Arithmetic

Math 2151: Discrete Math for Engineering

University of Western Ontario
Fall 2024

Diego Manco (he/him, from Colombia) Office MC 134
e-mail: dmanco@uwo.ca
Office hours: Mon 4:30-5:30pm, Tu 2-3pm, and Wed 2:30-3:30pm.

Arithmetic, first definitions

Definition

Recall that for $m, n \in \mathbb{Z}$, we say that $m|n$ when there is $k \in \mathbb{Z}$ s.t. $n = mk$. We read $m|n$ as m divides n or n is a multiple of m.

Theorem

- $1|a$ *and* $a|0$ *for any* $a \in \mathbb{Z}$.
- *The relation* $|$ *is reflexive and transitive.*
- $(a|b \wedge b|a)$ *implies* $a = \pm b$.
- $a|b$ *implies* $a|bc$ *for any* $c \in \mathbb{Z}$.
- $a|b$ *and* $a|c$ *implies that* $a|(xb + yc)$ *for any* $x, y \in \mathbb{Z}$. *Here* $xb + yc$ *is called a linear combination of* b *and* c.

Definition

We call an integer $p \in \mathbb{Z}^+$ a prime number if the only 2 positive divisors of p are 1 and p itself.

Primes are infinite

Theorem

Let n be an composite (not prime) with $n \geq 1$. Then, there is a prime that divides n.

Proof.

We have to show that the set S of composite numbers with no prime divisors is empty. Assume $S \neq \emptyset$. Then there is $m = minS$. Since m is composite $m = m_1 m_2$ with $1 < m_1 < m$ and $1 < m_2 < m$. So, $m_1 \notin S$ and so there is a prime divisor of m_1, p. $p | m_1 | m_1 m_2$, that is $p | m$, which is impossible. □

Primes are infinite

Theorem

There are infinitely many primes

Proof.

Assume there are finitely many primes $p_1, \ldots, p_n$. Consider the number

$$k = 1 + (p_1 p_2 \cdots p_n)$$

Since $k > p_i$, $k \neq p_i$ for $i = 1, \ldots, n$. So k is not a prime. This means that there is a prime p_j that divides p. Since $p_j | k$ and $p_j | (p_1 p_2 \cdots p_n)$,

$$p_j | (p_1 p_2 \cdots p_n - 1) = 1.$$

This means p_j is not a prime! This is a contradiction. □

Division algorithm

Theorem

If $a, b \in \mathbb{Z}$ with $b > 0$, then, there exist unique $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$.

Proof.

$\exists$xistence: If $b|a$ then $b = qa$ and we can take $r = 0$. Suppose then that b doesn't divides a and consider the set

$$S = \{a - tb : t \in \mathbb{Z} \wedge a - tb > 0\}$$

Exercise: show $S \neq \emptyset$. Since $S \neq \emptyset$ there is a minimum element $r = minS$. By definition of S, $r = a - qb$. Let's see that we can't have $r \geq b$. If $r = b$, then $a = r + qb = b + qb = q(b+1)$ which is impossible since b doesn't divide a. If $r > b$, then $r > r - b > 0$ and $r - b = a - qb > 0$, so $r - b \in S$ and $r - b < r$ which is impossible since r is minimum. □

Proof continues

Proof.

Uniqueness: We have q and r with $a = qb + r$ and $0 \leq r < b$. But we have to proof that they are unique. So, suppose there are q', r' s.t. $a = q'b + r'$ and $0 \leq r' < b$. Then $qb + r = q'b + r'$, and so

$$b|q - q'| = |r - r'| < b$$

Because since $0 \leq r, r' < b$, $|r - r'| < b$. This forces $|q - q'| < 1$, i.e. $|q - q'| = 0$ and so $q = q'$. This further forces $r = r'$ □

Theorem

If $a = qb + r$ *and* $0 \leq r < |b|$, *then*

$$q = \begin{cases} \lfloor \frac{a}{b} \rfloor, & b > 0 \\ \lceil \frac{a}{b} \rceil, & b < 0 \end{cases}$$

Examples

- Let's divide 93 by 12 we get 93=7(12)+9.
- Let's divide 93 by -12, we get 93=(-7)(-12)+9.
- Let's divide -93 by -12, we get -93=8(-12)+3.

