8\%5$? We have

$$\underbrace{8}_{=n} = \underbrace{1}_{=q} \cdot \underbrace{5}_{=d} + \underbrace{3}_{=r \in \{0,1,2,3,4\}},$$

so $8//5 = 1$ and $8\%5 = 3$. (This is taking the uniqueness of $8//5$ and $8\%5$ for granted, but we will prove this soon.)

Example 3.3.4. What are $19//5$ and $19\%5$? We have $19 = 3 \cdot 5 + 4$, so $19//5 = 3$ and $19\%5 = 4$.

Example 3.3.5. What are $(-7)//5$ and $(-7)\%5$? We have

$$\underbrace{-7}_{=n} = \underbrace{(-2)}_{=q} \cdot \underbrace{5}_{=d} + \underbrace{3}_{=r\in\{0,1,2,3,4\}},$$

so $(-7)//5 = -2$ and $(-7)\%5 = 3$.

So Theorem 3.3.1 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 3.3.1. 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 shall 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. We want to derive 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 find

$$\begin{aligned} 0 &= (q_1 d + r_1) - (q_2 d + r_2) = (r_1 - r_2) - (q_2 d - q_1 d) \\ &= (r_1 - r_2) - (q_2 - q_1)\, d. \end{aligned}$$

In other words,

$$r_1 - r_2 = (q_2 - q_1)\, d. \tag{1}$$

We are in one of the following three cases:

Case 1: We have $q_1 < q_2$.

Case 2: We have $q_1 = q_2$.

Case 3: We have $q_1 > q_2$.

Let us first consider Case 1. In this case, we have $q_1 < q_2$, so that $q_2 - q_1 > 0$. Since $q_2 - q_1$ is an integer, this entails that $q_2 - q_1 \geq 1$. We can multiply this inequality by d (since $d > 0$), thus obtaining $(q_2 - q_1)\, d \geq 1d = d$. In view of (1), we can rewrite this as $r_1 - r_2 \geq d$. However, $r_1 \leq d - 1$ (since $r_1 \in \{0, 1, \ldots, d-1\}$) and $r_2 \geq 0$ (since $r_2 \in \{0, 1, \ldots, d-1\}$). Hence, $r_1 -$

$\underbrace{r_2}_{\geq 0} \leq r_1 \leq d-1 < d$. This contradicts $r_1 - r_2 \geq d$. Thus, we have found a contradiction in Case 1.

Let us next consider Case 2. In this case, we have $q_1 = q_2$. Hence, we can rewrite (1) as $r_1 - r_2 = \underbrace{(q_2 - q_2)}_{=0} d = 0$, so that $r_1 = r_2$. Combining $q_1 = q_2$ with $r_1 = r_2$, we obtain $(q_1, q_2) = (r_1, r_2)$, which contradicts our assumption that the two quo-rem pairs (q_1, r_1) and (q_2, r_2) are distinct. Thus, we have found a contradiction in Case 2.

Finally, in Case 3, we have $q_1 > q_2$ and therefore $q_2 < q_1$. Thus, Case 3 is just a copy of Case 1 with the roles of the two pairs (q_1, r_1) and (q_2, r_2) switched (since the two quo-rem pairs (q_1, r_1) and (q_2, r_2) are playing identical roles). Hence, we obtain a contradiction in Case 3.

We have now obtained contradictions in all three Cases 1, 2 and 3. Thus, we always have a contradiction. Hence, our assumption was wrong. This completes our proof of the uniqueness of the quo-rem pair of n and d.

Now, let us come to the existence part. It is reasonable to try induction, but there is a hurdle: Induction on d does not work (there is no good way to use the induction hypothesis), whereas induction on n cannot be used as long as n can be negative. Fortunately, the latter hurdle is surmountable. One way around it is to **first** prove the existence of a quo-rem pair in the case when $n \in \mathbb{N}$ (that is, $n \geq 0$), and **afterwards** generalize this result to arbitrary integers n.

So let us prove the $n \in \mathbb{N}$ case:

Lemma 3.3.6. 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 3.3.6. Fix d. We apply strong induction on n:

Induction step:[1] Let $n \in \mathbb{N}$. Assume (as the induction hypothesis) that Lemma 3.3.6 is proved for all nonnegative integers smaller than n instead of n. In other words, assume that for each nonnegative integer $k < n$, there exists a quo-rem pair of k and d. We must prove that Lemma 3.3.6 also holds for n, i.e., that there exists a quo-rem pair of n and d.

If $n < d$, then such a pair can be explicitly constructed: it is $(0, n)$. (Indeed, $n = 0d + n$ and $n \in \{0, 1, \ldots, d-1\}$).

