2.4 THE INTEGERS AND DIVISION

In mathematics, specifying an axiomatic model for a system precedes all discussion of its properties. The number system serves as a foundation for many other mathematical systems.

Elementary school students learn algorithms for the arithmetic operations without ever seeing a definition of a "number" or of the operations that these algorithms are modeling.

These coursenotes precede discussion of division by the construction of the number system and of the usual arithmetic operations.

AXIOMS for the NATURAL NUMBERS

DEF: The ***natural numbers*** are a mathematical system

$$\mathcal{N} = \{\mathbf{N},\ 0 \in \mathbf{N},\ s : \mathbf{N} \to \mathbf{N}\}$$

in which the number 0 is called ***zero***, and the operation $s : \mathbf{N} \to \mathbf{N}$ is called ***successor***, such that

(1) $(\nexists n)[0 = s(n)]$. Zero is not the successor of any number.

(2) $(\forall m, n \in \mathbf{N})[m \neq n \Rightarrow s(m) \neq s(n)]$. Two different numbers cannot have the same successor.

(3) $(\forall S \subseteq \mathbf{N})\big[(0 \in S) \wedge (\forall n \in S)[s(n) \in S] \Rightarrow S = \mathbf{N}\big]$.

Given a subset S of the natural numbers, suppose that it contains the number 0, and suppose that whenever it contains a number, it also contains the successor of that number. Then $S = \mathbf{N}$.

Remark: Axiom (1) $\Rightarrow$ $\mathbf{N}$ has at least one other number, namely, the successor of zero. Let's call it ***one***. Using Axioms (1) and (2) together, we conclude that $s(1) \notin \{0, 1\}$. Etc.

ARITHMETIC OPERATIONS

DEF: The ***predecessor*** of a natural number n is a number m such that $s(m) = n$.
NOTATION: $p(n)$.

DEF: ***Addition*** of natural numbers.

$$n + m = \begin{cases} n & \text{if } m = 0 \\ s(n) + p(m) & \text{otherwise} \end{cases}$$

DEF: ***Ordering*** of natural numbers.

$$n \geq m \text{ means } \begin{cases} m = 0 \quad \text{or} \\ p(n) \geq p(m) \end{cases}$$

DEF: ***Multiplication*** of natural numbers.

$$n \times m = \begin{cases} 0 & \text{if } m = 0 \\ n + n \times p(m) & \text{otherwise} \end{cases}$$

OPTIONAL: (1) Define ***exponentiation***. (2) Define ***positional representation*** of numbers. (3) Verify that the usual base-ten methods for addition, subtraction, etc. produce correct answers.

DIVISION

DEF: Let n and d be integers with $d \neq 0$. Then d ***divides*** n if there exists a number q such that $n = dq$. NOTATION: $d \backslash n$.

DEF: The integer d is a ***factor*** of n or a ***divisor*** of n if $d \backslash n$.

DEF: A divisor d of n is ***proper*** if $d \neq n$.

DEF: The number one is called a ***trivial divisor***.

DEF: An integer $p \geq 2$ is ***prime*** if p has no nontrivial proper divisors, and ***composite*** otherwise.

Algorithm 2.4.1: Naive Primality Algorithm

Input: positive integer n
Output: smallest nontrivial divisor of n

For $d := 2$ **to** n
  If $d \backslash n$ **then exit**
  Continue with next iteration of for-loop.
Return (d)

Time-Complexity: $\mathcal{O}(n)$.

Theorem 2.4.1. *Let n be a composite number. Then n has a divisor d such that $1 < d \leq \sqrt{n}$.*

Proof: Straightforward. $\diamondsuit$

Algorithm 2.4.2: Less Naive Primality Algorithm

Input: positive integer n
Output: smallest nontrivial divisor of n

For $d := 2$ **to** $\sqrt{n}$
  If $d \backslash n$ **then exit**
  Continue with next iteration of for-loop.

