Topics in Discrete Mathematics

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 216

Subsection 1

Dividing

The Division Theorem

Division Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist integers q and r such that $a = qb + r$ and $0 \leq r < b$. Moreover, there is only one such pair of integers (q, r) that satisfies these conditions.

- The integer q is called the **quotient** and the integer r is called the **remainder**.
- Example: If $a = 23$ and $b = 10$, then the quotient is $q = 2$ and the remainder $r = 3$ because $23 = 2 \cdot 10 + 3$ and $0 \leq 3 < 10$.
- Example: If $a = -37$ and $b = 5$, then $q = -8$ and $r = 3$ because $-37 = -8 \cdot 5 + 3$ and $0 \leq 3 < 5$.

Proof of the Division Theorem I

- Let a and b be integers with $b > 0$.
  - We first show that the quotient and remainder exist, i.e., there exist integers q and r that satisfy the three conditions
    - $a = qb + r$
    - $r \geq 0$, and
    - $r < b$.

    Let $A = \{a - bk : k \in \mathbb{Z}\}$. The remainder is to be nonnegative, so let $B = A \cap \mathbb{N} = \{a - bk : k \in \mathbb{Z}, a - bk \geq 0\}$. To use the Well-Ordering Principle to select the least element of B, we must ensure that $B \neq \emptyset$.
    - If $a \geq 0$, then, clearly, $a = a - b \cdot 0 \in B$ and $B \neq \emptyset$.
    - If $a < 0$, since $b > 0$, if we take k to be a very negative number, we can certainly make $a - bk$ positive, so again $B \neq \emptyset$.

    Since $B \neq \emptyset$, by the Well-Ordering Principle we can choose r to be the least element of B. Then, since $r \in B \subseteq A = \{a - bk : k \in \mathbb{Z}\}$, there exists an integer q, such that $r = a - bq$, i.e., $a = qb + r$. Moreover, since $r \in B \subseteq \mathbb{N}$, $r \geq 0$.
    Now it only remains to show that $r < b$.

Proof of the Division Theorem II

- Continuing the Proof:
  - To finish the existence part, i.e., show that $r < b$, suppose, for the sake of contradiction, that $r \geq b$.
    We have $r = a - qb \geq b$. Let $r' = (a - qb) - b = r - b \geq 0$, so $r' = a - (q+1)b \geq 0$. Therefore, $r' \in B$ and $r' = r - b < r$. This contradicts the fact that r is the smallest element of B.
    We have proved that the integers q and r exist.
  - We now show that q and r are unique.
    Suppose, for the sake of contradiction, there are two different pairs of numbers (q, r) and (q', r'), such that $a = qb + r$, with $0 \leq r < b$, and $a = q'b + r'$, with $0 \leq r' < b$. Combining the two equations gives $qb + r = q'b + r'$ and, therefore, $r - r' = (q' - q)b$. Thus, $r - r'$ is a multiple of b. Since $0 \leq r, r' < b$, $|r - r'| \leq b - 1$. The only way that $r - r'$, with $|r - r'| \leq b - 1$, can be a multiple of b is if $r - r' = 0$, i.e., $r = r'$.
    Since $r = r'$, and $qb + r = a = q'b + r' = q'b + r$, we get also $q = q'$.
    So $(q, r) \neq (q', r')$ leads to $q = q'$ and $r = r'$, a contradiction.
    Therefore, the quotient and remainder are unique.

Corollary I

Corollary

Every integer is either even or odd, but not both.

- We have already shown that no integer can be both even and odd. Thus it remains to show that every integer is one or the other.

  Let n be any integer. By the Theorem, there exist integers q and r, such that $n = 2q + r$ where $0 \leq r < 2$.
  - If $r = 0$, then n is even;
  - If $r = 1$, then n is odd.

Corollary II

Corollary

Two integers are congruent modulo 2 if and only if they are both even or both odd.

- ($\Rightarrow$): Let a and b be integers with $a \equiv b \pmod 2$. So $a - b = 2n$ for some integer n. Now a is either even or odd.
  - If a is even, $a = 2k$ for some integer k. Then $b = a - 2n = 2k - 2n = 2(k - n)$ and so b is even.
  - If a is odd, then $a = 2k + 1$ for some integer k. Then $b = a - 2n = 2k + 1 - 2n = 2(k - n) + 1$, whence b is odd.

  In either case, a and b are either both even or both odd.
- ($\Leftarrow$): Suppose a and b are integers that are both even or both odd.
  - If a and b are both even, then $a = 2n$ and $b = 2m$ for some integers n and m. Then $a - b = 2n - 2m = 2(n - m)$ and so $a \equiv b \pmod 2$.
  - If a and b are both odd, then $a = 2n + 1$ and $b = 2m + 1$ for some integers n and m. Then $a - b = (2n + 1) - (2m + 1) = 2(n - m)$ and so $a \equiv b \pmod 2$.

  Thus if a and b are both even or both odd, then $a \equiv b \pmod 2$.

Div and Mod Operators

Definition (div and mod)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Consider the unique pair of numbers q and r with $a = qb + r$ and $0 \leq r < b$. We define the operations div and mod by

$$a \text{ div } b = q \quad \text{and} \quad a \bmod b = r.$$

- Example: These calculations illustrate the div and mod operations:
  - $11 \text{ div } 3 = 3$
  - $23 \text{ div } 10 = 2$
  - $-37 \text{ div } 5 = -8$
  - $11 \bmod 3 = 2$
  - $23 \bmod 10 = 3$
  - $-37 \bmod 5 = 3$
- Note that we have used the word "mod" in two different ways:
  - First, the word mod was used as the name of an equivalence relation. For example, $53 \equiv 23 \pmod{10}$. The meaning of $a \equiv b \pmod{n}$ is that $a - b$ is a multiple of n.
  - Second, mod is the binary operation "divide and take the remainder": For example, $53 \bmod 10 = 3$.

Equivalence $(\mod n)$ and the mod Operator

Proposition

Let $a, b, n \in \mathbb{Z}$, with $n > 0$. Then

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n.$$

- Let $a, b, n \in \mathbb{Z}$ with $n > 0$.
  - ($\Rightarrow$): Suppose $a \equiv b \pmod{n}$. Then $a - b = kn$, for some $k \in \mathbb{Z}$. Let $r = a \bmod n$, i.e., $a = qn + r$, for some $q \in \mathbb{Z}$. Then $b = a - kn = (qn + r) - kn = (q - k)n + r$, whence $r = b \bmod n$ also. Therefore $a \bmod n = b \bmod n$.
  - ($\Leftarrow$): Suppose $a \bmod n = b \bmod n = r$. Then, there exist $q_1, q_2 \in \mathbb{Z}$, such that $a = q_1 n + r$ and $b = q_2 n + r$. Thus, $a - b = (q_1 - q_2)n$, which shows that $n \mid (a - b)$. Therefore, $a \equiv b \pmod{n}$.

