Math 221 Winter 2023, Lecture 7: Elementary number theory

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

3. Elementary number theory

Number theory is commonly understood to be the study of integers, and particularly of those properties and features of integers that do not make much sense for rational, real or complex numbers. Divisibility is one such property; prime numbers are another. In this course, we will only cover the very basics of elementary number theory; there is no shortage of texts that go much deeper (some freely available ones are [Stein08], [Shoup08] and [Martin17]).

3.1. Divisibility

3.1.1. Definition

We begin by defining the one most important concept in number theory:

Definition 3.1.1. Let a and b be two integers.

We write $a \mid b$ (and we say that "a **divides** b", or "b is **divisible** by a", or "b is a **multiple** of a", or "a is a **divisor** of b"; yes, all these statements are equivalent) if there exists an integer c such that $b = ac$.

We write $a \nmid b$ if we don't have $a \mid b$.

Example 3.1.2. **(a)** We have $4 \mid 12$, because $12 = 4 \cdot 3$.

(b) We have $4 \nmid 11$, because there exists no integer c such that $11 = 4c$.

(c) We have $1 \mid b$ for every integer b, since $b = 1 \cdot b$.

(d) We have $a \mid a$ for every integer a, since $a = a \cdot 1$. In particular, $0 \mid 0$, which is somewhat controversial (but true in our opinion). (Some authors deliberately exclude 0 as a divisor on the grounds that $\frac{0}{0}$ is not well-defined, but I believe that making this an exception is more trouble than it is worth.)

(e) We have $a \mid 0$ for every integer a, since $0 = a \cdot 0$.

(f) An integer b satisfies $0 \mid b$ if and only if $b = 0$.

The well-known concepts of even and odd integers are instances of divisibility:

Definition 3.1.3. **(a)** An integer n is said to be **even** if $2 \mid n$.

(b) An integer n is said to be **odd** if $2 \nmid n$.

You probably know a few things about even and odd numbers already: e.g.,

1. The sum of two even numbers is even.
2. The sum of an even with an odd number is odd.
3. The sum of two odd numbers is even.

Strictly speaking, these claims (particularly the third one) are not at all obvious. So we need to understand divisibility better to even convince ourselves that such fundamental statements are true. We will do this in Lecture 8. First, let us prove some basic facts about divisibility.

3.1.2. Basic properties

In the next proposition, we shall let $\operatorname{abs} x$ denote the absolute value of a real number x. Thus,

$$\operatorname{abs} x = \begin{cases} x, & \text{if } x \geq 0; \\ -x, & \text{if } x < 0. \end{cases}$$

This absolute value $\operatorname{abs} x$ is normally called $|x|$, but I believe that writing "$\operatorname{abs} a \mid \operatorname{abs} b$" is less confusing than writing "$|a| \mid |b|$" (where four of the bars stand for absolute values, while the middle bar stands for divisibility).

Proposition 3.1.4. Let a and b be two integers. Then:
(a) We have $a \mid b$ if and only if $\operatorname{abs} a \mid \operatorname{abs} b$.
(b) If $a \mid b$ and $b \neq 0$, then $\operatorname{abs} a \leq \operatorname{abs} b$.
(c) If $a \mid b$ and $b \mid a$, then $\operatorname{abs} a = \operatorname{abs} b$.
(d) Assume that $a \neq 0$. Then, $a \mid b$ if and only if $\dfrac{b}{a} \in \mathbb{Z}$.

Proof. **(a)** Proposition 3.1.4 **(a)** says that the divisibility $a \mid b$ does not depend on the signs of a and b; in other words, it says that we can replace the numbers a and b by their absolute values without changing the truth (or falsity) of $a \mid b$.

