Contents

2. Number Theory

Now, I am become Death, the destroyer of worlds.

— Robert Oppenheimer

Mathematics, in its truest sense, originated as the study of numbers, specifically natural numbers. Ancient mathematicians from all around the world spent their days gazing at these numbers, trying to find properties like similarity in structures, patterns, decomposition, compositions and what not. In modern day mathematics, natural numbers and their elementary properties are studied under the umbrella of Number Theory. This is, if we are allowed to say, the mother of all branches of mathematics (arguably sharing the position with geometry). Even today, most of the research level pure mathematics has some connection, if not its genesis, with the Theory of Numbers. This chapter is devoted to a very naive and elementary yet illuminating study of the same.

Section 1 deals with the elements of natural numbers, its algebra, division, divisibility and the related notions of greatest common divisor and least common multiple. Section 2 revisits irreducibility under the better known name of prime numbers, followed by the (really) Fundamental Theorem of Arithmetic. Section 3 thru 5 deals with the notion of modular arithmetic, which is a relatively intermediate way of dealing with natural numbers, especially when huge computations, existence of solutions or a similar challenge is involved. The exposition is supplemented by a plethora of problems. Section 6 is a monologue on a miscellany of topics like digital representation, distribution of prime numbers and some other properties.

2.5 Powers and Chinese Remainder Theorem

This section is primarily devoted to the methods of solving certain equations in modular arithmetic. We start with the powers and then head towards simultaneous linear equations.

2.5.1 Powers in Modular Arithmetic

Fix $d \geq 2$. Given $a \in \mathbb{Z}$, we would like to solve the equation $X^n \equiv a \pmod{d}$ where $n \geq 1$ and try to find a complete list of solutions. If there is a solution, then a is called an n^{th} power or n^{th} and the solutions are called the n^{th} roots of a.

Before becoming too adventurous, let us list out some examples to see why such an analysis becomes interesting.

Example 33. 1. We want to see which numbers can be sum of two squares in $\mathbb{Z}$. Suppose $x = a^2 + b^2$. It is obvious that $x \geq 0$. It can be seen that $x = 0, 1, 2, 4, 5$ are sum of two squares in $\mathbb{Z}$. However, $3, 6, 7$, etc. are not. A detailed analysis would be done in a later chapter, but for now let us see that if $x \equiv 3 \pmod{4}$, then x is not the sum of two squares. Let $a \in \mathbb{Z}$. Then a is either even or odd. If a is even, then $4|a^2$. If a is odd then $2|a-1$ and $2|a+1$, so $4|a^2-1$. Hence, $a^2 \equiv 0, 1 \pmod{4}$, where the comma denotes all possibilities. Likewise, $b^2 \equiv 0, 1 \pmod{4}$. So, considering all cases we get $a^2 + b^2 \equiv 0, 1, 2 \pmod{4}$. Hence, if $x \equiv 3 \pmod{4}$, then x is not the sum of two squares. Lists out $1/4^{th}$ of our cases!

2. Now suppose we want to solve the equation $9X^2 + Y^3 = 12345$. Seems to be hard right? But here is the trick. Let $Y \in \mathbb{Z}$. Then we have three cases - (i) $3|Y$. Then clearly $9|Y^3$. (ii) $3|Y-1$. Then $[Y] = [1]$ so $[Y^2 + Y + 1] = 0 \implies 3|Y^2 + Y + 1$. Hence, $9|Y^3 - 1$. (ii) Likewise $3|Y+1$, our last case (why?) would yield $9|Y^3 + 1$. Hence $Y^3 \equiv 0, \pm 1 \pmod{9}$. Hence, the LHS $9X^2 + Y^3 \equiv 0, \pm 1 \pmod{9}$ for any pair of integer (X, Y). However, the RHS is $12345 \equiv 6 \pmod{9}$. So no solution exists.

