Chapter 8
As Simple as 2 + 2 = 1

Freedom, is the freedom to say two plus two make four. If that is granted, all else follows.

George Orwell (1903–1950)

Orwell was not speaking about mathematics in the quote above from his book *1984*. Rather, he was commenting on how totalitarian governments attempt to define, and impose, their own notion of reality on the public. Speaking mathematically, it is as clear as the back of your hand that $2 + 2 = 1$ and $1 + 2 = 0$. That is, if you belong to a three fingered species. We have grown so used to the ten fingers on our hands, that we forget that there is nothing special about base 10. Since the invention of the *number* 0 by Indian mathematicians of the fifth century, this means that all of our numbers are composed of the digits 0 through 9. To three fingered species this means that their number system uses the digits 0 through 2 so that 3 wraps around to 0 and 4 to 1. Thus $2+2 = 1$ and $1+2 = 0$ in base 3. Orwell's above statement is thus valid for all bases 5 and larger unless, of course as he alludes, the totalitarian regime in power says otherwise.

8.1 Modular Arithmetic

Often the remainder of a number after division is the only characteristic that is necessary to establish a mathematical property—the magnitude of the integer is not relevant. For example, all primes greater than 2 are odd independent of their magnitude. In base 2 looking at integers in this way essentially splits them into 2 disjoint sets. The first set contains the even integers, $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$

R. Nelson, *A Brief Journey in Discrete Mathematics*,
https://doi.org/10.1007/978-3-030-37861-5_8

and the second the odds, $\{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$. These two groups arise by skipping the integers by 2 (up and down) starting from a point determined by the remainder when an integer is divided by 2.

In base n integers are split into n disjoint sets depending on their remainder when divided by n (the possible remainders are 0 through $n-1$). Similar to odd even parity, these sets occur by skipping by n steps. For example, the set corresponding to a remainder of k is given by

$$\{\ldots, -3n+k, -2n+k, -n+k, k, n+k, 2n+k, \ldots\},$$
$$k = 0, \ldots, n-1$$

Mathematically, one uses modular arithmetic when the only characteristic necessary to establish a property is the parity of the number with respect to some base. Equality in such a system is customarily written as

$$b \equiv \beta \pmod{n}$$

which means that b and β leave the same remainder when divided by *modulus* n. This equation represents a *congruence relation* between b and β. A more concise notation used in this book when dealing with *modulo arithmetic* is written as

$$b \equiv_n \beta \tag{8.1}$$

As examples, the equations $38 \equiv_5 53$, $-2 \equiv_5 3$, and $-47 \equiv_5 -222$ are all valid since 38, 53, -2, -47, and -222 leave a remainder of 3 when divided by 5. Since $an + k \equiv_n bn + k$ for any integers a and b it is customary to write the right-hand side of a modulo equation by setting $b = 0$ or $b = -1$. Thus the equation $38 \equiv_5 53$ would typically be written as $38 \equiv_5 3$ or $38 \equiv_5 -2$.

The equation $b \equiv_n \beta$ is equivalent to the fact that $b - \beta$ is evenly divisible by n. In essence, both statements are a restatement of the equation $(b - \beta) \equiv_n 0$. In terms of the sets that we mentioned above, the equation means that b and β are in the same set. Negative numbers in modulo arithmetic can be viewed in terms of positive complements through the following equation:

$$n - b \equiv_n -b, \quad b = 0, \ldots, n-1 \tag{8.2}$$

For example, $9 \equiv_{10} -1$. In everyday life, clocks form a natural modulo system of order 12 provided that the hours are relabeled 0 through 11.

It is clear that the congruence relation is *reflexive* ($b \equiv_n b$), *symmetric* ($b \equiv_n \beta$ also means $\beta \equiv_n b$), and *transitive* ($b \equiv_n \beta$ and $\beta \equiv_n \gamma$ imply $b \equiv_n \gamma$). Other properties of modulo arithmetic include (ℓ is assumed to be an integer)

$$\begin{aligned} \ell + b &\equiv_n \ell + \beta && \text{addition property} \\ \ell b &\equiv_n \ell\beta && \text{multiplication property} \\ b^\ell &\equiv_n \beta^\ell \quad (\ell > 0) && \text{power property} \end{aligned}$$

One way to establish the last property is to use (A.7) to write

$$b^\ell - \beta^\ell = (b - \beta) \sum_{i=0}^{\ell-1} b^i \beta^{\ell-i-1}$$

The divisibility of $b^\ell - \beta^\ell$ by n then follows from the fact that $b - \beta$ is divisible by n. Notice that the combination of all three properties listed above imply that if p is a polynomial with integer coefficients and $b \equiv_n \beta$, then $p(b) \equiv_n p(\beta)$.