Clearly, in order to prove this, it suffices to show the following two statements:

1. We can replace a by $-a$ without changing the truth (or falsity) of $a \mid b$;
2. We can replace b by $-b$ without changing the truth (or falsity) of $a \mid b$;

But both of these statements are easy:

For the first statement, we assume that $a \mid b$. Thus, $b = ac$ for some integer c (by the definition of "$a \mid b$"). Hence, for this integer c, we have $b = ac = (-a)(-c)$, which allows us to conclude that $-a \mid b$ (since $-c$ is an integer, too). Thus, we have shown that $a \mid b$ implies $-a \mid b$. Conversely, a similar argument shows that $-a \mid b$ implies $a \mid b$ (indeed, it is the same argument with the roles of a and $-a$ swapped, because $-(-a) = a$). Thus, the statements $a \mid b$ and

$-a \mid b$ are equivalent. In other words, we can replace a by $-a$ without changing the truth (or falsity) of $a \mid b$. This proves the first of our above two statements.

The proof of the second statement is similar. (This time, you need to argue that $a \mid b$ implies $a \mid -b$. Again, write b as $b = ac$, and conclude that $-b = -ac = a(-c)$, so that $a \mid -b$.)

Thus, both statements are proved, so that the proof of Proposition 3.1.4 **(a)** is complete.

(b) Assume that $a \mid b$ and $b \neq 0$. We must show that $\operatorname{abs} a \leq \operatorname{abs} b$.

Let $x = \operatorname{abs} a$ and $y = \operatorname{abs} b$. Thus, x is a nonnegative integer and y is a positive integer (since $b \neq 0$). Thus, $x \geq 0$ and $y > 0$.

Proposition 3.1.4 **(a)** yields that $\operatorname{abs} a \mid \operatorname{abs} b$ (since $a \mid b$). In other words, $x \mid y$ (since $x = \operatorname{abs} a$ and $y = \operatorname{abs} b$). In other words, $y = xz$ for some integer z. Consider this z.

If we had $z \leq 0$, then we would have $y = \underbrace{x}_{\geq 0} \underbrace{z}_{\leq 0} \leq 0$ (by the standard rules for inequalities), which would contradict $y > 0$. Hence, we cannot have $z \leq 0$. Thus, $z > 0$, so that $z \geq 1$ (since z is an integer). Hence, $xz \geq x1$ (since $x \geq 0$ allows us to multiply any inequality by x without having to flip the sign). Therefore, $y = xz \geq x1 = x$. In other words, $x \leq y$. In other words, $\operatorname{abs} a \leq \operatorname{abs} b$ (since $x = \operatorname{abs} a$ and $y = \operatorname{abs} b$). This proves Proposition 3.1.4 **(b)**.

(c) Let $a \mid b$ and $b \mid a$. We must prove that $\operatorname{abs} a = \operatorname{abs} b$.

If $a = 0$, then this is easily done (because if $a = 0$, then $0 = a \mid b$ quickly leads to $b = 0$, and therefore $a = 0 = b$, so that $\operatorname{abs} a = \operatorname{abs} b$).

Likewise, this is easily done if $b = 0$.

It remains to handle the third possible case, which is when both a and b are $\neq 0$. Consider this case. In this case, Proposition 3.1.4 **(b)** yields $\operatorname{abs} a \leq \operatorname{abs} b$ (since $a \mid b$ and $b \neq 0$). However, we can also apply Proposition 3.1.4 **(b)** with the roles of a and b interchanged (since $b \mid a$ and $a \neq 0$), and thus obtain $\operatorname{abs} b \leq \operatorname{abs} a$. Combining this with $\operatorname{abs} a \leq \operatorname{abs} b$, we find $\operatorname{abs} a = \operatorname{abs} b$. Proposition 3.1.4 **(c)** is thus proved.

(d) This is quite straightforward:

Assume that $a \mid b$. Thus, there exists some integer c such that $b = ac$ (by the definition of "$a \mid b$"). This c must then be $\dfrac{b}{a}$ (since $b = ac$ implies $c = \dfrac{b}{a}$ in view of $a \neq 0$). Hence, $\dfrac{b}{a}$ is an integer, i.e., we have $\dfrac{b}{a} \in \mathbb{Z}$.