Subsection 2

Greatest Common Divisor

The Greatest Common Divisor

Definition (Common Divisor)

Let $a, b \in \mathbb{Z}$. An integer d is a **common divisor** of a and b if $d \mid a$ and $d \mid b$.

- Example: The common divisors of 30 and 24 are $-6, -3, -2, -1, 1, 2, 3$ and 6.

Definition (Greatest Common Divisor)

Let $a, b \in \mathbb{Z}$. An integer d is the **greatest common divisor** of a and b if

1. d is a common divisor of a and b;
2. if e is a common divisor of a and b, then $e \leq d$.

The greatest common divisor of a and b is denoted $\gcd(a, b)$.

- Example: The greatest common divisor of 30 and 24 is 6, and we write $\gcd(30, 24) = 6$.

Naive Algorithm for Finding the gcd

- An algorithm for computing the gcd of two positive integers a and b works as follows:
  - For every positive integer k from 1 to the smaller of a and b, see whether $k \mid a$ and $k \mid b$. If so, save that number k in a list.
  - Choose the largest number on the list. That number is $\gcd(a, b)$.
- Even though it works, this algorithm needs to perform a large number of divisions, so it is very slow.
- There is a clever procedure to calculate the greatest common divisor of two positive integers:
  - It was invented by Euclid.
  - It is very fast.
  - It is easily implemented as a computer program.

Euclid's Algorithm for Finding the gcd

Theorem (Euclid's Algorithm)

Let a and b be positive integers and let $c = a \bmod b$. Then $\gcd(a, b) = \gcd(b, c)$.

- The theorem says that, for positive integers a and b, we have
$$\gcd(a, b) = \gcd(b, a \bmod b).$$
- We are given that $c = a \bmod b$, i.e., $a = qb + c$, with $0 \leq c < b$. Let $d = \gcd(a, b)$ and let $e = \gcd(b, c)$. To show $d = e$, we prove that $d \leq e$ and $d \geq e$.
  - First, we show $d \leq e$. Since $d = \gcd(a, b)$, we know that $d \mid a$ and $d \mid b$. We can write $c = a - qb$. Since a and b are multiples of d, so is c. Thus d is a common divisor of b and c. However, e is the greatest common divisor of b and c, so $d \leq e$.
  - Next, we show $d \geq e$. Since $e = \gcd(b, c)$, we know that $e \mid b$ and $e \mid c$. Now $a = qb + c$, and hence $e \mid a$ as well. Since $e \mid a$ and $e \mid b$, we see that e is a common divisor of a and b. However, d is the greatest common divisor of a and b, so $d \geq e$.

Example: Calculating gcd(689, 234)

- We compute gcd(689, 234). Let $a = 689$ and $b = 234$. We find $c = 689 \bmod 234 = 221$.
- To find gcd(689, 234), it is enough to find gcd(234, 221) because these two values are the same.

$$689 \bmod 234 = 221 \quad \Rightarrow \quad \gcd(689, 234) = \gcd(234, 221).$$

- To calculate gcd(234, 221), we calculate $234 \bmod 221 = 13$. Thus gcd(234, 221) = gcd(221, 13).

$$234 \bmod 221 = 13 \quad \Rightarrow \quad \gcd(234, 221) = \gcd(221, 13).$$

- Next calculate $221 \bmod 13 = 0$. Thus, $13 \mid 221$. So clearly gcd(221, 13) = 13.

$$221 \bmod 13 = 0 \quad \Rightarrow \quad \gcd(221, 13) = 13.$$

- We are finished! We have done three divisions and we found

$$\gcd(689, 234) = \gcd(234, 221) = \gcd(221, 13) = 13.$$

Euclid's GCD Algorithm

Euclid's GCD Algorithm

Input: Positive integers a and b.
Output: $\gcd(a, b)$.

- Let $c = a \bmod b$.
- If $c = 0$, return the answer b and stop.
- If $c \neq 0$, calculate $\gcd(b, c)$ and return this as the answer.
- Example: We test the algorithm for $a = 63$ and $b = 75$.
  - Calculate $c = a \bmod b$ to get $c = 63 \bmod 75 = 63$.
  - Since $c \neq 0$, compute $\gcd(b, c) = \gcd(75, 63)$.
  - Restart with $a' = 75$ and $b' = 63$. Calculate $c' = 75 \bmod 63 = 12$. Since $12 \neq 0$, calculate $\gcd(b', c') = \gcd(63, 12)$.
  - Restart with $a'' = 63$ and $b'' = 12$. Calculate $c'' = 63 \bmod 12 = 3$. Since this is not zero, calculate $\gcd(b'', c'') = \gcd(12, 3)$.
  - Restart with $a''' = 12$ and $b''' = 3$. Calculate $c''' = 12 \bmod 3 = 0$. Now $c''' = 0$, so we return $b''' = 3$ and we are finished.
  - The final answer is that $\gcd(63, 75) = 3$.

Visualizations of Euclid's Algorithm

- Here is an overview of the calculation in chart form:

a	b	c
63	75	63
75	63	12
63	12	3
12	3	0

- Another way to visualize this computation is via a list:
  - The first two entries are a and b.
  - The list is extended by computing mod of the last two entries.
  - When we reach 0, we stop.
  - The next-to-last entry is the gcd of a and b.

  In this example, the list would be

$$(63, 75, 63, 12, 3, 0)$$

Correctness of Euclid's Algorithm

Theorem (Correctness of Euclid's Algorithm)

Euclid's Algorithm correctly computes $\gcd(a, b)$, for a, b positive integers.

- Suppose Euclid's Algorithm did not correctly compute gcd. Then there exist positive integers a and b for which it fails. For smallest counterexample, choose a, b such that $a + b$ is as small as possible.
  - If $a < b$, then $c = a \bmod b = a$. So, the first pass through Euclid's Algorithm will simply interchange the values a and b.
  - So let $a \geq b$. The first step calculates $c = \gcd(a, b)$.
    - If $c = 0$, $a \bmod b = 0$, which implies $b \mid a$. Since b is the largest divisor of b ($b > 0$ by hypothesis) and since $b \mid a$, $b = \gcd(a, b)$. The algorithm then gives the correct result, contradicting our hypothesis.
    - If $c \neq 0$, we have $a = qb + c$, where $0 < c < b$. We also have $b \leq a$, whence $b + c < a + b$. Thus b, c are positive integers with $b + c < a + b$. By the minimality of $a + b$, b and c are not a counterexample. Thus the algorithm correctly computes $\gcd(b, c)$ and returns its value. But, we proved $\gcd(a, b) = \gcd(b, c)$! So we get the correct answer, contradicting the hypothesis!

Size of Remainder in Euclid's Algorithm

- After two rounds of Euclid's Algorithm, the integers involved have decreased by at least 50%.

Proposition

Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. If $c = a \bmod b$, Then $c < \frac{a}{2}$.

