4. Number Theory (Part 3)

Terence Sim

Young man, in mathematics you don't understand things. You just get used to them.

If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.

John von Neumann, 1903 — 1957

Reading

Sections 8.3 (from page 473), 8.4 of Epp.

4.7. Modulo Arithmetic

1 Sep. 2017 is a Friday. What day of the week is 30 Sep.?

Your friend messages you, saying, "I'll see you in three hours". Your phone shows 11:30am now. What time will your friend show up?

To answer both questions, you are doing modulo arithmetic.

Definition 4.7.1 (Congruence modulo)

Let m and n be integers, and let d be a positive integer. We say that m is congruent to n modulo d, and write:

$$m \equiv n \pmod{d}$$

if, and only if,

$$d \mid (m - n).$$

Symbolically: $m \equiv n \pmod{d} \;\Leftrightarrow\; d \mid (m - n)$

Examples: Determine which of the following is true and which is false.

- $12 \equiv 7 \pmod{5}$
- $6 \equiv -8 \pmod{4}$
- $3 \equiv 3 \pmod{7}$
- $\forall a, b \in \mathbb{Z}$, not both zero, $a \equiv b \pmod{\gcd(a, b)}$

Answer:

Theorem 8.4.1 (Epp): Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (non-negative) remainder when divided by n
5. $a \, mod \, n = b \, mod \, n$

Proof: see page 480 of Epp.

Note that $a \, mod \, n$ is the non-negative remainder r, when a is divided by n. By the Quotient-Remainder Theorem, $0 \leq r < n$. Another name for this is the residue of a modulo n.

4.7.1. Arithmetic

Theorem 8.4.3 (Epp): Modulo Arithmetic

Let a, b, c, d and n be integers with $n > 1$, and suppose:

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$, for all positive integers m.

We will prove part 3. Try the rest yourself!

Proof:

1. For any integers a, b, c, d, n with $n > 1$:
2. Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$:
3. Then by Theorem 8.4.1 (Epp), there exist integers s, t such that $a = c + sn$ and $b = d + tn$.
4. Then $ab = (c + sn)(d + tn)$, by substitution.
5. $= cd + n(ct + sd + stn)$, by basic algebra.
6. Let $k = (ct + sd + stn)$. This is an integer by the closure property.
7. Thus $ab = cd + nk$.
8. By Theorem 8.4.1 (Epp), $ab \equiv cd \pmod{n}$. ■

A more useful form of part 3 is this Corollary:

Corollary 8.4.4 (Epp)

Let a, b, n be integers with $n > 1$. Then,

$$ab \equiv [(a\,mod\,n)(b\,mod\,n)] \pmod{n},$$

or, equivalently,

$$ab\,mod\,n \;=\; [(a\,mod\,n)(b\,mod\,n)]\,mod\,n.$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a\,mod\,n)^m] \pmod{n}.$$

Clarification: "$a\,mod\,n$" is an operation; it means calculate the residue of a. But "(mod n)" is not an operation; instead, it merely specifies the "clock" we are using.

Example:

Calculate: (a) $55 \cdot 26 \; mod \; 4$, (b) $144^4 \; mod \; 713$

Answer:

$$
\begin{aligned}
\text{(a)} \quad 55 \cdot 26 \; mod \; 4 &= [(55 \; mod \; 4)(26 \; mod \; 4)] \; mod \; 4 \\
&= (3)(2) \; mod \; 4 \\
&= 6 \; mod \; 4 \\
&= 2
\end{aligned}
$$

$$
\begin{aligned}
\text{(b)} \quad 144^4 \; mod \; 713 &= (144^2)^2 \; mod \; 713 \\
&= (144^2 \; mod \; 713)^2 \; mod \; 713 \\
&= (20736 \; mod \; 713)^2 \; mod \; 713 \\
&= 59^2 \; mod \; 713 \\
&= 3481 \; mod \; 713 \\
&= 629
\end{aligned}
$$

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 s such that $as = 1$. 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 $3^{-1} = -13$.

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 $3^{-1} = 27$.

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.

Such an equation is called a Diophantine equation.

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 $15\, mod\, 13 = 2$.
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.