

## Euler on the case $n = 3$ of Fermat's Last Theorem - Continued

Using our knowledge about Dedekind domains, we prove that, whenever  $p$  and  $q$  are coprime integers, where  $p$  is even and not divisible by 3, then the number  $2p(p^2 + 3q^2)$  is never a perfect cube.

Let  $\omega = \frac{-1 + i\sqrt{3}}{2}$  (a primitive cube root of unity). Then  $K = \mathbb{Q}(\omega) = \mathbb{Q}(i\sqrt{3})$  and its ring of integers is  $D_K = \mathbb{Z}\left[\frac{1 + i\sqrt{3}}{2}\right] = \mathbb{Z}[\omega]$ . A basis of  $D_K$  over  $\mathbb{Z}$  is given by  $1, \omega$ , so that the general form of its elements is  $\frac{u + i\sqrt{3}v}{2}$ , where  $u, v$  are integers such that  $u \equiv v \pmod{2}$ .

**We show that  $D_K$  is a PID.** We prove that  $cl(D_K) = 1$ . To this end, we consider the two embeddings  $\sigma_1, \sigma_2 : K \rightarrow \mathbb{C}$  (where  $\sigma_1$  is the identity) and compute the constant

$$C = \prod_{i=1}^2 (|\sigma_i(1)| + |\sigma_i(\omega)|) = \left(1 + \left|\frac{-1 + i\sqrt{3}}{2}\right|\right) \left(1 + \left|\frac{-1 - i\sqrt{3}}{2}\right|\right) = 2 \cdot 2 = 4.$$

We thus have to consider the prime ideals occurring in the factorizations of the ideals (2) and (3). These factorizations can be determined using Kummer's Criterion. The minimal polynomial of  $\omega$  over  $\mathbb{Q}$  is  $f(x) = \Phi_3(x) = x^2 + x + 1$ , irreducible modulo 2, whereas it splits as  $(x - \bar{1})^2$  modulo 3. Hence

- (2) is prime in  $D_K$ ,
- (3) =  $(3, \omega - 1)^2 = (\omega - 1)^2$  (because  $3 = (\omega - 1)(\bar{\omega} - 1)$ ).

All prime ideals we found are principal, which immediately implies our claim.

**Next we show that the numbers  $p + q\sqrt{-3}$  and  $p - q\sqrt{-3}$  are coprime in  $D_K$ .** Suppose by contradiction that they have a common prime factor  $d$  in  $D_K$ . Then  $d \mid 2p$ , but  $d \neq 2$ , since  $d$  divides  $p^2 + 3q^2$ , but 2 does not. Hence  $d \mid p$ . This, in turn, implies that  $d$  is not a prime factor of 3: otherwise  $p$  and 3 would not be coprime, against our assumption. On the other hand,  $d \mid 3q^2$ . Hence  $d \mid q$ . But this contradicts the coprimality of  $p, q$ .

As a consequence of our preceding claim, if the integer

$$p^2 + 3q^2 = (p + qi\sqrt{3})(p - qi\sqrt{3})$$

is a perfect cube, its prime factorization in  $D_K$  splits (up to units) into the factorizations of two cubes. Namely, there are two numbers  $s = \frac{u}{2}$  and  $t = \frac{v}{2}$  where  $u, v$  are integers for which  $u \equiv v \pmod{2}$ , such that

$$p + qi\sqrt{3} = (s + ti\sqrt{3})^3 \quad (1a)$$

$$p - qi\sqrt{3} = (s - ti\sqrt{3})^3 \quad (1b)$$

(It can be shown that we can neglect units other than  $1, -1$ .) Note that  $(1b)$  follows from  $(1a)$  by applying  $\sigma_2$ . This implies that

$$p^2 + 3q^2 = (s^2 + 3t^2)^3.$$

Hence, if  $2p(p^2 + 3q^2)$  is a perfect cube, so is  $2p$ .

From  $(1a)$  and  $(1b)$  we also deduce that

$$\begin{aligned} 2p &= 2s(s + 3t)(s - 3t) \\ q &= 3t(s + t)(s - t) \end{aligned}$$

The integers  $2s$  and  $s + 3t$  are coprime. If this were not the case, then  $2s$  and  $3s + 3t$  would have some common prime factor. This would not be  $3$ , since  $3$  does not divide  $p$ . But then the same factor would divide  $s + t$ , so that  $p$  and  $q$  would not be coprime, against our assumption. It follows that  $2s$ ,  $s + 3t$  and  $s - 3t$  are coprime. Consequently, if  $2p$  is a perfect square, so is each of these factors. But then the conclusion follows as in the previous note.