- We consider two cases:
  - $a < 2b$: Then $2b > a > 0$, so $a > 0$ and $a - b \geq 0$, but $a - 2b < 0$. Hence the quotient when a is divided by b is 1. So the remainder is $c = a - b$. Since $a < 2b$, we get $b > \frac{a}{2}$ and so $c = a - b < a - \frac{a}{2} = \frac{a}{2}$.
  - $a \geq 2b$: Thus, $b \leq \frac{a}{2}$. The remainder, upon division of a by b, is less than b. So $c < b$, and we have $b \leq \frac{a}{2}$, so $c < \frac{a}{2}$.

Number of Steps in Euclid's Algorithm

- If the numbers produced by Euclid's Algorithm are $(a, b, c, d, e, f, \ldots, 0)$, then, if $a \geq b$, we have $a \geq b \geq c \geq d \geq \cdots \geq 0$.
- By the Proposition, $c < \frac{a}{2}$ and $d < \frac{b}{2}$.
- Likewise, two steps later, $e < \frac{c}{2} < \frac{a}{4}$ and $f < \frac{d}{2} < \frac{b}{4}$.
- Thus, every two steps of Euclid's Algorithm decrease the integers with which we are working to less than half their current values.
- How large are the numbers after $2t$ passes of Euclid's Algorithm? After $2t$ steps the numbers drop by more than a factor of 2^t, i.e., the two numbers are less than $(2^{-t}a, 2^{-t}b)$.
- Euclid's Algorithm stops when the second number reaches zero, which is the same as when the second number is less than 1, i.e., as soon as we have $2^{-t}b \leq 1$.
- So $\log_2 [2^{-t}b] \leq \log_2 1 \;\Rightarrow\; -t + \log_2 b \leq 0 \;\Rightarrow\; \log_2 b \leq t$.
- Once $t \geq \log_2 b$, the algorithm must be finished, i.e., after $2 \log_2 b$ passes, the algorithm has completed its work.

The gcd as the Smallest Positive Linear Combination

Theorem

Let a and b be integers, not both zero. The smallest positive integer of the form $ax + by$, where x and y are integers, is $\gcd(a, b)$.

- Let a and b be integers (not both zero) and let $D = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$.
  - Since $a^2 + b^2 > 0$, $D \neq \emptyset$.
  - Thus, by Well-Ordering, D contains a least element d.

  The goal is to show that $d = \gcd(a, b)$.
  - $d \mid a$: Suppose that a is not divisible by d. Then $a = qd + r$, with $0 < r < d$. Now $d = ax + by$, so $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy) = aX + bY$, where $X = 1 - qx$ and $Y = -qy$. Since $0 < r < d$ and $r = aX + bY$, we get $r \in D$ and $r < d$, contradicting the fact that d is the least element of D.
  - $d \mid b$: This proof is analogous to $d \mid a$.
  - If $e \mid a$ and $e \mid b$, then $e \leq d$. Suppose $e \mid a$ and $e \mid b$. Then $e \mid (ax + by)$, whence $e \mid d$, so $e \leq d$ (because d is positive).
- Therefore d is the greatest common divisor of a and b.

Finding the Coefficients in the Linear Combination

- We saw that $\gcd(689, 234) = 13$: $689 \cdot (-1) + 234 \cdot 3 = 13$.
- Note that $\gcd(431, 29) = 1$: $431 \cdot 7 + 29 \cdot (-104) = 1$.
- Given a, b, how do we find x, y, such that $ax + by = \gcd(a, b)$?
- We extend Euclid's Algorithm by also keeping track of the quotients.
- We find x, y such that $431x + 29y = \gcd(431, 29) = 1$.
  The steps involved in calculating $\gcd(431, 29)$ are:

$$431 = 14 \cdot 29 + 25, 29 = 1 \cdot 25 + 4, 25 = 6 \cdot 4 + 1, 4 = 4 \cdot 1 + 0.$$

We solve all except last for the remainders:

$$25 = 431 - 14 \cdot 29, \ 4 = 29 - 1 \cdot 25, \ 1 = 25 - 6 \cdot 4.$$

Now we work from the bottom up:

$$1 = 25 - 6 \cdot 4 = 25 - 6 \cdot (29 - 1 \cdot 25) = -6 \cdot 29 + 7 \cdot 25.$$

Now we use $25 = 431 - 14 \cdot 29$:

$$1 = -6 \cdot 29 + 7 \cdot 25 = -6 \cdot 29 + 7 \cdot (431 - 14 \cdot 29) =$$
$$7 \cdot 431 + [-6 + 7 \cdot (-14)]29 = 7 \cdot 431 + (-104) \cdot 29.$$

Relatively Prime Numbers

Definition (Relatively Prime)

Let a and b be integers. We call a and b **relatively prime** provided $\gcd(a, b) = 1$.

Corollary

Let a and b be integers. There exist integers x and y such that $ax + by = 1$ if and only if a and b are relatively prime.

Proposition

Let a, b be integers, not both zero. Let $d = \gcd(a, b)$. If e is a common divisor of a and b, then $e \mid d$.

- Let a, b be integers, not both zero, and let $d = \gcd(a, b)$. Suppose $e \mid a$ and $e \mid b$. By the Theorem, there exist integers x and y such that $d = ax + by$. Since $e \mid a$ and $e \mid b$, $e \mid (ax + by)$, and so $e \mid d$.

Subsection 3

Modular Arithmetic

Integers mod n

- Arithmetic is the study of the basic operations: addition, subtraction, multiplication, and division.
- We usually study these operations in number systems such as the integers, $\mathbb{Z}$, or the rationals, $\mathbb{Q}$.
- Division is, perhaps, the most interesting example.
  - In the context of the rational numbers, we can calculate $x \div y$ for any $x, y \in \mathbb{Q}$ except when $y = 0$.
  - In the context of the integers, $x \div y$ is defined only if $y \neq 0$ and $y \mid x$.
- So in $\mathbb{Q}$ and $\mathbb{Z}$, the operation $\div$ takes on slightly different meanings.
- We now introduce a new context for $+, -, \times$, and $\div$, different from the traditional. To avoid confusion, we use $\oplus, \ominus, \otimes, \oslash$.
- The new set in which we perform arithmetic is $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, i.e., it contains all natural numbers from 0 to $n-1$ inclusive. We call this number system the **integers mod** n. The operations $\oplus, \ominus, \otimes, \oslash$ are called **addition mod** n, **subtraction mod** n, **multiplication mod** n, and **division mod** n.

