TWO APPLICATIONS OF UNIQUE FACTORIZATION

KEITH CONRAD

1. Introduction

.

We will use unique factorization to determine all the integral solutions to certain equations.

Theorem 1.1. *The integral solutions to $y^2 + y = x^3$ are $(x, y) = (0, 0)$ and $(0, -1)$.*

Since $y^2 + y = y(y + 1)$, this says in words that the only integer which is a product of two consecutive integers and is a cube is 0.

Theorem 1.2 (Fermat). *The integral solutions to $y^2 = x^3 - 2$ are $(x, y) = (3, 5)$ and $(3, -5)$.*

The proof of Theorem 1.1, which is really a warm-up for Theorem 1.2, will use unique factorization in **Z**. Although Theorem 1.2 is only about integers, its proof will go beyond **Z** and use unique factorization in the ring $\mathbf{Z}[\sqrt{-2}]$.

2. Proofs

Before we prove Theorems 1.1 and 1.2 we need a result about relatively prime numbers whose product is a power. (We say elements in a UFD are *relatively prime* when they have no irreducible factor in common: their only common divisors are units.)

Theorem 2.1. *Let R be a ring with unique factorization. If $a, b, c \in R$ are nonzero, $ab = c^n$, and a and b are relatively prime then there are units u and v as well as a' and b' in R such that $a = ua'^n$ and $b = vb'^n$.*

Proof. Decompose a, b, and c into irreducibles and collect together any irreducible factors which are equal up to unit multiple. This lets us write

$$a = up_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}, \quad b = vp_1'^{f_1}p_2'^{f_2}\cdots p_s'^{f_s}, \quad c = wq_1^{g_1}q_2^{g_2}\cdots q_t^{g_t},$$

where p_i, p_j', and q_k are all irreducibles and u, v, and w are units. Since a and b are relatively prime, no p_i and p_j' are unit multiples. We have

$$ab = uvp_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}p_1'^{f_1}p_2'^{f_2}\cdots p_s'^{f_s}$$

and

$$c^n = w^n q_1^{ng_1}q_2^{ng_2}\cdots q_t^{ng_t}.$$

Comparing the irreducible factorizations of ab and c^n shows from unique factorization that each p_i and p_j' has multiplicity divisible by n: each e_i and f_j is some ng_k. (Here is where we need relative primality of a and b). Since all the e_i's are divisible by n, a is u times an nth power. Similarly, b is v times an nth power. □

Example 2.2. Taking $n = 2$, in $\mathbf{Z}$ we have $(-4)(-9) = 6^2$ and -4 and -9 are each squares up to unit multiple. Notice neither -4 nor -9 is a square, so the equality up to unit multiple in the conclusion of Theorem 2.1 can't be weakened in general.

Now we are ready to prove the theorems from Section 1.

First we prove Theorem 1.1.

Proof. Suppose x and y are integers which satisfy $y^2 + y = x^3$. Write this as

$$y(y+1) = x^3.$$

Assuming neither y nor $y+1$ is 0, these integers are relatively prime (consecutive integers have no common factors except ± 1) and we can apply Theorem 2.1: their product is a cube so each one is a cube up to sign:

$$y = \pm a^3, \quad y + 1 = \pm b^3.$$

Since -1 is a cube, if there is a sign appearing then it can be absorbed into the cube and then rename a and b. Thus we have

$$y = a^3, \quad y + 1 = b^3.$$

The integers y and $y+1$ are consecutive, so a^3 and b^3 are consecutive cubes. The cubes spread apart pretty quickly:

$$\ldots, \ -64, \ -27, \ -8, \ -1, \ 0, \ 1, \ 8, \ 27, \ 64, \ \ldots.$$

We see immediately that the only consecutive cubes are -1 and 0 and also 0 and 1. Since $y = a^3$ is the smaller of the two cubes, $y = -1$ or $y = 0$. We get $x^3 = y^2 + y = 0$ in both cases. So (x, y) is $(0, -1)$ or $(0, 0)$.

