

# **APPENDIX 1:**

## **Sample Number Theory Sets**

**Our problem sets are based on those designed by the late Professor Arnold E. Ross over a 44 year period for use in his ongoing program at the Ohio State University.**

**Numerical Problems** (*Some food for thought*)

Mathematics, like all of the sciences, is based on experience. This summer we will explore a mathematical system which we have all experienced, namely the system of integers. The integers are the whole numbers

$$\dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

We denote the set of integers by the symbol  $\mathbf{Z}$ . So  $\mathbf{Z} = \{\dots - 3, -2, -1, 0, 1, 2, 3, \dots\}$ . As we all know, it is possible to add and multiply in  $\mathbf{Z}$ . It is also possible to subtract in  $\mathbf{Z}$ . But it is not always possible to divide evenly in  $\mathbf{Z}$ . For example, if we try to divide 1 by 2 in  $\mathbf{Z}$ , then we seek an integer  $x \in \mathbf{Z}$  such that  $2x = 1$ . But there is no such integer  $x$ . Early in school, most of us learn how to do long division with remainders. This is a simple process known to mathematicians as the *division algorithm*. For example, if we divide 1068 by 7 then we get a quotient of 152 and a remainder of 4.

$$\begin{array}{r} 152 \\ 7 \overline{) 1068} \\ \underline{1064} \\ 4 \end{array} \begin{array}{l} = \textit{quotient} \\ \\ \\ = \textit{remainder} \end{array} \qquad 1068 = 7 \cdot 152 + 4$$

More generally, if  $m$  is a fixed positive integer, then we can divide any integer  $a$  by  $m$  to get a quotient  $q$  and a remainder  $r$  where  $r$  is one of the numbers  $0, 1, 2, \dots, m - 1$ . We summarize this by writing  $a = m \cdot q + r$  where  $0 \leq r < m$ .

The division algorithm is a simple process. Nevertheless, as we shall see this summer, it has a large number of unexpectedly deep consequences and can be generalized in far-reaching ways. One of the most basic applications of the division algorithm is to our notation for integers. It is customary to use base ten notation to write down the elements of  $\mathbf{Z}$ . For example 1068 is our notation for  $1 \cdot 10^3 + 0 \cdot 10^2 + 6 \cdot 10 + 8$ . But we could equally well use the base seven or some other base. As an example, let's write 1068 to base 7. We begin by using the division algorithm to divide 1068 by 7. We have already done this above, where we obtained  $1068 = 7 \cdot 152 + 4$ . Next we divide the quotient 152 by 7 to get a new quotient 21 and a new remainder 5:  $152 = 7 \cdot 21 + 5$ . Continuing in this way, we obtain the following list of equations.

$$\begin{array}{rcl} 1068 & = & 7 \cdot 152 + 4 \\ 152 & = & 7 \cdot 21 + 5 \\ 21 & = & 7 \cdot 3 + 0 \\ 3 & = & 7 \cdot 0 + 3. \end{array}$$

From these calculations we deduce that  $1068 = 3 \cdot 7^3 + 0 \cdot 7^2 + 5 \cdot 7 + 4$ . Hence 1068 (to base ten) is equal to  $(3054)_7$  written to base 7. The four ‘digits’ in this base seven representation are the four remainders above.

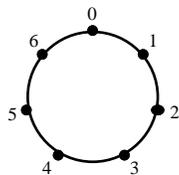
P1: Let  $N = 32701$  to base ten. Write  $N$  to base two, to base three, to base eleven. In the last case, introduce the new “digit”,  $T = 10$  if necessary.

P2: Without change of base, (a) add  $(6153)_7$  to  $(3455)_7$ ; (b) subtract  $(2346)_7$  from  $(4354)_7$ ; (c) multiply  $(632)_7$  by  $(435)_7$ ; (d) divide  $(5602)_7$  by  $(43)_7$ . Here the base is seven throughout.