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 (since $n - d < n$). We conclude that there exists a quo-rem pair of $n - d$ and d. We denote this pair by (q, r). Then, I claim that $(q + 1, r)$ is a quo-rem pair of n and d. Indeed, since (q, r) is a quo-rem pair of $n - d$ and d, we have

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

[1] Recall that a strong induction needs no base case (§1.9.4, Lecture 4).

Thus,

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

which shows that $(q + 1, r)$ is a quo-rem pair of n and d (since $r \in \{0, 1, \ldots, d - 1\}$). Thus, there exists a quo-rem pair of n and d. This completes our induction step, and thus Lemma 3.3.6 is proved. □

We now return to proving Theorem 3.3.1. 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 proving that there is **at least one** quo-rem pair of n and d if $n < 0$.

This can be done in several ways. One way is to proceed similarly to the proof of Lemma 3.3.6, but using strong induction on $-n$.

Alternatively, there is a slicker argument: We can reduce the "negative n" case to the "nonnegative n" case (which is already covered by Lemma 3.3.6). Namely, let $n \in \mathbb{Z}$ be negative. Then, the product $(1 - d)\, n$ is nonnegative (since both factors $1 - d$ and n are ≤ 0), so we can apply Lemma 3.3.6 to $(1 - d)\, n$ instead of n. Thus, we conclude that there exists a quo-rem pair (q, r) of $(1 - d)\, n$ and d. This pair (q, r) satisfies

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

(by the definition of a quo-rem pair). In other words,

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

Hence,

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

This shows that $(n + q, r)$ is a quo-rem pair of n and d. Hence, such a quo-rem pair exists. Hence, we have proved the existence of a quo-rem pair in the case when n is negative. This completes our proof of Theorem 3.3.1. □

3.3.2. An application: even and odd integers

We shall now use this theorem to derive some basic properties of even and odd numbers. Recall what these words mean:

Definition 3.3.7. **(a)** An integer n is said to be **even** if $2 \mid n$.
(b) An integer n is said to be **odd** if $2 \nmid n$.

In other words, an integer is called **even** if it is divisible by 2, and is called **odd** if it is not even.

Now we shall show the following:

Proposition 3.3.8. 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. Part **(a)** is a direct consequence of the definition of divisibility. But part **(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

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

For the sake of brevity, I shall refer to these two directions as the "$\Longrightarrow$" and "$\Longleftarrow$" directions (respectively).

Proof of the "$\Longrightarrow$" direction: Assume that n is odd. By Theorem 3.3.1, there exists a quo-rem pair (q, r) of n and 2. Consider this (q, r). By the definition of a quo-rem pair, this pair satisfies

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

If r were 0, then we would thus get $n = 2q + \underbrace{r}_{=0} = 2q$, which would show that n is even; but this is impossible because n is odd. Therefore, we must have $r \neq 0$, so that $r = 1$ (since $r \in \{0, 1\}$). Thus, $n = 2q + \underbrace{r}_{=1} = 2q + 1$. Hence, there exists some $k \in \mathbb{Z}$ such that $n = 2k + 1$ (namely, $k = q$). Thus we have shown the "$\Longrightarrow$" direction.

Proof of the "$\Longleftarrow$" direction: Assume that there exists some $k \in \mathbb{Z}$ such that $n = 2k + 1$. Consider this k.

We must show that n is odd. This means showing that $2 \nmid n$. This means proving that n cannot be written as $2c$ for an integer c.

To prove this, we assume the contrary. That is, we assume that $n = 2c$ for some integer c. Consider this c.

Now, the two pairs $(k, 1)$ and $(c, 0)$ both are quo-rem pairs of n and 2, because we have $n = 2k + 1$ and $n = 2c = 2c + 0$ (and 1 and 0 belong to $\{0, 1\}$). However, Theorem 3.3.1 says that the quo-rem pair of n and 2 is unique, so these two pairs $(k, 1)$ and $(c, 0)$ must be identical. But this is absurd, since their second entries 1 and 0 are different. So we find a contradiction. This concludes our proof that n is odd. Thus, we have shown the "$\Longleftarrow$" direction of Proposition 3.3.8 **(b)**.

This completes the proof of Proposition 3.3.8 **(b)** (since both directions are proved). □

Corollary 3.3.9. **(a)** The sum of any two even integers is even.
(b) The sum of any even integer with any odd integer is odd.
(c) The sum of any two odd integers is even.

Proof. We will only prove part **(c)**, since the other two parts are analogous (and even simpler).

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

The integer a is odd. Hence, Proposition 3.3.8 **(b)** shows that we can write a as $a = 2k+1$ for some integer k.

Similarly, we can write b as $b = 2\ell+1$ for some integer ℓ.

