Factorization

In $\mathbb{Z}$, we have the Fundamental Theorem of Arithmetic: every integer can be written as a product of prime integers in essentially one way, in the sense that any two factorizations have the same length and can be rearranged so that corresponding factors are associate. For example,

$$30 = (-2) \cdot 5 \cdot (-3) \quad \text{and} \quad 30 = 3 \cdot (-5) \cdot (-2)$$

are different factorizations of 30, but we can rearrange them as

$$30 = (-2) \cdot (-3) \cdot 5 \quad \text{and} \quad 30 = (-2) \cdot 3 \cdot (-5),$$

where -2 and -2 are associate, -3 and 3 are associate, and 5 and -5 are associate.

The most basic (but correct!) algorithm to actually *compute* the prime factorization of a given integer n goes something like this.

To find a prime factorization of n:
Search among all a with $1 < a < |n|$ for a divisor of n.

- If no such divisor is found, then n is prime and thus $n = n$ is a prime factorization of n.
- If such a divisor is found, with $n = ab$, then *recursively* find prime factorizations $a = p_1 \cdots p_h$ and $b = q_1 \cdots q_k$. Then $n = p_1 \cdots p_h q_1 \cdots q_k$ is a prime factorization of n.

We might try to use this procedure in any domain, replacing the word "prime" with "irreducible". However, there are many subtle ways it can fail. For a particular domain R and a particular element $x \in R$,

- Maybe R has no irreducible elements.
- Maybe R does have irreducible elements, but the factorization procedure never terminates. (Every factorization of x has infinite length.)
- Maybe the factorization procedure terminates only for *some* choices of the divisors a and b. (Some factorizations of x have infinite length.)
- Maybe the factorization procedure always terminates, but x has arbitrarily long factorizations.
- Maybe the factorizations of x are all of bounded length, but generally have *different* lengths.
- Maybe the factorizations of x are all of the same length, but cannot generally be rearranged so that corresponding factors are associates.

By the way, there are examples of domains where each of these things happens!

Definition 1 (Unique Factorization Domain)**.** *Let R be a domain. We say that R is a* unique factorization domain *(UFD) if every nonzero element of R can be written as a product of irreducibles in essentially one way. That is, for each $x \in R$, we can write $x = p_1 p_2 \cdots p_m$ where the p_i are irreducible, and if $x = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_\ell$, with the p_i and q_i irreducible, then $m = \ell$ and we can rearrange the q_i so that p_i and q_i are associates for each i.*

For example, $\mathbb{Z}$ is a UFD. The value of a UFD is that irreducibles act like the "building blocks" for all other elements, much like the prime numbers are the building blocks of the integers.

Lemma 1. *Let R be a UFD, and let $x, y \in R$. Suppose we have factored x and y as*

$$x = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \quad \text{and} \quad y = u p_1^{f_1} p_2^{f_2} \cdots p_m^{f_m},$$

where the e_i and f_i are natural numbers. (Note that this is always possible by taking associates.)

Then $x|y$ if and only if $e_i \leq f_i$ for each $i \in [1, m]$.

Proposition 2. *Every UFD is a GCD Domain.*

Proof. Let $x, y \in R$, and factor x and y as

$$x = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \quad \text{and} \quad y = u p_1^{f_1} p_2^{f_2} \cdots p_m^{f_m}.$$

Then

$$z = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_m^{\min(e_m, f_m)}$$

is a maximal common divisor of x and y. □

Some History

One of the historical threads that led to the development of modern abstract algebra was an attempt by 19th century mathematician Ernst Kummer to prove Fermat's Last Theorem using factorization. Recall that FLT is the assertion that the equation $a^n + b^n = c^n$ has no interesting integer solutions (a, b, c) if $n > 2$. Kummer's idea was to rearrange this equation as $a^n = c^n - b^n$. Now if ζ is a primitive nth root of unity, the right hand side factors as

$$a^n = (c - b)(c - \zeta b)(c - \zeta^2 b) \cdots (c - \zeta^{n-1} b).$$

For example, if $n = 4$ then i is a primitive 4th roots of unity and we have

$$a^4 = (c - b)(c - ib)(c + b)(c + ib)$$

This yields two different factorizations of a^n, which may lead to a contradiction.

The problem with Kummer's idea was that it only works if the ring $\mathbb{Z}[\zeta]$ is a UFD, which, at the time, was not known. Nobody had bothered to check! The idea that this line of attack might solve the famous FLT led to an explosion of new ideas in algebraic number theory that continues to this day.

Eventually it was found that $\mathbb{Z}[\zeta]$ is sometimes a UFD, but not always – so Kummer's idea did not work. But it is more useful to judge an idea not by what problems it *can't* solve, but by what problems it *can* and what new ideas it inspires. By this measure Kummer's attempt at FLT is among the most successful failures in mathematics.

Exercises

1. Suppose that R is a domain and $N : R \to \mathbb{N}$ a multiplicative norm. Show that if $x \in R$, then the irreducible factorizations of x have bounded length.