

1.7 When Factorisation Fails

WORKSHEET

The question

The set S consists of all the positive integers that leave a remainder of 1 upon division by 4. The set T consists of all the positive integers that leave a remainder of 3 upon division by 4.

- (i) Describe in words the sets $S \cup T$ and $S \cap T$.
- (ii) Prove that the product of any two integers in S is also in S . Determine whether the product of any two integers in T is also in T .
- (iii) Given an integer in T that is not a prime number, prove that at least one of its prime factors is in T .
- (iv) For any set X of positive integers, an integer in X (other than 1) is said to be *X-prime* if it cannot be expressed as the product of two or more integers *all in X* (and all different from 1).
 - (a) Show that every integer in T is either T -prime or is the product of an odd number of T -prime integers.
 - (b) Find an example of an integer in S that can be expressed as the product of S -prime integers in two distinct ways. [Note: $s_1 s_2$ and $s_2 s_1$ are not counted as distinct ways of expressing the product of s_1 and s_2 .]

Hints

Try the question on your own first. If you get stuck, read the hints *one at a time*, and go back to the question after each one. Hints marked *Pause and try* are the key steps.



Ask yourself List the first few members of S and T . Which members of S are S -prime, according to the definition in part (iv)?

STAGE 1 Union, intersection and products



Ask yourself How do you write a general member of S ? What is the product of two of them?

STAGE 2 A prime factor in T



Ask yourself Take a number in T that isn't prime. Its prime factors are all odd. What would happen if they were all in S ?

STAGE 3 An odd number of factors



Ask yourself If you multiply together an even number of members of T , where does the product land? What about an odd number?

STAGE 4 Two factorisations



Pause and try Find a number in S with two genuinely different factorisations into S -primes. *Hint:* use numbers like 9, which are S -prime only because their ordinary prime factors are missing from S .

Try this next

- 1 Another example.** Show that 693 has two different factorisations into S -primes. Can you find a general recipe for producing such examples?
- 2 Even numbers.** Let $E = \{2, 4, 6, 8, \dots\}$. Which numbers are E -prime? Show that 60 has more than one factorisation into E -primes.
- 3 $\mathbb{Z}[\sqrt{-5}]$.** Define the *norm* $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Show that $N(zw) = N(z)N(w)$. By showing that no element has norm 2 or 3, deduce that 2, 3 and $1 \pm \sqrt{-5}$ cannot be factorised further in $\mathbb{Z}[\sqrt{-5}]$.
- 4 Euclid's lemma in action.** **HARDER** Assuming Euclid's lemma (if a prime divides ab , it

divides a or b), prove that every integer greater than 1 has only one factorisation into primes, apart from the order of the factors.

Further reading

- ▶ **Ian Stewart & David Tall, *Algebraic Number Theory and Fermat's Last Theorem*** (CRC Press). The opening chapters tell the story of Lamé, Kummer and ideals at a level a keen first-year student can follow.
- ▶ **John Stillwell, *Elements of Number Theory***. Unique factorisation in the integers and in the Gaussian integers, compared side by side.
- ▶ **Harold Edwards, *Fermat's Last Theorem: A Genetic Introduction*** (Springer). For the ambitious: Kummer's work explained through its history.

The full guided solution, and what the question leads to at university, is in Section 1.7:
https://keithmcnulty.github.io/step_book_mcnulty/ch01/factorisation-fails.html