Modular Arithmetic Definitions and Propositions

(1) The “floor” function is defined by the formula

\[\lfloor x \rfloor := ( \text{the greatest integer less than or equal to } x).\]

This is also known as “the greatest integer function,” and in old texts is denoted by (whole) brackets. Examples: \([3.789] = 3; [-3.789] = -4.\]

(2) The “mod” operator is defined as follows:

\[x \mod y := x - y \cdot \lfloor x/y \rfloor\]

if \(y \neq 0\). For positive integers \(x\) and \(y\), \(x \mod y = \text{the remainder in integer division}\)

of \(x\) by \(y\). Examples: 110 mod 26 = 6; -52 mod 26 = 0.

(3) The “mod” relation is defined as follows:

\[a \equiv b \pmod{m}\] if and only if \(a \mod m = b \mod m\).

The above definitions make sense even for real numbers. When \(a, b, m\) are integers

and \(m > 0\),

\[a \equiv b \pmod{m}\] if and only if \(a - b\) is a multiple of \(m\).

Examples: 110 \(\equiv\) 6 (mod 26); -80 \(\equiv\) 24 (mod 26).

(4) Let \(a, b\) be integers. Then \(a|b\), read “\(a\) divides \(b\),” if and only if \(b\) is a multiple, i.e.,

an integer multiple, of \(a\): \(b = ka\) for some integer \(k\). Examples: 7|98; -5|100; but

8 \(\not|\) 26 (8 does not divide 26).

(5) Graham, Knuth, and Patashnik’s divisibility definition (assume that \(a\) and \(b\) are

integers):

\[a \div b\] if and only if \(a > 0\) and \(a|b\).

(6) The “greatest common divisor,” abbreviated gcd, of a set of integers is, of course, the

largest positive integer that divides every integer in the set. Examples: gcd(24, 52) = 4; gcd(54, 42) = 6.

(7) Let \(a, x, m\) be integers with \(m > 0\). Let \(g = \gcd(a, m)\). The number of solutions

of \(ax \equiv b \pmod{m}\) in the set \(\{1, 2, \ldots, m\}\) is 0 if \(g \nmid b\), and is \(g\) if \(g|b\), and

then if \(x_0\) is one solution, then all solutions are given by \(x = x_0 + (m/g)k\) for

\(k = \ldots, -2, -1, 0, 1, 2, 3, \ldots\), and \(g\) of them are in a complete set of residues.

(8) Modular arithmetic and algebra behave “as expected” for the operations of addition,

subtraction, and multiplication. If \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m}\), then \(a + c \equiv b + d \pmod{m}\), \(a - c \equiv b - d \pmod{m}\), and \(ac \equiv bd \pmod{m}\).

(9) But division and cancellation are trickier. Here are the cancellation rules.

\[ad \equiv bd \pmod{m}\] if and only if \(a \equiv b \pmod{m}\), assuming \(\gcd(d, m) = 1\).

\[ad \equiv bd \pmod{m'd}\] if and only if \(a \equiv b \pmod{m'}\), assuming \(d \neq 0\).

Combined: \(ad \equiv bd \pmod{m}\) if and only if \(a \equiv b \pmod{m/\gcd(d, m)}\).