Modular Addition and Multiplication

Definition (Modular Addition, Multiplication)

Let n be a positive integer and $a, b \in \mathbb{Z}_n$. We define

$$a \oplus b = (a + b) \bmod n \quad \text{and} \quad a \otimes b = (ab) \bmod n.$$

- The operations on the left are operations defined for $\mathbb{Z}_n$. The operations on the right are ordinary integer operations.
- Example: Let $n = 10$. We have the following:
  - $5 \oplus 5 = 0$
  - $5 \otimes 5 = 5$
  - $9 \oplus 8 = 7$
  - $9 \otimes 8 = 2$
- Notice that if $a, b \in \mathbb{Z}_n$, the results of the operations $a \oplus b$ and $a \otimes b$ are always defined and are elements of $\mathbb{Z}_n$.

Proposition (Closure of $\mathbb{Z}_n$ Under $\oplus, \otimes$)

Let $a, b \in \mathbb{Z}_n$. Then $a \oplus b \in \mathbb{Z}_n$ and $a \otimes b \in \mathbb{Z}_n$.

Properties of Addition and Multiplication mod n

Proposition (Properties of $\oplus, \otimes$)

Let n be an integer with $n \geq 2$.

- For all $a, b \in \mathbb{Z}_n$, $a \oplus b = b \oplus a$ and $a \otimes b = b \otimes a$. (**Commutativity**)
- For all $a, b, c \in \mathbb{Z}_n$, $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ and $a \otimes (b \otimes c) = (a \otimes b) \otimes c$. (**Associativity**)
- For all $a \in \mathbb{Z}_n$, $a \oplus 0 = a$, $a \otimes 1 = a$ and $a \otimes 0 = 0$. (**Identities**)
- For all $a, b, c \in \mathbb{Z}_n$, $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$. (**Distributivity**)

- We show, as an example, that $\oplus$ is associative, i.e., that if $a, b, c \in \mathbb{Z}_n$, $a \oplus (b \oplus c) = (a \oplus b) \oplus c$:
  $a \oplus (b \oplus c) = a \oplus (b + c + kn) = [a + (b + c + kn)] + jn = (a + b + c) + sn$
  where $k, j, s \in \mathbb{Z}$. Since $a + b + c + sn = (a + b + c) \bmod n$, we have $(a + b + c) \bmod n = (a + b + c + sn) \bmod n = (a + b + c + sn)$ because $a + b + c + sn \in \mathbb{Z}_n$. So $a \oplus (b \oplus c) = (a + b + c) \bmod n$. By a similar argument, $(a \oplus b) \oplus c = (a + b + c) \bmod n$.

Existence and Uniqueness of Solution for $a = b \oplus x$

- Let $a, b \in \mathbb{Z}$. We define $a - b$ to be the solution to $a = b + x$.
- We use this approach to define modular subtraction.

Proposition (Existence and Uniqueness of Solution for $a = b \oplus x$)

Let n be a positive integer, and let $a, b \in \mathbb{Z}_n$. Then there is one and only one $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

- Let $x = (a - b) \bmod n$. Clearly, $0 \leq x < n$, i.e., $x \in \mathbb{Z}_n$. Moreover, $x = (a - b) + kn$ for some integer k. We have $b \oplus x = (b + x) \bmod n = [b + (a - b + kn)] \bmod n = (a + kn) \bmod n = a$, because $0 \leq a < n$.
- To show uniqueness, suppose $a = b \oplus x$ and $a = b \oplus y$, for $x, y \in \mathbb{Z}_n$. Then $b \oplus x = (b + x) \bmod n = b + x + kn = a$, and $b \oplus y = (b + y) \bmod n = b + y + jn = a$ for some integers k, j. Combining these, we have $b + x + kn = b + y + jn$ $\Rightarrow x = y + (k - j)n \Rightarrow x = y \pmod{n} \Rightarrow x \bmod n = y \bmod n$ $\Rightarrow x = y$ because $0 \leq x, y < n$.

Modular Subtraction

Definition (Modular Subtraction)

Let n be a positive integer and let $a, b \in \mathbb{Z}_n$. We define $a \ominus b$ to be the unique $x \in \mathbb{Z}_n$ such that $a = b \oplus x$.

- Alternatively, we could have defined $a \ominus b$ to be $(a - b) \bmod n$.

Proposition

Let n be a positive integer and let $a, b \in \mathbb{Z}_n$. Then $a \ominus b = (a - b) \bmod n$.

- To prove that $a \ominus b = (a - b) \bmod n$, we consult the definition. We must show
  - $[(a - b) \bmod n] \in \mathbb{Z}_n$;
  - if $x = (a - b) \bmod n$, then $a = b \oplus x$.

  The first is obvious because $(a - b) \bmod n$ is an integer in $\mathbb{Z}_n$.
  For the second, note that $x = a - b + kn$ for some integer k. Then $b \oplus x = (b + (a - b + kn)) \bmod n = (a + kn) \bmod n = a$.

Modular Reciprocals

- Given $a, b \in \mathbb{Z}_{10}$ (with $b \neq 0$), is there a solution to $a = b \otimes x$? If so, is it unique?
- Consider the following three cases.
  - Let $a = 6$ and $b = 2$. There are two solutions to $6 = 2 \otimes x$, namely $x = 3$ and $x = 8$.
  - Let $a = 7$ and $b = 2$. There are no solutions to $7 = 2 \otimes x$.
  - Let $a = 7$ and $b = 3$. There is one and only one solution to $7 = 3 \otimes x$, namely $x = 9$. In this case it makes sense to write $7 \oslash 3 = 9$.
- In $\mathbb{Q}$, we can define $a \div b$ to be $a \cdot b^{-1}$ so that division by b is defined to be multiplication by b's reciprocal.
- The reciprocal of $x \in \mathbb{Q}$ is a $y \in \mathbb{Q}$ such that $xy = 1$.
- We use reciprocals in $\mathbb{Z}_n$ to define division in $\mathbb{Z}_n$:

Definition (Modular Reciprocal)

Let n be a positive integer and let $a \in \mathbb{Z}_n$. A **reciprocal** of a is an element $b \in \mathbb{Z}_n$, such that $a \otimes b = 1$. An element of $\mathbb{Z}_n$ that has a reciprocal is called **invertible**.

Reciprocals in $\mathbb{Z}_{10}$

- We investigate reciprocals in $\mathbb{Z}_{10}$ by looking at the multiplication table:

$\otimes$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

  - Element 0 does not have a reciprocal.
  - Elements $2, 4, 5, 6$ and 8 do not have reciprocals.
  - Elements $1, 3, 7$ and 9 are have unique reciprocals.
  - Notice the elements of $\mathbb{Z}_{10}$ that have reciprocals are precisely those integers in $\mathbb{Z}_{10}$ that are relatively prime to 10.
  - The reciprocal of 3 is 7, and the reciprocal of 7 is 3; both 1 and 9 are their own reciprocals.

Uniqueness of the Reciprocal

Proposition (Uniqueness of Reciprocals)

Let n be a positive integer and let $a \in \mathbb{Z}_n$. If a has a reciprocal in $\mathbb{Z}_n$, then it has only one reciprocal.

