

## Session 7, July 17

### The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every integer (greater than 1) can be factored into primes in essentially only one way. A compact way to say this is “ $\mathbf{Z}$  has unique prime factorization.” Let’s state the theorem more formally.

*The Fundamental Theorem of Arithmetic: If  $n$  is any integer greater than 1,  $n$  can be factored into (not necessarily distinct) primes*

$$n = p_1 p_2 p_3 \dots p_s.$$

*Furthermore, any other factorization of  $n$  into primes is, except possibly for the order of factors, the same as this one.*

Before we study the Fundamental Theorem in  $\mathbf{Z}$ , let’s see how it plays out in another number system, namely  $2\mathbf{Z}$ , which is the set of all even numbers.

1. Is  $2\mathbf{Z}$  closed under addition and multiplication? Explain.
2. List eight composites and ten primes in  $2\mathbf{Z}$ .
3. In  $2\mathbf{Z}$ , factor each number into primes.
 

(a) 12	(b) 14	(c) 8
(d) 16	(e) 24	(f) 30
(g) 144	(h) 36	(i) 40
4. Give two ways to characterize primes and to explain why 202 is a prime in  $2\mathbf{Z}$ :
  - (a) One that would make sense to the people who live in “the land of evens.”
  - (b) One that would make sense to people who live in Boston (and, hence, who know about all kinds of odd things, including odd numbers).
5. Does unique prime factorization hold true in  $2\mathbf{Z}$ ? Explain.

Well, we have a problem. In  $2\mathbf{Z}$ , we have two different factorizations of 36 into primes:

$$36 = 6 \cdot 6 = 18 \cdot 2.$$

(By the way, why are 6 and 18 primes?) But, some clever mathematician or student in this land of evens might imagine “ghost factors” lying behind the primes in the number system. Maybe 18 would equal  $2b^2$  for some ghost  $b$  and 6 might be  $2b$ . Then the mystery disappears:

$$\begin{aligned} 6 \cdot 6 &= 2b \cdot 2b = 2^2 b^2 \\ 18 \cdot 2 &= 2b^2 \cdot 2 = 2^2 b^2 \end{aligned}$$

This restores unique factorization, though the needed factors are “ideal numbers,” factors that are not really numbers in  $2\mathbf{Z}$ . However, these ideal numbers may be gradually accepted in the world of evens (although people may refer to them as “odd”).

6. Show that 200 can be factored into primes in more than one way in  $2\mathbf{Z}$ . Resolve the conflict with ghost factors.
7. Find all prime factorizations of 216 in  $2\mathbf{Z}$ . Resolve the conflict with ghost factors.
8. Characterize all numbers that have two or more distinct prime factorizations in  $2\mathbf{Z}$ .

Now that we have investigated prime factorization in another number system, let's go back to  $\mathbf{Z}$ .

9. Show that every integer greater than 1 is a product of primes. (Note: We're not yet concerned with the *uniqueness* of prime factorization.)

**Reminder:** Let  $a$  and  $d$  be integers. We say  $d \mid a$  (" $d$  divides  $a$ ") if there is an integer  $k$  such that  $a = dk$ . (So...  $7 \mid 280$  is a true statement, but  $7 \mid 281$  is a false statement.)

10. Prove or Disprove and Salvage if Possible:
  - (a) Let  $a, b, c \in \mathbf{Z}$ . If  $a \mid bc$ , then  $a \mid b$  or  $a \mid c$ .
  - (b) Let  $a, b, c \in \mathbf{Z}$ . If  $a \mid bc$  and  $a \nmid b$ , then  $a \mid c$ .
11. Which of the following equations have integral solutions? Why?
  - (a)  $5x + 7y = 1$
  - (b)  $21x + 3y = 1$
  - (c)  $14x + 119y = 1$
  - (d)  $1001x + 1502y = 1$
12. Show that if  $a \mid b$  and  $\gcd(a, b) = 1$ , then  $a \mid c$ . (Hint: What does  $\gcd(a, b) = 1$  imply?)
13. Let  $p$  be prime. Show that if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .
14. Does the statement in Problem 13 hold true in  $2\mathbf{Z}$ ?
15. Let  $p$  be prime. Show that if  $p$  divides a product of integers, then  $p$  must divide one of the factors.
16. Let  $p$  be prime. Show that if  $p$  divides a product of primes, then  $p$  must be equal to one of them.
17. Prove the Fundamental Theorem of Arithmetic. Here is the start of the proof.

We have already shown that every integer greater than 1 can be factored into primes. Next, suppose you have somehow managed to factor some integer  $n$  in two ways:

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_r$$

Well then,  $p_1 \mid q_1 q_2 \dots q_r$ . So by Problem 16,  $p_1$  must equal some  $q_i$ , say  $p_1 = q_1$ . Now, finish the proof!

If you proved the Fundamental Theorem (congratulations!), here are some exploratory problems for your mathematical pleasure. . .

18. Prove that there are infinitely many primes in  $\mathbf{Z}$ .
19. Compute  $4!$  (4 factorial) in  $\mathbf{Z}_5$ . Compute  $6!$  in  $\mathbf{Z}_7$ . Compute  $10!$  in  $\mathbf{Z}_{11}$ . Any conjectures?
20.  $\mathbf{Z}_5[x]$  is the set of all polynomials in  $x$  with coefficients in  $\mathbf{Z}_5$ . Factor  $x^4 - 1$  into linear factors in  $\mathbf{Z}_5[x]$ . Factor  $x^6 - 1$  in  $\mathbf{Z}_7[x]$ . Factor  $x^{10} - 1$  in  $\mathbf{Z}_{11}[x]$ . Any conjectures?
21. Expand  $(x + y)^2$  in  $\mathbf{Z}_2[x]$ . Expand  $(x + y)^3$  in  $\mathbf{Z}_3[x]$ . Expand  $(x + y)^5$  in  $\mathbf{Z}_5[x]$ . Any conjectures?
22. The cancellation law states that if  $ab = ac$ , then  $b = c$ .
  - (a) Does this always hold true in  $\mathbf{Z}$ ?
  - (b) Does the cancellation law hold in  $\mathbf{Z}_{15}$ ? In  $\mathbf{Z}_7$ ? How does the cancellation law differ in  $\mathbf{Z}_{15}$  and  $\mathbf{Z}_7$ ?