Consider these k and ℓ. Now, from $a = 2k+1$ and $b = 2\ell+1$, we obtain

$$a+b = (2k+1)+(2\ell+1) = 2k+2\ell+2 = 2\left(k+\ell+1\right),$$

which is clearly even. This proves Corollary 3.3.9 **(c)**. □

Remark 3.3.10. Corollary 3.3.9 **(c)** is a property specific to the number 2. For example, it is not true that the sum of any two integers not divisible by 3 is divisible by 3.

3.3.3. Basic properties of quotients and remainders

Here are some elementary facts about quotients and remainders:

Proposition 3.3.11. 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 $n = (n//d)\,d + (n\%d)$.
(e) If $n \in \mathbb{N}$, then $n//d \in \mathbb{N}$.

Note that part **(a)** of this proposition can be restated as follows: The remainder $n\%d$ is an element of $\{0,1,\ldots,d-1\}$ that is congruent to n modulo d. Part **(c)** says that, conversely, any element c of $\{0,1,\ldots,d-1\}$ that is congruent to n modulo d must be this remainder $n\%d$. Thus, together, these two parts uniquely characterize the remainder $n\%d$ as the only element of $\{0,1,\ldots,d-1\}$ that is congruent to n modulo d. This characterization is good to keep in mind, as it describes the remainder independently of the quotient.

Proof of Proposition 3.3.11. We set

$$q := n//d \qquad \text{and} \qquad r := n\%d.$$

Thus, (q,r) is a quo-rem pair of n and d (by the definition of a quo-rem pair). In other words, we have $n = qd+r$ and $q \in \mathbb{Z}$ and $r \in \{0,1,\ldots,n-1\}$. We can now prove all five parts of the proposition:

(d) We have $n = \underbrace{q}_{=n//d} d + \underbrace{r}_{=n\%d} = (n//d)\, d + (n\%d)$. This proves Proposition 3.3.11 **(d)**.

(a) We have $n\%d = r \in \{0, 1, \ldots, d-1\}$. Moreover, from $n = qd + r$, we obtain $r - n = r - (qd + r) = -qd$, which is clearly divisible by d. Hence, $d \mid r - n$. Equivalently, $r \equiv n \bmod d$. In other words, $n\%d \equiv n \bmod d$ (since $r = n\%d$). Thus, Proposition 3.3.11 **(a)** is proved (since we have shown that $n\%d \in \{0, 1, \ldots, d-1\}$ as well).

(c) Let $c \in \{0, 1, \ldots, d-1\}$ satisfy $c \equiv n \bmod d$. We must show that $c = n\%d$.

From $c \equiv n \bmod d$, we obtain $d \mid c - n$. In other words, $c - n = de$ for some $e \in \mathbb{Z}$. Consider this e. From $c - n = de$, we obtain $c = n + de$, so that $n = c - de = (-e)\, d + c$. This (combined with $c \in \{0, 1, \ldots, d-1\}$) shows that $(-e, c)$ is a quo-rem pair of n and d. However, (q, r) is also a quo-rem pair of n and d (by its definition). Since there is only one quo-rem pair of n and d (by Theorem 3.3.1), this shows that $(-e, c) = (q, r)$. Hence, $c = r = n\%d$. This proves Proposition 3.3.11 **(c)**.

(b) Again, this is an "if and only if" statement, and we shall prove its "$\Longrightarrow$" and "$\Longleftarrow$" directions separately:

$\Longrightarrow$: Assume that $d \mid n$. We must prove that $n\%d = 0$. In other words, we must prove that $r = 0$.

Indeed, $d \mid n$ yields that $n \equiv 0 \bmod d$ (by Proposition 3.2.3 in Lecture 7). In other words, $0 \equiv n \bmod d$. Since we furthermore have $0 \in \{0, 1, \ldots, d-1\}$, we can thus apply Proposition 3.3.11 **(c)** to $c = 0$, and conclude that $0 = n\%d$. In other words, $n\%d = 0$. This proves the "$\Longrightarrow$" direction (i.e., it proves that if $d \mid n$, then $n\%d = 0$).

$\Longleftarrow$: If $n\%d = 0$, then $d \mid n$ because

$$n = qd + \underbrace{r}_{=n\%d=0} = qd.$$

This proves the "$\Longleftarrow$" direction. Thus, both directions are proved, so that Proposition 3.3.11 **(b)** holds.

(e) Assume that $n \in \mathbb{N}$. Recall that $r \in \{0, 1, \ldots, d-1\}$, so that $r \leq d - 1 < d$. But $n = qd + \underbrace{r}_{<d} < qd + d$. Hence, $qd + d > n \geq 0$ (since $n \in \mathbb{N}$). In other words, $qd > -d$.