- Suppose a had two reciprocals, $b, c \in \mathbb{Z}_n$ with $b \neq c$. Consider $b \otimes a \otimes c$. Using associativity, we get $b = b \otimes 1 = b \otimes (a \otimes c) = (b \otimes a) \otimes c = 1 \otimes c = c$, contradicting $b \neq c$.
- The reciprocal of a is also called the **inverse** of a and denoted a^{-1}.
- The superscript -1 needs care because it has multiple meanings:
  - In the integers or rationals, $a^{-1} = \frac{1}{a}$.
  - In the context of relations or functions, R^{-1} stands for the relation formed by reversing all the ordered pairs in R.
  - In $\mathbb{Z}_n$, a^{-1} is the reciprocal of a.

Proposition (Mutuality of Reciprocals)

Let n be a positive integer and let $a \in \mathbb{Z}_n$. Suppose a is invertible and $b = a^{-1}$. Then b is invertible and $a = b^{-1}$.

Modular Division

Defintion (Modular Division)

Let n be a positive integer, a any element in $\mathbb{Z}_n$ and b an invertible element of $\mathbb{Z}_n$. Then $a \oslash b$ is defined to be $a \otimes b^{-1}$.

- Example: In $\mathbb{Z}_{10}$, calculate $2 \oslash 7$.
  Since $7^{-1} = 3$, we get $2 \oslash 7 = 2 \otimes 3 = 6$.
- For arbitrary n, we would like to know
  - which elements of $\mathbb{Z}_n$ are invertible;
  - how we calculate a^{-1} for invertible a.
- In $\mathbb{Z}_{10}$, the only invertible elements are $1, 3, 7$ and 9, i.e., those elements relatively prime to 10.
- In the next slide, we also look at $\mathbb{Z}_9$.

Invertible Elements in $\mathbb{Z}_9$

- The multiplication table for $\mathbb{Z}_9$.

$\otimes$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

- The invertible elements of $\mathbb{Z}_9$ are 1, 2, 4, 5, 7 and 8 (these are all relatively prime to 9).
- The noninvertible elements are 0, 3 and 6 (none of these are relatively prime to 9).

Characterization of Invertibility

Theorem (Invertibility)

Let n be a positive integer and let $a \in \mathbb{Z}_n$. Then a is invertible if and only if a and n are relatively prime.

- Recall that a and b are relatively prime if and only if there is an integer solution to $ax + by = 1$.
- Let n be a positive integer and let $a \in \mathbb{Z}_n$.
  - ($\Rightarrow$): Suppose a is invertible. Then, there is an element $b \in \mathbb{Z}_n$, such that $a \otimes b = 1$, i.e., $(ab) \bmod n = 1$. Thus $ab + kn = 1$, for some integer k. Therefore, a and n are relatively prime.
  - ($\Leftarrow$): Suppose a and n are relatively prime. Then, there are integers x and y such that $ax + ny = 1$. Let $b = x \bmod n$. So $b = x + kn$, for some integer k. Substituting into $ax + ny = 1$, we have $1 = ax + ny = a(b - kn) + ny = ab + (y - ka)n$. Therefore, $a \otimes b = ab \pmod{n} = 1$. Thus, b is the reciprocal of a and, therefore, a is invertible in $\mathbb{Z}_n$.

An Example in $\mathbb{Z}_{431}$

- Example: In $\mathbb{Z}_{431}$, find 29^{-1}.

  We have already found integers x and y such that $431x + 29y = 1$, namely $x = 7$ and $y = -104$. Therefore, $(-104 \cdot 29) \bmod 431 = 1$. Since $-104 \notin \mathbb{Z}_{431}$, we can take $b = -104 \bmod 431 = 327$. Now $29 \otimes 327 = (29 \cdot 327) \bmod 431 = 9483 \bmod 431 = 1$. Therefore $29^{-1} = 327$.

- Example: In $\mathbb{Z}_{431}$, calculate $30 \oslash 29$.

  Since $29^{-1} = 327$, we get

$$30 \oslash 29 = 30 \otimes 327 = (30 \cdot 327) \bmod 431 = 9810 \bmod 431 = 328.$$

Subsection 4

The Chinese Remainder Theorem

Solving a Simple Modular Equation

- Solve the equation $x \equiv 4 \pmod{11}$.

  We would like to find x such that $x - 4$ is a multiple of 11, i.e., such that $x - 4 = 11k$, for some integer k. We can rewrite this as $x = 4 + 11k$ where k can be any integer. So the solutions are

$$\ldots, -18, -7, 4, 15, 26, \ldots.$$

Solving Another Modular Equation

- Solve the equation $3x \equiv 4 \pmod{11}$.
- If x_0 was a solution to $3x \equiv 4 \pmod{11}$, then, if $x_1 = x_0 + 11$, $3x_1 = 3(x_0 + 11) = 3x_0 + 33 \equiv 3x_0 \equiv 4 \pmod{11}$, so x_1 is also a solution. If there is a solution, then there is a solution in $\{0, 1, 2, \ldots, 10\} = \mathbb{Z}_{11}$.
- We seek a number $x \in \mathbb{Z}_{11}$ for which $3x \equiv 4 \pmod{11}$. We have $3x \equiv 4 \pmod{11} \Leftrightarrow (3x) \bmod 11 = 4 \Leftrightarrow 3 \otimes x = 4$ where $\otimes$ is modular multiplication in $\mathbb{Z}_{11}$.
  How do we solve the equation $3 \otimes x = 4$? We multiply both sides by $3^{-1} = 4$: $3 \otimes x = 4 \Rightarrow 4 \otimes 3 \otimes x = 4 \otimes 4 \Rightarrow 1 \otimes x = 5 \Rightarrow x = 5$.
- There are no other solutions in $\mathbb{Z}_{11}$: If $x' \in \mathbb{Z}_{11}$ were another solution, we would have $3 \otimes x' = 4$, and when we $\otimes$ both sides by 4, we would find $x' = 5$.

Solution of a Modular Equation

Proposition

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose a and n are relatively prime and consider the equation $ax \equiv b \pmod{n}$.
The set of solutions to this equation is $\{x_0 + kn : k \in \mathbb{Z}\}$, where $x_0 = a_0^{-1} \otimes b_0$, $a_0 = a \bmod n$, $b_0 = b \bmod n$, and $\otimes$ is modular multiplication in $\mathbb{Z}_n$.
The integer x_0 is the only solution to this equation in $\mathbb{Z}_n$.

