Algebra.

Recap: Elements of number theory. Euclidean algorithm and greatest common divisor.

Theorem 1 (division representation).

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

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 greatest common divisor (gcd) and denoted $d = (a, b)$.

Definition. Two integers $a, b \in \mathbb{Z}$, are called relatively prime 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,

$$\begin{gathered} a = bq + r, (a,b) = (b,r) \\ b = rq_1 + r_1, (b,r) = (r,r_1), \\ r = r_1 q_2 + r_2, (r,r_1) = (r_1,r_2), \\ r_1 = r_2 q_3 + r_3, (r_1,r_2) = (r_2,r_3), \dots , \\ r_{n-1} = r_n q_{n+1}, (r_{n-1},r_n) = (r_n,0) \\ b > r_1 > r_2 > r_3 > \cdots r_n > 0 \Rightarrow \exists d \le b, d = r_n = (a,b) \end{gathered}$$

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 Euclidean algorithm, one can develop a continued fraction representation for rational numbers,

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

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 Euclidean algorithm, $r = a - bq\,, r_1 = b - rq_1, r_2 = r - r_1q_2,\ r_3 = r_1 - r_2q_3, \ldots, r_n = r_{n-2} - r_{n-1}q_n$. Indeed, the successive substitution gives, $r = a - bq\,, r_1 = b - (a - bq\,)q_1 = k_1a + l_1b, r_2 = r - (k_1a + l_1b)q_2 = k_2a + l_2b, , \ldots, r_n = r_{n-2} - (k_{n-1}a + l_{n-1}b)q_n = k_na + l_nb = d = (a, b)$.

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.

<u>Recap: Elements of number theory. Modular arithmetic.</u>

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 $n = 3$,

$$\begin{aligned} [0]_3 &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ [1]_3 &= \{\ldots, -2, 1, 4, 7, \ldots\} \\ [2]_3 &= \{\ldots, -1, 2, 5, 8, \ldots\} \\ [3]_3 &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} = [0]_3 \end{aligned}$$

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 $Z_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, 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, $\forall [r]_n, (\exists [r^{-1}]_n \in Z_n) \Leftrightarrow \big((r, n) = 1\big)$.

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}: $[7]_{14} \cdot [2]_{14} = [14]_{14} = [0]_{14}$.