Notes on Modular Arithmetic

Scribe: Diantha Gardener Lecturer/Editor: Chris Eppolito

10 February 2020

Proposition (Division Algorithm)**.** *Let $n, d \in \mathbb{Z}$ with $d \in \mathbb{Z}^+$. Then there exists a unique pair $q, r \in \mathbb{Z}$ satisfying both $n = dq + r$ and $0 \leq r \leq d - 1$.*

In $n = dq+r$, we d is the *dividend* or *modulus*, q is the *quotient*, and r is the *remainder*. This proposition is better called the *Quotient-Remainder Theorem.*

Example 1. For $n = 7$ and $d = 3$ we have $7 = n = dq + r = 3 \cdot 2 + 1$.

Definition. Given modulus $d \in \mathbb{Z}^+$, for any $a, b \in \mathbb{Z}$. We say a is equivalent to b modulo d when a and b have the same remainder under division by d. We write $a \equiv b \pmod 3$

Example 2. We have the following reductions modulo 3.

$$\begin{aligned} -3 &= 3 \cdot (-1) + 0 \equiv 0 \pmod 3 & \qquad 0 &= 3 \cdot 0 + 0 \equiv 0 \pmod 3 \\ -2 &= 3 \cdot (-1) + 1 \equiv 1 \pmod 3 & \qquad 1 &= 3 \cdot 0 + 1 \equiv 1 \pmod 3 \\ -1 &= 3 \cdot (-1) + 2 \equiv 2 \pmod 3 & \qquad 2 &= 3 \cdot 0 + 2 \equiv 2 \pmod 3 \end{aligned}$$

Proposition. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. The following are equivalent.*

1. *We have $a \equiv b \pmod m$.*
2. *Both a and b have the same remainder modulo m.*
3. *We have $m \mid (a - b)$.*
4. *We have $a = mk + b$ for some $k \in \mathbb{Z}$.*

Proof. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.
(1 $\iff$ 2): This is the definition of $a \equiv b \pmod m$.
(2 $\implies$ 3): Assume a and b have the same remainder modulo m. Applying the Division Algorithm we obtain $a = mq_1 + r$ and $b = mq_2 + r$ for some $q_1, q_2, r \in \mathbb{Z}$ with $0 \leq r \leq m - 1$. Now

$$a - b = (mq_1 + r) - (mq_2 + r) = (mq_1 - mq_2) + (r - r) = m(q_1 - q_2),$$

and $q_1 - q_2 \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under subtraction. Hence $m \mid (a - b)$ by definition.
(3 $\implies$ 4): Assume $m \mid (a - b)$. By definition of divisibility there is a $k \in \mathbb{Z}$ s.t. $a - b = mk$. Adding b to both sides we obtain $a = (a - b) + b = mk + b$.
(4 $\implies$ 1): Suppose $a = mk + b$ for some $k \in \mathbb{Z}$. Note $b = mq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r \leq m - 1$ by the Division Algorithm. Now $a = mk + b = mk + (mq + r) = m(k + q) + r$; noting $k + q \in \mathbb{Z}$ by closure and $0 \leq r \leq m - 1$, we have r is the remainder of a modulo m by the uniqueness of remainders. Hence a and b have the same remainder modulo m. □

Proposition. *Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv c \pmod m$ and $b \equiv d \pmod m$, then*

1. *$ab \equiv cd \pmod m$, and*
2. *$a + b \equiv c + d \pmod m$.*

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ satisfy $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. By the previous proposition, there are integers $k_1, k_2 \in \mathbb{Z}$ such that $a = mk_1 + c$ and $b = mk_2 + d$.

Part 1: Taking the product we obtain

$$ab = (mk_1 + c)(mk_2 + d) = mk_1mk_2 + cmk_2 + mk_1d + cd = m(k_1mk_2 + ck_2 + k_1d) + cd.$$

Moreover, $k_1mk_2 + ck_2 + k_1d \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Hence $ab \equiv cd \pmod{m}$ by previous proposition.

Part 2: Taking the sum we obtain

$$a + b = (mk_1 + c) + (mk_2 + d) = m(k_1 + k_2) + (c + d).$$

Moreover $k_1 + k_2 \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$. Hence $a + b \equiv c + d \pmod{m}$ by previous proposition.

We conclude the original statement is true. $\square$

We obtain a new arithmetic system for each $m \in \mathbb{Z}^+$ as follows. Define the *class* of integer a modulo m as $m\mathbb{Z} + a := \{mq + a : q \in \mathbb{Z}\}$. When m is fixed in context, we sometimes write $[a] = m\mathbb{Z} + a$. The set of classes modulo m is denoted

$$\mathbb{Z}/m\mathbb{Z} := \{m\mathbb{Z} + a : a \in \mathbb{Z}\} = \{m\mathbb{Z} + r : 0 \leq r \leq m - 1,\ r \in \mathbb{Z}\}.$$

Indeed, the class of an integer is equal to the class of its remainder. This is because $a = mq + r$ by the Division Algorithm and thus $a \equiv r \pmod{m}$ by our proposition above.

The operations modulo m are $[a] \cdot [b] = [ab]$ and $[a] + [b] = [a + b]$. Previous proposition yields that these operation are "well-defined", i.e. independent of choice of representatives.