- Next we solve a pair of congruence equations in different moduli. The general form is

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Solution of a System of Modular Equations: Example

- Solve the pair of equations $\begin{cases} x & \equiv & 1 \pmod 7 \\ x & \equiv & 4 \pmod{11} \end{cases}$

  Since $x \equiv 1 \pmod 7$, we can write $x = 1 + 7k$, for some integer k. We can substitute $1 + 7k$ for x in the second equation: $x \equiv 4 \pmod{11}$. We get $1 + 7k \equiv 4 \pmod{11} \Rightarrow 7k \equiv 3 \pmod{11}$. To solve this equation, we need to $\otimes$ both sides by $7^{-1} = 8$ working in $\mathbb{Z}_{11}$. We find $7 \otimes k = 3 \Rightarrow 8 \otimes 7 \otimes k = 8 \otimes 3 \Rightarrow k = 2$. We know that we want all values of x with $x = 1 + 7k$, k any integer of the form $k = 2 + 11j$, j is any integer. Combining these two, we have $x = 1 + 7k = 1 + 7(2 + 11j) = 15 + 77j$, $j \in \mathbb{Z}$. Equivalently, the solution set to the equations is

$$\{x \in \mathbb{Z} : x \equiv 15 \pmod{77}\}.$$

The Chinese Remainder Theorem

The Chinese Remainder Theorem

Let a, b, m, n be integers with m and n positive and relatively prime. There is a unique integer x_0 with $0 \leq x_0 < mn$ that solves the pair of equations $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$. Furthermore, every solution to these equations differs from x_0 by a multiple of mn.

- From $x \equiv a \pmod{m}$, we get $x = a + km$, $k \in \mathbb{Z}$. Substituting into $x \equiv b \pmod{n}$, we get $a + km \equiv b \pmod{n} \Rightarrow km \equiv b - a \pmod{n}$. Let $m' = m \bmod n$, and $c = (b - a) \bmod n$. Now solving $km \equiv b - a \pmod{n}$ is equivalent to solving $km' \equiv c \pmod{n}$. Thus, in $\mathbb{Z}_n$, $k \otimes m' = c \Rightarrow k = (m')^{-1} \otimes c$. Let $d = (m')^{-1} \otimes c$, so the values for k that we want are $k = d + jn$, $j \in \mathbb{Z}$. Finally, we substitute $k = d + jn$ into $x = a + km$ to get

$$x = a + km = a + (d + jn)m = a + dm + jnm, \ j \in \mathbb{Z}.$$

So the original system reduces to $x = a + dm \pmod{mn}$.

System of Three Modular Equations

- Suppose we want to solve a system of three equations. For example, solve for all x:

$$\begin{cases} x & \equiv & 3 & (\text{mod } 9) \\ x & \equiv & 5 & (\text{mod } 10) \\ x & \equiv & 2 & (\text{mod } 11) \end{cases}$$

We can solve the first two equations by the usual method

$$\left\{ \begin{array}{rcl} x & \equiv & 3 \ (\text{mod } 9) \\ x & \equiv & 5 \ (\text{mod } 10) \end{array} \right\} \Rightarrow \ x \equiv 75 \ (\text{mod } 90).$$

$$\begin{aligned} & x = 3 + 9k \\ & 3 + 9k \equiv 5 \pmod{10} \ \Rightarrow \ 9k \equiv 2 \pmod{10} \\ & \Rightarrow \ k = 9 \otimes 2 = 8 \ \Rightarrow \ k = 8 + 10j \\ & x = 3 + 9k = 3 + 9(8 + 10j) = 75 + 90j \end{aligned}$$

Next, we combine with the last equation and solve by the usual method:

$$\left\{ \begin{array}{rcl} x & \equiv & 75 \ (\text{mod } 90) \\ x & \equiv & 2 \ (\text{mod } 11) \end{array} \right\} \Rightarrow \ x \equiv 255 \ (\text{mod } 990).$$

Subsection 5

Factoring

Idea of the Fundamental Theorem

- Every positive integer can be factored into primes in (essentially) a unique fashion.
- Example: The integer 60 can be factored into primes as $60 = 2 \cdot 2 \cdot 3 \cdot 5$. It can also be factored as $60 = 5 \cdot 2 \cdot 3 \cdot 2$, but the primes in the two factorizations are exactly the same.
- This is true of all positive integers:
  - We can treat 1 as the empty product of primes.
  - We can consider prime numbers to be already factored into primes: a prime, say 17, is the product of just one prime: 17.
  - Composite numbers are the product of two or more primes.

An Important Lemma

Lemma

Suppose $a, b, p \in \mathbb{Z}$ and p is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

- Let a, b, p be integers with p prime and suppose $p \mid ab$. Suppose, for the sake of contradiction, that p divides neither a nor b. Since p is a prime, the only divisors of p are ± 1 and $\pm p$.
  - Since p is not a divisor of a, the largest divisor they have in common is 1, whence $\gcd(a, p) = 1$. Thus, there are integers x and y such that $ax + py = 1$.
  - Similarly, b and p are relatively prime, whence, there are integers w and z such that $bz + pw = 1$.

  Multiplying $ax + py = 1$ and $bz + pw = 1$, we get
  $1 = (ax + py)(bz + pw) = abxz + pybz + paxw + p^2yw$.
  All four of these terms are divisible by p. This implies that $p \mid 1$, which is a contradiction.

An Extension of the Lemma

Lemma

Suppose $p, q_1, q_2, \ldots, q_t$ are prime numbers. If $p \mid (q_1 q_2 \cdots q_t)$, then $p = q_i$, for some $1 \leq i \leq t$.

- We use induction on t.
  - If $t = 1$, then $p \mid q_1$. Since q_1 is prime, the only positive number $\neq 1$ that divides q_1 is q_1. Therefore, we must have $p = q_1$.
  - Assume that the statement is true for $t = k$, i.e., that if $p \mid (q_1 q_2 \cdots q_k)$, then $p = q_i$, for some $1 \leq i \leq k$.
  - Suppose, now that $p \mid (q_1 q_2 \cdots q_{k+1})$. Then $p \mid [(q_1 q_2 \cdots q_k) \cdot q_{k+1}]$. By the preceding lemma, we get that $p \mid (q_1 q_2 \cdots q_k)$ or $p \mid q_{k+1}$.
    - If $p \mid (q_1 q_2 \cdots q_k)$, by the induction hypothesis, $p = q_i$, for some $1 \leq i \leq k$.
    - If $p \mid q_{k+1}$, then, using the argument of the base case, $p = q_{k+1}$.

    Thus, in every case $p = q_i$, for some $1 \leq i \leq k + 1$.

This concludes the proof of the Lemma.

The Fundamental Theorem: Existence

The Fundamental Theorem of Arithmetic

Let n be a positive integer. Then n factors into a product of primes. The factorization of n into primes is unique up to the order of the primes.

- We first show existence:
  - Suppose that not all positive integers factor into primes. Let X be the set of all positive integers that do not factor into primes. Note that $1 \notin X$. Also $2 \notin X$ because 2 is a prime.
    By the Well-Ordering Principle, there is a least element x of X. Since $x \neq 1$ and x is not prime, it is composite. Thus, there is an integer a with $1 < a < x$ and $a \mid x$. So, there is an integer b with $ab = x$. Since $a < x$, $1 < \frac{x}{a} = b$. Because $1 < a$, we get $b < ab = x$. Thus $1 < b < x$. Therefore a and b are both positive integers less than x. Since x is the least element of X, neither a nor b is in X, so both a and b can be factored into primes. Suppose the prime factorizations of a and b are $a = p_1 p_2 \cdots p_s$ and $b = q_1 q_2 \cdots q_t$. Then $x = ab = (p_1 p_2 \cdots p_s)(q_1 q_2 \cdots q_t)$ is a prime factorization of x, contradicting $x \in X$. So all positive integers can be factored into primes.