To state properties having combinations of modular terms, assume that $a \equiv_n \alpha$ and $b \equiv_n \beta$. Then

$$\begin{aligned} a \pm b &\equiv_n \alpha \pm \beta \\ ab &\equiv_n \alpha\beta \end{aligned} \tag{8.3}$$

To establish the last equation, note that the quantity $\alpha b - \alpha\beta = \alpha(b - \beta)$ is divisible by n and thus $\alpha b \equiv_n \alpha\beta$. Similarly $ab - \alpha b = b(a - \alpha)$ is divisible by n and thus $ab \equiv_n \alpha b$. These two equations, along with symmetry and transitivity, yield $ab \equiv_n \alpha\beta$. This relationship provides another way to establish the power property in the first list, $b^\ell \equiv_n \beta^\ell$. To see this, set $a = b$ and $\alpha = \beta$ and repeat $\ell - 1$ times.

The following two properties can be used to cancel ℓ in the following equations:

$$\begin{aligned} \ell + b \equiv_n \ell + \beta \quad &\Longrightarrow \quad b \equiv_n \beta \\ \ell b \equiv_n \ell\beta \quad &\Longrightarrow \quad b \equiv_n \beta \\ &\qquad \text{provided that } n \text{ and } \ell \text{ are coprime} \end{aligned}$$

In this last equation, n and ℓ must not have any common factors for the relationship to hold in general. To show this, write $\ell b - \ell\beta = \ell(b - \beta)$. If ℓ is divisible by n, then there is no necessity for $b - \beta$ to also be divisible by n. Thus ℓ cannot be cancelled from the equation and still guarantee the equality. If ℓ and n are co-prime, however, then the only way $\ell(b - \beta)$ is divisible by n is for $b - \beta$ to be divisible by n. Thus $b \equiv_n \beta$.

8.2 Fermat's Little Theorem

At this point it makes sense to ask—what use is such a concept? Many applications seem like tricky test questions. To illustrate one example: what is the remainder when 19^{317} is divided by 3? To determine the answer, note that $19 \equiv_3 1$ since $19 = 3 \cdot 6 + 1$. The power property above then yields the answer: $19^{317} \equiv_3 1$.

For another example, let ℓ be an integer with digits d_i, $i = 0, \ldots, m$ where the i'th digit corresponds to the i'th power of 10. This corresponds to the polynomial

$$\ell = d_0 + d_1 10^1 + \cdots + d_m 10^m$$

Suppose that $\ell \equiv_3 0$. Then is it possible to say anything about the digits comprising ℓ? To answer this, note that $10 \equiv_3 1$ and thus $10^i \equiv_3 1$. Using the multiplication property shows that $d_i 10^i \equiv_3 d_i$ and thus $\ell \equiv_3 d_0 + d_1 + \cdots + d_m$. These observations imply that the sum of the digits of ℓ must be divisible by 3 for ℓ to be divisible by 3. A straightforward generalization concerns base n integers written as

$$\ell = d_0 + d_1 n^1 + \cdots + d_m n^m$$

A similar argument shows that $\ell \equiv_{n-1} d_0 + \cdots + d_m$ (since $n \equiv_{n-1} 1$). Thus, octal integers are divisible by 7 if the sum of their digits is divisible by 7.

As another example, a number is divisible by 11 if the alternating ($\pm$) sum of its digits is divisible by 11 (this arises from the fact that $10 \equiv_{11} -1$). There are a wealth of results along these lines.

Modulo arithmetic also leads to many basic results of number theory. For example, assume that p is a prime number and consider the binomial expansion

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$$
$$= a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$$

In this expression, the binomial coefficient in the summation is divisible by p since p is contained in the numerator[1] but not the denominator. Hence

$$\binom{p}{i} \equiv_p 0, \quad i = 1, \ldots, n-1$$

which implies that

$$(a+b)^p \equiv_p a^p + b^p \tag{8.4}$$

A result that follows from this is due to Pierre de Fermat (1607–1665) which is aptly called *Fermat's Little Theorem.* It states that

$$x^p \equiv_p x \tag{8.5}$$

for x integer and p prime. To prove it, observe that the claim clearly holds for $x = 0$. Thus, assume it holds up to a value of $x = a$. Using (8.4) we can write

$$(a+1)^p \equiv_p a^p + 1^p \equiv_p a + 1$$

where the last step follows from the induction assumption. This equation is simply a restatement of (8.5) for the next highest integer and establishes the result.