If we had $q < 0$, then we would have $q \leq -1$ (since q is an integer) and therefore $qd \leq (-1)\, d$ (since we can multiply the inequality $q \leq -1$ by the positive number d); but this would contradict $qd > -d = (-1)\, d$. Hence, we cannot have $q < 0$. Thus, $q \geq 0$, so that $q \in \mathbb{N}$. In other words, $n//d \in \mathbb{N}$ (since $q = n//d$). This proves Proposition 3.3.11 **(e)**. □

Quotients and remainders are closely connected to the so-called floor function:

Definition 3.3.12. The **integer part** (aka **floor**) of a real number x is defined to be the largest integer that is $\leq x$. It is denoted by $\lfloor x \rfloor$.

For example,

$$\lfloor 3.8 \rfloor = 3, \qquad \lfloor 4.2 \rfloor = 4, \qquad \lfloor 5 \rfloor = 5, \qquad \left\lfloor \sqrt{2} \right\rfloor = 1,$$
$$\lfloor \pi \rfloor = 3, \qquad \lfloor 0.5 \rfloor = 0, \qquad \lfloor -1.2 \rfloor = -2$$

(make sure you understand the last example! -1 is not ≤ -1.2, but -2 is).

Now, here is the connection to quotients and remainders:

Proposition 3.3.13 ("explicit formulas" for quotient and remainder)**.** Let $n \in \mathbb{Z}$, and let d be a positive integer. Then,

$$n//d = \left\lfloor \frac{n}{d} \right\rfloor \qquad \text{and} \qquad n\%d = n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor.$$

Proof. Proposition 3.3.11 **(a)** yields $n\%d \in \{0, 1, \ldots, d-1\}$. Hence, $n\%d \geq 0$ and $n\%d \leq d - 1 < d$.

Proposition 3.3.11 **(d)** yields $n = (n//d)\, d + (n\%d)$. Thus,

$$n = (n//d)\, d + \underbrace{(n\%d)}_{<d} < (n//d)\, d + d = ((n//d) + 1)\, d.$$

Dividing both sides of this inequality by d (we can do this, since $d > 0$), we obtain $\dfrac{n}{d} < (n//d) + 1$.

On the other hand,

$$n = (n//d)\, d + \underbrace{(n\%d)}_{\geq 0} \geq (n//d)\, d.$$

Dividing both sides of this inequality by d (we can do this, since $d > 0$), we obtain $\dfrac{n}{d} \geq n//d$.

Now, the integer $n//d$ is $\leq \dfrac{n}{d}$ (since $\dfrac{n}{d} \geq n//d$), but the next-larger integer $(n//d) + 1$ is not (since $\dfrac{n}{d} < (n//d) + 1$). Thus, $n//d$ is the largest integer that is $\leq \dfrac{n}{d}$. In other words, $n//d = \left\lfloor \dfrac{n}{d} \right\rfloor$ (by the definition of the floor $\left\lfloor \dfrac{n}{d} \right\rfloor$).

Solving the equation $n = (n//d)\, d + (n\%d)$ for $n\%d$, we find

$$n\%d = n - \underbrace{(n//d)}_{= \left\lfloor \frac{n}{d} \right\rfloor} d = n - \left\lfloor \frac{n}{d} \right\rfloor d = n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor.$$

Thus, Proposition 3.3.13 is proved. □

3.3.4. Base-b representation of nonnegative integers

Division with remainder is the main ingredient in a feature of integers that you may well be taking for granted, but actually needs to proved: the fact that every integer can be uniquely expressed in decimal notation, or, more generally, in base-b notation for any given integer $b > 1$.

What does this mean? For example,

$$\begin{aligned} 3401 &= 3 \cdot 1000 + 4 \cdot 100 + 0 \cdot 10 + 1 \cdot 1 \\ &= 3 \cdot 10^3 + 4 \cdot 10^2 + 0 \cdot 10^1 + 1 \cdot 10^0. \end{aligned}$$

Thus, we have written the fairly large number 3401 as a pretty short sum of powers of 10, with the coefficients being integers between 0 and 9 (commonly known as "digits").

This can be done for any nonnegative integer. This can also be done with any fixed integer $b > 1$ instead of 10, except that the coefficients ("generalized digits") will then be integers between 0 and $b - 1$. This is called the "base-b representation" of the integer.