Return (d)

Time-Complexity: $\mathcal{O}(\sqrt{n})$.

Example 2.4.1: Primality Test 731.

Upper Limit: $\lfloor \sqrt{731} \rfloor = 27$, since $729 = 27^2$.

$\neg(2 \backslash 731)$: leaves $3, 5, 7, 9, 11, \ldots, 25, 27$ 13 cases

$\neg(3, 5, 7, 9, 11, 13, 15 \backslash 731)$: however, $17 \backslash 731$

AHA: $731 = 17 \times 43$.

N.B. To accelerate testing, divide only by primes 2, 3, 5, 7 ,11, 13, 17.

MERSENNE PRIMES

Prop 2.4.2. *If* $m, n > 1$ *then* $2^{mn} - 1$ *is not prime.*

Proof:

$$\begin{array}{rrrrr} & 2^{m(n-1)} & +\cdots & +2^m & +1 \\ \text{(times)} & & \times & 2^m & -1 \\ \hline 2^{mn} & +2^{m(n-1)} & +\cdots & +2^m & \\ & -2^{m(n-1)} & -\cdots & -2^m & -1 \\ \hline 2^{mn} & & & & -1 \end{array}$$

Example 2.4.2:

$$\begin{aligned} 2^6 - 1 &= 2^{3\cdot 2} - 1 \\ &= (2^{3\cdot 1} + 1)(2^3 - 1) = 9 \cdot 7 = 63 \\ &= 2^{2\cdot 3} - 1 \\ &= (2^{2\cdot 2} + 2^{2\cdot 1} + 1)(2^2 - 1) = 21 \cdot 3 = 63 \end{aligned}$$

Mersenne studied the CONVERSE of Prop 2.4.2:
Is $2^p - 1$ prime when p is prime?

DEF: A ***Mersenne prime*** is a prime number of the form $2^p - 1$, where p is prime.

Example 2.4.3: primality of $2^p - 1$

prime p	$2^p - 1$	Mersenne?
2	$2^2 - 1 = 3$	yes (1)
3	$2^3 - 1 = 7$	yes (2)
5	$2^5 - 1 = 31$	yes (3)
7	$2^7 - 1 = 127$	yes (4)
11	$2^{11} - 1 = 2047 = 23 \cdot 89$	no
11213	$2^{11213} - 1$	yes (23)
19937	$2^{19937} - 1$	yes (24)
3021377	$2^{3021377} - 1$	yes (37) [late 1998]

Fundamental Theorem of Arithmetic

Theorem 2.4.3. *Every positive integer can be written uniquely as the product of nondecreasing primes.*

Proof: §2.5 proves this difficult lemma:
if a prime number p divides a product mn of integers, then it must divide either m or n. $\diamondsuit$

Example 2.4.4: $720 = 2^4 3^2 5^1$ is written as a ***prime power factorization***.

DIVISION THEOREM

Theorem 2.4.4. *Let n and d be positive integers. Then there are unique nonnegative integers q and $r < d$ such that $n = qd + r$.*

TERMINOLOGY: n = ***dividend***, d =***divisor***, q = ***quotient***, and r = ***remainder***.

Algorithm 2.4.3: Division Algorithm

Input: dividend $n > 0$ and divisor $d > 0$
Output: quotient q and remainder $0 \leq r < d$

$q := 0$
While $n \geq d$
  $q := q + 1$
  $n := n - d$
  Continue with next iteration of while-loop.
Return (quotient: d; remainder: n)

Time-Complexity: $\mathcal{O}(n/d)$.

Remark: ***Positional representation*** uses only $\Theta(\log n)$ digits to represent a number. This facilitates a faster algorithm to calculate division.

Example 2.4.5: divide 7 into 19

n	d	q
19	7	0
12	7	1
5	7	2

GREATEST COMMON DIVISORS

DEF: The ***greatest common divisor*** of two integers m, n, not both zero, is the largest positive integer d that divides both of them.
NOTATION: $\gcd(m, n)$.