Fermat's little theorem can be used as a test to determine if an integer n is prime. For example, suppose for some x that $x^n \not\equiv_n x$. Then the theorem implies that n is not prime. No statement can be made; however, if Fermat's equation holds since it can do so for composite n. In fact, there are composite integers n that satisfy Fermat's equation for every value x that is relatively prime to n.

[1] The numerator equals $p(p-1)!$.

Such *Carmichael numbers* pose a formidable test to Fermat since they present the appearance of being prime. There are an infinite number of such Carmichael numbers masquerading as primes, at least through the eyes of Fermat's test. The smallest such number is 561.

8.3 Lagrange's Theorem

Another result from modular arithmetic is due to Lagrange and deals with the roots of a polynomial modulo a prime. A polynomial $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ has degree k modulo n if a_k is the highest coefficient that is not divisible by n. The theorem states that the number of roots of a polynomial modulo p, where p is prime, cannot exceed its degree. The proof of this proceeds by induction starting with a degree 1 polynomial where the result is obvious. Assume the proposition holds up to degree $n-1$. Suppose polynomial f has degree n modulo p. If f does not have a root, then there is nothing to prove. Therefore, assume that a root b exists so that $f(b) \equiv_p 0$. Write

$$\begin{aligned} f(x) - f(b) &= \sum_{i=1}^{n} a_i (x^i - b^i) \\ &= (x-b) \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} x^j b^{i-j-1} \qquad \text{from equation (A.7)} \\ &= (x-b) \sum_{j=0}^{n-1} x^j \sum_{i=j+1}^{n} a_i b^{i-j-1} \\ &= (x-b) \sum_{j=0}^{n-1} c_j x^j \end{aligned}$$

where c_j is defined as

$$c_j = \sum_{i=j+1}^{n} a_i b^{i-j-1}$$

Thus $f(x)$ can be written as

$$f(x) = f(b) + (x-b) \sum_{j=0}^{n-1} c_j x^j \equiv_p (x-b) \sum_{j=0}^{n-1} c_j x^j$$

By the induction hypothesis, the polynomial $\sum_{j=0}^{n-1} c_j x^j$ can have at most $n-1$ roots. This, along with the assumption that b is a root, implies there can be at most n roots to $f(x)$ modulo p and thus establishes the result.

8.4 Wilson's Theorem

The theorems of Fermat and Lagrange just discussed can be used to extract a deep result. Fermat's result (8.5) can be rewritten as $x^{p-1} - 1 \equiv_p 0$ which shows that there are $p-1$ roots modulo p with the values $1, 2, \ldots, p-1$. Consider the polynomial (see (3.1) for the falling factorial notation)

$$(x-1)^{\underline{(p-1)}} = (x-1)(x-2)\cdots(x-(p-1))$$

This clearly also has roots $1, 2, \ldots, p-1$ modulo p. Using the result (3.13) we can write

$$\begin{aligned}
(x-1)^{\underline{(p-1)}} &= \sum_{i=1}^{p-1} (-1)^{p-i-1} \begin{bmatrix} p-1 \\ i \end{bmatrix} (x-1)^i \\
&= \sum_{i=1}^{p-1} (-1)^{p-i-1} \begin{bmatrix} p-1 \\ i \end{bmatrix} \sum_{j=0}^{i} \binom{i}{j} (-1)^{i-j} x^i \\
&= \sum_{i=1}^{p-1} (-1)^{p-1} \begin{bmatrix} p-1 \\ i \end{bmatrix} \\
&\quad + \sum_{j=1}^{p-1} x^j \sum_{i=j}^{p-1} (-1)^{p-j-1} \binom{i}{j} \begin{bmatrix} p-1 \\ i \end{bmatrix} \\
&= (-1)^{p-1} \begin{bmatrix} p-1 \\ p-1 \end{bmatrix} + \sum_{j=1}^{p-1} e_{j,p-1} x^j
\end{aligned}$$

where we have defined

$$e_{j,p-1} = \sum_{i=j}^{p-1} (-1)^{p-j-1} \binom{i}{j} \begin{bmatrix} p-1 \\ i \end{bmatrix}, \quad j = 0, \ldots, p-1$$

If p is a prime greater than 2, then we can use (3.5), and the observation that $c_{p-1,p-1} = 1$, to simplify the above expression:

$$(x-1)^{\underline{(p-1)}} = (p-1)! + x^{p-1} + \sum_{j=1}^{p-2} e_{j,p-1} x^j$$