For instance, let us find the base-4 representation of the integer 3401: This will be a representation of 3401 in the form

$$3401 = r_6 4^6 + r_5 4^5 + r_4 4^4 + r_3 4^3 + r_2 4^2 + r_1 4^1 + r_0 4^0,$$

where each r_i is a "base-4 digit" (i.e., an element of $\{0, 1, 2, 3\}$). Here, we are tacitly assuming that 4^6 is the highest power of 4 that we need; but we don't actually know this yet, so we must be prepared to add higher powers ($4^7, 4^8, 4^9, \ldots$) if needed.

How do we find these base-4 digits $r_0, r_1, \ldots, r_6$?

We start by identifying r_0. Indeed, on the RHS[2] of the equation

$$3401 = r_6 4^6 + r_5 4^5 + r_4 4^4 + r_3 4^3 + r_2 4^2 + r_1 4^1 + r_0 4^0,$$

all but the last addends are multiples of 4, whereas the last addend is $r_0 4^0 = r_0$. Hence, we can rewrite this equation as follows (factoring out the 4):

$$3401 = 4 \cdot \left(r_6 4^5 + r_5 4^4 + r_4 4^3 + r_3 4^2 + r_2 4^1 + r_1 4^0 \right) + r_0.$$

Since $r_0 \in \{0, 1, 2, 3\}$, this equation reveals that the pair

$$\left(r_6 4^5 + r_5 4^4 + r_4 4^3 + r_3 4^2 + r_2 4^1 + r_1 4^0,\ r_0 \right)$$

is a quo-rem pair of 3401 and 4. In particular, we must have

$$r_0 = 3401 \% 4 = 1 \qquad \text{and}$$
$$r_6 4^5 + r_5 4^4 + r_4 4^3 + r_3 4^2 + r_2 4^1 + r_1 4^0 = 3401 // 4 = 850.$$

[2] "RHS" means "right hand side".

Thus, we have identified the last base-4 digit r_0 as 1. In order to find the remaining digits, we analyze the latter equation

$$850 = r_6 4^5 + r_5 4^4 + r_4 4^3 + r_3 4^2 + r_2 4^1 + r_1 4^0.$$

In this equation, the only addend on the RHS not divisible by 4 is $r_1 4^0 = r_1$, so we can rewrite this equation as

$$850 = 4 \cdot \left(r_6 4^4 + r_5 4^3 + r_4 4^2 + r_3 4^1 + r_2 4^0 \right) + r_1,$$

and thus conclude that

$$r_1 = 850\%4 = 2 \qquad \text{and}$$
$$r_6 4^4 + r_5 4^3 + r_4 4^2 + r_3 4^1 + r_2 4^0 = 850//4 = 212.$$

Thus, we have identified the base-4 digit r_1 as 2. In order to find the remaining digits, we analyze the latter equation

$$212 = r_6 4^4 + r_5 4^3 + r_4 4^2 + r_3 4^1 + r_2 4^0.$$

In this equation, the only addend on the RHS not divisible by 4 is $r_2 4^0 = r_2$, so we can rewrite this equation as

$$212 = 4 \cdot \left(r_6 4^3 + r_5 4^2 + r_4 4^1 + r_3 4^0 \right) + r_2,$$

and thus conclude that

$$r_2 = 212\%4 = 0 \qquad \text{and}$$
$$r_6 4^3 + r_5 4^2 + r_4 4^1 + r_3 4^0 = 212//4 = 53.$$

Thus, we have identified the base-4 digit r_2 as 0. In order to find the remaining digits, we analyze the latter equation

$$53 = r_6 4^3 + r_5 4^2 + r_4 4^1 + r_3 4^0.$$

In this equation, the only addend on the RHS not divisible by 4 is $r_3 4^0 = r_3$, so we can rewrite this equation as

$$53 = 4 \cdot \left(r_6 4^2 + r_5 4^1 + r_4 4^0 \right) + r_3,$$

and thus conclude that

$$r_3 = 53\%4 = 1 \qquad \text{and}$$
$$r_6 4^2 + r_5 4^1 + r_4 4^0 = 53//4 = 13.$$

Thus, we have identified the base-4 digit r_3 as 1. In order to find the remaining digits, we analyze the latter equation

$$13 = r_6 4^2 + r_5 4^1 + r_4 4^0.$$

In this equation, the only addend on the RHS not divisible by 4 is $r_4 4^0 = r_4$, so we can rewrite this equation as

$$13 = 4 \cdot \left(r_6 4^1 + r_5 4^0 \right) + r_4,$$

and thus conclude that

$$\begin{aligned} r_4 &= 13 \% 4 = 1 \qquad \text{and} \\ r_6 4^1 + r_5 4^0 &= 13 // 4 = 3. \end{aligned}$$

Thus, we have identified the base-4 digit r_4 as 1. In order to find the remaining digits, we analyze the latter equation

$$3 = r_6 4^1 + r_5 4^0.$$

In this equation, the only addend on the RHS not divisible by 4 is $r_5 4^0 = r_5$, so we can rewrite this equation as

$$3 = 4 \cdot \left(r_6 4^0 \right) + r_5,$$

and thus conclude that

$$\begin{aligned} r_5 &= 3 \% 4 = 3 \qquad \text{and} \\ r_6 4^0 &= 3 // 4 = 0. \end{aligned}$$

Thus, we have identified the base-4 digit r_5 as 3. Moreover, the equation $r_6 4^0 = 0$ shows that $r_6 = 0$.

