November 07, 2021

Algebra.

<u>Recap: Elements of number theory. Euclidean algorithm and greatest common divisor.</u>

Theorem 1 (division representation).

$$\forall a, b \in \mathbb{Z}, b > 0, \exists q, r \in \mathbb{Z}, 0 \le r < b: a = bq + r$$

Proof. If a is a multiple of b, then $\exists q \in \mathbb{Z}, r = 0 : a = bq = bq + r$. Otherwise, if $a > 0$, then $\exists q > 0 \in \mathbb{Z} : bq < a < b(q + 1)$, and $\exists r = a - bq \in \mathbb{Z} : 0 < r < b$. If $a < 0$, then $\exists q < 0 \in \mathbb{Z} : b(q - 1) < a < bq$, and $\exists r = a - b(q - 1) \in \mathbb{Z} : 0 < r < b$, which completes the proof.

Definition. A number $d \in \mathbb{Z}$ is a common divisor of two integer numbers $a, b \in \mathbb{Z}$, if $\exists n, m \in \mathbb{Z}: a = nd, b = md$.

A set of all positive common divisors of the two numbers $a, b \in \mathbb{Z}$ is limited because these divisors are smaller than the magnitude of the larger of the two numbers. The greatest of the divisors, d, is called the <u>greatest common divisor</u> (gcd) and denoted $d = (a, b)$.

Definition. Two integers $a, b \in \mathbb{Z}$, are called <u>relatively prime</u> if they have no common divisor larger than 1, i. e. $(a, b) = 1$.

Theorem 2. $\forall a, b, q, r \in \mathbb{Z}, (a = bq + r) \Rightarrow \big((a, b) = (b, r)\big)$

Proof. Indeed, if d is a common divisor of $a, b \in \mathbb{Z}$, then $\exists n, m \in \mathbb{Z}: a = nd, b = md \Rightarrow r = a - bq = (n - mq)d$. Therefore, d is also a common divisor of b and $r = a - bq$. Conversely, if d' is a common divisor of b and $r = a - bq$, then $\exists n', m' \in \mathbb{Z}: b = m'd', a - bq = n'd' \Rightarrow a = (n' + m'q)d'$, so d' is a common divisor of b and a. Hence, the statement of the theorem is valid for any divisor of a, b, and for gcd in particular.

Corollary 1 (Euclidean algorithm). In order to find the greatest common divisor $d = (a, b)$, one proceeds iteratively performing successive divisions,

$$a = bq + r, (a, b) = (b, r)$$

$$b = rq_1 + r_1, (b, r) = (r, r_1),$$

$$r = r_1 q_2 + r_2, (r, r_1) = (r_1, r_2),$$

$$r_1 = r_2 q_3 + r_3, (r_1, r_2) = (r_2, r_3), \dots, r_{n-1} = r_n q_{n+1}$$

$$b > r_1 > r_2 > r_3 > \cdots r_n > 0 \Rightarrow \exists d \le b, d = r_n = (a, b)$$

The last positive remainder, r_n, in the sequence $\{r_k\}$ is (a, b), the gcd of the numbers a and b. Indeed, the Eucleadean algorithm ensures that

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n = d$$

Examples.

a. $(385, 105) = (105, 70) = (70, 35) = (35, 0) = 35$
b. $(513, 304) = (304, 209) = (209, 95) = (95, 19) = (19, 0) = 19$

Continued fraction representation. Using the Eucleadean algorithm, one can develop a continued fraction representation for rational numbers,

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}}}$$

This is accomplished by successive substitution, which gives,

$$\frac{a}{b} = q + \frac{r}{b} = q + \frac{1}{\frac{b}{r}}, \frac{b}{r} = q_1 + \frac{r_1}{r} = q_1 + \frac{1}{\frac{r}{r_1}}, \frac{r}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}, \dots, \frac{r_{n-1}}{r_n} = q_{n+1}.$$

Exercise. Show the continued fraction representations for $\frac{385}{105}, \frac{513}{304}, \frac{105}{385}, \frac{304}{513}$.

Example. $\frac{105}{385} = \frac{1}{\frac{385}{105}} = \frac{1}{3+\frac{1}{\frac{105}{70}}} = \frac{1}{3+\frac{1}{1+\frac{1}{\frac{70}{35}}}} = \frac{1}{3+\frac{1}{1+\frac{1}{2}}}$.

