REVIEW: Basic Notation and Properties of the Integers

We will standard notation for the following number systems:

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the set of all *integers*;

$\mathbb{N} = \{1, 2, 3, \ldots\}$, the set of all *natural numbers*;

$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\right\}$, the set of all *rational numbers*;

$\mathbb{R}$, the set of real numbers, including $\mathbb{Q}$ but also π, $\sqrt{2}$, etc.; intuitively, all numbers on the 'number line';

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ where $i = \sqrt{-1}$, the set of all *complex numbers*.

Number theory is concerned primarily with properties of $\mathbb{Z}$; but to fully understand $\mathbb{Z}$ often requires raising our sights to other number systems, as we shall see.

Let a and b be integers. We say that a *divides* b, if $b = ka$ for some integer k. In symbols, this relationship is written as $a \mid b$. In this case we also say that a is a *divisor* of b, or that b is a *multiple* of a. If this relation does not hold, i.e. a does not divide b, we write $a \nmid b$. Thus, for example, we have $3 \mid 6$ and $4 \nmid 6$. The number 6 has exactly eight divisors: 1, 2, 3, 6, -1, -2, -3 and -6.

Divisibility is an example of a *relation*. Another example of a relation is the 'less than relation'; thus, for example, 5 is *less than* 7, denoted $5 < 7$. We distinguish between *relations* and *operations*. Operations, such as addition (as in '$5 + 7$') and multiplication (as in '5×7') yield numerical values; not so for a relation such as '$5 < 7$' which is simply a statement expressing a relationship between two numbers. Thus for any two numbers a and b, the statement $a < b$ is either true or false; but it does not have a numerical value. Just so for divisibility: $a|b$ is either true or false, depending on the values of a and b; but it is a statement, not a number. We have not yet begun to divide (which would be an operation).

Several properties of divisibility are well known and easily verified; for example

Proposition 1. *Let a, b, c be integers.*

(a) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(b) If c divides both a and b, then c also divides their sum $a + b$ as well as their difference $a - b$.

Proof. If $b = ka$ and $c = \ell b$ for some integers k and ℓ, then $c = (k\ell)a$. This proves (a).

Next, suppose $a = rc$ and $b = sc$; then $a + b = (r + s)c$ and $a - b = (r - s)c$. This proves (b). $\square$

The divisors of 6 are $\pm1, \pm2, \pm3, \pm6$. The divisors of 20 are $\pm1, \pm2, \pm4, \pm5, \pm10, \pm20$. The numbers 6 and 20 have four *common divisors* are $\pm1, \pm2$, of which the largest is 2. We write $gcd(6, 20) = 2$ (the *greatest common divisor* of 6 and 20 is 2).

Note that every integer divides 0. (For example, 5 divides 0 since $5 = 5 \times 0$.) The divisors of 0 are $0, \pm1, \pm2, \pm3, \ldots$. The common divisors of 6 and 0 are $\pm1, \pm2, \pm3, \pm6$, the greatest of which is 6; thus $gcd(6, 0) = 6$.

Similarly we can define $gcd(a, b)$ for any two integers a and b, provided that a and b are not both zero. (The value of $gcd(0, 0)$ is undefined since the common divisors of 0 and 0 include all integers, of which there is no largest.) Two integers a and b are *relatively prime*, or *coprime*, if $gcd(a, b) = 1$.

An integer $n > 1$ is *prime* if its only positive divisors are 1 and n; otherwise it is *composite*. The number 1 is in a class by itself, neither prime nor composite.

The Division Algorithm

Now we will start to divide! Let a and d be integers with d positive. There exist unique integers q and r such that

$$a = qd + r \quad \text{and} \quad r \in \{0, 1, 2, \ldots, d - 1\}.$$

'Unique' means that there is only one choice for q and r satisfying these conditions. We q the *quotient*, and r the *remainder*, when a is *divided* by d. Note that d divides a iff the remainder $r = 0$.
Examples:

$70 = 6 \times 11 + 4$. When 70 is divided by 11, the quotient is 6 and the remainder is 4. Clearly $11 \not| 70$.

$70 = 5 \times 11 + 15$. However, 15 is not in the required range $\{0, 1, 2, \ldots, 10\}$, so it is not the remainder (and 5 is not the quotient).

$-70 = (-7) \times 11 + 7$. When -70 is divided by 11, the quotient is -7 and the remainder is 7.

Congruences

Fix a positive integer n. Given integers a and b, we say that a is *congruent* to b (modulo n) if $b - a$ is divisible by n; in symbols, this is written $a \equiv b \mod n$ (or if the choice of modulus n is understood, we simply write $a \equiv b$). If this relation does not hold, i.e. a is *not* congruent to b, we write $a \not\equiv b$. The following properties hold for congruences:

Proposition 2. *Fix a positive integer n as the modulus in each of the following congruences. For all integers a, b, c we have*
(a) $a \equiv a$.
(b) If $a \equiv b$ then $b \equiv a$.
(c) If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.
(d) If $a \equiv b$ and $c \equiv d$, then $a + c \equiv b + d$ and $ac \equiv bd$.

