Modular Arithmetic and the Chinese Remainder Thoerem

Discrete Mathematics 27100 Winter 2022

February 2 and 4, 2022

Corresponding sections in Margaret Fleck's "Building Blocks for Theoretical Computer Science": Sections 4.10,4.11.,4.12
Corresponding sections in Rosen's "Discrete Mathematics and Its Applications": Sections 4.1,4.4
Corresponding material in Professor Kurtz's lecture notes: Lecture 4

1 Modular Arithmetic

Recall the division theorem:

Theorem 1.1 (Division Theorem)**.** *For all $n \in \mathbb{Z}$ and all $d \in \mathbb{N}$, there is a unique pair of integers (q, r) such that*

1. $n = qd + r$
2. $0 \leq r \leq d - 1$

Usually, when we do division, we focus on the quotient q. In modular arithmetic, we ignore the quotient and only look at the remainder.

Definition 1.2 (Mod n Operation)**.** *We define $n \mod d$ to be the remainder when we divide n by d.*

Example 1.3. *Some examples of the mod n operation are as follows.*

1. $7 \mod 3 = 1$
2. $23 \mod 5 = 3$
3. $39 \mod 8 = 7$

Mod n can also be seen as a congruence relation and this is extremely useful.

Definition 1.4 (Mod n Congruence Relation)**.** *We say that $a \equiv b \mod n$ if $n \mid b - a$.*

Example 1.5. *Some examples of the mod n congruence relation are as follows.*

1. $7 \equiv 1 \mod 3$
2. $23 \equiv 8 \mod 5$

3. $76 \equiv -4 \mod 8$

Warning 1.6. *Be careful not to confuse the mod n operation with the mod n congruence relation. For example, $10 \equiv 3 \mod 7$ and $10 \mod 7 = 3$ are correct but $10 = 3 \mod 7$ is incorrect because $3 \mod 7 = 3$. When doing modular arithmetic, we will generally want to use the mod n congruence relation.*

1.1 Addition, Subtraction, and Multiplication Modulo n

A key property of the modulo n operation is that it interacts very nicely with arithmetic operations. In particular, in order to compute $x + y$, $x - y$, or $x * y$ modulo n, it is sufficient to know $x \mod n$ and $y \mod n$.

Lemma 1.7. *For all $n \in \mathbb{N}$ and all $a, b, c \in \mathbb{Z}$, if $a \equiv b \mod n$ and $b \equiv c \mod n$ then $a \equiv c \mod n$.*

Proof. If $a \equiv b \mod n$ and $b \equiv c \mod n$ then $\exists x \in \mathbb{Z}(b = a + xn)$ and $\exists y \in \mathbb{Z}(c = b + yn)$. Now $c = b + yn = a + xn + yn = a + (x + y)n$ so $a \equiv c \mod n$, as needed. □

Lemma 1.8. *For all $n \in \mathbb{N}$ and all $a, a', b, b' \in \mathbb{Z}$, if $a' \equiv a \mod n$ and $b' \equiv b \mod n$ then $a' + b' \equiv a + b \mod n$ and $a' - b' \equiv a - b \mod n$*

Proof. If $a' \equiv a \mod n$ and $b' \equiv b \mod n$ then $\exists x \in \mathbb{Z}(a' = a + xn)$ and $\exists y \in \mathbb{Z}(b' = b + yn)$. Now

$$a' + b' = a + xn + b + yn = a + b + (x + y)n$$

and

$$a' + b' = a + xn - (b + yn) = a - b + (x - y)n$$

so $a' + b' \equiv a + b \mod n$ and $a' - b' \equiv a - b \mod n$, as needed. □

Lemma 1.9. *For all $n \in \mathbb{N}$ and all $a, a', b, b' \in \mathbb{Z}$, if $a' \equiv a \mod n$ and $b' \equiv b \mod n$ then $a'b' \equiv ab \mod n$*

