5 Inverses

In this section, we study under which conditions there is a multiplicative inverse in modular arithmetic. Specifically, we consider the following four statements.

I. The integer a has a multiplicative inverse in $\mathbb{Z}_n$.

II. The linear equation $a \cdot_n x = b$ has a solution in $\mathbb{Z}_n$.

III. The linear equation $ax + ny = 1$ has a solution in the integers.

IV. The integers a and n are relative prime.

We will see that all four statements are equivalent, and we will prove all necessary implications to establish this, except for one, which we will prove in the next section.

Examples. Before starting the proofs, we compute multiplicative inverses for a few values of n and a; see Table 1. Except for $a = 0$, all values of a have multiplicative inverses if $n = 2, 3, 5, 7$ but not if $n = 4, 6, 8, 9$. In the latter case, we have multiplicative inverses for some values of a but not for all. We will later find out that the characterizing condition for the existence of the multiplicative inverse is that n and a have no non-trivial common divisor.

$n = 2$	a	0	1						
	a'		1						
$n = 3$	a	0	1	2					
	a'		1	2					
$n = 4$	a	0	1	2	3				
	a'		1		3				
$n = 5$	a	0	1	2	3	4			
	a'		1	2	3	4			
$n = 6$	a	0	1	2	3	4	5		
	a'		1				5		
$n = 7$	a	0	1	2	3	4	5	6	
	a'		1	4	5	2	3	6	
$n = 8$	a	0	1	2	3	4	5	6	7
	a'		1		3		5		7
$n = 9$	a	0	1	2	3	4	5	6	7	8
	a'		1	5		7	2		4	8

Table 1: Values of n for which a has a multiplicative inverse a'. Black entries indicate the inverse does not exist.

Linear equations modulo n. Here we prove "I $\iff$ II". The *multiplicative inverse* of an integer $a \in \mathbb{Z}_n$ is another integer $a' \in \mathbb{Z}_n$ such that $a' \cdot_n a = a \cdot_n a' = 1$. We note that the multiplicative inverse is unique, if it exists. Indeed, if $a'' \cdot_n a = 1$ then we can multiply with a' from the right and get $a' \cdot_n (a \cdot_n a') = a'' \cdot_n (a \cdot_n a')$ and therefore $a' = a''$. If a has a multiplicative inverse, we can use it to solve a linear equation. Multiplying with the inverse from the left and using associativity, we get

$$\begin{aligned} a \cdot_n x &= b; \\ (a' \cdot_n a) \cdot_n x &= a' \cdot_n b; \\ x &= a' \cdot_n b. \end{aligned}$$

Since the multiplicative inverse is unique, so is the solution $x = a' \cdot_n b$ to the linear equation. We thus proved a little bit more than I $\implies$ II, namely also the uniqueness of the solution.

A. If a has a multiplicative inverse a' in $\mathbb{Z}_n$ then for every $b \in \mathbb{Z}_n$, the equation $a \cdot_n x = b$ has the unique solution $x = a' \cdot_n b$.

Every implication has an equivalent contrapositive form. For a statement I $\implies$ II this form is $\neg$II $\implies \neg$I. We state the contrapositive form in this particular instance.

A'. If $a \cdot_n x = b$ has no solution in $\mathbb{Z}_n$ then a does not have a multiplicative inverse.

To prove A' we just need to assume that it is false, that is, that $\neg$II and I both hold. But if we have I then we also have II. Now we have $\neg$II as well as II. But this is a contradiction with they cannot both be true. What we have seen here is a very simple version of a proof by contradiction. More complicated versions will follow later.

By setting $b = 1$, we get $x = a'$ as a solution to $a \cdot_n x = 1$. In other words, $a' \cdot_n a = a \cdot_n a' = 1$. Hence, II $\implies$ I. This particuar implication is called the converse of I $\implies$ II, which should not be confused with the contrapositive. The converse is a new, different statement, while the contrapositive is logically eqivalent to the original implication, no matter what the specifics of the implication are.

Linear equations in two variables. Here we prove "II $\iff$ III". Recall that $a \cdot_n x = 1$ is equivalent to $ax \bmod n = 1$. Writing $ax = qn + r$ with $0 \le r < n$, we see that $ax \bmod n = 1$ is equivalent to the existence of an integer q such that $ax = qn + 1$. Writing $y = -q$ we get

$$ax + ny = 1.$$

All steps in the above derivation are reversible. Hence, we proved that II is equivalent to III. We state the specific result.

B. The equation $a \cdot_n x = b$ has a solution in $\mathbb{Z}_n$ iff there exist integers x and y such that $ax + ny = 1$.

Implications are transitive, that is, if I implies II and II implies III then I implies III. We can do the same chain of implications in the other direction as well. Hence, if I $\iff$ II and II $\iff$ III, as we have established above, we also have I $\iff$ III. We again state this specific result for clarity.

C. The integer a has a multiplicative inverse in $\mathbb{Z}_n$ iff there exist integers x and y such that $ax + ny = 1$.

Greatest common divisors. Here we prove "III $\implies$ IV$''$. We will prove IV $\implies$ III later. We say an integer i *factors* another integer j if j/i is an integer. Furthermore, j is a *prime number* if its only factors are $\pm j$ and ± 1. The *greatest common divisor* of two integers j and k, denoted as $\gcd(j, k)$, is the largest integer d that is a factor of both. We say j and k and *relative prime* if $\gcd(j, k) = 1$.

D. Given integers a and n, if there exist integers x and y such that $ax + ny = 1$ then $\gcd(a, n) = 1$.

PROOF. Suppose $\gcd(a, n) = k$. Then we can write $a = ik$ and $n = jk$. Substituting these into the linear equation gives

$$\begin{aligned} 1 &= ax + ny \\ &= k(ix + jy). \end{aligned}$$

But then k is a factor of 1 and therefore $k = \pm 1$. This implies that the only common factors of a and n are ± 1 and therefore $\gcd(a, n) = 1$. □

Summary. We have proved relationships between the statements I, II, III, IV; see Figure 5. We will see later that

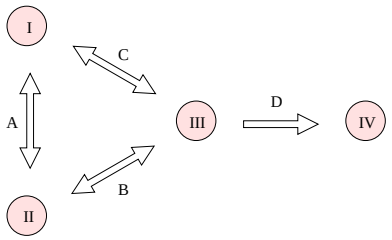

Figure 5: Equivalences between statements.

the implication proved by D can also be reversed. Thus computing the greatest common divisor gives a test for the existence of a multiplicative inverse.