**Exploration**

To help us gain insight and perspective on  $\mathbf{Z}$ , we will also investigate a number of alternative systems of arithmetic. Some fundamental examples of systems of arithmetic are given by so-called *modular arithmetics*. Probably the easiest way to explain what we mean by a modular arithmetic is to first look at a simple example.

Consider the set  $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ . This is the set of possible remainders we obtain if we divide by 7 using the division algorithm. The number 7 is called the modulus of our system, and  $\mathbf{Z}_7$  is called the system of least non-negative residues modulo 7. We are going to equip  $\mathbf{Z}_7$  with two operations: addition and multiplication. To describe these operations, it is convenient to arrange the elements of  $\mathbf{Z}_7$  in a circle, as follows.



Now suppose we want to add two elements of  $\mathbf{Z}_7$ , say we want to add 5 to 6. Then we start at 6 on the above circle and proceed clockwise a total of 5 units. That brings us to 4. So we say  $5 + 6 = 4$  in  $\mathbf{Z}_7$ . Here are some more examples of addition in  $\mathbf{Z}_7$ .

$$1 + 2 = 3; \quad 6 + 6 = 5; \quad 2 + 5 = 0; \quad 3 + 4 + 5 + 6 = 4.$$

It is also possible to multiply in  $\mathbf{Z}_7$ . Suppose for example, we want to multiply 6 by 2. Then we just add 6 to itself twice:  $6 \cdot 2 = 6 + 6 = 5$ . Similarly, to multiply 5 by 4 we add 5 to itself 4 times:  $5 \cdot 4 = 5 + 5 + 5 + 5 = 6$ . Here are a few more examples of multiplication in  $\mathbf{Z}_7$ .

$$2 \cdot 3 = 6; \quad 3 \cdot 4 = 5; \quad 4 \cdot 6 = 3; \quad 5 \cdot 5 \cdot 5 = 6.$$

Once we understand addition and multiplication, we can try to do more interesting calculations in  $\mathbf{Z}_7$ .

P3: How many of the following can you find in  $\mathbf{Z}_7$ ?

$$4 \cdot 5, \quad 2 - 6, \quad 1/2, \quad 2/5, \quad \sqrt{2}, \quad \sqrt{-3}, \quad \sqrt{-1}, \quad \sqrt[3]{6} ?$$

To get you started on this one, let's take a look at the third example: What is  $1/2$  in  $\mathbf{Z}_7$ ? To answer this question, we must first realize that  $1/2$  stands for the multiplicative inverse of 2 in  $\mathbf{Z}_7$ . Thus  $1/2$  is an element  $x$  in  $\mathbf{Z}_7$  for which  $2x = 1$ . Can you find an element  $x \in \mathbf{Z}_7$  such that  $2x = 1$ ? Is there more than one such  $x$ ? Note that  $\mathbf{Z}_7$  has only seven elements. If all else fails, you can always just try out all seven possible values of  $x$ .

P4: How many of the following can you find in  $\mathbf{Z}_{11}$ ? In  $\mathbf{Z}_{35}$ ? In  $\mathbf{Z}_9$ ? Any conjectures?

$$7 + 8, \quad 4 - 9, \quad 3 \cdot 5, \quad 5^2, \quad 5^3, \quad 1/5, \quad 3/8, \quad \sqrt{3}, \quad \sqrt{-2}, \quad \sqrt{-6}.$$

### Ingenuity

P5: Can you find an integer  $n > 1$  such that the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}$$

is an integer?

[I]t is impossible to be a mathematician without being a poet in soul . . . [T]he poet has only to perceive that which others do not perceive, to look deeper than others look. And the mathematician must do the same thing.

– Sonya Kovalevskaya

PROMYS Number Theory

Problem Set #1

Boston University, July 5, 2004

### Reading Search

Q1: What is a perfect number? Give four examples of perfect numbers.

Q2: What is a Mersenne prime? Give four examples of Mersenne primes.

Q3: What is the meaning of  $\sum_{\substack{d|N \\ d>0}} \frac{1}{d}$ ? Compute the value of this sum for some small values of  $N$ .