Proof. If $a' \equiv a \mod n$ and $b' \equiv b \mod n$ then $\exists x \in \mathbb{Z}(a' = a + xn)$ and $\exists y \in \mathbb{Z}(b' = b + yn)$. Now

$$a'b' = (a + xn)(b + yn) = ab + ayn + xnb + xyn^2 = ab + (ay + bx + xyn)n$$

so $a'b' \equiv ab \mod n$, as needed. □

1.2 $\mathbb{Z}_n$

Since addition, subtraction, and multiplication interact well with the mod n operation, we can define a whole system of arithmetic which just uses remainders modulo n. This system is called $\mathbb{Z}_n$

Definition 1.10. *Given a natural number $n > 1$, the ring $\mathbb{Z}_n$ is defined as follows:*

1. $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$

2. *Given $a, b \in \mathbb{Z}_n$, we define $a+b$ to be $a+b \mod n$, we define $a-b$ to be $a-b \mod n$, and we define $ab = ab \mod n$*

Remark 1.11. *Technically, we should only have the elements $\{0, 1, \dots, n-1\}$ in $\mathbb{Z}_n$. However, it is often convenient to allow all integers to be elements of $\mathbb{Z}_n$. To do this, given $a \in \mathbb{Z}$, we set $a = a \mod n$ in $\mathbb{Z}_n$. Thus, we can think of $\mathbb{Z}_n$ as applying the $\mod n$ operation to every integer.*

Example 1.12.

1. *In $\mathbb{Z}_5$, $2-4=3$.*

2. *In $\mathbb{Z}_{15}$, $4*7=13$.*

Example 1.13. *The multiplication table for $\mathbb{Z}_5$ is as follows:*

	$\times 0$	$\times 1$	$\times 2$	$\times 3$	$\times 4$
$\times 0$	0	0	0	0	0
$\times 1$	0	1	2	3	4
$\times 2$	0	2	4	1	3
$\times 3$	0	3	1	4	2
$\times 4$	0	4	3	2	1

1.3 Invertibility in $\mathbb{Z}_n$

Definition 1.14. *We say that $a \in \mathbb{Z}_n$ is invertible if $\exists a^{-1} \in \mathbb{Z}_n(a^{-1}a = 1)$ in $\mathbb{Z}_n$ (or equivalently, $a^{-1}a \equiv 1 \mod n$).*

Remark 1.15. *If we want to allow all integers to be elements of $\mathbb{Z}_n$, we say that $a \in \mathbb{Z}$ is invertible in $\mathbb{Z}_n$ if $a \mod n$ is invertible in $\mathbb{Z}_n$. If so, we take $a^{-1} = (a \mod n)^{-1}$ in $\mathbb{Z}_n$. Note that $a^{-1}a \equiv (a \mod n)^{-1}(a \mod n) \equiv 1 \mod n$).*

Remark 1.16. *Note that if a has an inverse in $\mathbb{Z}_n$ then this inverse must be unique. To see this, let b, b' be two inverses of a in $\mathbb{Z}_n$ and observe that in $\mathbb{Z}_n$, $b = b(ab') = bab' = (ba)b' = b'$.*

Example 1.17.

1. *In $\mathbb{Z}_5$, $2^{-1} = 3$ as $2*3=6$ and $6 \equiv 1 \mod 5$*

2. *In $\mathbb{Z}_9$, $4^{-1} = 7$ as $4*7=28$ and $28 \equiv 1 \mod 9$*

3. *In $\mathbb{Z}_{12}$, $7^{-1} = 7$ as $7*7=49$ and $49 \equiv 1 \mod 12$*

4. *6 is not invertible in $\mathbb{Z}_{21}$*

Lemma 1.18. *For all natural numbers $n > 1$, $a \in \mathbb{Z}_n$ is invertible if and only if $gcd(a, n) = 1$*

Proof. If $gcd(a, n) = 1$ then by Bézout's identity, $\exists x, y \in \mathbb{Z}(xa + yn = 1)$. This implies that $ax \equiv 1 \mod n$ so we can take $a^{-1} = x \mod n$. Conversely, if a is invertible in $\mathbb{Z}_n$ then in $\mathbb{Z}$, $a^{-1}a = 1 + kn$ for some $k \in \mathbb{Z}$. Rearranging, we have that $1 = a^{-1}a - kn$. Since $gcd(a, n) \mid a$ and $gcd(a, n) \mid n$, $gcd(a, n) \mid a^{-1}a - kn = 1$. Thus, $gcd(a, n) = 1$, as needed. $\square$

