例 1. 求证: 每个合数一定有素因子.

证明. 假设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数. 如果 p 不是素数, 则存在整数 $1 < q < p$, 使得 $q \mid p$. 根据整除的传递性, 由于 $p \mid n$, 有 $q \mid n$. 这与 p 是 n 的最小正因数矛盾. 所以 p 是素数, 合数 n 必有素因子. □

例 2. 求证: 若 $5 \mid n$, $11 \mid n$, 则 $55 \mid n$.

证明. 由条件得 $n = 5q_1$, $n = 11q_2$, 其中 q_1, q_2 为整数. 联立两式得 $(11 - 5 \cdot 2)n = 55(q_1 - q_2 \cdot 2)$, 其中 $q_1 - q_2 \cdot 2$ 也是整数, 所以 $55 \mid n$. □

例 3. 求证: 每个奇整数的平方必有 $8k + 1$ 的形式.

证明. 每个奇整数的平方必有形式 $(2n + 1)^2$, 其中 n 是整数. 若其也有 $8k + 1$ 的形式, 则

$$\begin{aligned} (2n+1)^2 &= 8k+1 \\ 4n^2 + 4n + 1 &= 8k + 1 \\ n(n+1) &= 2k. \end{aligned}$$

为使 k 为整数, 需要 $2 \mid n(n + 1)$. 而 n 和 $n + 1$ 中一定有一数是 2 的倍数, 故结论成立. □

例 4. 求 1414 和 666 的最大公因数, 并求出它们的线性表达式.

解. 使用拓展欧几里得算法:

$$\begin{aligned} 1414 &= 666 \cdot 2 + 82 & \qquad 82 &= 1414 + 666 \cdot (-2) \\ 666 &= 82 \cdot 8 + 10 & 10 &= 1414 \cdot (-8) + 666 \cdot 17 \\ 82 &= 10 \cdot 8 + 2 & 2 &= 1414 \cdot 65 + 666 \cdot (-138) \\ 10 &= 2 \cdot 5 + 0. \end{aligned}$$

得到它们的最大公因数是 2, 并且线性表达式为 $1414 \cdot (65 + 666k) + 666 \cdot (-138 - 1414k) = 2$, 其中 k 取任何整数.

例 5. 求证: $\sqrt{2}$, $\sqrt{7}$, $\sqrt{17}$ 都不是有理数.

证明. 假设 p 是素数, 且 $\sqrt{p}$ 是有理数, 则 $\sqrt{p} = m/n$, 其中 m, n 是互质的正整数.

i) 经变换得 $pn^2 = m^2$, 根据整除的定义, 有 $p \mid m^2$. 又因为 p 是素数, 有 $p \mid m$.

ii) 由 $p \mid m$ 得, 存在整数 k, 使得 $m = pk$.

iii) 将 $m = pk$ 代入 $pn^2 = m^2$, 得 $n^2 = pk^2$, 则类似步骤 (1), 有 $p \mid n$,

iv) 由 (1)(3) 得 m 与 n 都有因数 $p > 1$, 这与 m, n 互质矛盾.

v) 假设有误, 故 $\sqrt{p}$ 是无理数. 而 2, 7, 17 都是素数, 所以 $\sqrt{2}$, $\sqrt{7}$, $\sqrt{17}$ 都不是有理数. □

例 6. 求证: 形如 $4k + 3$ 的素数有无穷多个.

证明. 首先, 要证明形如 $4k+3$ 的正整数必含有形如 $4k+3$ 的素因数: 任意奇素数都只能写成 $4k+1$ 或 $4k+3$ 两种形式. 若将两个形如 $4k+1$ 的数 $4n_1+1$, $4n_2+1$ 相乘, 即

$$\begin{aligned}(4n_1+1)(4n_2+1) &= 16n_1n_2+4n_1+4n_2+1 \\ &= 4(4n_1n_2+n_1+n_2)+1.\end{aligned}$$

经过数学归纳得, 有限个形如 $4k+1$ 的数的乘积仍为形式为 $4k+1$ 的数. 因此, 将形如 $4k+3$ 的整数分解为若干个素因数的乘积时, 这些素因数中必须含有形如 $4k+3$ 的素数.

假设所有形如 $4k+3$ 的素数 $p_1, p_2, \ldots, p_n$ 都不大于一正整数 N. 令 $q = 4(p_1p_2\cdots p_n) - 1$. 那么任何 p_i $(i = 1, 2, \ldots, n)$ 都不是 q 的素因数, 否则将得到 $p_i \mid 1$, 这不可能.

若 q 是素数, 由 $q = 4(p_1p_2\cdots p_n) - 1 = 4(p_1p_2\cdots p_n - 1) + 3$ 得知它是 $4k+3$ 形式的素数, 并且 $q > N$; 若 q 不是素数, 由上述推理得其必含有形如 $4k+3$ 的素因数, 而且任何 p_i $(i = 1, 2, \ldots, n)$ 都不是 q 的素因数. 所以 q 是形如 $4k+3$ 且一定大于 N 的素数. □

例 7. 设 p 是合数 n 的最小素因数. 求证: 若 $p > n^{1/3}$, 则 n/p 是素数.

证明. 根据算术基本定理, n 能被唯一分解为一系列素数的乘积, 即

$$n = p_1p_2\cdots p_k \quad (1 < p_1 \le p_2 \le \cdots \le p_k < n,\ k \ge 1).$$

经过放缩, 得到 $p_1^k \le n$, 即 $p_1 \le n^{1/k}$. 若 $k \ge 3$, 则 $p_1 \le n^{1/3}$. 但根据题意, 有 $p_1 > n^{1/3}$, 从而有 $k < 3$, 即 k 只能取值 1 或 2. 接下来分别考虑 k 的取值情况. 若 k 取 1, 那么 $n = p_1$ 是素数, 不符合题意. 所以 k 只能取 2. 那么 $n = p_1p_2$, 其中 p_1 是 n 的最小素因数, 故 $p = p_1$. 所以 $n/p = n_2$, 根据上述分解, 它是素数. □