Corollary 2 (Diophantine equation). $(d = (a,b)) \Rightarrow (\exists\, k, l \in \mathbb{Z} : d = ka + lb)$

Proof. Consider the sequence of remainders in the Eucleadean algorithm, $r = a - bq$, $r_1 = b - rq_1$, $r_2 = r - r_1 q_2$, $r_3 = r_1 - r_2 q_3$, ..., $r_n = r_{n-2} - r_{n-1} q_n$. Indeed, the successive substitution gives, $r = a - bq$, $r_1 = b - (a - bq)q_1 = k_1 a + l_1 b$, $r_2 = r - (k_1 a + l_1 b)q_2 = k_2 a + l_2 b$, , ..., $r_n = r_{n-2} - (k_{n-1}a + l_{n-1}b)q_n = k_n a + l_n b = d = (a, b)$.

It follows that if d is a common divisor of a and b, then equation $ax + by = d$, called the Diophantine equation, has solution for integer $x, y \in \mathbb{Z}$.

Exercise. Find the representation $d = ka + lb$ for the pairs (385,105) and (513,304) considered in the above examples.

Recap: Elements of number theory. Modular arithmetic.

Definition. For $a, b, n \in \mathbb{Z}$, the congruence relation, $a \equiv b \bmod n$, denotes that, $a - b$ is a multiple of n, or, $\exists q \in \mathbb{Z}, a = nq + b$.

All integers congruent to a given number $r \in \mathbb{Z}$ with respect to a division by $n \in \mathbb{Z}$ form congruence classes, $[r]_n$. For example, for $n = 3$,

$$[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

$$[1]_3 = \{\dots, -2, 1, 4, 7, \dots\}$$

$$[2]_3 = \{\dots, -1, 2, 5, 8, \dots\}$$

$$[3]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\} = [0]_3$$

There are exactly n congruence classes mod n, forming set Z_n. In the above example $n = 3$, the set of equivalence classes is $Z_3 = \{[0]_3, [1]_3, [2]_3\}$. For general n, the set is $Z_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$, because $[n]_n = [0]_n$.

One can define addition and multiplication in Z_n in the usual way,

$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

$$([a]_n)^p = [a^p]_n, p \in \mathbb{N}$$

Here the last relation for power follows from the definition of multiplication.

Exercise. Check that so defined operations do not depend on the choice of representatives a, b in each equivalence class.

Exercise. Check that so defined operations of addition and multiplication satisfy all the usual rules: associativity, commutativity, distributivity.

In general, however, it is impossible to define division in the usual way: for example, $[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$, but one cannot divide both sides by $[3]_6$ to obtain $[2]_6 = [0]_6$. In other words, for general n an element $[a]_n$ of Z_n could give $[0]_n$ upon multiplication by some of the elements in Z_n and therefore would not have properties of an algebraic inverse, so there may exist elements in Z_n which do not have inverse. In practice, this means that if we try to define an inverse element, $[r^{-1}]_n$, to an element $[r]_n$ employing the usual relation, $[r]_n \cdot [r^{-1}]_n = [1]_n$, there might be no element $[r^{-1}]_n$ in class Z_n satisfying this equation. However, it is possible to define the inverse for some special values of r and n. The corresponding classes $[r]_n$ are called invertible in Z_n.

Definition. The congruence class $[r]_n \in Z_n$ is called invertible in Z_n, if there exists a class $[r^{-1}]_n \in Z_n$, such that $[r]_n \cdot [r^{-1}]_n = [1]_n$.

Theorem. Congruence class $[r]_n \in Z_n$ is invertible in Z_n, if and only if r and n are mutually prime, $(r, n) = 1$. Or, $\forall [r]_n, (\exists [r^{-1}]_n \in Z_n) \Leftrightarrow ((r, n) = 1)$.

To find the inverse of $[a] \in Z_n$, we have to solve the equation, $ax + ny = 1$, which can be done using Eucleadean algorithm. Then, $ax \equiv 1 \bmod n$, and $[a]^{-1} = [x]$.

Examples.