Forget that we assumed $a \mid b$. We thus have shown that $\dfrac{b}{a} \in \mathbb{Z}$ if $a \mid b$. The same argument (done in reverse) yields that conversely, if $\dfrac{b}{a} \in \mathbb{Z}$, then $a \mid b$. Combining these two facts, we conclude that $a \mid b$ if and only if $\dfrac{b}{a} \in \mathbb{Z}$. This proves Proposition 3.1.4 **(d)**. □

This was a warm-up (if somewhat laborious to write up). Here are some slightly more substantial properties of divisibility:

Theorem 3.1.5 (rules for divisibility)**. (a)** We have $a \mid a$ for each $a \in \mathbb{Z}$. (This is called **reflexivity of divisibility**.)

(b) If $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$. (This is called **transitivity of divisibility**.)

(c) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$, then $a_1 a_2 \mid b_1 b_2$. (This is called **multiplying two divisibilities**.)

(d) If $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$, then $d \mid a + b$. (This is often restated as "a sum of two multiples of d is again a multiple of d".)

Proof. **(a)** Let $a \in \mathbb{Z}$. Then, $a = a \cdot 1$, so that $a \mid a$ (since 1 is an integer). This proves Theorem 3.1.5 **(a)**.

(b) Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$.
From $a \mid b$, we see that there exists an integer x such that $b = ax$.
From $b \mid c$, we see that there exists an integer y such that $c = by$.
Consider these integers x and y. Now,

$$c = \underbrace{b}_{=ax} y = axy.$$

Hence, there exists some integer z such that $c = az$ (namely, $z = xy$). This shows that $a \mid c$. Theorem 3.1.5 **(b)** is thus proven.

(c) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$.
From $a_1 \mid b_1$, we see that $b_1 = a_1 c_1$ for some integer c_1.
From $a_2 \mid b_2$, we see that $b_2 = a_2 c_2$ for some integer c_2.
Consider these integers c_1 and c_2. Now,

$$\underbrace{b_1}_{=a_1 c_1} \underbrace{b_2}_{=a_2 c_2} = a_1 c_1 a_2 c_2 = (a_1 a_2) \underbrace{(c_1 c_2)}_{\text{an integer}}.$$

Thus, $a_1 a_2 \mid b_1 b_2$. This proves Theorem 3.1.5 **(c)**.

(d) Let $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$.
From $d \mid a$, we see that $a = dx$ for some integer x.
From $d \mid b$, we see that $b = dy$ for some integer y.
Consider these integers x and y. Now,

$$a + b = dx + dy = d \underbrace{(x + y)}_{\text{an integer}}.$$

Thus, $d \mid a + b$. This proves Theorem 3.1.5 **(d)**. □

Theorem 3.1.5 **(b)** tells us that divisibilities can be chained together: If $a \mid b$ and $b \mid c$, then $a \mid c$. Therefore, you will often see a statement of the form "$a \mid b$ and $b \mid c$" rewritten as "$a \mid b \mid c$", just like two inequalities $a \leq b$ and $b \leq c$ can be chained together to form $a \leq b \leq c$. More generally, the statement

$$"a_1 \mid a_2 \mid \cdots \mid a_k"$$

shall mean that each of the numbers $a_1, a_2, \ldots, a_k$ divides the next (i.e., that $a_1 \mid a_2$ and $a_2 \mid a_3$ and so on, ending with $a_{k-1} \mid a_k$). By induction on k, it is easy to see that such a chain of divisibilities always entails $a_1 \mid a_k$.

How can you spot divisibilities between actual numbers? For small values of a, there are several known **divisibility criteria**, which give simple methods to check whether a given integer b is divisible by a (without computing $\frac{b}{a}$). Here are some:

Theorem 3.1.6. Let $b \in \mathbb{N}$. Write b in decimal notation. Then:
(a) We have $2 \mid b$ if and only if the last digit of b is 0 or 2 or 4 or 6 or 8.
(b) We have $5 \mid b$ if and only if the last digit of b is 0 or 5.
(c) We have $10 \mid b$ if and only if the last digit of b is 0.
(d) We have $3 \mid b$ if and only if the sum of the digits of b is divisible by 3.
(e) We have $9 \mid b$ if and only if the sum of the digits of b is divisible by 9.

