So now we begin on four classes on number theory. The purpose of taking it up now is that we're still practicing proofs. And number theory is a nice self-contained elementary subject as we'll treat it, which has some quite elegant proofs and illustrates contradiction and other structures that we've learned about. A little bit of induction, and definitely some applications of the well-ordering principle.

The ultimate punchline of the whole unit is to understand the RSA crypto system and how it works. Along the way, we will-- today, actually-- establish one of those mother's milk facts that we all take for granted about unique factorization of integers into primes. But in fact, that's a theorem that merits some proof as an example, and the homework shows where we exhibited a system of numbers which didn't factor uniquely.

And finally, we will be able to knock off the *Die Hard* story once and for all.

So let's begin by stating the rules of the game. We're going to assume all of the usual algebraic rules for addition and multiplication and subtraction. So you may know some of these rules have names like the first equality is called distributivity of multiplication over plus-- of times over plus-- and then the second rule here is called commutativity of multiplication, and here are some more familiar rules. This is called associativity of multiplication. This is called the additive identity. a minus a is 0-- or actually additive inverse. 0 is the additive identity and minus a is the inverse of a. a plus 0 equals a is the definition of 0 being an additive identity. a plus 1 is greater than a.

So these are all standard algebraic facts that we're going to take for granted and not worry about. And one more fact that we also know and we're going to take as an axiom, if I divide a positive number-- sorry. If I divide a number a by a positive number b, then when we're talking about integers, what I'm going to get is a quotient and a remainder. What's the definition of the quotient and a remainder?

Well, the division theorem says that if I divide a by b, that means if I take the quotient times b plus the remainder I get a. And in fact, there's a unique quotient of a/b and there's a unique remainder of a/b where the remainder-- what makes it unique is the remainder is constrained to be in the interval greater than or equal to 0 and less than the divisor b.

So we're going to take this fact for granted too. Proving it is not worth thinking about too hard, because it's one of those facts that's so elementary that it's hard to think of other things that would more legitimately prove it. I'm sure it could be proved by induction, but I haven't really thought that through. OK.

A key relation that we're going to be looking at today is the relation of divisibility between integers. So by the way, all of the variables for the next week or so are going to be understood to range over the integers. So when I say

number, I mean integer. When I talk about variables a and c and k, I mean that they're taking integer values.

So I'm going to define c divides a using this vertical bar notation. It's read as divides. c divides a if and only if a is equal to k times c for some k. And there are a variety of synonyms for a divides b, like-- a is a-- a divides c-- sorry-- c divides a is to say that a is a multiple of c and c is a divisor of a.

OK. Let's just practice this. So 5 divides 15? Well, because 15 is 3 times 5. A number n divides 0. Every number n divides 0. Even 0 divides 0, because 0 is equal to 0 times n. So 0 is a multiple of every number.

Another trivial fact that follows from the definition is that if c divides a, then c divides any constant times a. Well, let's just check that out, how it follows from the definition. If I'm given that c divides a, that means that a is equal to k prime c for some k prime. That implies that if I multiply both sides of this equality by s, I get that s a is equal to s k prime c, and if I parenthesize the s k prime, I can call that to be k, and I have found, sure enough, that s a is a multiple of c. That's a trivial proof, but we're just practicing with the definitions.

So we have just verified this fact that if c divides a, then c divides a constant times a. As a matter of fact, if c divides a and c divides b, then c divides a plus b. Let's just check that one. What we've got is c divides a means that a is equal to k1 times c. And c divides b means that b is equal to k2 times c. So that means that a plus b is simply k1 plus k2 times c, where what I've done here is used the distributivity law to factor c out and used the fact that multiplication is commutative so that I can factor out on either side.

OK. Let's put those facts together. If c divides a and c divides b, then c divides s a plus t b, where s and t are any integers are all. So a combination of two numbers, a and b, like this is called a linear combination of a and b-- an integer linear combination, but since we're only talking about integers, I'm going to stop saying integer linear combination and just say linear combination. A linear combination of a and b is what you get by of multiplying them by coefficients s and t and adding.

OK. So we've just figured out that in fact if c divides a and c divides b, then c divides an integer linear combination of b. When c divides two numbers, it's called a common divisor of those two numbers. So we could rephrase this observation by saying common divisors of a and b divide integer linear combinations of a and b, which is a good fact to just file away in your head.

Now, what we're going to be focusing on for the rest of today is the concept of the greatest common divisor of a and be, called the GCD of a and b. The greatest common divisor of a and b exists by the well-ordering principle, because it's a set of non-negative integers with an upper bound. Namely, a is an upper bound on the greatest common divisor of a and b. So as we did in an exercise, or I think in the text, that implies that there will be the greatest one among all the common divisors, assuming there are any. But 1 is always a common divisor, so there

are guaranteed to be some.

Let's look at some examples.

The greatest common divisor of 10 and 12. You can check. It's 2. Mainly because 10 factors into 2 times 5 and 12 factors into 2 times 6, and the 6 and the 5 have no common factors. So the only one that they share is 2.

The GCD of 13 and 12 is 1. They have no common factors in common. You can see that because 13 is a prime, and so it has no factors other than 1 and 13, and 13 doesn't divide 12 because it's too big. So it's got to be 1.

The GCD of 17 and 17 is 17. That's a general phenomenon. The GCD of n and n is always n.

The greatest common divisor of 0 and n is equal to n for any positive n. That's because everything is a divisor of 0 and it means the GCD of 0 and n is simply the greatest divisor of n, which is of course n by itself.

One final fact to set things up for the next segment is to think about the GCD of a prime and a number, and it's either 1 or p. The reason is that the only divisors of a prime are plus/minus 1 and plus/minus p. So if p divides a, the GCD is p, and otherwise the GCD is 1.