Numbers in different basis

We usually represent integers in base 10. For example 1999 is a number in base 10, meaning that

$$1999 = 1(10)^3 + 9(10)^2 + 9(10) + 9(10)^0$$

We can obtain this representation from the division algorithm in the following way.

$$\begin{aligned} 1999 &= 10(199) + 9 && \text{divide by 10} \\ 199 &= 10(19) + 9 && \text{divide by 10} \\ 19 &= 10(1) + 9 && \text{divide by 10} \\ 1 &= 10(0) + 1 && \text{divide by 10} \end{aligned}$$

We get that

$$1999 = 1(10)^3 + 9(10)^2 + 9(10) + 9(10)^0$$

Let's now calculate 1999 in base 3, we are looking for integers $r_0, \ldots, r_k$ s.t. $0 \leq r_i \leq 7$, and

$$1999 = r_k 8^k + r_{k-1} 8^{k-1} + \cdots + r_1 8 + r_0.$$

In this case we write $1999 = (r_k r_{k-1} \cdots r_1 r_0)_8$

$$\begin{aligned}
2999 &= 3(666) + 1 \\
666 &= 3(222) + 0 \\
222 &= 3(74) + 0 \\
74 &= 3(24) + 2 \\
24 &= 3(8) + 0 \\
8 &= 3(2) + 2 \\
2 &= 3(0) + 2
\end{aligned}$$

Thus,

$$1999 = (2202001)_3$$

Binary, octal and hexagesimal basis

Definition

Given a natural number $b \geq 2$, the base b representation of a natural number N is $(a_k a_{k-1} \cdots a_0)$ where $a_0, \ldots, a_k$ are integers with $0 \leq a_i < b$ and

$$N = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b^1 + r_0 b^0$$

Let's find the binary (base 2), octal (base 8) and hexagesimal (base 16) representations of 1999. We start with binary reasoning as we did before.
1999=2(999)+1,999=2(499)+1, 499=2(249)+1,
249=2(124)+1,124=2(62)+0,62=2(31)+0,
31=2(15)+1,15=2(7)+1,7=2(3)+1,3=2(1)+1,2=2(0)+1. So,

$$1999 = (11111001111)_2$$

Binary, octal and hexagesimal basis

We could do something similar to get 1999 in base 8, but it's easiear when converting base 2 to base 8 to do the following. Divide the number you want to convert into blocks of 3 (because $2^3 = 8$)

$$\underbrace{011}\,\underbrace{111}\,\underbrace{001}\,\underbrace{111}$$

Then transform each block to decimal to get the desired expresion.

$$(11111001111)_2 = (3717)_8$$

This works because

$$\begin{aligned}
&(11111001111)_2 \\
=&2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 0 + 0 + 2^3 + 2^2 + 2^1 + 2^0 \\
=&(0 + 2 + 1)2^9 + (2^2 + 2 + 1)2^6 + (0 + 0 + 1)2^3 + (2^2 + 2 + 1)2^0 \\
=&3(8^3) + 7(8^2) + 1(8^1) + 7(8^0)
\end{aligned}$$

Binary, octal, and hexagesimal basis

For base 16 we need 16 symbols to be able to account for the fact that in an expression $(r_k r_{k-1} \cdots r_0)_{16}$, $0 \leq r_i < 16$. We use the symbols 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E, and F. For example $F_{16} = 15$, $(1A)_{16} = 16 + 10 = 26$.
Let's now convert $1999 = (11111001111)_2$ to base 16. Since $2^4 = 16$ we divide in groups of 4.