Example 3.1.7. Let $b = 10835$. Then, $2 \nmid b$, since the last digit of b is neither 0 nor 2 nor 4 nor 6 nor 8 (but 5). However, $5 \mid b$, since the last digit of b is 0 or 5. Do we have $3 \mid b$? The sum of the digits of b is $1 + 0 + 8 + 3 + 5 = 17$, which is not divisible by 3. Thus, b is not divisible by 3. Hence, b is not divisible by 9 either, because if we had $9 \mid b$, then we would get $3 \mid 9 \mid b$ (by Theorem 3.1.5 **(b)**), which would contradict the previous sentence.

How do we prove Theorem 3.1.6?

The easiest part is part **(c)**: If you multiply a number (written in decimal) by 10, then its decimal representation just grows a new digit 0 at the end. Thus, if $10 \mid b$, then the last digit of b is 0. Conversely, if the last digit of b is 0, then $b = 10b'$, where b' is the number b with its last digit removed. For example, $390 = 10 \cdot 39$.

Parts **(a)** and **(b)** of Theorem 3.1.6 are somewhat trickier, and parts **(d)** and **(e)** more so. To get simple proofs for these parts, we will now introduce another type of relation between integers, known as **congruence modulo** n.

3.2. Congruence modulo n

3.2.1. Definition

Definition 3.2.1. Let $n, a, b \in \mathbb{Z}$. We say that a is **congruent to** b **modulo** n if and only if $n \mid a - b$.

We shall use the notation "$a \equiv b \bmod n$" for "a is congruent to b modulo n".

We shall use the notation "$a \not\equiv b \bmod n$" for "a is not congruent to b modulo n".

Example 3.2.2. (a) Is $3 \equiv 7 \bmod 2$? This would mean that $2 \mid 3 - 7$, which is true (since $3 - 7 = -4 = 2 \cdot (-2)$). So yes, we do have $3 \equiv 7 \bmod 2$.

(b) Is $3 \equiv 6 \bmod 2$? This would mean that $2 \mid 3 - 6$, which is false (since $3 - 6 = -3$ is not divisible by 2). So we have $3 \not\equiv 6 \bmod 2$.

(c) We have $a \equiv b \bmod 1$ for any integers a and b. This is because $1 \mid a - b$ (since 1 divides every integer).

(d) Two integers a and b satisfy $a \equiv b \bmod 0$ if and only if $a = b$ (since 0 divides only 0 itself).

(e) For any two integers a and b, we have $a + b \equiv a - b \bmod 2$, since $(a + b) - (a - b) = 2b$ is clearly divisible by 2.

The word "modulo" in the phrase "a is congruent to b modulo n" has been invented by Gauss and should be read as something like "with respect to". You can translate the statement "a is congruent to b modulo n" as "a equals b up to a multiple of n". Indeed, the definition of congruence can be restated as follows:

$$a \equiv b \bmod n \qquad \text{if and only if} \qquad a = b + nc \text{ for some } c \in \mathbb{Z}.$$

As we will soon see, congruence modulo 2 is essentially parity:

- Two even numbers are always congruent (to each other) modulo 2.
- Two odd numbers are always congruent (to each other) modulo 2.
- An even number is never congruent to an odd number modulo 2.

We will soon prove this.

3.2.2. Basic properties

First, we shall prove some fundamental properties of congruence.

Proposition 3.2.3. Let $n, a \in \mathbb{Z}$. Then, $a \equiv 0 \bmod n$ if and only if $n \mid a$.

Proof. By the definition of congruence, we have the following equivalences:

$$(a \equiv 0 \bmod n) \iff (n \mid a - 0) \iff (n \mid a).$$

Proposition 3.2.3 thus follows. □

Proposition 3.2.4. Let $n \in \mathbb{Z}$. Then:

(a) We have $a \equiv a \bmod n$ for every $a \in \mathbb{Z}$. (This is called the **reflexivity of congruence**.)