Properties (a)–(c) say that congruence modulo n is an equivalence relation. Property (d) says that sums and products are well-defined for congruence classes.

Proof. Since $a - a = 0$ is divisible by n, (a) holds. If $b - a = kn$ then $a - b = (-k)n$, which proves (b). If $b - a$ and $c - b$ are divisible by n then so is their sum $c - a = (b - a) + (c - b)$ by Proposition 1; this proves (c).

If $b - a = rn$ and $d - c = sn$, then $(b + d) - (a + c) = (r + s)n$ so $a + c \equiv b + d$; also

$$bd - ac = (b - a)d + (d - c)a = rnd + sna = (rd + sa)n$$

so $ac \equiv bd$. □

Let us use congruences to show that the equations $x^2 - 3y^2 = 104$ has no solution in integers. First observe that for every integer a, we have $a^2 \equiv 0$ or $1 \mod 3$. (By the Division Algorithm, we have $a = 3q + r$ for some $r \in \{0, 1, 2\}$ so $a \equiv 0$, 1 or $2 \mod 3$; and we check that $a^2 \equiv 0$ or $1 \mod 3$ in each case.) It follows that $x^2 - 3y^2 \equiv 0$ or $1 \mod 3$ for all integers x, y; however $104 \equiv 2 \mod 3$.

Modular Arithmetic

Again fix a positive integer n. The set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$ is a number system with addition and multiplication defined modulo n. Thus for example the number system $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ has addition and multiplication defined by the tables

Addition in $\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplication in $\mathbb{Z}_4$

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

A statement like $2+3 = 1$, valid in $\mathbb{Z}_4$, must not be taken out of context; the statement does not hold in $\mathbb{Z}$, where the operation of addition, and the numbers themselves, have a different meaning. To be precise, we should use different symbols in $\mathbb{Z}_4$. This is often resolved by denoting $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ or $\{[0]_4, [1]_4, [2]_4, [3]_4\}$ where the new symbols represent the congruence classes modulo 4:

$$\overline{0} = 4\mathbb{Z} = \{4k \,:\, k \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, 12, 16, \ldots\};$$
$$\overline{1} = 4\mathbb{Z} + 1 = \{4k + 1 \,:\, k \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, 13, 17, \ldots\};$$
$$\overline{2} = 4\mathbb{Z} + 2 = \{4k + 2 \,:\, k \in \mathbb{Z}\} = \{\ldots, -6, -2, 2, 6, 10, 14, 18, \ldots\};$$
$$\overline{3} = 4\mathbb{Z} + 3 = \{4k + 3 \,:\, k \in \mathbb{Z}\} = \{\ldots, -5, -1, 3, 7, 11, 15, 19, \ldots\}.$$

These are simply the equivalence classes for the equivalence relation of congruence modulo 4. With this understanding we have

$$\begin{aligned}\overline{2} + \overline{3} &= \{\ldots, -6, -2, 2, 6, \ldots\} + \{\ldots, -5, -1, 3, 7, \ldots\}\\ &= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\} = \overline{1}.\end{aligned}$$

However, we soon find the extra notation tiresome, and drop them the way one outgrows training wheels on a bicycle. At this point our perspective changes: rather than regarding $\mathbb{Z}_4$ as 'coming from $\mathbb{Z}$', we regard $\mathbb{Z}_4$ as a number system that exists in its own right alongside the other number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc. However one should always remember that $\mathbb{Z}_4$ is *not* a subset of $\mathbb{Z}$. The fallacy of this notion (encouraged by our abuse of the symbols $0, 1, 2, 3$ to represent two things in different contexts) is emphasized by the fact that the statement $2+3 = 5 = 1$ is true in $\mathbb{Z}_4$, but false in $\mathbb{Z}$. Similarly, $\mathbb{Z}_3$ is *not* a subset of $\mathbb{Z}_4$, despite our laziness in using the same symbols $\overline{0}, \overline{1}, \overline{2}$ in these different contexts. Note that $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\} = \{[0]_3, [1]_3, [2]_3\}$ where in this context

$$\overline{0} = 3\mathbb{Z} = \{3k \,:\, k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\};$$
$$\overline{1} = 3\mathbb{Z} + 1 = \{3k + 1 \,:\, k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, 10, 13, \ldots\};$$
$$\overline{2} = 3\mathbb{Z} + 2 = \{3k + 2 \,:\, k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}.$$

These are quite different from the elements of $\mathbb{Z}_4$ listed above; and our use of the same symbols is pure laziness. If there is any danger of confusion, we should go back to the old notation

$$[a]_n = n\mathbb{Z} + a = \{kn + a \,:\, k \in \mathbb{Z}\} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \ldots\}.$$