MATH1050 Basic results on divisibility

1. Here is a (probably not exhaustive) list of properties of the integer system needed in the proofs of the results below. We have been tacitly assuming them (together with some others not mentioned here) since school-days. We will (be made to) look into them and formulate them more carefully in order to study them when we are doing an *algebra* course or an *analysis* course.

   (a) *The sum, the difference, and the product of any two (not necessarily distinct) integers are integers.*
   In symbols, this reads:

   Suppose $x, y \in \mathbb{Z}$. Then $x + y \in \mathbb{Z}$, $x - y \in \mathbb{Z}$, and $xy \in \mathbb{Z}$.

   These 'operations' obey certain 'laws of arithmetic' which we have learnt and accepted since school days.

   (b) *The sum and the product of any two (not necessarily distinct) positive integers are positive integers. Moreover, every integer is either positive or negative or zero.*

2. **Definition. (Divisibility.)**

   Let u, v be integers.

   u is said to be **divisible** *by v if there exists some integer k such that $u = kv$.*

   Digression on logic.

   How to read and use the passage which we refer to as 'definition for divisibility'?

   (a) This passage explains the word '*divisible*' in the 'world of integers' by telling us what exactly is meant by the statement

   ($\star$) '*(the integer) u is divisible by (the integer) v*'.

   It is:

   ($\star\star$) '*there exists some integer k such that $u = kv$.*'

   The word '*if*' which links ($\star$) and ($\star\star$) in the passage should be understood as '*if and only if*'.

   Remark. Before you start considering for a given pair of objects u, v whether it is true that u is divisible by v, you have to make sure that u, v are integers in the first place.

   (b) Suppose it is already known (whether proved or assumed) that a given integer x is divisible by a given integer y.

   Question. What does this definition provides in the context of deducing something else from the statement '*x is divisible by y*'?

   Answer. According to definition, the statement

   '*there exists some integer k such that $x = ky$*'

   holds. This tells us three things, which we can use subsequently:

   (1) x, y collectively 'generates' an object k. This k is an object which may 'depend' on x, y.

   (2) This k is an integer.

   (3) This k is related to x, y through the equality $x = ky$.

   (c) Suppose it is known that x, y are integers.

   Question. What to do to verify the statement '*x is divisible by y*' according to definition?

   Answer. To verify this statement is the same as to verify the statement

   '*there exists some integer k such that $x = ky$*',

   It suffices to name some candidate object k which we hope will satisfy simultaneously:

   (1) k is an integer.

   (2) $x = ky$.

   And then, verify (1), (2) are indeed satisfied by the named candidate.

   (It does not matter how an appropriate candidate is found. Of course, if none is found, none can be named for the completion of the argument.)

3. **Examples on divisibility.**

(a) 6 *is divisible by* 2.

Justification.

[Roughwork.

According to definition, this statement reads: '*there exists some integer* k *such that* $6 = k \cdot 2$.'

To justify this statement, we name a concrete object k which satisfies simultaneously: (1) k is an integer, and (2) $6 = k \cdot 2$.]

$6 = 3 \cdot 2$ and 3 is an integer.

(b) 8 *is divisible by* -2.

Justification. $8 = (-4) \cdot (-2)$ and -4 is an integer.

(c) 0 *is divisible by* 0.

Justification. $0 = 1 \cdot 0$ and 1 is an integer.

(d) *No integer except* 0 *is divisible by* 0.

Formally presented, this reads:

'*Let* x *be an integer. Suppose* x *is divisible by* 0. *Then* $x = 0$.'

Justification.

Let x be an integer. Suppose x is divisible by 0. [Ask: $x = 0$?]

By definition, there exists some integer k such that $x = k \cdot 0$.

Then $x = 0$.

4. **Theorem (1). (Properties of divisibility.)**

The statements below hold:

(a) *Suppose* x *is an integer. Then* x *is divisible by* x.

(b) *Let* x, y *be integers. Suppose* x *is divisible by* y *and* y *is divisible by* x. *Then* $|x| = |y|$.

