Reading Assignment 1
Lecture 1

1. Read Course Syllabus.
2. Read the content below about The Division Algorithm.

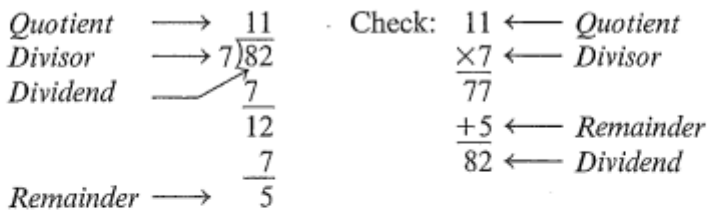
The Division Algorithm

Our starting point is the set of all integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. We assume that you are familiar with the arithmetic of integers and with the usual order relation ($<$) on the set $\mathbb{Z}$. We also assume the

WELL-ORDERING AXIOM *Every nonempty subset of the set of nonnegative integers contains a smallest element.*

If you think of the nonnegative integers laid out on the usual number line, it is intuitively plausible that each subset contains an element that lies to the left of all the other elements in the subset—that is the smallest element. On the other hand, the Well-Ordering Axiom does not hold in the set $\mathbb{Z}$ of all integers (there is no smallest negative integer). Nor does it hold in the set of all nonnegative rational numbers (the subset of all positive rationals does not contain a smallest element because, for any positive rational number r, there is always a smaller positive rational—for instance, $r/2$).

So here we go. Consider the following grade-school division problem:



The division process stops when we reach a remainder that is less than the divisor. All the essential facts are contained in the checking procedure, which may be verbally summarized like this:

$$\text{dividend} = (\text{divisor})\,(\text{quotient}) + (\text{remainder}).$$

Here is a formal statement of this idea, in which the dividend is denoted by a, the divisor by b, the quotient by q, and the remainder by r:

Theorem 1.1 The Division Algorithm

Let a, b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \le r < b.$$

Theorem 1.1 allows the possibility that the dividend a might be negative but requires that the remainder r must not only be less than the divisor b but also must be *nonnegative*. To see why this last requirement is necessary, suppose $a = -14$ is divided by $b = 3$, so that $-14 = 3q + r$. If we only require that the remainder be less than the divisor 3, then there are many possibilities for the quotient q and remainder r, including these three:

$$-14 = 3(-3) + (-5), \quad \text{with } -5 < 3 \qquad [\textit{Here } q = -3 \textit{ and } r = -5.]$$
$$-14 = 3(-4) + (-2), \quad \text{with } -2 < 3 \qquad [\textit{Here } q = -4 \textit{ and } r = -2.]$$
$$-14 = 3(-5) + 1, \quad \text{with } 1 < 3 \qquad [\textit{Here } q = -5 \textit{ and } r = 1.].$$

When the remainder is also required to be nonnegative as in Theorem 1.1, then there is exactly one quotient q and one remainder r, namely, $q = -5$ and $r = 1$, as will be shown in the proof.

The fundamental idea underlying the proof of Theorem 1.1 is that division is just repeated subtraction. For example, the division of 82 by 7 is just a shorthand method for repeatedly subtracting 7:

82			
−7			
75	⟵ $82 - 7 \cdot 1$	40	
−7		−7	
68	⟵ $82 - 7 \cdot 2$	33	⟵ $82 - 7 \cdot 7$
−7		−7	
61	⟵ $82 - 7 \cdot 3$	26	⟵ $82 - 7 \cdot 8$
−7		−7	
54	⟵ $82 - 7 \cdot 4$	19	⟵ $82 - 7 \cdot 9$
−7		−7	
47	⟵ $82 - 7 \cdot 5$	12	⟵ $82 - 7 \cdot 10$
−7		−7	
40	⟵ $82 - 7 \cdot 6$	5	⟵ $82 - 7 \cdot 11$

The subtractions continue until you reach a nonnegative number less than 7 (in this case 5). The number 5 is the remainder, and the *number* of multiples of 7 that were subtracted (namely, 11, as shown at the right of the subtractions) is the quotient.

