CHAPTER I: FUNDAMENTALS

Section 2: Modular Arithmetic

In this set of notes, we will largely focus on the notion of a group. This abstract idea can be applied and utilized in many different branches of mathematics and in fact on many different kinds of sets. However, before we get to this, we should first lay a concrete foundation that we will be able to draw upon as things get more abstract. Therefore, in this section we are going to discuss the properties of the integers and modular arithmetic. These foundational topics deal with "numbers", something that we are quite familiar with and will yield many good examples for us as things get trickier.

We will denote the set of integers $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$ by $\mathbb{Z}$ and the set of natural numbers $\{1,2,3,\ldots\}$ by $\mathbb{N}$. The integers have two operations defined on them: addition and multiplication. All of the following facts will be taken as known. Both operations (addition and multiplication) are commutative and associative. There is an additive identity 0 (that is, for all $a \in \mathbb{Z}$, $a+0=a$). There is a multiplicative identity 1 (that is, for all $a \in \mathbb{Z}$, $a \cdot 1 = a$). Every integer a has an additive inverse $-a$ satisfying $a+(-a)=0$. Finally, the distributive property holds; namely for $a,b,c \in \mathbb{Z}$, $a(b+c)=ab+ac$. Both additive and multiplicative structures are interesting topics of study, but for now, we wish to focus on the multiplicative structure of $\mathbb{Z}$. We begin with the concept of divisibility.

Definition: Let $a,b \in \mathbb{Z}$. We say that a ***divides*** b if there is an integer n such that $an=b$. We denote this by writing $a \mid b$. In this case, a is called a ***divisor*** (or ***factor***) of b and b is ***divisible*** by a. Clearly every natural number other than 1 has at least two factors, 1 and itself. If a number has *only* these two factors, it is called ***prime***. A natural number with more than two factors is called ***composite***. Notice that 1 is neither prime nor composite. It is called a ***unit***. A natural number d is called the ***greatest common divisor*** of a and b (denoted by $\gcd(a,b)$) if (1) it divides both a and b and (2) for any *other* common divisor of a and b, say c, we have $c \mid d$. If $\gcd(a,b)=1$, we say that a and b are ***relatively prime***.

Theorem 1: Let $a,b,c \in \mathbb{Z}$.

(a) The only divisors of 1 are ± 1.

(b) If $a \mid b$ and $b \mid a$, then $a = \pm b$.
(c) If $a \mid b$ and $b \mid c$, then $a \mid c$.
(d) If $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for any $s, t \in \mathbb{Z}$.

Proof: We only prove parts (a) and (b). Parts (c) and (d) will be left as an exercise.

(a) Suppose that $ab = 1$. We want to show that both a and b must be ± 1. First note that neither a nor b can be zero. Suppose that both a and b are positive. Since $ab \geq \max\{a, b\} \geq 1$, we have that $a = b = 1$. Now, in the general case, if $ab = 1$, then also $|a||b| = 1$. But by the above this means that $|a| = |b| = 1$. Thus both a and b are ± 1.

(b) Let m and n be integers such that $am = b$ and $bn = a$. Then $b = bmn$. Thus $0 = b(mn - 1)$. Since the product of nonzero integers is nonzero, we must have either $b = 0$ or $mn = 1$. In the former case, $a = b = 0$, and in the latter case, $n = \pm 1$ (by part (a)), so $a = \pm b$.

We now come to two very important results that at first glance seem quite obvious.

Theorem 2: There are infinitely many prime numbers.

Theorem 3 (Fundamental Theorem of Arithmetic): Every natural number other than 1 has a unique prime factorization.

Having covered the idea of divisibility, we can now proceed to modular arithmetic.

Definition: Let m be a natural number and let a, b be integers. We say that a is ***congruent*** to b modulo m if m divides $a - b$. This is denoted by $a \equiv b \pmod{m}$. The natural number m is called the ***modulus***. The set of all integers congruent to a is called the ***congruence class*** of a modulo m (or ***residue class***) and is denoted by $[a]_m = \{b \in \mathbb{Z} : a \equiv b \pmod{m}\}$. When often leave off the subscript if the modulus is clear from the context.

Example 1: Since 5 divides the difference of 31 and 1, we have that $31 \equiv 1 \pmod{5}$.

