The Begin of an Exciting Story
UTK – M351 – Algebra I
Spring 2004, Jochen Denzler

Problem 22 of your homework is actually the begin of an exciting story. To explain this, I need to change the ring in Problem 22 (which I have chosen for simplicity) a little bit. I could have asked the same problem (division with remainder) for the ring

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a \in \mathbb{Z}, b \in \mathbb{Z}\} \quad \text{with } \omega = \frac{-1 + i\sqrt{3}}{2}$$

instead of

$$\mathbb{Z}[i] = \{a + bi \mid a \in \mathbb{Z}, b \in \mathbb{Z}\} .$$

The significance of ω is that $z = \omega$ is a complex solution of $z^3 = 1$, as compared to $z = i$, which is a complex solution of $z^4 = 1$.

And the ring $\mathbb{Z}[\omega]$ plays an important role in the early days of the famous Fermat problem, which made the headlines a few years ago: Fermat had claimed that there are no (nonzero) integer solutions u, v, w to the equation $u^3+v^3 = w^3$, nor to $u^4+v^4 = w^4$, nor to $u^5+v^5 = w^5$, etc., for any integer exponent $n \geq 3$. (In contrast, for $n = 2$, you have many such solutions, the simplest ones being $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$.) And I said 'nonzero', because we don't care for trivial solutions like $5^3 + 0^3 = 5^3$. As nobody knew how to prove Fermat's claim for general exponent n, people would naturally start tackling specific exponents n, one at a time. $n = 4$ was the easiest, but the next more difficult one, $n = 3$ will be the hero of our story. And you already see that we are in the right company with the number ω, which was designed as one other solution to $z^{\mathbf{3}} = 1$ (next to the obvious real solution $z = 1$), when we are dealing with third powers as in the equation $u^{\mathbf{3}} + v^{\mathbf{3}} = w^{\mathbf{3}}$.

To appreciate the one crucial idea people had in those days, think of the following simpler problem: I ask you "are there integers u, v such that $u^2 + v^2 + 1 = 0$?" – You immediately reply "No way, there are not even real numbers u, v that could satisfy the equation, let alone integers."

Well, the same easy answer is not available for $u^3+v^3 = w^3$, because there *are* real solutions, like e.g. $(\sqrt[3]{7})^3 + (\sqrt[3]{5})^3 = (\sqrt[3]{12})^3$. But maybe we can find some other class of numbers comprising more than only the integers, but certainly not all real or complex numbers; a class of numbers that has two properties: (1) We can show that even in that larger class of numbers there is no soluton. (2) We actually gain an *advantage* that simplifies the work in that larger class of numbers, as compared to the set $\mathbb{Z}$. This miraculaous class of numbers is the ring $\mathbb{Z}[\omega]$, which contains $\mathbb{Z}$ as a subring but is itself a subring of $\mathbb{C}$ (not a subring of $\mathbb{R}$). It was shown that there are no nontrivial solutions $u^3 + v^3 = w^3$ in the ring of numbers $\mathbb{Z}[\omega]$, and therefore not in the smaller ring $\mathbb{Z}$ either.

What made $\mathbb{Z}[\omega]$ such an advantageous ring to work in? The answer is that you can write $u^3 + v^3 = (u + v)(u + \omega v)(u + \omega^2 v)$. And they would start (kind of): "Let p be a prime number dividing w. Then it must divide $w^3 = u^3 + v^3$, and so it must either divide $u + v$ or $u + \omega v$ or $u + \omega^2 v$ etc." You have seen a very simple version of this kind of game in the proof that there are no integer solutions of $u^2 = 2v^2$ (i.e., $\sqrt{2}$ is not rational). Remember? 2 must divide u^2, so 2 must divide u, but then u^2 is divisible by 4, and then v^2 must be even, etc.

Now there was only one problem: Prime numbers were taylormade for the ring $\mathbb{Z}$, not for the ring $\mathbb{Z}[\omega]$ (and the concept of a ring wasn't invented yet in those days anyways). So it was necessary to rebuild the whole arithmetic from scratch, starting with divisibility, division with

remainder (there we go with our problem 22) all the way up to prime numbers, but this time for the ring $\mathbb{Z}[\omega]$. They did it, and a lot more along these lines. And the Fermat problem became the midwife for a whole area of mathematics, at the borderline between abstract algebra (which was not invented then) and number theory (which the ancient Greeks knew already, but which needed to be re-invented for the new numbers).

And even though the whole story is much deeper than our M351 course, I feel you should have heard about this background, because our course, too, is on the borderline between abstract algebra and number theory. And without this history, some of the stuff might not have made it into the curriculum. I have taken the history lightly here. It was actually Euler, who proved the case $n = 3$ in the first half of the 18th century. But the general reconstruction of arithmetic dates more than 100 years later, with Kummer, Dirichlet, Dedekind being some of the big names. My focus is not on historic detail, but on a perspective that sheds light on today's mathematics. I do not know and have not investigated how much of the modern point of view can actually be recognized in Euler's original proof.

You find the proof that $u^3 + v^3 = w^3$ has no nontrivial solutions in $\mathbb{Z}[\omega]$ in the classical book by Niven and Zuckerman: "Introduction to the theory of numbers" (for instance). They also give the proof that $u^4 + v^4 = w^4$ has no solutions in integers. Since this proof does not use exotic number rings, they put it in an altogether different chapter. Both proofs (and the book as a whole) is feasible reading for *A* students (and in parts for B students, too), but you need to take some time for it. If I had to present the $n = 3$ proof in class for an honors version of M351, I'd probably take 2–3 classes for it (*after* the number theory we will yet do, and still omitting some technicalities).