Lecture 5  More on primes and divisibility
Last time ended with

**Proposition 1.6.7** Given \( a, d \in \mathbb{Z} \), \( d \geq 1 \), there exist unique \( q, r \in \mathbb{Z} \) such that
\[
a = qd + r \quad \text{and} \quad 0 \leq r < d.
\]

[Finish proof of uniqueness from previous notes]

This proposition gives us an algorithm to find the greatest common divisor of two integers.

**Def** Given nonzero integers \( m, n \), the greatest common divisor \( d = \gcd(m, n) \) is the unique natural number with the properties.
(i) \( d \mid m \) and \( d \mid n \),
(ii) If \( x \mid m \) and \( x \mid n \) then \( x \mid d \).
We say that \( m \) and \( n \) are relatively prime if \( \gcd(m, n) = 1 \).

**Algorithm:** To find \( \gcd(m, n) \), apply Prop. 1.6.7 repeatedly and take the last non-zero remainder, as in the following example:

Find \( \gcd(81, 66) \):

(\text{i}) \( 81 = 1 \cdot 66 + 15 \)
(\text{ii}) \( 66 = 4 \cdot 15 + 6 \)
(\text{iii}) \( 15 = 2 \cdot 6 + 3 \)
(\text{iv}) \( 6 = 2 \cdot 3 + 0 \)

So 3 is the gcd. Indeed, (\text{iv}) shows 3 \mid 6, then (\text{iii}) shows 3 \mid 15, then (\text{ii}) shows 3 \mid 66, then (\text{i}) shows 3 \mid 81. So 3 \mid 81 and 3 \mid 66.
On the other hand, we can write, by substituting the equations into each of the 
\[ 3 = 15 - 2 \cdot 6 \]
\[ = 15 - 2(66 - 4 \cdot 15) \]
\[ = (81 - 66) - 2(66 - 4(81 - 66)) \]
\[ = 9 \cdot 81 - 11 \cdot 66 \]
So if \( x|81 \) and \( x|66 \), then \( x| (9 \cdot 81 - 11 \cdot 66) = 3 \).
So \( 3 \) satisfies both properties in the definition of \( \gcd \).

**Proposition (1.6.11, 10.13)** Given non-zero integers \( m, n \in \mathbb{Z} \),
there are \( a, b \in \mathbb{Z} \) such that
\[ am + bn = \gcd (m, n). \]
"\( \gcd (m, n) \) is an integer linear combination of \( m \) and \( n \)."

**Proof:** see Goodman.

**Problem:** Find \( \gcd (119, 35) \) and find \( a, b \in \mathbb{Z} \) such that
\[ 119a + 35b = \gcd (119, 35) \]

**Solution:**
\[ 119 = 3 \cdot 35 + 14 \]
\[ 35 = 2 \cdot 14 + 7 \]
\[ 14 = 2 \cdot 7 + 0 \]
So \( \boxed{\gcd (119, 35) = 7} \)

Now
\[ 7 = 35 - 2 \cdot 14 = 35 - 2(119 - 3 \cdot 35) \]
\[ = -2 \cdot 119 + 7 \cdot 35. \]
So \( \boxed{a = -2, b = 7} \).

**Proposition (1.6.19)** If \( p \in \mathbb{N} \) is prime, \( a, b \in \mathbb{Z} \), and \( p|ab \), then either \( p|a \) or \( p|b \).
Proof: Since $p$ is prime, and $\gcd(p,a)$ is a divisor of $p$, 
\[ \gcd(p,a) = 1 \text{ or } p. \]

Case: $\gcd(p,a) = p$. Then $p | a$ by def of gcd, so we are done.

Case: $\gcd(p,a) = 1$. Then $\exists s, t \in \mathbb{Z}$ such that 
\[ sp + ta = 1 \]

Then 
\[ spb + tab = b \]

Since $p | ab$, we have $p | spb + tab = b$, and we are done. \( \square \)

Theorem (1.6.21) The prime factorization of a natural number is unique up to the order of the factors.

Proof: Induction on $n$. For $n = 1$, only the empty product is possible, so the base case holds.

Suppose that for all $k < n$, $k$ has a unique prime factorization (up to the order of the factors). Suppose 
\[ n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t \]
are two prime factorizations of $n$. We may assume, by reordering the factors if necessary, that 
\[ p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_s \]
\[ q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_t \]

Also by swapping $p$'s and $q$'s if necessary, we may assume $p_1 \leq q_1$. Since $p_1 | n = q_1 \cdots q_t$, we must have 
\[ p_1 | q_2 \text{ for some } i. \]
Since $p_1$ and $q_2$ are prime, we must have $p_1 = q_2$. 

Then $p_1 \leq q_1 \leq q_2 = p_1$, so $p_1 = q_1$. Then

$$\frac{n}{p_1} = \frac{p_2 p_3 \cdots p_s}{q_1 q_2 q_3 \cdots q_t} = \frac{n}{q_1}$$

since this number is $< n$, we know it has a unique factorization.

The order of the factors is fixed by the assumption that the factors increase from left to right, so we have $s = t$ and $p_j = q_j$ for all $j$.

Thus the two factorizations of $n$ were the same, and the induction step is complete. \(\blacksquare\)