3. Let us now answer a theoretical question. How many residue class solutions are there to the equation $X^2 \equiv 1 \pmod{100}$. Seems like $[\pm 1]$ are the only solutions right? Umm... not exactly. Observe that $51^2 = 2601$, so $51^2 \equiv 1 \pmod{\ }$. So even $[51]$ is a residue class solution distinct from the other two. So this calls for some analysis. The point to note is that we technically want to solve $100|X^2 - 1$. So X must be odd. Further $25|X^2 - 1 = (X-1)(X+1)$. But $(X-1, X+1) = (X-1, 2) \leq 2$. Hence we must have $25|(X-1)$ or $25|(X+1)$ (why?). We claim this is sufficient, that is if a is odd and $a \equiv \pm 1 \pmod{25}$, then $a^2 \equiv 1 \pmod{100}$. This is an easy check, DIY! So of the 100 residue classes modulo 100, we get that the only possibilities are $[1], [49], [51], [99]$. Fill in the gaps.

Needless to say further, an analysis of powers in modular arithmetic thus becomes very important. However, a complete analysis would be pretty advanced (but very interesting). So we instead just state a theorem and list the n^{th} power residues for some special integers.

Theorem 23. *Let $d \geq 2$. Define $f : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ as $f([a]) = [a^2]$. Let $I = Im(f)$. Then the following are true.*

1. *f is multiplicative.*
2. *If $d \geq 3$, then f is not injective (equivalently, not surjective).*

3. *$f([a])$ is a unit if and only if $[a]$ is a unit.*

4. *If d is a prime, then $f([a]) = f([b])$ if and only if $[a] = [b]$ or $[a] = [-b]$.*

5. *$I = \{f([a]) : 0 \leq a \leq d/2\}$.*

6. *$|I| \leq \frac{d}{2} + 1$.*

7. *If d is a prime, then $xy \in I$ if and only if $x = 0$, $y = 0$, $x, y \in I$ OR $x, y \notin I$.*

Proof. We just prove the inequality. The key point to observe is $f([x]) = f([-x])$. So, every nonzero square, say $[a]^2$ in $\mathbb{Z}/d\mathbb{Z}$ for $d \geq 3$ has at least two preimages, namely, $[a]$ and $[-a]$. It may so happen that these are equal. This happens if and only if $d|2a$. If d is odd, then we must have $d|a$, which is a contradiction as $[a]^2 \neq [0]$. If d is even, we must have $d/2|a$ but $d \not| a$. Thus, $[a] = [d/2]$ which is a valid case if and only if $4 \not| d$ (why?). Nevertheless, we have $|I| = 1+|I \setminus \{0\}|$ and by the above observation $|I \setminus \{0\}| \leq \frac{d}{2}$ (why?). Hence, we have $|I| \leq \frac{d}{2} + 1$. □

The theorem is interesting, but we would only care about the special cases. If $n = 2, 3, 4 \ldots$, then an n^{th} power is also called a *quadratic residue*, *cubic residue*, etc. We now list the set of quadratic (QR) and cubic (CR) residues for some special integers. It is a simple check using case analysis. We omit brackets.

d	QR	CR
2	0,1	0,1
3	0,1	0,1,2
4	0,1	0,1,3
5	0,1,4	0,1,2,3,4
6	0,1,3,4	0,1,2,3,4,5
7	0,1,2,4	0,1,-1
8	0,1,4	0,1,3,5,7
9	0,1,4,7	0,1,8
10	0,1,4,5,6,9	0,1,2,3,4,5,6,7,8,9 (hehe)

These are extremely helpful while solving some Olympiad type problems as we saw. We will not deal with this now. Instead let us focus on another type of problem.

2.5.2 Chinese Remainder Theorem

Let us start with a fun problem. *Siva bought a pack of 100 apples and some of them had worms in it. So he discarded them. The remaining apple, he wanted to distribute (Yoda Style!) into groups containing equal number of apples. However, here he faced a problem - when he made two groups, the distribution was uneven as one of the groups had one apple short. So he tried to make three groups. Alas! Again, one of the groups was one apple short. He repeated this for four groups and five groups and always got one apple short. Frustrated he went to the apple store, bought a phone (never let them know your next move) and ordered a few apples from Bigstazo, a grocery app. He decides to distribute the apples evenly into seven groups (in his frustration, he forgot that he never checked six). What is the least number of apples which he must buy?*

