Proof of Thm 2.6

Since \( \gcd(a, b) = 1 \), by Thm 2.4,
we have integers \( x, y \) such that
\[ ax + cy = 1. \]

Multiply both sides by \( b \), \( abx + bcy = b \).
Since \( clab \) and \( clbc \), \( c \) must also divide \( b \).

Cor 2.7 If \( p | ab \) and \( p \nmid a \), then \( p \nmid b \).

Cor 2.8 If \( p | a, p \nmid a_1 \), \( \ldots \), then \( p \nmid a_i \) for some \( i \).

Proof: Induction.

§ 2.3 The Linear Diophantine Equation

Thm 2.9. The linear diophantine equation
\[ ax + by = c, \]
has a integral solution if and only if \( d | c \), where \( d = \gcd(a, b) \). Furthermore, if \( (x_0, y_0) \) is a solution of this equation, then the set of solutions of the equation consists of all integer pairs \( (x, y) \), where
\[ x = x_0 + t \frac{b}{d}, \quad y = y_0 - t \frac{a}{d}, \]
for any integer \( t \).
Ex. Solve the diophantine equation

\[ 156x + 1740y = 48 \]

Solution

\[ 1740 = 156 \times 11 + 24 \]
\[ 156 = 24 \times 6 + 12 \]
\[ 24 = 12 \times 2 \]
\[ 12 = 156 - 24 \times 6 = 156 - (1740 - 156 \times 11) \times 6 \]
\[ = 156 - 1740 \times 6 + 156 \times 66 \]
\[ = 156 \times 67 + 1740 \times (-6) \]

\[ 48 = 156 \times 268 + 1740 \times (-24) \]
\[ 156 = 12 \times 13 \]
\[ 1740 = 12 \times 145 \]
\[ x_0 = 268, \quad y_0 = -24 \]
\[ x = 268 + 145t, \quad y = -24 - 13t \]

Ex. Solve the diophantine

\[ 17x + 19y = 23 \]

Solution

\[ \gcd(17, 19) = 1 \]
\[ 1 = 17 \times 1 + 2 \]
\[ 19 = 17 \times 1 + 2 \]
\[ 17 = 2 \times 8 + 1 \]

\[ \gcd(23, 29) = 1 \]
\[ 1 = \ldots \]
Ex. A man pays $1.43 for some pears and apples.
If pears cost 17¢ each and apples, 15¢ each,
how many of each of each did he buy?
Solution. Suppose he buys x pears and y apples.
then \[ 17x + 15y = 143 \]
\[ 17 = 15 \times 1 + 2 \]
\[ 15 = 2 \times 7 + 1 \]
\[ 1 = 15 - 2 \times 7 = 15 - (17 - 15) \times 7 = -17 \times 7 + 15 \times 8 \]

§ 2.4. The Fundamental Theorem of Arithmetic

For each integer \( n > 1 \), there exists primes
\( p_1 \leq p_2 \leq \ldots \leq p_r \) such that
\[ n = p_1 p_2 \ldots p_r \]
This factorization is unique.

Proof. "Existence." We want to show that each integer
has at least one prime factorization. We proceed with
induction. Now we may easily check that \( n = 2, 3, 4, 5 \)
has such factorization. So we assume it is true for all
\( 1 < m < k \) and we would like to prove that it is also true
for \( m = k+1 \).
If \( k+1 \) is a prime, we are done. If not, \( k+1 = ab \) with \( 1 < a < k+1 \), \( 1 < b < k+1 \). By our induction hypothesis, both \( a \) and \( b \) have prime factorizations; therefore \( k+1 \) also has one (by multiplying the two).

"Uniqueness"

By induction, assume for all \( 1 < m \leq k \), \( m \) has unique prime factorization. For \( m = k+1 \), if there are two prime factorizations

\[
\frac{k+1}{p_1} = p_1 p_2 \cdots p_r = p_1 p_2' \cdots p_s'
\]

with \( p_1 \leq p_2 \leq \cdots \leq p_r \), \( p_1' \leq p_2' \leq \cdots \leq p_s' \).

Now \( p_1 | p_1 p_2 \cdots p_r \). So \( p_1 | p_i \) for some \( i \).

Same argument shows that \( p_1 | p_j \) for some \( j \).

Hence

\[
p_i = p_j' \geq p_1'
\]

\[
p_i' = p_i \geq p_1
\]

So \( p_1 = p_1' \).

\[
\frac{k+1}{p_1} = p_2 \cdots p_r = p_2' \cdots p_s'
\]

\( \frac{k+1}{p_1} \) is an integer \( \leq k \), by our induction hypothesis. It must have unique factorization. Therefore (\( r \geq 5 \))

\[
p_2 = p_2', \quad p_3 = p_3', \quad \cdots \quad p_r = p_r'
\]