Thus, altogether, we have found the representation of 3401 we were looking for:

$$3401 = \underbrace{r_6}_{=0} 4^6 + \underbrace{r_5}_{=3} 4^5 + \underbrace{r_4}_{=1} 4^4 + \underbrace{r_3}_{=1} 4^3 + \underbrace{r_2}_{=0} 4^2 + \underbrace{r_1}_{=2} 4^1 + \underbrace{r_0}_{=1} 4^0.$$

In analogy to the decimal system, we can state this as "the number 3401 written in base-4 is 0311021" (since the base-4 digits $r_6, r_5, \ldots, r_0$ have been identified as $0, 3, 1, 1, 0, 2, 1$). Commonly, one would omit the leading zeroes, so this would become 311021.

The method we just used can be used for any given integer $b > 1$ instead of 4: To find the "base-b digits" of a nonnegative integer n, we first divide n by b with remainder, then divide the resulting quotient again by b with remainder, then divide the resulting quotient again by b with remainder, and so on, until

we are left with the quotient 0. The remainders obtained in the process will then be the base-b digits of n (from right to left). This process must eventually come to an end because (since $b > 1$) each quotient will be smaller than the preceding one.

We can summarize this as a theorem:

Theorem 3.3.14. Let $b > 1$ be an integer. Let $n \in \mathbb{N}$. Then:

(a) We can write n in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$k \in \mathbb{N} \qquad \text{and} \qquad r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

(b) If $n < b^{k+1}$ for some $k \in \mathbb{N}$, then we can write n in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

(c) These $r_0, r_1, \ldots, r_k$ are unique (when k is given). Moreover, they can be explicitly computed by the formula

$$r_i = \left(n//b^i\right) \% b \qquad \text{for each } i \in \{0, 1, \ldots, k\}.$$

That is, they can be explicitly computed by

$$\begin{aligned} r_0 &= n \% b, \\ r_1 &= (n//b) \% b, \\ r_2 &= \left(n//b^2\right) \% b, \\ r_3 &= \left(n//b^3\right) \% b, \\ &\ldots, \\ r_k &= \left(n//b^k\right) \% b. \end{aligned}$$

Proof. Forget that n was fixed (but keep b fixed). We shall prove the following two claims:

> *Claim 1:* Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $n < b^{k+1}$. Then, we can write n in the form
>
> $$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$
>
> with
>
> $$r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

Claim 2: Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Assume that n has been written in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

Then,

$$r_i = \left(n // b^i\right) \% b \qquad \text{for each } i \in \{0, 1, \ldots, k\}.$$

Once these two claims are proved, Theorem 3.3.14 will follow, because

- Theorem 3.3.14 **(b)** follows directly from Claim 1.
- Theorem 3.3.14 **(c)** follows directly from Claim 2.
- Theorem 3.3.14 **(a)** follows from Claim 1 (since we can pick $k \in \mathbb{N}$ high enough that $n < b^{k+1}$ holds[3]).

Hence, it remains to prove Claim 1 and Claim 2.

Proof of Claim 1. We proceed by induction on k:

Base case: For $k = 0$, Claim 1 is saying that every $n \in \mathbb{N}$ satisfying $n < b$ can be written in the form $n = r_0 \cdot b^0$ with $r_0 \in \{0, 1, \ldots, b-1\}$. But this is obvious: Since $n \in \mathbb{N}$ and $n < b$, we have $n \in \{0, 1, \ldots, b-1\}$, and thus we can just pick $r_0 = n$ and have $n = r_0 \cdot b^0$ (since $r_0 \cdot \underbrace{b^0}_{=1} = r_0 = n$). Hence, Claim 1 is proved for $k = 0$.

Induction step: We make a step from $k-1$ to k. Thus, we let k be a positive integer. Assume (as the induction hypothesis) that Claim 1 holds for $k-1$ instead of k. We must now show that Claim 1 holds for k as well.