Let us represent this as a modular arithmetic problem. Essentially, if N is the number of apples, then $0 \leq N \leq 100$. Also, from given info $N \equiv 1 \pmod 2$, $N \equiv 2 \pmod 3$, $N \equiv 3 \pmod 4$, $N \equiv 4 \pmod 5$. We want to see what is the least r such that 7 divides $N + r$. You may solve this problem

pretty easily by what we have done, but we would like you to think of this problem not just as an interesting riddle but... a SYSTEM of linear congruences. That is a system like $X \equiv a_1 \pmod{b_1}$, $X \equiv a_2 \pmod{b_2}$,... $X \equiv a_n \pmod{b_n}$.

The first observation is that we may not be able to solve such a system of equation always. For example $X \equiv 1 \pmod 4$ and $X \equiv 2 \pmod 6$ has no solution as each equation leads to a different parity (odd or even nature) of X. The problem lies in the fact that $(4, 6) = 2 \neq 1$ as we are essentially checking the equation's consistency modulo the GCD 2. However, were they consistent, will a solution exist? The answer is YES and is a corollary of this remarkable ancient theorem of mathematics.

Theorem 24 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_k$ be integers with GCD $(m_i, m_j) = 1$ whenever $i \neq j$. Let m be the product $m = m_1 m_2 \cdots m_k$. Let $a_1, \ldots, a_k$ be integers. Consider the system of congruences:*

$$\begin{array}{ll} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \\ \vdots & \vdots \\ x \equiv a_k & \pmod{m_k} \end{array}$$

Then there exists one and only one $x \in \mathbf{Z}_m$ satisfying this system. That is to say, there is an integer solution x_0 of this system of congruence and all other solutions are given by $x_k = a + km$ where $k \in \mathbb{Z}$.

The proof can be done in many ways. However, to make it more useful we simply present an algorithm to find the solution.

ALGORITHM: We may solve the system of congruences as follows.

1. For each $i = 1, \ldots, k$, let $z_i = m/mi = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$. Observe that $(m_i, z_i) = 1$.
2. For each $i = 1, \ldots, k$, let $y_i \equiv z_i^{-1} \pmod{m_i}$ be any inverse.
3. For each $i = 1, \ldots, k$, let $u_i = a_i x_i z_i$. Observe that $u_i \equiv 0 \pmod{m_j}$ for $j \neq i$ and $u_i \equiv a_i \pmod{m_i}$
4. Define $x_0 = u_1 + \ldots + u_k$. Then x_0 is a solution, as desired.

A wonderful trick! Let us see two examples.

Example 34. Solve Siva's Problem.

Proof. Merging two equations, we may restate it as - find an integer $0 \leq x \leq 100$ such that

$$\begin{array}{ll} x \equiv 2 & \pmod 3 \\ x \equiv 3 & \pmod 4 \\ \vdots & \vdots \\ x \equiv 4 & \pmod 5 \end{array}$$

We can directly observe that this implies

$$\begin{array}{ll} x \equiv -1 & (\text{mod } 3) \\ x \equiv -1 & (\text{mod } 4) \\ \vdots & \vdots \\ x \equiv -1 & (\text{mod } 5) \end{array}$$

So $x' = -1$ is a solution. By the CRT, all other solutions will be of the form $x' + k(3.4.5) = x' + 60k$. So $x = 60k - 1$ for some $k \in \mathbb{Z}$. But $0 \leq x \leq 100$. Hence, $x = 59$. To make it divisible by 7. The least r should be 4 (this is essentially the remainder left by -59 when divided by 7). We urge readers to give a more direct proof using the algorithm presented above, right from scratch. □

Example 35. Find a multiplicative inverse of 13 modulo 70.