(b) If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $b \equiv a \bmod n$. (This is called the **symmetry of congruence**.)

(c) If $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$. (This is called the **transitivity of congruence**.)

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n,$$

then

$$a_1 + a_2 \equiv b_1 + b_2 \bmod n; \tag{1}$$
$$a_1 - a_2 \equiv b_1 - b_2 \bmod n; \tag{2}$$
$$a_1 a_2 \equiv b_1 b_2 \bmod n. \tag{3}$$

(In other words, two congruences modulo n can be added, subtracted or multiplied.)

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $a \equiv b \bmod m$.

Proof. **(a)** Let $a \in \mathbb{Z}$. Then, $n \mid a - a$ because $a - a = 0 = n \cdot 0$. But this means that $a \equiv a \bmod n$. Thus, Proposition 3.2.4 **(a)** follows.

(b) Let $a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$. Thus, $n \mid a - b$.

We must prove that $b \equiv a \bmod n$, i.e., that $n \mid b - a$.

However, $b - a = (a - b) \cdot (-1)$, so that $a - b \mid b - a$. Hence, $n \mid a - b \mid b - a$. Therefore, by the transitivity of divisibility, $n \mid b - a$. But this means precisely that $b \equiv a \bmod n$. Thus, Proposition 3.2.4 **(b)** is proved.

(c) Let $a, b, c \in \mathbb{Z}$ be such that $a \equiv b \bmod n$ and $b \equiv c \bmod n$.

From $a \equiv b \bmod n$, we obtain $n \mid a - b$.

From $b \equiv c \bmod n$, we obtain $n \mid b - c$.

Recall that a sum of two multiples of n is again a multiple of n (this is Theorem 3.1.5 **(d)**). Thus, from $n \mid a - b$ and $n \mid b - c$, we obtain $n \mid (a - b) + (b - c)$. Since $(a - b) + (b - c) = a - c$, we can rewrite this as $n \mid a - c$. In other words, $a \equiv c \bmod n$. This proves Proposition 3.2.4 **(c)**.

(d) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n.$$

Thus, $n \mid a_1 - b_1$ and $n \mid a_2 - b_2$.

From $n \mid a_1 - b_1$, we see that $a_1 - b_1 = nc_1$ for some integer c_1.

From $n \mid a_2 - b_2$, we see that $a_2 - b_2 = nc_2$ for some integer c_2.

Consider these integers c_1 and c_2.

From $a_1 - b_1 = nc_1$, we obtain $a_1 = b_1 + nc_1$. Similarly, $a_2 = b_2 + nc_2$.

Adding the equalities $a_1 = b_1 + nc_1$ and $a_2 = b_2 + nc_2$ together, we find

$$a_1 + a_2 = (b_1 + nc_1) + (b_2 + nc_2) = b_1 + b_2 + n(c_1 + c_2).$$

Thus, $a_1 + a_2$ differs from $b_1 + b_2$ by a multiple of n (namely, by $n(c_1 + c_2)$). In other words, $n \mid (a_1 + a_2) - (b_1 + b_2)$. Hence,

$$a_1 + a_2 \equiv b_1 + b_2 \bmod n.$$

Subtracting the equalities $a_1 = b_1 + nc_1$ and $a_2 = b_2 + nc_2$ from one another, we obtain

$$a_1 - a_2 = (b_1 + nc_1) - (b_2 + nc_2) = b_1 - b_2 + n(c_1 - c_2).$$

Thus, $a_1 - a_2$ differs from $b_1 - b_2$ by a multiple of n (namely, by $n(c_1 - c_2)$). Hence,

$$a_1 - a_2 \equiv b_1 - b_2 \bmod n.$$

Multiplying the equalities $a_1 = b_1 + nc_1$ and $a_2 = b_2 + nc_2$ together, we find

$$\begin{aligned} a_1 a_2 &= (b_1 + nc_1)(b_2 + nc_2) = b_1 b_2 + b_1 nc_2 + nc_1 b_2 + nc_1 nc_2 \\ &= b_1 b_2 + n(b_1 c_2 + c_1 b_2 + nc_1 c_2). \end{aligned}$$