Example 3. We make operation tables for $\mathbb{Z}/6\mathbb{Z}$ below.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Note that in $\mathbb{Z}/6\mathbb{Z}$ we have $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$. Such elements $a, b \in \mathbb{Z}/m\mathbb{Z}$ with $a \neq [0] \neq b$ are called *nontrivial zero divisors* in $\mathbb{Z}/m\mathbb{Z}$. To better understand multiplication modulo m, we must understand zero-divisors. Obviously every divisor $d \mid m$ with $d \notin \{\pm 1, \pm m\}$ yields a nontrivial zero-divisor of $\mathbb{Z}/m\mathbb{Z}$; indeed $m = dk$ for some $k \in \mathbb{Z}$ yields $[d] \cdot [k] = [dk] = [m] = [0]$, and the assumption $d \notin \{1, m\}$ yields $1 < |k| < |m|$, so $[d] \neq [0] \neq [k]$. Dual to zero divisors are units; an $a \in \mathbb{Z}$ is a *unit* modulo $m \in \mathbb{Z}^+$ when there is an $s \in \mathbb{Z}$ such that $as \equiv 1 \pmod{m}$.

Example 4. We see 1 and 5 are the only units modulo 6 by examining the multiplication table.

We next study the greatest common divisor in order to obtain a characterization of units modulo m.

Definition. The *greatest common divisor* of integers $a, b \in \mathbb{Z}$, denoted $\gcd(a, b)$, is the largest integer which divides both a and b.

Remark. Note that $\gcd(0, 0)$ is ill-defined because every integer divides 0. Otherwise $\max(|a|, |b|)$ is an upper bound for $\gcd(a, b)$.

Example 5. We compute $\gcd(18, 26)$ using the definition below.

$$\begin{aligned}
\gcd(18, 26) &= \max\{n \in \mathbb{Z} : n \mid 18 \text{ and } n \mid 26\} \\
&= \max(\{n \in \mathbb{Z} : n \mid 18\} \cap \{n \in \mathbb{Z} : n \mid 26\}) \\
&= \max(\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\} \cap \{\pm 1, \pm 2, \pm 13, \pm 26\}) \\
&= \max\{\pm 1, \pm 2\} \\
&= 2
\end{aligned}$$

Remark. This method of computing $\gcd(a,b)$ by trial divisions is inefficient. There's a better way!

Algorithm (Euclid's Algorithm)**.** Let $a, b \in \mathbb{Z}$ such that $(a,b) \neq (0,0)$.

1. Let $n_0 \coloneqq \max(|a|,|b|)$ and $d_0 \coloneqq \min(|a|,|b|)$.
2. While $d_i \neq 0$:
   (a) Apply the Division Algorithm to obtain $n_i = d_i q_i + r_i$ for some $q_i, r_i \in \mathbb{Z}$ with $0 \leq r_i < d_i$.
   (b) Set $n_{i+1} \coloneqq d_i$ and $d_{i+1} \coloneqq r_i$, increment i, and continue.
3. Output n_k (i.e. the last value of n).

Example 6. We compute $\gcd(18,26)$ via Euclid's Algorithm.

$$\begin{array}{llcr} n_0 \coloneqq 26, & d_0 \coloneqq 18 & \rightsquigarrow & 26 = 18 \cdot 1 + 8 \\ n_1 \coloneqq 18, & d_0 \coloneqq 8 & \rightsquigarrow & 18 = 8 \cdot 2 + 2 \\ n_2 \coloneqq 8, & d_0 \coloneqq 2 & \rightsquigarrow & 8 = 2 \cdot 4 + 0 \\ n_3 \coloneqq 2, & d_0 \coloneqq 0 & \rightsquigarrow & \gcd(18,26) = 2. \end{array}$$

Our next example illustrates the method of *back substitution* to obtain a nice expression for the gcd.

Example 7. We compute $\gcd(5,8)$ via Euclid's Algorithm.

$$\begin{array}{lcr} 8 = 5 \cdot 1 + 3 & \rightsquigarrow & 3 = 8 - 5 \cdot 1 \\ 5 = 3 \cdot 1 + 2 & \rightsquigarrow & 5 = 5 - 3 \cdot 1 \\ 3 = 2 \cdot 1 + 1 & \rightsquigarrow & 1 = 3 - 2 \cdot 1 \\ 2 = 1 \cdot 2 + 0 & \rightsquigarrow & \gcd(5,8) = 1 \end{array}$$

On the other hand, using the right column of the above table we have the following.

$$\begin{aligned} \gcd(5,8) = 1 &= 3 \cdot 1 - 2 \cdot 1 \\ &= 3 \cdot 1 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 - 5 \cdot 1 \\ &= (8 - 5 \cdot 1) \cdot 2 - 5 \cdot 1 = 8 \cdot 2 + 5 \cdot (-3) \end{aligned}$$

Applying back substitution as above, we express $\gcd(a,b)$ as an integral linear combination of a and b.

Proposition (Bèzout's Lemma)**.** *For all $a, b \in \mathbb{Z}$ with $(a,b) \neq (0,0)$, there are $s, t \in \mathbb{Z}$ with*

$$\gcd(a,b) = as + bt.$$

Idea of Proof. Apply Euclid's Algorithm and then use back-substitution. □

Proposition. *Let $a, m \in \mathbb{Z}$ with $m > 0$. Integer a is a unit modulo m if and only if* $\gcd(a,m) = 1$.

Proof. Let $a, m \in \mathbb{Z}$ with $m > 0$ be arbitrary.
($\Longrightarrow$): Assume a is a unit modulo m. Thus there is an $s \in \mathbb{Z}$ such that $as \equiv 1 \pmod{m}$. Now by a previous proposition there is a $t \in \mathbb{Z}$ such that $as + mt = 1$. Thus every common divisor of a and m divides 1 by elementary properties of divisibility. Hence $\gcd(a,m) = 1$ as the only positive divisor of 1 is 1.
($\Longleftarrow$): Assume $\gcd(a,m) = 1$. Thus by Bèzout's Lemma there are $s, t \in \mathbb{Z}$ with $as + mt = 1$. Thus $as \equiv 1 \pmod{m}$ by a previous proposition. Hence a is a unit modulo m by definition.
We conclude the original statement is true. □