620-113 Explorations in Number Theory

**Theorem 1** (Euclid, Prop. 30, Book VII). If \( p \) is prime and \( p \mid ab \), then either \( p \mid a \) or \( p \mid b \).

*Proof.* We have two choices - either \( p \mid a \) or \( p \notmid a \). If the former is true then we have succeeded. However if \( p \notmid a \) then there exists an integer \( c \) such that \( pc = ab \). Since \( p \notmid a \) then \( p \) and \( a \) are coprime. By Theorem 5 there exists integers \( x \) and \( y \) such that \( 1 = px + ay \). Therefore

\[
\begin{align*}
b &= b(px + ay) \\
   &= pbx + aby \\
   &= pbx + pcy \\
   &= p(bx + cy)
\end{align*}
\]

and thus \( p \mid b \). \( \Box \)

**Remark 1.** This only works for primes - e.g. \( 6 \mid 12 = 3 \cdot 4 \) but \( 6 \notmid 3 \) and \( 6 \notmid 4 \).

**Example 1.** Factor the following integers into prime factors

1. \( 540 = 2^2 \cdot 3^3 \cdot 5 \)
2. \( 3750 = 2 \cdot 3^3 \cdot 5^4 \)
3. \( 4725 = 3^3 \cdot 5^2 \cdot 7 \)
4. \( 3718 = 2 \cdot 11 \cdot 13^2 \)
5. \( 3234 = 2 \cdot 3 \cdot 7 \cdot 11^2 \cdot 13 \)

**Theorem 2** (The Fundamental Theorem of Arithmetic). Except for the order of the factors every positive integer \( n > 1 \) can be expressed uniquely as a product of primes

\[
(1) \quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}
\]

*Proof.* Proof by contradiction. Let

\[
(1) \quad n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad r, s > 1
\]

and suppose we order the prime factors

\[
p_1 \leq p_2 \leq \cdots \leq p_r \quad \text{and} \quad q_1 \leq q_2 \leq \cdots \leq q_s
\]

and without loss of generality \( r \leq s \). The it is immediate that \( p \mid q_1 q_2 \cdots q_s \) and from Theorem 1 we know that \( p_i \mid q_i \) for some \( 1 \leq i \leq s \). But \( p_1 \) and \( q_1 \) are both primes so this implies \( p_1 = q_1 \), and furthermore that \( p_1 \geq q_1 \). A similar argument can be applied for \( q_1 \), namely that \( q_1 \mid p_1 p_2 \cdots p_r \) and by Theorem 1 \( q_1 \mid p_j \) for some \( 1 \leq j \leq r \). This

\[1\]
implies $q_1 = p_j \geq p_1$. Combining both these results we have in fact $p_1 = q_1$. Now divide out these equal factors to yield

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s.$$

The above argument can be repeated to show that

$$p_2 = q_2$$

$$\vdots$$

$$p_r = q_r.$$

If $r < s$ then we would have

$$\frac{n}{p_1 p_2 \cdots p_r} = 1 = q_{r+1} \cdots q_s,$$

which is false because each $q_j > 1$. Therefore we have $r = s$ and $p_i = q_i$ for $1 \leq i \leq r$ and the representation is unique. □

**Theorem 3** (Euclid, Prop. 20, Book IX of the Elements). *The number of primes is infinite.*

*Euclid’s proof.* Proof by contradiction. Suppose the number of primes is infinite and these are $p_1, p_2, \ldots, p_r$. Consider the integer $n = p_1 p_2 \ldots p_r + 1$. Clearly $n > p_i$ for all $i = 1, \ldots, r$ and therefore must be composite. By Theorem 1 of the first Lecture $n$ must have prime divisors $p_i$. Therefore $p_i \mid n$ for some $i$, but this implies $p_i \mid 1$ which is impossible. □

*Kummer’s proof.* Suppose there are only a finite number of primes $p_1 < p_2 < \ldots < p_r$ and let $N = p_1 p_2 \ldots p_r > 2$. Now consider $N - 1$, which being a product of primes has a prime divisor $p_i$. Therefore $p_i \mid N - 1$ and $p_i \mid N$ which implies $p_i \mid N - (N - 1) = 1$ which is impossible. □