In the preceding example we looked at the numbers

$$82 - 7 \cdot 1, \quad 82 - 7 \cdot 2, \quad 82 - 7 \cdot 3, \text{ and so on.}$$

In other words, we looked at numbers of the form $82 - 7x$ for $x = 1, 2, 3, \ldots$ and found the smallest nonnegative one (namely, 5). In the proof of Theorem 1.1 we shall do something very similar.

Proof of Theorem 1.1* ▸ Let a and b be fixed integers with $b > 0$. Consider the set S of all integers of the form

$$a - bx, \qquad \text{where } x \text{ is an integer and } a - bx \geq 0.$$

Note that x may be any integer—positive, negative, or 0—but $a - bx$ must be nonnegative. There are four main steps in the proof, as indicated below.

Step 1 *Show that S is nonempty by finding a value for x such that $a - bx \geq 0$.*

Proof of Step 1: We first show that $a + b|a| \geq 0$. Since b is a positive integer by hypothesis, we must have

$$\begin{aligned} b &\geq 1 \\ b|a| &\geq |a| \qquad [\textit{Multiply both sides of the preceding inequality by } |a|.] \\ b|a| &\geq -a \qquad [\textit{Because } |a| \geq -a \textit{ by the definition of absolute value.}] \\ a + b|a| &\geq 0. \end{aligned}$$

*For an alternate proof by induction of part of the theorem, see Example 2 in Appendix C.

Now let $x = -|a|$. Then

$$a - bx = a - b(-|a|) = a + b|a| \geq 0.$$

Hence, $a - bx$ is in S when $x = -|a|$, which means that S is nonempty.

Step 2 *Find q and r such that $a = bq + r$ and $r \geq 0$.*

Proof of Step 2: By the Well-Ordering Axiom, S contains a smallest element—call it r. Since $r \in S$, we know that $r \geq 0$ and $r = a - bx$ for some x, say $x = q$. Thus,

$$r = a - bq \text{ and } r \geq 0, \qquad \text{or, equivalently,} \qquad a = bq + r \text{ and } r \geq 0.$$

Step 3 *Show that $r < b$.*

Proof of Step 3: We shall use a "proof by contradiction" (which is explained on page 506 of Appendix A). We want to show that $r < b$. So suppose, on the contrary, that $r \geq b$. Then $r - b \geq 0$, so that

$$0 \leq r - b = (a - bq) - b = a - b(q + 1).$$

Since $a - b(q + 1)$ is nonnegative, it is an element of S by definition. But since b is positive, it is certainly true that $r - b < r$. Thus

$$a - b(q + 1) = r - b < r.$$

The last inequality states that $a - b(q + 1)$—which is an element of S—is less than r, the *smallest* element of S. This is a contradiction. So our assumption that $r \geq b$ is false, and we conclude that $r < b$. Therefore, we have found integers q and r such that

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

Step 4 *Show that r and q are the only numbers with these properties (that's what "unique" means in the statement of the theorem).*

Proof of Step 4: To prove uniqueness, we suppose that there are integers q_1 and r_1 such that $a = bq_1 + r_1$ and $0 \leq r_1 < b$, and prove that $q_1 = q$ and $r_1 = r$.

Since $a = bq + r$ and $a = bq_1 + r_1$, we have

$$bq + r = bq_1 + r_1$$

so that

$$(*) \qquad b(q - q_1) = r_1 - r.$$

Furthermore,

$$0 \leq r < b$$
$$0 \leq r_1 < b.$$

Multiplying the first inequality by -1 (and reversing the direction of the inequality), we obtain

$$-b < -r \leq 0$$
$$0 \leq r_1 < b.$$

Adding these two inequalities produces

$$\begin{aligned} -b < r_1 - r < b & \\ -b < b(q - q_1) < b & \quad [\textit{By Equation } (*)] \\ -1 < q - q_1 < 1 & \quad [\textit{Divide each term by } b.] \end{aligned}$$

But $q - q_1$ is an *integer* (because q and q_1 are integers) and the only integer strictly between -1 and 1 is 0. Therefore $q - q_1 = 0$ and $q = q_1$. Substituting $q - q_1 = 0$ in Equation $(*)$ shows that $r_1 - r = 0$ and hence $r = r_1$. Thus the quotient and remainder are unique, and the proof is complete. ■*