So let $n \in \mathbb{N}$ be such that $n < b^{k+1}$. Then, Proposition 3.3.11 **(e)** (applied to $d = b$) yields $n // b \in \mathbb{N}$. Moreover, $n \% b \in \{0, 1, \ldots, b-1\}$ (by the definition of a remainder). Hence, $n \% b \geq 0$. Now, Proposition 3.3.11 **(d)** (applied to $d = b$) yields

$$n = (n // b)\, b + \underbrace{(n \% b)}_{\geq 0} \geq (n // b)\, b.$$

Hence, $(n // b)\, b \leq n < b^{k+1}$. Dividing this inequality by the positive number b, we obtain $n // b < b^{k+1} / b = b^k$.

Now, recall our induction hypothesis, which says that Claim 1 holds for $k-1$ instead of k. In other words, if $m \in \mathbb{N}$ is such that $m < b^{(k-1)+1}$, then we can write m in the form[4]

$$m = s_{k-1} \cdot b^{k-1} + s_{k-2} \cdot b^{k-2} + \cdots + s_1 \cdot b^1 + s_0 \cdot b^0$$

[3] Indeed, the assumption $b > 1$ ensures that the sequence $\left(b^0, b^1, b^2, \ldots\right)$ is strictly increasing and thus eventually outgrows any given integer, including our n. Or we can argue this directly: An easy induction (on n) shows that $n < b^{n+1}$, and thus we can simply take $k = n$.

[4] We are deliberately using the letters m and s_i instead of n and r_i here, since the letter n is already taken (and the letters r_i will be needed for something different).

with

$$s_0, s_1, \ldots, s_{k-1} \in \{0, 1, \ldots, b-1\}.$$

We can apply this to $m = n//b$ (since $n//b \in \mathbb{N}$ and $n//b < b^k = b^{(k-1)+1}$), and conclude that we can write $n//b$ in the form

$$n//b = s_{k-1} \cdot b^{k-1} + s_{k-2} \cdot b^{k-2} + \cdots + s_1 \cdot b^1 + s_0 \cdot b^0$$

with

$$s_0, s_1, \ldots, s_{k-1} \in \{0, 1, \ldots, b-1\}.$$

Let us do this. Thus,

$$\begin{aligned} n &= \underbrace{(n//b)}_{= s_{k-1} \cdot b^{k-1} + s_{k-2} \cdot b^{k-2} + \cdots + s_1 \cdot b^1 + s_0 \cdot b^0} b + (n\%b) \\ &= \left(s_{k-1} \cdot b^{k-1} + s_{k-2} \cdot b^{k-2} + \cdots + s_1 \cdot b^1 + s_0 \cdot b^0 \right) b + (n\%b) \\ &= s_{k-1} \cdot b^k + s_{k-2} \cdot b^{k-1} + \cdots + s_1 \cdot b^2 + s_0 \cdot b^1 + \underbrace{(n\%b)}_{= (n\%b) \cdot b^0} \\ &= s_{k-1} \cdot b^k + s_{k-2} \cdot b^{k-1} + \cdots + s_1 \cdot b^2 + s_0 \cdot b^1 + (n\%b) \cdot b^0. \end{aligned}$$

Note that the coefficients $n\%b, s_0, s_1, \ldots, s_{k-1}$ on the right hand side here all belong to $\{0, 1, \ldots, b-1\}$ (as we know). Thus, through this equality, we have written n in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}$$

(namely, with $r_0 = n\%b$ and $r_1 = s_0$ and $r_2 = s_1$ and ... and $r_{k-1} = s_{k-2}$ and $r_k = s_{k-1}$). Hence, n can be written in this form.

We have thus proved that if $n \in \mathbb{N}$ is such that $n < b^{k+1}$, then we can write n in the form

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0$$

with

$$r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}.$$

In other words, we have proved Claim 1 for our k. This completes the induction step. Thus, Claim 1 is proved by induction. □

Proof of Claim 2. We could prove this by induction as well, but let us instead go for a direct proof.

By assumption, we have

$$n = r_k \cdot b^k + r_{k-1} \cdot b^{k-1} + \cdots + r_1 \cdot b^1 + r_0 \cdot b^0 = \sum_{j=0}^{k} r_j \cdot b^j = \sum_{j=0}^{k} r_j b^j.$$

Now, we must prove that $r_i = \left(n//b^i\right)\%b$ for each $i \in \{0, 1, \ldots, k\}$. So let us fix an $i \in \{0, 1, \ldots, k\}$.

