4.7.2. Inverses

Normal arithmetic has the *Cancellation Law for Multiplication* (T7 of Appendix A (Epp)):

For integers a, b, c with $a \neq 0$, if

$$ab = ac \tag{1}$$

then $b = c$.

This is not true in modulo arithmetic:

$$ab \equiv ac \pmod{n} \text{ does not imply } b \equiv c \pmod{n}$$

Example:

Clearly, $3 \times 1 \equiv 3 \times 5 \pmod 6$.
But, $1 \not\equiv 5 \pmod 6$.

When "cancelling" a on both sides of Equation (1), we are really multiplying with the multiplicative inverse of a. By definition, the multiplicative inverse is a number b such that $ab = 1$. Thus we need a suitable inverse that works with modulo arithmetic.

Definition 4.7.2 (Multiplicative inverse modulo n)

For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is called the multiplicative inverse of a modulo n. We may write the inverse as a^{-1}.

Because the commutative law still applies in modulo arithmetic, we also have $a^{-1}a \equiv 1 \pmod{n}$.

Note that multiplicative inverses are not unique, since if s is such an inverse, then so is $(s + kn)$ for any integer k (Why?)

Example:

Consider $a = 5$ and $n = 9$: By inspection, $5 \cdot 2 \equiv 1 \pmod 9$, so $5^{-1} = 2 \pmod 9$.

Other multiplicative inverses include: $2+9 = 11$, $2-9 = -7$, $2 + 900 = 902$.

Given any integer a, its multiplicative inverse a^{-1} may not exist. This next theorem tells us exactly when it exists.

Theorem 4.7.3 (Existence of multiplicative inverse)

For any integer a, its multiplicative inverse modulo n (where $n > 1$), a^{-1}, exists if, and only if, a and n are coprime.

Recall that two numbers are coprime, or *relatively prime*, iff their gcd is 1.

Corollary 4.7.4 (Special case: n is prime)

If $n = p$ is a prime number, then all integers a in the range $0 < a < p$ have multiplicative inverses modulo p.

Proof: (Forward direction)

1. For any integers a, n with $n > 1$:
2. If a^{-1} exists:
3. Then $a^{-1}a \equiv 1 \pmod{n}$, by definition of multiplicative inverse.
4. Then $a^{-1}a = 1 + kn$, for some integer k, by Theorem 8.4.1 (Epp).
5. Re-write: $aa^{-1} - nk = 1$, by basic algebra.
6. (Claim: all common divisors of a and n are ± 1.)
7. Take any common divisor, d, of a and n.
8. $d \mid a$ and $d \mid n$ by definition of common divisor.
9. So $d \mid 1$ by Line 5 and Theorem 4.1.1.
10. Thus, $d = 1$ or $d = -1$ by Theorem 4.3.2 (Epp).
11. Hence $\gcd(a, n) = 1$.

Proof: (Backward direction)

1. For any integers a, n with $n > 1$:
2. If $\gcd(a, n) = 1$:
3. Then by Bézout's Identity, there exist integers s, t such that $as + nt = 1$.
4. Thus $as = 1 - tn$, by basic algebra.
5. Then by Theorem 8.4.1 (Epp), $as \equiv 1 \pmod{n}$. ■

Note that the above tells us how to find a multiplicative inverse for a modulo n: simply run the Extended Euclidean Algorithm!

Example:

Find $3^{-1} \pmod{40}$.

1. Since 3 is prime, and $40 = 2^3 \cdot 5$, it is easy to see that $\gcd(3, 40) = 1$.
2. Also, note that $40 = 3(13) + 1$.
3. Re-write: $3(-13) = 1 - 40$.
4. Thus by Theorem 8.4.1 (Epp), $3(-13) \equiv 1 \pmod{40}$.
5. Thus $3^{-1} = -13 \pmod{40}$.

But this is ugly. We prefer a positive inverse. This can be corrected simply by adding a multiple of 40, eg. $-13 + 40 = 27$. Hence $3^{-1} = 27 \pmod{40}$.

Example:

Find $2^{-1} \pmod 4$.

Note that $\gcd(2,4) = 2$, so 2 and 4 are not coprime. Thus, by Theorem 4.7.3, 2^{-1} does not exist.

Indeed, we can check this:

$$\begin{aligned} 2 \cdot 1 &\equiv 2 \pmod 4, \\ 2 \cdot 2 &\equiv 0 \pmod 4, \\ 2 \cdot 3 &\equiv 2 \pmod 4. \end{aligned}$$

By Theorem 8.4.3 (Epp), these calculations suffice to conclude that 2^{-1} does not exist.

The use of multiplicative inverses leads us to a Cancellation Law for modulo arithmetic:

Theorem 8.4.9 (Epp)

For all integers a, b, c, n, with $n > 1$ and a and n are coprime, if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof sketch

Since a and n are coprime, Theorem 4.7.3 guarantees the existence of a multiplicative inverse a^{-1}.

Multiply both sides of $ab \equiv ac \pmod{n}$ with a^{-1} gives the desired answer.

Quiz: In T7 of Appendix A (Epp) (Cancellation Law for integers), it is explicitly stated that $a \neq 0$. Yet the above theorem doesn't seem to require this. Why not?

Example:

Solve the equation $5x + 13y = 75$ for integers x, y.

1. Re-write: $5x = 75 - 13y$.
2. Then $5x \equiv 75 \pmod{13}$, by Theorem 8.4.1 (Epp).
3. Re-write: $5x \equiv 5 \cdot 15 \pmod{13}$.
4. Note that 5 and 13 are coprime.
5. Thus, $x \equiv 15 \pmod{13}$, by Theorem 8.4.9 (Epp).
6. Thus, $x \equiv 2 \pmod{13}$, because $15\ \mathit{mod}\ 13 = 2$.
7. So $x = 2$ is a solution.
8. Substituting back into the equation: $5(2) + 13y = 75$.
9. And thus $y = 5$.

Other solutions include: $(x, y) = (15, 0), (-11, 10), (28, -5)$.

4.8. Summary

1. We have learned many things in Number Theory:
   (a) Divisibility
   (b) Primes and prime factorization
   (c) Well ordering principle
   (d) Quotient-Remainder Theorem
   (e) Number bases
   (f) Greatest common divisor
   (g) Modulo arithmetic
2. Yet we have merely scratched the surface of a deep and fascinating field that has many applications.
3. Many Open Questions remain in Number Theory. Now and then someone will announce a breakthrough in one of these Questions. It is fun to follow their development, even if we don't fully understand their esoteric proofs.