The Fundamental Theorem: Uniqueness

- We continue with the proof of uniqueness:
  - Suppose, for the sake of contradiction, that some positive integers can be factored into primes in two distinct ways.
    Let Y be the set of all such integers with two (or more) distinct factorizations. Note that $1 \notin Y$ because 1 can be factored only as the empty product of primes. The supposition is that $Y \neq \emptyset$, and therefore Y contains a least element y. Thus y can be factored into primes in two distinct ways: $y = p_1 p_2 \cdots p_s$ and $y = q_1 q_2 \cdots q_t$, where the two lists of primes are not rearrangements of one another.
  - Claim: The list $(p_1, p_2, \ldots, p_s)$ and the list $(q_1, q_2, \ldots, q_t)$ have no elements in common (i.e., $p_i \neq q_j$, for all i and j).
    - If the two lists had a prime r in common, then y/r would be a smaller integer (than y) that factors into primes in two distinct ways, contradicting the fact that y is smallest in Y.
  - Now consider p_1. Notice that $p_1 \mid y$, so $p_1 \mid (q_1 q_2 \cdots q_t)$. Then p_1 must equal one of the q_s, contradicting the claim.

Infinitude of Primes

Theorem (Infinitude of Primes)

There are infinitely many prime numbers.

- Suppose, for the sake of contradiction, that there are only finitely many prime numbers. In such a case, we could list them all: $2, 3, 5, 7, \ldots, p$ where p is the (alleged) last prime number. Let $n = (2 \cdot 3 \cdot 5 \cdot \cdots \cdot p) + 1$. That is, n is the positive integer formed by multiplying together all the prime numbers and then adding 1. Is n a prime? The answer is no. Clearly n is greater than the last prime p, so n is not prime. Since n is not prime, n must be composite. Let q be any prime. Because $n = (2 \cdot 3 \cdots q \cdots p) + 1$, when we divide n by q, we are left with a remainder of 1. We see that there is no prime number q with $q \mid n$, contradicting the Fundamental Theorem.

Primes in Prime Factorizations of Divisors

- Suppose a and b are positive integers. Then, they can be factored into primes as

$$a = 2^{e_2}3^{e_3}5^{e_5}7^{e_7}\cdots \quad \text{and} \quad b = 2^{f_2}3^{f_3}5^{f_5}7^{f_7}\cdots .$$

- Example: If $a = 24$ we would have

$$24 = 2^3 3^1 5^0 7^0 \cdots .$$

- Suppose $a \mid b$. Let p be a prime and suppose it appears e_p times in the prime factorization of a. Since $p^{e_p} \mid a$ and $a \mid b$, we have $p^{e_p} \mid b$, and therefore $p^{e_p} \mid p^{f_p}$. Thus $e_p \leq f_p$. In other words, if $a \mid b$, then the number of factors of p in the prime factorization of a is less than or equal to the number of factors of p in the prime factorization of b.

The Formula for Finding the Greatest Common Divisor

- If $a = 2^{e_2}3^{e_3}5^{e_5}7^{e_7}\cdots$ and $b = 2^{f_2}3^{f_3}5^{f_5}7^{f_7}\cdots$ and if $d = \gcd(a, b)$, then
$$d = 2^{x_2}3^{x_3}5^{x_5}7^{x_7}\cdots,$$
where $x_2 = \min\{e_2, f_2\}$, $x_3 = \min\{e_3, f_3\}$, $x_5 = \min\{e_5, f_5\}$, etc.
- Example: For $24 = 2^3 3^1 5^0 7^0\cdots$ and $30 = 2^1 3^1 5^1 7^0\cdots$, we get
$$\begin{aligned}\gcd(24, 30) &= 2^{\min\{3,1\}}3^{\min\{1,1\}}5^{\min\{0,1\}}7^{\min\{0,0\}}\ldots \\ &= 2^1 3^1 5^0 7^0\cdots = 6.\end{aligned}$$

Theorem (GCD Formula)

Let a, b be positive integers with

$$a = 2^{e_2}3^{e_3}5^{e_5}7^{e_7}\cdots \quad \text{and} \quad b = 2^{f_2}3^{f_3}5^{f_5}7^{f_7}\cdots.$$

Then $\gcd(a, b) = 2^{\min\{e_2,f_2\}}3^{\min\{e_3,f_3\}}5^{\min\{e_5,f_5\}}7^{\min\{e_7,f_7\}}\ldots$.

Irrationality of $\sqrt{2}$

Proposition

There is no rational number x such that $x^2 = 2$.

- We want to show that the set $\{x \in \mathbb{Q} : x^2 = 2\}$ is empty. Suppose, for the sake of contradiction, that there is a rational number x such that $x^2 = 2$. Then, there are integers a and b, such that $x = \frac{a}{b}$. We therefore have $(\frac{a}{b})^2 = 2$, which can be rewritten $a^2 = 2b^2$. Consider the prime factorization of the integer $n = a^2 = 2b^2$.
  - On the one hand, since $n = a^2$, the prime 2 appears an even number (perhaps zero) of times in the prime factorization of n.
  - On the other hand, since $n = 2b^2$, the prime 2 appears an odd number of times in the prime factorization of n.

  This contradicts the Fundamental Theorem and, therefore, there is no rational number x such that $x^2 = 2$.

Subsection 6

Euler's φ Function

Euler's φ Function

- How many integers, from 1 to n inclusive, are relatively prime to n?
- Example: Suppose $n = 10$. There are ten numbers in $\{1, 2, \ldots, 10\}$. Of them, the following are relatively prime to 10: $\{1, 3, 7, 9\}$. So there are four numbers from 1 to 10 that are relatively prime to 10.
- The notation $\varphi(n)$ stands for the number of integers from 1 to n (inclusive) that are relatively prime to n.
- The function φ is known as **Euler's totient** or **Euler's phi function**.
- More Examples: Let us evaluate the following:
  - $\varphi(14) = |\{1, 3, 5, 9, 11, 13\}| = 6$;
  - $\varphi(15) = |\{1, 2, 4, 7, 8, 11, 13, 14\}| = 8$;
  - $\varphi(16) = |\{1, 3, 5, 7, 9, 11, 13, 15\}| = 8$;
  - $\varphi(17) = |\{1, 2, 3, \ldots, 16\}| = 16$;
  - $\varphi(25) = |\{1, 2, \ldots, 25\} - \{5, 10, 15, 20, 15\}| = 5^2 - 5 = 20$;
  - $\varphi(5041) = \varphi(71^2) =$
    $|\{1, 2, \ldots, 5041\} - \{1 \cdot 71, 2 \cdot 71, 3 \cdot 71, \ldots, 71 \cdot 71\}| = 71^2 - 71$.
  - $\varphi(2^{10}) = |\{1, 2, \ldots, 2^{10}\} - \{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots, 2^9 \cdot 2\}| = 2^{10} - 2^9$.