(c) *Let* x, y, z *be integers. Suppose* x *is divisible by* y *and* y *is divisible by* z. *Then* x *is divisible by* z.

We are going to prove Statement (a) and Statement (c). The proof of Statement (b) is left as an exercise.

5. **Proof of Statement (a) of Theorem (1)**.

Let $x \in \mathbb{Z}$. [What to prove? Un-wrap definition.]

$x = 1 \cdot x$.

Note that $1 \in \mathbb{Z}$.

[So there indeed exists some $k \in \mathbb{Z}$, namely, $k = 1$, such that $x = kx$.]

Hence x is divisible by x.

6. **Proof of Statement (c) of Theorem (1).**

Let $x, y, z \in \mathbb{Z}$.

Suppose x is divisible by y and y is divisible by z.

[Roughwork.

What to deduce? 'x *is divisible by* z'. This, according to definition, is:

'there exists some integer k such that $x = kz$.'

What is the objective? To name an appropriate object k which simultaneously satisfies: (1) k is an integer, and (2) $x = kz$.

How? See what information the assumption is providing.]

Since x is divisible by y, there exists some $g \in \mathbb{Z}$ such that $x = gy$.

Since y is divisible by z, there exists some $h \in \mathbb{Z}$ such that $y = hz$.

Now $x = ghz$.

Since $g, h \in \mathbb{Z}$, we have $gh \in \mathbb{Z}$.

[So there indeed exists some $k \in \mathbb{Z}$, namely, $k = gh$, such that $x = kz$.]

Then x is divisible by z.

7. **Theorem (2). (Further properties of divisibility.)**

Let n be integers. The statements below hold:

(a) *Let x, y be integers. Suppose x is divisible by n and y is divisible by n. Then $x + y$ is divisible by n.*

(b) *Let x, y be integers. Suppose x is divisible by n or y is divisible by n. Then xy is divisible by n.*

Proof of Theorem (2). Exercise.

8. **Examples on divisibility and mathematical induction.**

(a) *$n^3 - n$ is divisible by 3 for any $n \in \mathbb{N}$.*

Justification (by mathematical induction).

For any $n \in \mathbb{N}$, denote by $P(n)$ the proposition

'$n^3 - n$ is divisible by 3'.

- $0^3 - 0 = 0 = 0 \cdot 3$ and $0 \in \mathbb{Z}$.
  Hence, by definition, $0^3 - 0$ is divisible by 3.
  Then $P(0)$ is true.
- Let $k \in \mathbb{N}$. Suppose $P(k)$ is true. Then $k^3 - k$ is divisible by 3.
  We prove that $P(k+1)$ is true:

  By definition, there exists some $q \in \mathbb{Z}$ such that $k^3 - k = 3q$.
  We have $(k+1)^3 - (k+1) = (k^3 - k) + 3k^2 + 3k = 3(q + k^2 + k)$.
  Since $q, k \in \mathbb{Z}$, we have $q + k^2 + k \in \mathbb{Z}$.
  Then, by definition, $(k+1)^3 - (k+1)$ is divisible by 3.
  Hence $P(k+1)$ is true.

By the Principle of Mathematical Induction, $P(n)$ is true for any $n \in \mathbb{N}$.

(b) The statements below can be proved with the help of mathematical induction.

i. *$n(2n^2 + 1)$ is divisible by 3 for any $n \in \mathbb{N}$.*

ii. *$(2n+1)(2n+3)(2n+5)$ is divisible by 3 for any $n \in \mathbb{N}$.*

iii. *$(2n+1)(2n+3)(2n+5)(2n+7)(2n+9)$ is divisible by 5 for any $n \in \mathbb{N}$.*

iv. *$2^{4n+3} + 3^{3n+1}$ is divisible by 11 for any $n \in \mathbb{N}$.*

v. *$2^{n+1} + 3^{2n-1}$ is divisible by 7 for any positive integer n.*

9. **Definition. (Prime numbers.)**

Let p be an integer. Suppose $p \neq -1$ and $p \neq 0$ and $p \neq 1$. Then we say p is a prime number if the statement (PR) holds:

(PR) *p is divisible by no integer other than $1, -1, p, -p$.*

Remark. A more useful formulation of the statement (PR) is given below:

(PR') *Let u be an integer. Suppose p is divisible by u. Then $u = 1$ or $u = -1$ or $u = p$ or $u = -p$.*

10. **Definition. (Composite numbers.)**

Let n be an integer. Suppose $n \neq -1$ and $n \neq 0$ and $n \neq 1$. Then we say n is a composite number if n is not a prime number.

