PROFESSOR: So now we're ready to put together the facts that the gcd is a linear combination to prove two cool results-- one fun, and the other important and serious. Let's begin with the Die Hard example. So we looked at the Die Hard state machine, and we figured out the behavior of it with jugs of size 3 and 5 gallons, and also with jugs of size 3 and 6 gallons. Let's look at the general case now.

Suppose that I have jugs of a gallons and b gallons, where a and b are positive integers. Now, when we looked at the state machine, we figured out that under the Die Hard rules, the number of gallons in each bucket at any stage is a linear combination of the bucket sizes. So at any point after any sequence of moves of Die Hard moves, in each bucket there will be a linear combination of a and b.

Now, the point is that linear combinations of a and b are the same as multiples of the gcd. The reason is that the gcd is a divisor of a and b, of course. It's a common divisor, and therefore it divides any linear combination of a and b. So any linear combination of a and b is a multiple of the gcd, and the gcd is itself a linear combination.

So linear combinations of a and b are the same as multiples of gcd. So that gives us a pretty good understanding of what the amounts that we can get in the various buckets are. We can only get multiples of gcd's, but in fact, you can get any multiple of the gcd of a and b into a bucket, providing it will fit in the bucket. That's the same as saying that you can get any linear combination amount of a and b into a bucket if there is room for it in the bucket. So let's see how to do that.

So suppose I have a linear combination of a and b, sa plus tb, that will fit in bucket b, meaning it's greater than or equal to 0, and it's less than b. So it's a number of gallons that could fit into bucket b. How do I get that amount into bucket b? And here's how.

We can assume that s is positive. We've already seen that we can arrange that to be the case. And so what we're going to do is repeat the following procedure s times.

I'm going to fill up bucket a and pour it into bucket b. Whenever b gets filled up, I'll just dump it so that it's empty, and I can keep filling up bucket a and pouring it into bucket b. And I repeat that s times.

Now, when I do that, the total number of times that I've filled bucket a is s times. So the total amount of water that I have taken from the faucet, or from the fountain, is s times a. And I've poured it into b and then dumped it, leaving only some amount that's in b that's less than b. So the amount that's left after pouring in sa gallons and dumping out what won't fit, I'm left with some amount that's non-negative and less than b in bucket b.

OK. Now, the point is that the number of emptyings of bucket b must be exactly t, which is why the amount of water that's left in bucket b is sa minus tb. And the reason why it has to be minus t is that if I've got sa there, if I had more than t emptyings, I would have had bucket b go negative. There just isn't enough room for it.

And if I had fewer than t emptyings, then the bucket would have an amount larger than b in it. So the only possible number of emptyings of b is minus t. Remember, t is negative, so minus t is a positive number. And that means that I've put in sa and taken out tb, and I'm left with exactly the linear combination sa minus tb. So in fact, there's no need to count, because you don't need to know what s and t are.

Because knowing that you can get any desired amount that's a multiple of the gcd into bucket b, you just keep doing this process until you get the amount that you want. So you fill bucket a. You pour it into b.

When b fills, you empty it. You just keep track of how many gallons there are in bucket b, and you keep going until you get the amount that you want. And then you're done.