### Asking Good Questions

P1: Compare the following mathematical systems with each other:  $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$ ,  $2\mathbf{Z}$ ,  $\mathbf{Z}_3$ ,  $\mathbf{Z}_6$ ,  $\mathbf{Z}_8$ ,  $\mathbf{Z}_{11}$ . Each of these systems has two operations (addition and multiplication). Which of these systems resemble each other in regard to the essential properties of the operations?

### Exploration

P2: Consider the set of all polynomials in  $x$  with coefficients in  $\mathbf{Z}_3$ . Denote this set of polynomials by  $\mathbf{Z}_3[x]$ . Consider  $f(x) = x^2 + 2x + 1 \in \mathbf{Z}_3[x]$  and  $g(x) = 2x^2 + x + 1 \in \mathbf{Z}_3[x]$ . Calculate  $f(x) + g(x)$  and  $f(x) \cdot g(x)$ . Factor  $x^4 - 1$  into linear factors in  $\mathbf{Z}_5[x]$  and  $x^6 - 1$  into linear factors in  $\mathbf{Z}_7[x]$ .

### Prove or Disprove and Salvage if Possible

*In resolving questions and problems posed in our problem sets, one has to make use of many properties which one associates with integers. Make a list (inventory) of such properties and see if this inventory suffices for every discussion of questions of arithmetic which we undertake. If this inventory proves to be adequate for such discussion, then we shall consider it as an acceptable description of the integers.*

P3:  $a|a$  for every  $a \in \mathbf{Z}$ .

P4:  $a|b \Rightarrow b|a$  for all  $a$  and  $b$  in  $\mathbf{Z}$ .

P5: For all  $a, b, c \in \mathbf{Z}$ , if  $a|b$  and  $b|c$  then  $a|c$ .

P6:  $a|b \Rightarrow a|bc$  for all integers  $a, b, c$ .

P7: For all  $a, b, c$  in  $\mathbf{Z}$ , if  $a|b$  and  $a|c$  then  $a|(b + c)$ .

P8: For all  $a, b, c \in \mathbf{Z}$ ,  $a|bc \Rightarrow a|b$  or  $a|c$ .

### Numerical Problems (Some food for thought)

P9: Using division to base seven, write  $N = (34652)_7$  to base two, to base five, to base eleven.

P10: Write each of the following numbers to base three: 3, 9, 27, 243,  $1/3$ ,  $1/9$ ,  $1/27$ . Write each of these numbers to base two. Any conjectures?

P11: Find the following elements in  $\mathbf{Z}_5$ :  $-1$ ,  $1/2$ ,  $2/3$ ,  $\sqrt{-1}$ . How many of these elements can you find in  $\mathbf{Z}_6$ ? in  $\mathbf{Z}_{10}$ ? in  $\mathbf{Z}_{11}$ ? in  $\mathbf{Z}_{13}$ ?

P12: Make a list of the perfect squares in  $\mathbf{Z}_5$ , in  $\mathbf{Z}_{17}$ , in  $\mathbf{Z}_{19}$ , in  $\mathbf{Z}_{21}$ . How many squares are there in each case? Any conjectures?

P13: Calculate the sums:  $\sum_{\substack{d|6 \\ d>0}} \frac{1}{d}$ ,  $\sum_{\substack{d|28 \\ d>0}} \frac{1}{d}$ . Can you make an interesting conjecture? Perhaps another example may

help:  $\sum_{\substack{d|496 \\ d>0}} \frac{1}{d}$ . Calculate this sum and compare its value to the values of the first two sums.

### The Art of Counting

P14: Consider the set  $S = \{a, b, c, d\}$ . How many distinct subsets of  $S$  are there? How many distinct subsets of the set  $T = \{c, d, e, f, g, h\}$  are there? The sets  $S$  and  $T$  have 4 and 6 elements respectively. How many elements are there in  $S \cap T$ ? in  $S \cup T$ ? In general, if you know the number of elements in each one of two given sets  $S$  and  $T$ , can you say how many elements there are in  $S \cup T$ ?