SRQR: Diophantine $ax + by = c$ (April 2, 2021)

> Is there some term for variables like r and s in this section that when multiplied with a gcd return an original number? That relationship seems like a useful one to have a designated term for, rather than just relying on a description of those values' uses.

If there is a succinct word, I don't know it. I do know that, if d is a divisor of a, then a/d is sometimes called the *complementary divisor* — for example, 3 is a divisor of 21, and 7 is its complementary divisor since $3 \cdot 7 = 21$. So you could say that, if r is the integer with the property that $\gcd(a, b) \cdot r = a$, then r is the "divisor of a complementary to $\gcd(a, b)$."

> At the bottom of page 35 in the corollary, what does the author mean by "integral values of t?"

"Integral values of t" here means that t is allowed to be any integer.

> Example 2.4 shows that the Diophantine equation $ax + by = c$ can have a finite but nonzero number of solutions if the solutions are restricted to only positive integers. If we allow solutions to be any integer, is it true that there will always be either zero or infinitely many solutions?

Yep! This is part of what theorem 2.9 says. The first part of that theorem tells you precisely when there are any solutions at all. The second part tells you that, if there's one solution, there have to be infinitely many.

> I am confused on how to finish up the Diophantine equations after finding the gcd.

Broadly, the steps for finding one *particular* solution for $ax + by = c$ are:

(1) Find $d = \gcd(a, b)$.
(2) Use the backwards part of the Euclidean algorithm to write $ar + bs = d$ for integers r, s. These integers r and s are sometimes called *Bézout coefficients* for a and b (because theorem 2.3 is sometimes called *Bézout's theorem*).
(3) Multiply both sides of $ar + bs = d$ by c/d so that you get $ax + by = c$ for integers x, y.

Once you've found a particular solution this way, you can use theorem 2.9 to describe all solutions.

> Could you please elaborate on Example 2.5 on page 36 where it says, "Upon multiplying the relation $1 = 1 \cdot (-3) + 4 \cdot 1$ by 44 to get $44 = 1 \cdot (-132) + 4 \cdot 44$"? Why we need to multiply it by 44?

You're asking about why to do step (3) listed above. Note that in this example, we're trying to solve the Diophantine equation

$$x + 4z = 44.$$

When we find the equation

$$1 \times (-3) + 4 \cdot 1 = 1,$$

what we've found is a solution to the equation $x' + 4z' = 1$ – namely, $x' = -3$ and $y' = 1$. This isn't the same equation, but if we multiply this equation by 44, we get $(44x') + 4 \cdot (44z') = 44$. In other words, taking $x = 44x'$ and $z = 44z'$ will yield a solution to the equation that we're actually interested in solving!

> There are a lot of theorems, rules and relationships developed in this chapter, how much should we focus on memorization? Both in the context of this class as well as in the context of a career of mathematics.

My experience has been that, if I spend enough time studying the proof of a result by working through lots of examples and really internalizing the *why* of it all, that understanding persists in my memory without much effort. If I later try to recall something, I may not remember the theorem statement verbatim right away, but I can think about my understanding of examples to reconstruct the statement of the theorem.

> Is there a good way of intuitively grasping why Diophantine equations only have solutions when the right hand side is divisible by the gcd of the right hand terms?

At one level, the answer to this is a little bit of formalism: if the diophantine equation

$$ax + by = c$$

has a solution, the LHS is clearly divisible by $d = \gcd(a, b)$, so the RHS had better be too!

But I think a more useful response to this question is sort of a combination of my responses to the previous three questions. There is a way to intuitively grasp this, and the way is to work through lots of examples of these kinds of diophantine equations using the method described in the textbook (and summarized above).