Algorithm 2.4.4: Naive GCD Algorithm

Input: integers $m \leq n$ not both zero
Output: $\gcd(m, n)$

$g := 1$
For $d := 1$ **to** m
  If $d \backslash m$ **and** $d \backslash n$ **then g:=d**
  Continue with next iteration of for-loop.
Return (g)

Time-Complexity: $\Omega(m)$.

Algorithm 2.4.5: Primepower GCD Algorithm

Input: integers $m \leq n$ not both zero
Output: $\gcd(m, n)$
(1) Factor $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ into prime powers.
(2) Factor $n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ into prime powers.
(3) $g := p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_r^{\min(a_r,b_r)}$
Return (g)

Time-Complexity:
depends on time needed for factoring

DEF: The ***least common multiple*** of two positive integers m, n is the smallest positive integer d divisible by both m and n.
NOTATION: $\operatorname{lcm}(m, n)$.

Theorem 2.4.5. *Let m and n be positive integers. Then* $mn = \gcd(m, n)\operatorname{lcm}(m, n)$.

Proof: The Primepower LCM Algorithm uses max instead of min. ♢

RELATIVE PRIMALITY

DEF: Two integers m and n, not both zero, are ***relatively prime*** if $\gcd(m, n) = 1$.
NOTATION: $m \perp n$.

Proposition 2.4.6. *Two numbers are relatively prime if no prime have positive exponent in both their prime power factorizations.*

Proof: Immediate from the definition above. ♢

Remark: Proposition 2.4.6 is what motivates the notation $m \perp n$. Envision the integer n expressed as a tuple in which the kth entry is the exponent (possibly zero) of the kth prime in the prime power factorization of n. The dot product of two such representations is zero iff the numbers represented are relatively prime. This is analogous to orthogonality of vectors.

MODULAR ARITHMETIC

DEF: Let n and $m > 0$ be integers. The ***residue*** of dividing n by m is, if $n \geq 0$, the remainder, or otherwise, the smallest nonnegative number obtainable by adding an integral multiple of m.

DEF: Let n and $m > 0$ be integers. Then **n mod m** is the residue of dividing n by m.

Prop 2.4.7. *Let n and $m > 0$ be integers. Then $n - (n \textbf{ mod } m)$ is a multiple of m.*

Example 2.4.6: $19 \textbf{ mod } 7 = 5$; $17 \textbf{ mod } 5 = 2$; $-17 \textbf{ mod } 5 = -3$.

DEF: Let b, c, and $m > 0$ be integers. Then b is ***congruent to*** c ***modulo*** m if m divides $b - c$.
NOTATION: $b \equiv c \textbf{ mod } m$.

Theorem 2.4.8. *Let $a, b, c, d, m > 0$ be integers such that $a \equiv b \textbf{ mod } m$ and $c \equiv d \textbf{ mod } m$. Then*

$$a + c \equiv b + d \textbf{ mod } m \text{ and } ac \equiv bd \textbf{ mod } m.$$

Proof: *Straightforward.* ♢

CAESAR ENCRYPTION

DEF: ***Monographic substitution*** is enciphering based on a permutation of an alphabet $\pi : A \to A$. Then ciphertest is obtained from plaintext by replacing each occurrence of each letter by its substitute.

letter	A	B	C	D	E	F	$\cdots$	X	Y	Z
subst	Q	W	E	R	T	Y	$\cdots$	B	N	M

DEF: A monographic substitution cipher is called ***cyclic*** if the letters of the alphabet are represented by numbers 0, 1, ..., 25 and there is a number m such that $\pi(n) = m + n$ **mod** 26.

An ancient Roman parchment is discovered with the following words:

HW WX EUXWH

What can it possibly mean?

Hint: Julius Caesar encrypted military messages by cyclic monographic substitution.