We have

$$n = \sum_{j=0}^{k} r_j b^j = \sum_{j=0}^{i-1} r_j b^j + \sum_{j=i}^{k} r_j b^j \tag{2}$$

(here, we have split our sum into two parts: one part which contains the addends for $j \in \{0, 1, \ldots, i-1\}$, and one part which contains the addends for $j \in \{i, i+1, \ldots, k\}$). We can rewrite the second sum as follows:

$$\sum_{j=i}^{k} r_j \underbrace{b^j}_{=b^i b^{j-i}} = \sum_{j=i}^{k} r_j b^i b^{j-i} = b^i \sum_{j=i}^{k} r_j b^{j-i}.$$

Thus, we can rewrite (2) as

$$n = \sum_{j=0}^{i-1} r_j b^j + b^i \sum_{j=i}^{k} r_j b^{j-i}. \tag{3}$$

Let us set

$$q' := \sum_{j=i}^{k} r_j b^{j-i} \qquad \text{and} \qquad r' := \sum_{j=0}^{i-1} r_j b^j.$$

With these notations, we can rewrite (3) as

$$n = r' + b^i q' = q' b^i + r'. \tag{4}$$

Note that both sums $q' = \sum_{j=i}^{k} r_j b^{j-i}$ and $r' = \sum_{j=0}^{i-1} r_j b^j$ are integers (indeed, b^{j-i} is always an integer in the first sum, since $j \geq i$ entails $j - i \in \mathbb{N}$).

We have assumed that $r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}$. In particular, the integers $r_0, r_1, \ldots, r_k$ are all ≥ 0 and $\leq b-1$. In other words, each $j \in \{0, 1, \ldots, k\}$ satisfies $r_j \geq 0$ and $r_j \leq b-1$. Hence, $r' = \sum_{j=0}^{i-1} r_j b^j \geq 0$ (since all the integers r_j are ≥ 0, and so is b) and

$$r' = \sum_{j=0}^{i-1} \underbrace{r_j}_{\leq b-1} b^j \leq \sum_{j=0}^{i-1} (b-1)\, b^j = (b-1) \underbrace{\sum_{j=0}^{i-1} b^j}_{\substack{=b^0+b^1+\cdots+b^{i-1} \\ = \dfrac{b^i-1}{b-1} \\ \text{(by Corollary 1.6.3 from Lecture 3,} \\ \text{applied to } b \text{ and } i \text{ instead of } q \text{ and } n)}}$$

$$= (b-1) \cdot \frac{b^i - 1}{b-1} = b^i - 1.$$

Thus, $r' \in \left\{0, 1, \ldots, b^i - 1\right\}$.

The equality (4) says that $n = q' b^i + r'$. In light of $q' \in \mathbb{Z}$ and $r' \in \left\{0, 1, \ldots, b^i - 1\right\}$, this shows that (q', r') is a quo-rem pair of n and b^i. Therefore, in particular, q' is the quotient of the division of n by b^i. In other words,

$$q' = n // b^i.$$

However,

$$\begin{aligned} q' &= \sum_{j=i}^{k} r_j b^{j-i} = r_i b^0 + r_{i+1} b^1 + r_{i+2} b^2 + \cdots + r_k b^{k-i} \\ &= r_i \underbrace{b^0}_{=1} + \underbrace{\left(r_{i+1} b^1 + r_{i+2} b^2 + \cdots + r_k b^{k-i} \right)}_{= \left(r_{i+1} b^0 + r_{i+2} b^1 + \cdots + r_k b^{k-i-1} \right) b} \\ &= r_i + \left(r_{i+1} b^0 + r_{i+2} b^1 + \cdots + r_k b^{k-i-1} \right) b. \end{aligned}$$

Thus, $q' - r_i = \left(r_{i+1} b^0 + r_{i+2} b^1 + \cdots + r_k b^{k-i-1} \right) b$, which is clearly divisible by b. That is, $b \mid q' - r_i$. In other words, $q' \equiv r_i \bmod b$. In other words, $r_i \equiv q' \bmod b$. Since we furthermore have $r_i \in \{0, 1, \ldots, b-1\}$ (because $r_0, r_1, \ldots, r_k \in \{0, 1, \ldots, b-1\}$), we thus conclude that $r_i = q' \% b$ (by Proposition 3.3.11 **(c)**, applied to q', b and r_i instead of n, d and c). In view of $q' = n // b^i$, we can rewrite this as $r_i = \left(n // b^i \right) \% b$.

Forget that we fixed i. We thus have shown that $r_i = \left(n // b^i \right) \% b$ for each $i \in \{0, 1, \ldots, k\}$. This proves Claim 2. □

Now, both Claims 1 and 2 are proved. As explained above, this completes the proof of Theorem 3.3.14. □

The inductive proof of Claim 1 in the above proof is just a formal avatar of the algorithm for writing a nonnegative integer n in base b that we demonstrated on an example before the theorem. The formula $r_i = \left(n // b^i \right) \% b$ from Claim 2, on the other hand, gives an alternative way of computing each base-b digit of n directly.