Remark. Such a formulation for the notion of *composite numbers* is not user-friendly because the 'defining condition' '*n is not a prime number*' involves the word *not*, and hence is difficult to use in practice.

11. **Theorem (3). (Re-formulation of the definition of composite numbers.)**

Let n be an integer. Suppose $n \neq -1$ and $n \neq 0$ and $n \neq 1$.

Then n is a composite number if and only if the statement (CO) holds:

(CO) *There exist some integers u, v such that $n = uv$ and $1 < |u| < |n|$ and $1 < |v| < |n|$.*

Remark. In plain words, Theorem (3) is saying that a given integer n is a composite number exactly when it is possible to express n as a product of two integers of strictly smaller magnitude.

Then in light of its definition, a given integer p is a prime number exactly when it is impossible to express p as a product of two integers of strictly smaller magnitude.

12. **Examples on prime numbers and composite numbers.**

    (a) $\pm 2, \pm 3, \pm 5, \pm 7, \cdots$ are prime numbers.

    (b) $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \cdots$ are composite numbers.

    Remark. Determining whether an arbitrary given integer is a prime number or a composite number can be 'difficult' in the sense that there is no known 'general formula' giving every prime number. Theorem (3) is all we have.

13. **Proof of Theorem (3).**

    Let n be a integer. Suppose $n \neq -1$ and $n \neq 0$ and $n \neq 1$.

    [We are going to verify the two logically independent statements below:

    (a) *Suppose* (CO) *holds. Then* n *is a composite number.*

    (b) *Suppose* n *is a composite number. Then* (CO) *holds.*

    This will be done in two separate paragraphs.]

    (a) Suppose that there exist some integers u, v such that $n = uv$ and $1 < |u| < |n|$ and $1 < |v| < |n|$.

        [We want to deduce that n is a composite number.
        What is it according to definition? '*u is not a prime number.*'
        So what we really want to deduce is: *n is divisible by some integer other than* $1, -1, n, -n$.
        Ask: How to name such an integer?]

        By definition of divisibility, n is divisible by u.

        Since $|u| > 1$, we have $u \neq 1$ and $u \neq -1$.

        Since $|u| < n$, we have $u \neq n$ and $u \neq -n$.

        Then n is divisible by some integer, namely u, which is not amongst $1, -1, n, -n$.

        By definition, n is not a prime number. Hence n is a composite number.

    (b) Suppose n is a composite number.

        [We want to deduce the statement (CO).
        This amounts to verifying '*there exists some integers* u, v *such that* $n = uv$ *and* $1 < |u| < |n|$ *and* $1 < |v| < |n|$'.
        Ask: How to name appropriate u, v?]

        Then n is not a prime number.

        Therefore n is divisible by some integer, say, u, which is not amongst $1, -1, n, -n$.

        By definition, there exists some integer v such that $n = uv$.

        [Reminder. Now we have some candidate u, v. It remains to see whether $1 < |u| < |n|$ and $1 < |v| < |n|$.]

        We have $|n| = |uv| = |u| \cdot |v|$.

        Recall that $n \neq 0$. Then $|u| \neq 0$ and $|v| \neq 0$. Therefore $|u| \geq 1$ and $|v| \geq 1$.

        Since u is not amongst $1, -1$, we have $|u| > 1$.

        Since $|v| \geq 1$, we have $|n| = |u| \cdot |v| \geq |u|$. Since u is not amongst $n, -n$, we have $|u| < |n|$.

        Therefore $1 < |u| < |n|$.

        Since $|n| = |u| \cdot |v|$ and $1 < |u| < |n|$, we have $1 < |v| < |n|$.