

## UNIQUE FACTORIZATION

**Lemma 1.** *If  $a$  and  $b$  are not both zero, and  $g = \gcd(a, b)$ , then there exist integers  $m$  and  $n$  such that*

$$am + bn = g.$$

An immediate consequence:

**Corollary 2.** *If  $a$  and  $b$  are relatively prime, then there exist integers  $m$  and  $n$  such that*

$$am + bn = 1.$$

**Lemma 3.** *If  $a$  and  $b$  are relatively prime, and  $a \mid bc$ , then  $a \mid c$ .*

*Proof.* Find integers  $m$  and  $n$  such that

$$am + bn = 1.$$

Multiply by  $c$ :

$$acm + bcn = c.$$

Since  $a \mid bc$ , there is an integer  $q$  such that

$$bc = aq.$$

Hence,

$$c = acm + bcn = acm + aqn = a(cm + qn),$$

which proves that  $a \mid c$ .

An easy consequence:

**Proposition 4.** *If  $p$  is a prime and  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .*

Note that the conclusion fails if  $a$  and  $b$  are not relatively prime, for example  $6 \mid 10 \cdot 15$ , but 6 does not divide 10, nor does 6 divide 15.

*Proof.* What can you say about  $\gcd(p, a)$ ?

**Proposition 5.** *Even number  $n \geq 2$  can be written as a product of primes, that is, there exist primes  $p_1, p_2, p_3, \dots, p_r$  such that*

$$n = p_1 p_2 p_3 \cdots p_r.$$

Note: we allow  $r$  to be 1, in which case,  $n$  is a prime itself.

**Theorem 6.** *[Unique Factorization] The list of primes in Proposition 5 is unique, up to order.*

Note: the statement is false, if we don't have primes:

$$30 = 2 \times 15 = 3 \times 10 = 5 \times 6.$$

**Question:** Is this an obvious theorem?

That is, in any system like the integers, in which primes can be defined (as irreducible elements), must it be the case that factorization into primes is unique?

The answer is “no” as the following 2 surprising examples demonstrate:

**Strange Example #1.** Let

$$R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Addition and multiplication are defined by

$$\begin{aligned}(a + b\sqrt{-5}) + (c + d\sqrt{-5}) &= (a + c) + (c + d)\sqrt{-5} \\ (a + b\sqrt{-5}) \times (c + d\sqrt{-5}) &= (ac - 5bd) + (ad + bc)\sqrt{-5}\end{aligned}$$

The number  $1 + 0\sqrt{-5}$  acts like the number 1 and  $0 + 0\sqrt{-5}$  acts like the number 0. A number  $p = a + b\sqrt{-5}$  is a **prime** in set  $R$  if  $p$  cannot be factored, other than  $p \times 1$  and  $(-p) \times (-1)$ . It can be shown that 2, 3,  $1 + \sqrt{-5}$ , and  $1 - \sqrt{-5}$  are all primes in  $R$ . But now we have two distinct ways of factoring 6 into primes:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

**Strange Example #2.** Let

$$S = \{1, 5, 9, 13, 17, \dots\}$$

denote the set of all positive integers of the form  $4n + 1$ . An element  $p$  in  $S$  is called an  $S$ -prime if  $p > 1$  and the only divisors of  $p$  among the elements of  $S$  are 1 and  $p$ . For example,  $p = 49$  is an  $S$ -prime. An element  $n > 1$  in  $S$  which is not an  $S$ -prime is called an  $S$ -composite.

- (a) Show that every  $S$ -composite is a product of  $S$ -primes.
- (b) Find the smallest element of  $S$  which can be expressed as a product of  $S$ -primes in more than one way.

Note: in both “strange” examples, Proposition 4 fails to hold.