Proof. Firstly, observe that the question makes sense as $(13, 70) = 1$. One could simply use Euclid's Algorithm to find GCD and then get a Bezout equation, completing the proof. But we will use CRT. Observe that $70 = 2 \cdot 5 \cdot 7$.
Suppose $13x \equiv 1 \pmod{70}$. By CRT, that is equivalent to saying $13x \equiv 1 \pmod{m_i}$ for $i = 1, 2, 3$, where $m_1 = 2, m_2 = 5, m_3 = 7$. After some reduction, it becomes

$$\begin{array}{ll} x \equiv 1 & (\text{mod } 2) \\ 3x \equiv 1 & (\text{mod } 5) \\ \vdots & \vdots \\ (-1)x \equiv 1 & (\text{mod } 7) \end{array}$$

It is now reduced to finding the multiplicative inverse of x modulo a prime, which is known to be, by Fermat's Little Theorem, simply x^{p-2}. where p is the prime. Doing this, we get

$$\begin{array}{ll} x \equiv 1 & (\text{mod } 2) \\ x \equiv 2 & (\text{mod } 5) \\ \vdots & \vdots \\ x \equiv -1 & (\text{mod } 7) \end{array}$$

Now an application of the CRT algorithm would yield - $z_1 = 35, z_2 = 14, z_3 = 10$. Hence $y_1 = 1, y_2 = -1, y_3 = 5$. Finally $x_0 = 1{\cdot}1{\cdot}35 + 2{\cdot}(14){\cdot}(-1) + \cdot + (-1){\cdot}(10){\cdot}(5) = 35 - 28 - 50 = -43$. Hence -43 (thus 27) is a multiplicative inverse of 13 modulo 70. You may complain that this proof was far longer than the straightforward approach. However, this method is *stable* in the sense that if we slightly change the value 13 to some other residue, we will have to make only minor modifications to make our solution work. □

Time for some problems!

2.5.3 Exercises

1. Find the smallest four consecutive positive integers such that the least is divisible by 4 , the next by 9, the next by 25 and the greatest by 49.

2. Solve the system of congruences simultaneously

$$2x \equiv 1(\text{mod}5)$$
$$3x \equiv 9(\text{mod}6)$$
$$4x \equiv 1(\text{mod}7)$$
$$5x \equiv 9(\text{mod}11)$$

3. A photographer comes to take a group photograph of the students of the final year class in a school. He tries to arrange them in equal rows. But with 2, 3 or 4 rows, he finds that there is one person left over each time. However, when he puts them into 5 equal rows, there is no such problem. What is the smallest number of students in the class consistent with this situation?

4. Here is an ancient Chinese problem. A gang of 17 pirates steal a sack of gold coins. When they try to divide the loot equally, there are three coins left over. They fight over these extra coins and one pirate is killed. They try to divide the coins equally a second time, but now there are 10 left over. Again they fight and another of the gang meets an untimely end. Fortunately for the remainder of the gang, when they try to divide the loot, a third time an equal distribution results. What is the smallest number of coins they can have stolen?

5. List out the quadratic, cubic and quartic residues modulo n for $2 \leq n \leq 30$.

6. Find all integers $n_1, \ldots, n_{14}$ such that $n_1^2 + n_2^2 + \ldots + n_{14}^2 = 1599$.

7. Suppose 9 does not divide n. Let $n_1 = n$ and n_k =sum of digits of n_{k-1}. Show that n_k is eventually constant and this constant value is precisely the remainder of n modulo 9.

8. Find all integer solutions (x, y) of the following equations.

   (a) $x^2 + (x+1)^2 + \ldots (x+2001)^2 = y^2$.

   (b) $x^5 - y^4 = 4$.

   (c) (Russian Mathematical Olympiad) $x^3 - y^5 = (x+y)^2$, x, y prime.

   (d) (Hungarian MO, reformulated) $(x+1)^2 + (x+2)^2 + \ldots + (x+99)^2 = y^y$.

   (e) $x^2 - y! = 2001$.

   (f) $x^3 + y^4 = 7$.

9. Suppose $d \geq 2$ and $a \in \mathbb{Z}$ is such that $(a, d) = 1$. Suppose $n \geq 1$ is the least natural number such that $[a]_d^n = [1]_d$. Show that $n | \phi(d)$. [Hint: Use division lemma.]

10. Let p be an odd prime. Show that $[a]_p$ is a quadratic residue if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

11. Give two proofs of this fact - if p is an odd prime, show that $[-1]_p$ is a quadratic residue if and only if $4 | p - 1$.