Computing Euler's φ Function

Lemma

Suppose p and q are unequal primes. Then we have:

1. $\varphi(p) = p - 1$;
2. $\varphi(p^2) = p^2 - p$;
3. $\varphi(p^n) = p^n - p^{n-1}$, where n is a positive integer;
4. $\varphi(pq) = pq - q - p + 1 = (p-1)(q-1)$.

1. We have $\varphi(p) = |\{1, 2, \ldots, p-1\}| = p - 1$;
2. $\varphi(p^2) = |\{1, 2, \ldots, p^2\} - \{1 \cdot p, 2 \cdot p, \ldots, p \cdot p\}| = p^2 - p$;
3. $\varphi(p^n) = |\{1, 2, \ldots, p^n\} - \{1 \cdot p, 2 \cdot p, \ldots, p^{n-1} \cdot p\}| = p^n - p^{n-1}$;
4. Here, we apply inclusion-exclusion:

$$\begin{aligned}
\varphi(pq) &= |\{1, 2, \ldots, pq\} - (\{1 \cdot p, 2 \cdot p, \ldots, q \cdot p\} \cup \{1 \cdot q, 2 \cdot q, \ldots, p \cdot q\})| \\
&= |\{1, 2, \ldots, pq\}| - |\{1 \cdot p, 2 \cdot p, \ldots, q \cdot p\}| \\
&\quad - |\{1 \cdot q, 2 \cdot q, \ldots, p \cdot q\}| + |\{pq\}| \\
&= pq - q - p + 1 = (p-1)(q-1).
\end{aligned}$$

Totient of a Product of Distinct Primes

Proposition

Suppose $n = p_1 p_2 \cdots p_t$ where the p_i's are distinct primes. Then

$$\begin{aligned}\varphi(n) &= n - \frac{n}{p_1} - \cdots - \frac{n}{p_t} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots + \frac{n}{p_{t-1} p_t} \\ &\quad - \frac{n}{p_1 p_2 p_3} - \frac{n}{p_1 p_2 p_4} - \cdots - \frac{n}{p_{t-2} p_{t-1} p_t} + \cdots \pm \frac{n}{p_1 p_2 \cdots p_t}.\end{aligned}$$

This formula simplifies to

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right).$$

- For $1 \le i \le t$, let $D_i = \{x : 1 \le x \le n \text{ and } p_i \mid x\}$. We apply Inclusion-Exclusion:

$$\begin{aligned}\varphi(n) &= |\{1, 2, \ldots, n\} - (D_1 \cup D_2 \cup \cdots \cup D_n)| \\ &= |\{1, 2, \ldots, n\}| - |D_1| - |D_2| - \cdots - |D_t| \\ &\quad + |D_1 \cap D_2| + |D_1 \cap D_3| + \cdots + |D_{t-1} \cap D_t| \\ &\quad - |D_1 \cap D_2 \cap D_3| - |D_1 \cap D_2 \cap D_4| - \cdots - |D_{t-2} \cap D_{t-1} \cap D_t| \\ &\quad + \cdots \pm |D_1 \cap D_2 \cap \cdots \cap D_t| \\ &= n - \frac{n}{p_1} - \cdots - \frac{n}{p_t} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots + \frac{n}{p_{t-1} p_t} \\ &\quad - \frac{n}{p_1 p_2 p_3} - \frac{n}{p_1 p_2 p_4} - \cdots - \frac{n}{p_{t-2} p_{t-1} p_t} + \cdots \pm \frac{n}{p_1 p_2 \cdots p_t}.\end{aligned}$$

Applying the Proposition

- Consider $n = 2 \cdot 3 \cdot 11 = 66$. We compute, with the long formula:

$$\begin{aligned}
\varphi(66) &= 66 - \frac{66}{2} - \frac{66}{3} - \frac{66}{11} + \frac{66}{2 \cdot 3} + \frac{66}{2 \cdot 11} + \frac{66}{3 \cdot 11} - \frac{66}{2 \cdot 3 \cdot 11} \\
&= 66 - 33 - 22 - 6 + 11 + 3 + 2 - 1 \\
&= 20
\end{aligned}$$

and with the simplified formula:

$$\begin{aligned}
\varphi(66) &= 66 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) \\
&= 66 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{10}{11} \\
&= 20.
\end{aligned}$$

Euler Totient Formula

Theorem (Euler Totient Formula)

Let n be any positive integer. Factor n into primes $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, where the p_i's are distinct primes and the exponents a_i are all positive integers. Then,

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right).$$

- For $1 \leq i \leq t$, let $D_i = \{x : 1 \leq x \leq n \text{ and } p_i \mid x\}$. We apply again Inclusion-Exclusion:

$$\begin{aligned}
\varphi(n) &= |\{1, 2, \ldots, n\} - (D_1 \cup D_2 \cup \cdots \cup D_n)| \\
&= |\{1, 2, \ldots, n\}| - |D_1| - |D_2| - \cdots - |D_t| \\
&\quad + |D_1 \cap D_2| + |D_1 \cap D_3| + \cdots + |D_{t-1} \cap D_t| \\
&\quad - |D_1 \cap D_2 \cap D_3| - |D_1 \cap D_2 \cap D_4| - \cdots - |D_{t-2} \cap D_{t-1} \cap D_t| \\
&\quad + \cdots \pm |D_1 \cap D_2 \cap \cdots \cap D_t| \\
&= n - \frac{n}{p_1} - \cdots - \frac{n}{p_t} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots + \frac{n}{p_{t-1} p_t} \\
&\quad - \frac{n}{p_1 p_2 p_3} - \frac{n}{p_1 p_2 p_4} - \cdots - \frac{n}{p_{t-2} p_{t-1} p_t} + \cdots \pm \frac{n}{p_1 p_2 \cdots p_t}.
\end{aligned}$$

Multiplicativity of φ

Theorem (Multiplicativity of φ)

Let m, n be positive integers, such that $\gcd(m, n) = 1$. Then $\varphi(mn) = \varphi(m)\varphi(n)$.

- Let $m = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ and $n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$ be the prime decompositions of m and n. Then, since all primes are distinct ($\gcd(m, n) = 1$), we get

$$\begin{aligned}
\varphi(mn) &= \varphi(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}) \\
&= mn\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_t}\right) \\
&= \left[m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)\right]\left[n\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_t}\right)\right] \\
&= \varphi(m)\varphi(n).
\end{aligned}$$