Thus, $a_1 a_2$ differs from $b_1 b_2$ by a multiple of n (namely, by $n(b_1 c_2 + c_1 b_2 + nc_1 c_2)$). Therefore,

$$a_1 a_2 \equiv b_1 b_2 \bmod n.$$

Altogether, we have proved all claims of Proposition 3.2.4 **(d)** now.

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$.

Thus, $n \mid a - b$. Hence, $m \mid n \mid a - b$, so that $m \mid a - b$ (by the transitivity of divisibility). But this means that $a \equiv b \bmod m$. Thus, Proposition 3.2.4 **(e)** follows. □

Proposition 3.2.4 **(b)** says that congruences can be turned around: From $a \equiv b \bmod n$, we can always obtain $b \equiv a \bmod n$. (This is very different from divisibilities, for which $a \mid b$ almost never implies $b \mid a$.)

Proposition 3.2.4 **(c)** says that congruences can be chained together: From $a \equiv b \bmod n$ and $b \equiv c \bmod n$, we can always obtain $a \equiv c \bmod n$. This is analogous to Theorem 3.1.5 **(b)**, and leads to a similar convention: Instead of writing "$a \equiv b \bmod n$ and $b \equiv c \bmod n$", we will often just write "$a \equiv b \equiv c \bmod n$", understanding that (by Proposition 3.2.4 **(c)**) this chain of congruences automatically implies $a \equiv c \bmod n$. More generally, the statement

$$\text{"}a_1 \equiv a_2 \equiv \cdots \equiv a_k \bmod n\text{"}$$

shall mean that each of the numbers $a_1, a_2, \ldots, a_k$ is congruent to the next modulo n (i.e., that $a_i \equiv a_{i+1} \bmod n$ for each $i \in \{1, 2, \ldots, k-1\}$). By induction on k, it is easy to see that such a chain of congruences always entails $a_1 \equiv a_k \bmod n$ (and, better yet: $a_i \equiv a_j \bmod n$ for all i and j).

Note that we can only chain together two congruences modulo the same n, not two congruences modulo two different n's. For example, if we know that $a \equiv b \bmod 2$ and $b \equiv c \bmod 3$, then we cannot conclude any congruence between a and c.

Proposition 3.2.4 **(d)** says that congruences modulo n (for a fixed integer n) can be added, subtracted and multiplied together (just like equalities). Before you get over-enthusiastic, keep in mind that

- they cannot be divided by one another: We have $2 \equiv 0 \bmod 2$ and $2 \equiv 2 \bmod 2$ but $2/2 \not\equiv 0/2 \bmod 2$.
- they cannot be taken to each other's power: We have $2 \equiv 2 \bmod 2$ and $2 \equiv 0 \bmod 2$ but $2^2 \not\equiv 2^0 \bmod 2$.

However, we can take a congruence to a k-th power for a fixed $k \in \mathbb{N}$:

Exercise 1. Let $n, a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$. Let $k \in \mathbb{N}$. Prove that $a^k \equiv b^k \bmod n$.

This exercise is Exercise 1 **(b)** on homework set #3.

Now, let us prove Theorem 3.1.6 **(e)**, restating it as follows:

Proposition 3.2.5. Let $m \in \mathbb{N}$. Let s be the sum of the digits of m written in decimal. (For instance, if $m = 302$, then $s = 3 + 0 + 2 = 5$.)
Then, $9 \mid m$ if and only if $9 \mid s$.

