The Fundamental Theorem of Arithmetic (FTA) and primes.

Throughout, p and q (sometimes with subscripts) denote primes, i.e. positive integers n s.t. $d \mid n$, $d > 0 \Rightarrow d = 1$ or $d = n$.

If $d > 1$ is not prime, it's composite. By def'n, 1 is neither prime nor composite.

Thm 1.6. Every $n > 1$ can be written as a product of one or more primes.

Proof: induction on n. It's true for $n = 2$. Now assume it's true for $n = 1, 2, \ldots, k-1$. If k is prime, we're done. If not, then $\exists$ an integer a with $a \mid k$ and $1 < a < k$. Write $k = ab$: then also $1 < b < k$. Now apply induction to a and b. $\square$

Consequently, we have our first distribution-of-primes result:

Thm 1.7 (Euclid). $\exists$ infinitely many primes.

Proof: suppose not. Suppose there are (only) K primes $p_1, p_2, \ldots, p_K$. Define

$$N = p_1 p_2 \cdots p_K + 1. \qquad (*)$$

Note that $N > p_K$, so N can't be a prime. So by Thm. 1.6, $\exists\, j \in \{1, 2, \ldots, K\}$ with

$p_j | N$. Of course $p_j | (p_1 p_2 \cdots p_k)$ as well, so by $(*)$ and linearity of divisibility, $p_j | 1$. Contradiction (if $p_j | 1$ then, since $1 | p_j$ and $1, p_j > 0$, we'd have $p_j = 1$: but 1 is not prime).

So $\exists$ infinitely many primes. $\square$

<u>Thm. 1.8:</u> If $p \nmid a$, then $(a, p) = 1$.

<u>Proof</u>: If $(a,p) \neq 1$ then either $(a,p) = 0$, in which case $a = 0$, so $p | a$, or $(a,p) > 1$. In the latter case, $\exists c > 1$: $c | a$ and $c | p$. But $c | p$ and $c > 1 \Rightarrow c = p$. So $p | a$. $\square$

<u>Thm. 1.9.</u>

$p | ab \Rightarrow p | a$ or $p | b$.

<u>Proof</u>: spz $p | ab$. If $p | a$ then we're done. If not then $(a, p) = 1$ by Thm. 1.8, so $p | b$ by Thm 1.5. $\square$

We have the following refinement of Thm. 1.6 above:

<u>Thm. 1.10 (FTA).</u>

Every $n > 1$ has a representation as a product of primes that's <u>unique</u> up to order.

<u>Proof.</u>

Use induction on n. If $n = 2$ we're done. Now assume the thm. is true for $2 \leq n \leq k-1$: we show that this implies the case $n = k$.

If k is prime, we're done. If not then, by Thm 1.6, k has an expression

$$k = p_1 p_2 \cdots p_s$$

for primes p_j, $1 \le j \le s$ and $s \ge 2$. Suppose we also have

$$k = q_1 q_2 \cdots q_t$$

for primes q_j, $1 \le j \le t$. Then

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \qquad (**)$$

Now p_1 divides the left side and therefore the right. By Thm. 1.9 extended to n-term products, we have $p_1 | q_j$ for some j. We can assume $j = 1$, since we're not concerned with order. But q_1 is prime, so $p_1 = q_1$. So $(**)$ yields

$$p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t.$$

Both sides are $< k$ and are > 1 (since we assumed k is not prime), so by induction on k,

$$\{p_2, p_3, \ldots, p_s\} = \{q_2, q_3, \ldots, q_s\}.$$

Combining this with the fact that $p_1 = q_1$ yields our result. $\square$

<u>Note.</u> Let p_m denote the m^{th} smallest prime. By FTA, $\exists$ unique non-negative integers $a_1, a_2, a_3, \ldots,$ of which only finitely many are positive, such that

$$n = \prod_{m=1}^{\infty} p_m^{a_m}.$$

Remark: in writing such products, we'll always tacitly assume that the a_m's are non-negative integers, almost all of which $= 0$.

Thm 1.11.

For n as above,

$$d \mid n \iff d = \prod_{m=1}^{\infty} p_m^{c_m}$$

where $0 \le c_m \le a_m$ for all m.
(Proof omitted.)

And finally:

Thm. 1.12.
If $a = \prod_{m=1}^{\infty} p_m^{a_m}$ and $b = \prod_{m=1}^{\infty} p_m^{b_m}$,

then

$$(a,b) = \prod_{m=1}^{\infty} p_m^{\min\{a_m, b_m\}}.$$

(Proof omitted.)