

THE RULES OF MODULAR ARITHMETIC
Math 104 - Dr. Evans
UCSD Winter 2004

Modular arithmetic is the set of rules for addition, subtraction, and multiplication modulo n . The first six rules are the same as integer arithmetic. For all the following rules, let a, b, c, d be integers and n be an integer greater than or equal to 2.

1. Binary Operations If $a \equiv b \pmod{n}$, then

$$a + c \equiv b + c \pmod{n}$$

$$a - c \equiv b - c \pmod{n}$$

$$a \cdot c \equiv b \cdot c \pmod{n}$$

2. Associative Law

$$(a + b) + c \equiv a + (b + c) \pmod{n}$$

$$(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{n}$$

3. Distributive Law

$$a \cdot (b + c) \equiv a \cdot b + a \cdot c \pmod{n}$$

4. Commutative Law

$$a \cdot b \equiv b \cdot a \pmod{n}$$

5. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$a \cdot c \equiv b \cdot d \pmod{n}$$

6. If $a \equiv b \pmod{n}$, then

$$a^k \equiv b^k \pmod{n} \text{ for all positive integers } k$$

Incidentally, rules 3 and 4 allow us to factor polynomials as normal. For example, $x^2 - 1 \equiv (x + 1)(x - 1) \pmod{n}$. However, this does not mean that we can find the zeros of a polynomial simply by setting each of the factors equal to zero (see #10 below).

Some rules are different from integer arithmetic. Be careful not to make these mistakes!

7. Division No division or fractions are allowed. $x \equiv \frac{b}{a} \pmod{n}$ doesn't make sense!

8. Cancellation $a \cdot c \equiv b \cdot c \pmod{n}$ does not imply that $a \equiv b \pmod{n}$.

9. Unique Solutions to Linear Equations $ax \equiv b \pmod{n}$ can have zero, one, or many solutions.

10. Zero Divisors $a \cdot b \equiv 0 \pmod{n}$ does not imply that $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$. In particular, polynomials are allowed to have more solutions than the degree of the polynomial.