3 is invertible mod 10, i. e. in Z_{10}, because $[3]_{10} \cdot [7]_{10} = [21]_{10} = [1]_{10}$, but is not invertible mod 9, i. e. in Z_9, because $[3]_9 \cdot [3]_9 = [0]_9$.

7 is invertible in Z_{15}: $[7]_{15} \cdot [13]_{15} = [91]_{15} = [1]_{15}$, but is not invertible in Z_{14}: $[7]_{14} \cdot [2]_{14} = [14]_{14} = [0]_{14}$.

Solutions to selected homework problems.

1. Using mathematical induction, prove that
    a. $P_n: \sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Solution.

<u>Basis</u>: $P_1: \sum_{k=1}^{1} k^2 = 1 = \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6}$

<u>Induction</u>: $P_n \Rightarrow P_{n+1}$, where $P_{n+1}: \sum_{k=1}^{n+1} k^2 = 1^2 + 2^2 + 3^2 + \cdots + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$

<u>Proof</u>: $\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)}{6}(n(2n+1) + 6n + 6) = \frac{(2n+1)(2n^2+7n+6)}{3} = \frac{(n+1)(n+2)(2n+3)}{6}$,

where we used the induction hypothesis, P_n, to replace the sum of the first n terms with a formula given by P_n. ¤

    b. $P_n: \sum_{k=1}^{n} k^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$

Solution.

<u>Basis</u>: $P_1: \sum_{k=1}^{1} k^3 = 1 = \left[\frac{1(1+1)}{2}\right]^2$

<u>Induction</u>: $P_n \Rightarrow P_{n+1}$, where $P_{n+1}: \sum_{k=1}^{n+1} k^3 = 1^3 + 2^3 + 3^3 + \cdots + (n+1)^3 = \left[\frac{(n+1)(n+2)}{2}\right]^2$

<u>Proof</u>: $\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^{n} k^3 + (n+1)^3 = \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 = \left[\frac{(n+1)}{2}\right]^2 (n^2 + 4n + 4) = \left[\frac{(n+1)(n+2)}{2}\right]^2$, where we used the induction hypothesis, P_n, to replace the sum of the first n terms with a formula given by P_n. ¤

c. $P_n: \sum_{k=1}^{n} \frac{1}{k^2+k} = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$

Solution.

Basis: $P_1: \sum_{k=1}^{1} \frac{1}{k^2+k} = \frac{1}{2} = \frac{1}{1+1}$

Induction: $P_n \Rightarrow P_{n+1}$, where $P_{n+1}: \sum_{k=1}^{n+1} \frac{1}{k^2+k} = \frac{n+1}{n+2}$

Proof: $\sum_{k=1}^{n+1} \frac{1}{k^2+k} = \sum_{k=0}^{n} \frac{1}{k^2+k} + \frac{1}{(n+1)(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{n+1}{n+2}$. ¤

e. $P_n: \forall n, \exists k, 5^n + 3 = 4k$

Solution.

Basis: $P_1: n = 1, \exists k, 5^1 + 3 = 8 = 4k \Leftrightarrow k = 2$

Induction: $P_n \Rightarrow P_{n+1}$, where $P_{n+1}: \forall n, \exists q, 5^{n+1} + 3 = 4q$

Proof: $5^{n+1} + 3 = 5\cdot 5^n + 3 = 5\cdot(4k-3) + 3 = 5\cdot 4k - 12 = 4\cdot(5k-3)$.

Where we used the induction hypothesis, P_n, to replace 5^n with a formula, $5^n = 4k - 3$, given by P_n. ¤

2.   Prove by mathematical induction that for any natural number n,
   a. $5^n + 6^n - 1$ is divisible by 10
   b. $9^{n+1} - 8n - 9$ is divisible by 64

Solution of (b)

Basis: $P_1: 9^2 - 72 - 9 = 0$ is divisible by 64

Induction: $P_n \Rightarrow P_{n+1}$, where $P_{n+1}: \exists k \in \mathbb{Z}, 9^{n+2} - 8(n+1) - 9 = 64k$

Proof: $9^{n+2} - 8(n+1) - 9 = 9\cdot 9^{n+1} - 8n - 17 = 9(9^{n+1} - 8n - 9) + 64n + 64 = 64k$ if $P_n: \exists k' \in \mathbb{Z}, 9^{n+1} - 8n - 9 = 64k'$