Proof. Let the integer m have decimal representation $m_d m_{d-1} \cdots m_0$ (where m_d is the leading digit). Thus,

$$m = m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0 \qquad \text{and}$$
$$s = m_d + m_{d-1} + \cdots + m_0.$$

However, $10 \equiv 1 \bmod 9$ (since $10 - 1 = 9$ is divisible by 9). Hence, by Exercise 1, we have $10^k \equiv 1^k \bmod 9$ for every $k \in \{0, 1, \ldots, d\}$. Multiplying this congruence with the obvious congruence $m_k \equiv m_k \bmod 9$, we obtain[1]

$$m_k \cdot 10^k \equiv m_k \cdot 1^k \bmod 9 \qquad \text{for every } k \in \{0, 1, \ldots, d\}.$$

[1] The reason why we can multiply two congruences together is Proposition 3.2.4 **(d)** (specifically, (3)).

In other words,

$$m_k \cdot 10^k \equiv m_k \bmod 9 \qquad \text{for every } k \in \{0, 1, \ldots, d\}$$

(since $m_k \cdot \underbrace{1^k}_{=1} = m_k$). In other words, we have

$$\begin{aligned} m_d \cdot 10^d &\equiv m_d \bmod 9; \\ m_{d-1} \cdot 10^{d-1} &\equiv m_{d-1} \bmod 9; \\ m_{d-2} \cdot 10^{d-2} &\equiv m_{d-2} \bmod 9; \\ &\ldots; \\ m_0 \cdot 10^0 &\equiv m_0 \bmod 9. \end{aligned}$$

Adding these $d+1$ many congruences together, we obtain[2]

$$m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0 \equiv m_d + m_{d-1} + \cdots + m_0 \bmod 9.$$

In other words,

$$m \equiv s \bmod 9$$

(since $m = m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0$ and $s = m_d + m_{d-1} + \cdots + m_0$). Turning this congruence around (i.e., applying Proposition 3.2.4 **(b)**), we obtain $s \equiv m \bmod 9$.

Now, if $9 \mid m$, then $m \equiv 0 \bmod 9$ (by Proposition 3.2.3), whence $s \equiv m \equiv 0 \bmod 9$ (here we are tacitly using Proposition 3.2.4 **(c)**), which entails $9 \mid s$ (again by Proposition 3.2.3). Thus, we have shown that if $9 \mid m$, then $9 \mid s$.

Conversely, if $9 \mid s$, then $s \equiv 0 \bmod 9$ (by Proposition 3.2.3), whence $m \equiv s \equiv 0 \bmod 9$, which in turn entails $9 \mid m$ (by Proposition 3.2.3). Thus, we have shown that if $9 \mid s$, then $9 \mid m$.

Now we have proved that each of the statements $9 \mid m$ and $9 \mid s$ implies the other. In other words, we have $9 \mid m$ if and only if $9 \mid s$. This proves the proposition. □

In other words, Theorem 3.1.6 **(e)** is proven. A similar argument (with 9 replaced by 3) can be used to prove Theorem 3.1.6 **(d)**. In fact, $s \equiv m \bmod 9$ entails $s \equiv m \bmod 3$ by Proposition 3.2.4 **(e)**, because $3 \mid 9$.

Parts **(a)** and **(b)** of Theorem 3.1.6 can be proved along similar lines, but are in fact easier. Indeed, if $m \in \mathbb{N}$ has decimal representation $m_d m_{d-1} \cdots m_0$, then $m \equiv m_0 \bmod 10$ (since the number $m - m_0$ has decimal representation $m_d m_{d-1} \cdots m_1 0$ and thus is divisible by 10), and therefore (by Proposition 3.2.4 **(e)**) we have $m \equiv m_0 \bmod 2$ and $m \equiv m_0 \bmod 5$ as well.

[2]The reason why we can add two congruences together is Proposition 3.2.4 **(d)** (specifically, (1)). To be very pedantic, we have to apply (1) several times, since we are adding not two but $d+1$ many congruences together.

References

[Martin17] Kimball Martin, *An (algebraic) introduction to Number Theory, Fall 2017*, December 25, 2017.

[Shoup08] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, 2nd edition, Cambridge University Press 2008, with errata 2017.

[Stein08] William Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer 2008, updated version 2017.