$$\underbrace{0111}\underbrace{1100}\underbrace{1111}$$

And then transform each block to hexagesimal. $(0111)_2 = 7 = 7_8$, $(1100)_2 = 12 = C_16$, $1111 = 15 = F_{16}$, and so

$$1999 = (111100111)_2 = (7CF)_{16}$$

Greatest common divisor

L

et $a, b \in \mathbb{Z}$, where either $a \neq 0$ or $b \neq 0$. $c \in \mathbb{Z}^+$ (positive integers) is the greatest common divisor of a, b if

- $c|a$ and $c|b$
- for any positive common divisor of a and b, d, $d|c$.

c is unique and we call it $c = gcd(a, b)$

Although the definition makes sense for negative integers, one usually focuses on the set of positive integers $\mathbb{Z}^+$. In the set $\mathbb{Z}^+$, the divisibility relation $|$ is a partial order and for $a, b \in \mathbb{Z}^+$ $gcd(a, b) = a \wedge b$ in this partial order.

Greatest common divisors exist

The proof of this theorem says that $gcd(a,b)$ is the minimum linear combination of a and b

Theorem

Let $a,b \in \mathbb{Z}^+$, then there is a unique greatest common divisor of a and b and we call it $gcd(a,b)$

Proof.

Consider the set $S = \{as + bt : s,t \in \mathbb{Z} \wedge as + bt > 0\}$. $S \neq \emptyset$ (why?). By the well ordering principle there is $c = minS$. Since $c \in S$, $c = ax + by$. First of all, if $d|a$ and $d|b$, then $d|(ax + by) = c$.
Let's now prove $c|a$. By contradiction suppose $\neg(c|a)$, then $a = qc + r$, $0 < r < c$. So, $r = a - qc = a - qax - qby = a(1 - z) - b(qy) \in S$. This is impossible. Similarly $c|b$.
Uniqueness is easy, prove it! $\square$

Euclidean algorithm

The Euclidean algorighm allows not only finding the gcd of two numbers but also expressing it as a linear combination of the two.

Theorem

Euclidean Algorithm Let $z, b \in \mathbb{Z}^+$. Set $r_0 = a$, and $r_1 = b$ and apply the division algorithm iteratively as follows:

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2 \\
&\dots \\
r_i &= q_{i+1} r_{i+1} + r_{i+2}, && 0 < r_{i+2} < r_{i+1} \\
&\dots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n.
\end{aligned}
$$

The last nonzero remainder is $gcd(a, b) = r_n$

Proof of the Euclidean algorithm

Proof.

By the last equation $r_n | r_{n-1}$. Since r_n divides both r_n and r_{n-1}, by the second to last equation, $r_n | r_{n-2}$. Continuing in this way we realize that $r_n | r_1$ and $r_n | r_0$. So, r_n is a common divisor.
Now, suppose $c|a$ and $c|b$. By the first equation, since $c|r_0$ and $c|r_1$, $c|r_2$. By the second equation, since $c|r_1$ and $c|r_2$, $c|r_3$. Continuing this way we conclude that $c|r_n$ as we wanted to show. □

Next we will show an example of calculating the gcd of two numbers using the Euclidean algorithm and expressing this gcd as a linear combination of the two numbers.

Examples

Find $gcd(2020, 322)$ and express it as a linear combination of 2020 and 322.

$$
\begin{align}
2020 &= 322(6) + 88 \tag{1}\\
322 &= 88(3) + 58 \tag{2}\\
88 &= 58(1) + 30 \tag{3}\\
58 &= 30(1) + 28 \tag{4}\\
30 &= 28(1) + 2 \tag{5}\\
28 &= 2(14) + 0 \tag{6}
\end{align}
$$

This means that $2 = gcd(2020, 322)$. Now,

$$
\begin{aligned}
2 &= 30 - 28, && \text{from (5)}\\
&= 30 - (58 - 30) = -58 + 2(30), && \text{from (4)}\\
&= -58 + 2(88 - 58) = 2(88) - 3(58), && \text{from (3)}\\
&= 2(88) - 3(322 - 3(88)) = 11(88) - 3(3222)\\
&= 11(2020 - 6(322)) - 3(322) = 11(2020) - 69(322)
\end{aligned}
$$