Our next step is to consider the polynomial defined by subtracting Fermat's equation from the falling factorial

$$\begin{aligned} f(x) &= (x-1)^{\underline{(p-1)}} - \left(x^{p-1} - 1\right) \\ &= (p-1)! + 1 + \sum_{j=1}^{p-2} e_{j,p-1} x^j \\ &= \sum_{j=0}^{p-2} e_{j,p-1} x^j \end{aligned} \tag{8.6}$$

In the last equation we have extended the definition of the coefficients to include the constant term

$$e_{0,p-1} = (p-1)! + 1 \tag{8.7}$$

From its definition, it is clear that f has the same roots as the two functions that define it. Thus it has $p-1$ roots modulo p. But this is impossible according to Lagrange's theorem since f has of degree $p-2$ modulo p which only allows $p-2$ roots. Hence, f must be identically equal to 0 modulo p which implies that all of its coefficients must equal 0 modulo p:

$$e_{j,p-1} \equiv_p 0, \quad j = 0, \ldots, p-2$$

This establishes the following set of identities:

$$\begin{gathered} (p-1)! + 1 \equiv_p 0 \\ \sum_{i=j}^{p-1} (-1)^{p-j-1} \binom{i}{j} \begin{bmatrix} p-1 \\ i \end{bmatrix} \equiv_p 0, \quad j = 1, \ldots, p-2 \end{gathered} \tag{8.8}$$

These ruminations lead us to the deep result mentioned above. Wilson's theorem named after John Wilson (1741–1793) states that the equation

$$(n-1)! + 1 \equiv_n 0 \tag{8.9}$$

is satisfied if and only if n is a prime number. The if portion is simply the first identity above (8.8) that deals with the constant coefficient of f. To prove the only if portion of Wilson's theorem, assume that n is composite and also satisfies $(n-1)! + 1 \equiv_n 0$. Then it must be the case that n is divisible by an integer $k < n$. But $(n-1)!$ necessarily contains k and thus $(n-1)! + 1 \not\equiv_k 0$ for any $k < n$. This violates the assumption that n is composite.

Wilson's theorem provides another method to test if a number is prime—simply see if $(n-1)! + 1 \equiv_n 0$. Like Fermat's little theorem, it also is a poor test since factorials increase rapidly. Wilson's theorem does provide entertainment by producing a wealth of parlor tricks. For example, from the theorem we know that $72! \equiv_{73} -1$ since 73 is prime. Thus, since $72 \equiv_{73} -1$, we can use (8.3) to conclude that $71! \equiv_{73} 1$. Following this example, we can write the general equation $(p-2)! \equiv_p 1$ for p prime.

8.5 Cryptography

A less flippant application of modular arithmetic than numeric divisibility challenges is a procedure that is used millions of times a day on the Internet. It is called *public key cryptography*. The objective of cryptography is to create a secure communications channel between two participants such that an eavesdropper cannot decode their communications. To explain this procedure, suppose that A wants to send a secure message to B and that C is listening to the communication. Both A and B share a large prime number p and a base number n. These can also be known by C. Let e_a be an integer only known by A and similarly let e_b be an integer only known by B. Participant A computes the value

$$v_a \equiv_p n^{e_a}$$

and sends it on the channel to B. Likewise, B computes

$$v_b \equiv_p n^{e_b}$$

and sends it to A. Note that C can listen to these communications; they take place on an insecure channel.

Now the magic starts. Participant A takes the communication it received from B and computes

$$w_a \equiv_p v_b^{e_a}$$

This computed value cannot be determined by C because e_a is only known to A. Likewise, B computes

$$w_b \equiv_p v_a^{e_b}$$

which also cannot be computed by C. But A and B now share the same value because $w = w_a = w_b$. This follows from the power property of modular arithmetic since

$$v_b \equiv_p n^{e_b} \quad \Longrightarrow \quad (v_b)^{e_a} \equiv_p (n^{e_b})^{e_a}$$

and

$$v_a \equiv_p n^{e_a} \quad \Longrightarrow \quad (v_a)^{e_b} \equiv_p (n^{e_a})^{e_b}$$

The value of w can now be used as a key for a cryptographic scheme for the duration of the communication and C cannot *easily* break the code because everything is calculated modulo a large prime. I need the word *easily* in this last statement because if there was a fast way to calculate the value of e_a or e_b from w (remember p, n, v_a, and v_b are all assumed to be known by C), then C could break the code. Solving for such values is called the *discrete logarithm problem* which is currently computationally intractable for large p.