These are the solutions we expected, although strictly speaking our argument assumed y and $y+1$ are not 0 in order to apply Theorem 2.1. So what we have really shown in this case is that there is no solution with y not 0 or -1. For those two y-values we have the two obvious solutions, so they are the only ones. □

Now we prove Theorem 1.2.

Proof. Assume x and y are integers satisfying $y^2 = x^3 - 2$. First we determine the parity of x and y. If x is even then $8|x^3$, so $y^2 \equiv -2 \equiv 6 \bmod 8$. However, a direct check of all integers modulo 8 shows the only squares modulo 8 are 0, 1, and 4. Thus x has to be odd, so y is also odd. All we will need to know is that *x is odd.*

We now rewrite the equation $y^2 = x^3 - 2$ as

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}). \tag{2.1}$$

We have factored $y^2 + 2$ in $\mathbf{Z}[\sqrt{-2}]$ and will copy the idea in the proof of Theorem 1.1. Our first task is to show $y \pm \sqrt{-2}$ are relatively prime in $\mathbf{Z}[\sqrt{-2}]$. The key idea is to pick some unknown common divisor of $y + \sqrt{-2}$ and $y - \sqrt{-2}$, write down some divisiblity relations with it in $\mathbf{Z}[\sqrt{-2}]$, and then take norms down to $\mathbf{Z}$ to draw conclusions. Recall $\mathrm{N}(a + b\sqrt{-2}) = a^2 + 2b^2$ and the norm is multiplicative and takes nonnegative values. In particular, if $\alpha|\beta$ in $\mathbf{Z}[\sqrt{-2}]$ then $\mathrm{N}(\alpha)|\,\mathrm{N}(\beta)$ in $\mathbf{Z}$.

Let d be a common divisor of $y + \sqrt{-2}$ and $y - \sqrt{-2}$. We want to show $d = \pm 1$. A divisor of two numbers divides their difference, so d divides $(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$, which doesn't involve y. So $d|2\sqrt{-2}$ in $\mathbf{Z}[\sqrt{-2}]$, and taking norms turns this into $\mathrm{N}(d)|8$ in $\mathbf{Z}$. At the same time, $\mathrm{N}(d)$ divides $\mathrm{N}(y + \sqrt{-2}) = y^2 + 2 = x^3$, which is odd, so $\mathrm{N}(d)$ is odd. The only odd positive divisor of 8 is 1, so $\mathrm{N}(d) = 1$. Therefore $d = \pm 1$, so $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime.

So far we have not used unique factorization in $\mathbf{Z}[\sqrt{-2}]$. Now we do. Equation (2.1) expresses a cube as a product of two relatively prime factors. Therefore $y + \sqrt{-2}$ is a unit times a cube. The units in $\mathbf{Z}[\sqrt{-2}]$ are ± 1, which are both cubes. Therefore $y + \sqrt{-2}$ is a pure cube:

$$y + \sqrt{-2} = (m + n\sqrt{-2})^3 = (m^3 - 6mn^2) + (3m^2n - 2n^3)\sqrt{-2}.$$

Equating real and imaginary parts,

$$y = m(m^2 - 6n^2), \quad 1 = n(3m^2 - 2n^2).$$

From the second equation $n = \pm 1$. If $n = 1$ then $1 = 3m^2 - 2$, so $m^2 = 1$. Thus $m = \pm 1$, which makes $y = \pm(1 - 6) = \pm 5$ and $x^3 = 25 + 2 = 27$ so $x = 3$. We have recovered the solutions $(3, \pm 5)$. If $n = -1$ then $1 = -(3m^2 - 2)$, so $3m^2 = 1$. This has no integral solutions, so we are done. The only integer solutions to $y^2 = x^3 - 2$ are $(3, \pm 5)$. □

While $y^2 = x^3 - 2$ has finitely many integral solutions, it has infinitely many rational solutions. In addition to $(3, \pm 5)$, the next simplest rational solutions are

$$\left(\frac{129}{100}, \pm\frac{383}{1000}\right) \text{ and } \left(\frac{164323}{29241}, \pm\frac{66234835}{5000211}\right).$$