Remark 1.19. *Recall that for all integers x, y, k such that x, y are not both 0, $gcd(x - ky, y) = gcd(x, y)$. Thus for any natural number $n > 1$ and any integer a, $gcd(a, n) = gcd(a \mod n, n)$. Thus, we can again extend this result to all $a \in \mathbb{Z}$ by replacing a with $a \mod n$.*

Proposition 1.20. *For all natural numbers $n > 1$ and all $a, b \in \mathbb{Z}_n$, ab is invertible if and only if a and b are both invertible. Moreover, in this case, $(ab)^{-1} = a^{-1}b^{-1}$ (where the multiplication is done in $\mathbb{Z}_n$).*

Proof. Observe that if $a, b \in \mathbb{Z}_n$ are both invertible then $a^{-1}b^{-1}ab = a^{-1}b^{-1}ba = a^{-1}a = 1$. Conversely, if ab is invertible then $(ab)^{-1}ab = ((ab)^{-1}a)\, b = ((ab)^{-1}b)\, a = 1$ so both a and b are invertible in $\mathbb{Z}_n$. $\square$

Corollary 1.21. *For all $n \in \mathbb{N}$ and all $a, b \in \mathbb{Z}$, $gcd(ab, n) = 1$ if and only if $gcd(a, n) = 1$ and $gcd(b, n) = 1$.*

Proof. If $n = 1$ then $gcd(ab, n) = gcd(a, n) = gcd(b, n) = 1$. If $n > 1$, observe that $gcd(ab, n) = 1$ if and only if ab is invertible in $\mathbb{Z}_n$, which is true if and only if both a and b are invertible in $\mathbb{Z}_n$, which in turn is true if and only if $gcd(a, n) = gcd(b, n) = 1$. $\square$

1.4 Division in $\mathbb{Z}_p = \mathbb{F}_p$

If p is prime then $\forall a \in [p-1](gcd(a, p) = 1)$. Thus, every element of $\mathbb{Z}_p$ except 0 is invertible. This allows us to define division in $\mathbb{Z}_p$

Definition 1.22. *Let p be a prime number. Given $a, b \in \mathbb{Z}_p$ such that $b \neq 0$, we define $\frac{a}{b}$ to be $\frac{a}{b} = ab^{-1}$*

Since we have division in $\mathbb{Z}_p$, $\mathbb{Z}_p$ is a finite field which is often denoted as $\mathbb{F}_p$

2 The Chinese Remainder Theorem

Theorem 2.1 (Chinese Remainder Theorem)**.** *Let $\{d_1, \ldots, d_k\}$ be a set of natural numbers such that*

1. $\forall i(d_i > 1)$
2. *For all $i, j \in [k]$ such that $i \neq j$, $gcd(d_i, d_j) = 1$ (i.e. each pair of these numbers is relatively prime)*

For any set of remainders $\{r_1, \ldots, r_k\}$ such that $\forall i, 0 \leq r_i < d_i$, there exists a unique integer n such that

1. $\forall i \in [k](n \mod d_i = r_i)$
2. $0 \leq n < \prod_{i=1}^{k} d_i$

Proof. To prove that n exists, we describe how to find such an n. The idea is to find an integer e_i for each $i \in [k]$ such that

1. $e_i \equiv 1 \mod d_i$
2. $\forall j \in [k] \setminus \{i\}(e_i \equiv 0 \mod d_j)$

We can then take $n = \sum_{i=1}^{k} r_i e_i \mod \prod_{i=1}^{k} d_i$.

To find e_i, we do the following

1. Observe that since $\forall j \in [k] \setminus \{i\}(gcd(d_i, d_j) = 1)$, we have that $gcd(d_i, \prod_{j\in[k]\setminus\{i\}} d_j) = 1$. Thus, $\prod_{j\in[k]\setminus\{i\}} d_j$ is invertible in $\mathbb{Z}_{d_i}$. Let a_i be the inverse of $\prod_{j\in[k]\setminus\{i\}} d_j$ in $\mathbb{Z}_{d_i}$.
2. Take $e_i = a_i \prod_{j\in[k]\setminus\{i\}} d_j$. Now observe that since a_i is the inverse of $\prod_{j\in[k]\setminus\{i\}} d_j$ in $\mathbb{Z}_{d_i}$, $a_i \prod_{j\in[k]\setminus\{i\}} d_j \equiv 1 \mod d_i$. Moreover, for all $j \in [k] \setminus \{i\}$, $d_j \mid e_i$ so $e_i \equiv 0 \mod d_j$.