If we divide an integer a by a modulus m, we get a quotient and a remainder (by the Division Algorithm). In symbols,

$$a = mq + r \quad (\text{for } 0 \le r < m)$$

Clearly, the difference $a - r$ is a multiple of the modulus m, so $a \equiv r \pmod{m}$. Therefore, every integer is congruent modulo m to some integer between 0 and $m-1$ (inclusive). Put another way, there are exactly m distinct congruence classes modulo m, namely $[0],[1],\ldots,[m-1]$. These classes are mutually disjoint. The set of all congruence classes modulo m is denoted by $\mathbb{Z}_m$.

Congruences with the same modulus have many of the same properties as equations.

Theorem 4: Let a,b,c,d be integers.

(a) $a \equiv a \pmod{m}$.

(b) $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$, and $ac \equiv bd \pmod{m}$.

These properties help us understand the algebraic structure of the set $\mathbb{Z}_m$. For example, let $[a]$ and $[b]$ be distinct elements of $\mathbb{Z}_m$. Note that by part (b) above, we can represent a congruence class by any element in the class. Since a is congruent to $a+km$ (modulo $\mathbb{Z}_m$) for any integer k, $[a]=[a+km]$. Also, by part (d), we see that $[a]+[b]=[a+b]$ and $[a][b]=[ab]$. It is interesting to note that while addition and multiplication behave similar with congruences as they do with equalities, division is not so kind. For example, even though $24 \equiv 18 \pmod{6}$, we cannot divide both sides by 2 and get a valid congruence (12 is not congruent to 9 (mod 6)).

There are other very interesting differences between $\mathbb{Z}$ (with addition and multiplication) and $\mathbb{Z}_m$ (with modular arithmetic). One is that $\mathbb{Z}_m$ has *zero divisors*. Recall that in $\mathbb{Z}$, if the product of two integers is zero, then one of the two integers must be zero. That is not true in $\mathbb{Z}_m$. Consider [3] and [4] in $\mathbb{Z}_{12}$. Clearly, $[3][4]=[12]$. But recall from our discussion above that $\mathbb{Z}_{12}=\{[0],[1],\ldots,[11]\}$. The class [12] is not an element of $\mathbb{Z}_{12}$. However, modulo

12, $[12]=[0]$ (since $12\equiv 0 \pmod{12}$). So we see that in $\mathbb{Z}_{12}$, $[3][4]=[0]$. Hence we have nonzero divisors of zero.

Another interesting difference between the algebraic structures of $\mathbb{Z}$ and $\mathbb{Z}_m$ is that many elements of $\mathbb{Z}_m$ have multiplicative inverses. Recall, that an element $[a]$ of $\mathbb{Z}_m$ has a ***multiplicative inverse*** (and is said to be ***invertible***) if there exists an element $[b]$ such that $[a][b]=[1]$. For example, in $\mathbb{Z}_9$, $[1][1]=[1]$, $[2][5]=[10]=[1]$, $[4][7]=[28]=[1]$ and $[8][8]=[64]=[1]$. The other nonzero elements [3] and [6] are zero divisors. This is quite different from $\mathbb{Z}$, where there are no zero divisors and only ± 1 are invertible.

Example 2: Compute the congruence class modulo 5 of 4^{239}.

Recalling that $4\equiv -1 \pmod{5}$, this becomes quite simple:

$$4^{239}\equiv (-1)^{239}\equiv -1\equiv 4 \pmod{5}.$$

Thus in $\mathbb{Z}_5$, $[4^{239}]=[4]$.

Example 3: Compute the congruence class modulo 9 of 4^{239}.

Of course, one way to accomplish this would be to multiply 4 by itself 239 times and then reduce our answer modulo 9. Obviously, this is impractical. One way to use the results of this section is to notice that as we multiply 4 over and over, every time our product becomes larger than 8, we can reduce it THEN. Of course, even though that keeps our numbers much smaller, it still requires 238 multiplications. But this is where a little ingenuity comes into play. Notice that $4^3\equiv 1 \pmod{9}$. It follows that as we compute 4^{239}, every three of them give us a factor of 1, which of course we can ignore. Dividing 239 by 3, we see that there are 79 such groups of three 4's. The remaining two 4's multiply to 16, which is 7 modulo 9. In symbols,

$$4^{239}\equiv 4^{3\cdot 79+2}\equiv (4^3)^{79}(4^2)\equiv (1)^{79}(16)\equiv 7 \pmod{9}.$$

Thus in $\mathbb{Z}_9$, $[4^{239}]=[7]$.