If we take $n = \sum_{i=1}^{k} r_i e_i$ then for all $i \in [k]$, $n \equiv r_i e_i + \sum_{j\in[k]\setminus\{i\}} r_j e_j \equiv r_i \mod d_i$. In order to make n less than $\prod_{i=1}^{k} d_i$ we take $n = \sum_{i=1}^{k} r_i e_i \mod \prod_{i=1}^{k} d_i$ (note that this does not affect any of the remainders because for all $i \in [k]$, $\prod_{i=1}^{k} d_i \equiv 0 \mod d_i$).

To show that n is unique, assume that n' also satisfies these conditions. Now observe that $\forall i \in [k](n' - n \equiv 0 \mod d_i)$ so $d_i \mid (n' - n)$.

Since $\{d_1, \ldots, d_k\}$ are relatively prime, the least common multiple of $\{d_1, \ldots, d_k\}$ is $\prod_{i=1}^{k} d_i$ so $\prod_{i=1}^{k} d_i \mid (n' - n)$. Since $0 \leq n < \prod_{i=1}^{k} d_i$ and $0 \leq n' < \prod_{i=1}^{k} d_i$, we must have that $n' = n$, as needed. □

Example 2.2. *Find an integer n such that*

1. $n \equiv 4 \mod 5$
2. $n \equiv 4 \mod 6$
3. $n \equiv 1 \mod 7$

Answer: We take the following steps

1. *To find an integer e_1 such that $e_1 \equiv 1 \mod 5$, $e_1 \equiv 0 \mod 6$, and $e_1 \equiv 0 \mod 7$, start with $6 * 7 = 42$. Since $42 \equiv 2 \mod 5$ and $2^{-1} = 3$ in $\mathbb{Z}_5$, we can take $e_1 = 3 * 42 = 126$.*
2. *To find an integer e_2 such that $e_2 \equiv 0 \mod 5$, $e_2 \equiv 1 \mod 6$, and $e_2 \equiv 0 \mod 7$, start with $5 * 7 = 35$. Since $35 \equiv 5 \mod 6$ and $5^{-1} = 5$ in $\mathbb{Z}_6$, we can take $e_2 = 5 * 35 = 175$.*
3. *To find an integer e_3 such that $e_3 \equiv 0 \mod 5$, $e_3 \equiv 0 \mod 6$, and $e_3 \equiv 1 \mod 7$, start with $5 * 6 = 30$. Since $30 \equiv 2 \mod 7$ and $2^{-1} = 4$ in $\mathbb{Z}_7$, we can take $e_3 = 4 * 30 = 120$.*
4. *Now that we have found e_1, e_2, and e_3, we can take $n = 4e_1 + 4e_2 + e_3 = 504 + 700 + 120 = 1324$.*
5. *If we want that $0 \leq n < 5 * 6 * 7 = 210$, then we can instead take $1324 \mod 210$. Dividing 1324 by 210, we get a remainder of $1324 - 6 * 210 = 1324 - 1260 = 64$ so we can take $n = 64$.*

Remark 2.3. *Rather than finding e_i and then multiplying it by r_i, we can instead directly find a number c_i such that $c_i \prod_{j\in[k]\setminus\{i\}} d_j \equiv r_i \mod d_i$ and then take $x_i = c_i \prod_{j\in[k]\setminus\{i\}} d_j$ instead of $r_i e_i$.*

For example, here we have that $42 \equiv 2 \mod 5$ and $2 * 2 \equiv 4 \mod 5$ so we can take $x_1 = 2 * 42 = 84$ instead of $r_1 e_1 = 4 * 126 = 504$. Observe that $504 \equiv 84 \mod 210$ so we will end up with the same result modulo 210.