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, 且合数 n 必有素因子. □

例 2. 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, 所以结论成立. □

例 3. 求证: 若 $5 \mid n$, $11 \mid n$, 则 $55 \mid n$.

证明. 由题意得, 必存在正整数 q_1, q_2 使得 $n = 5q_1, n = 11q_2$. 将两边同时乘以 11 或 5, 得到 $11n = 55q_1, 5n = 55q_2$. 由 $n = 11n - (5n) \cdot 2 = 55(q_1 - q_2 \cdot 2)$ 可以看出 $55 \mid n$. □

例 4. 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

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

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 $n = p_1 p_2$, 其中 p_1 是 n 的最小素因数, 故 $p = p_1$. 所以 $n/p = p_2$, 是一个素数. □

例 5. 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 $4n_1+1$ 和 $4n_2+1$ 相乘, 即

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

经过归纳, 可知有限个形如 $4k+1$ 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 6. 设 $m > n$ 是正整数. 证明 $2^n-1 \mid 2^m-1$ 的充要条件是 $n \mid m$. 以任一正整数 $a > 2$ 代替 2, 结论仍成立吗?

证明. 首先证明充分性. 由 $n \mid m$ 可知, 存在正整数 k 使得 $m = kn$. 所以

$$\begin{aligned}2^m-1 &= 2^{kn}-1 \\ &= (2^n-1)(2^{(k-1)n}+2^{(k-2)n}+\cdots+2^n+1).\end{aligned}$$

可以看出 $2^n-1 \mid 2^m-1$.

接下来证明必要性. 使用带余除法, 得到 $m = nq+r$ $(0 \le r < n)$. 所以

$$\begin{aligned}2^m-1 &= 2^{kn+r}-1 = 2^{kn}2^r-1 \\ &= 2^{kn}2^r-2^r+2^r-1 \\ &= 2^r(2^{kn}-1)+2^r-1 \\ &= N(2^n-1)+2^r-1,\end{aligned}$$

其中 N 是某个整数, 因为之前证明了 $2^n-1 \mid 2^{km}-1$. 根据 $2^n-1 \mid 2^m-1$, 可知 $2^n-1 \mid 2^r-1$. 但由于 $2^r-1 < 2^n-1$, 必须有 $2^r-1=0$, 即 $r=0$. 代入 $m = nq+r$ 中, 可以得到 $n \mid m$. □

例 7. 设奇数 $a > 2$. 设使得 $a \mid 2^d - 1$ 的最小正整数 $d = d_0$. 证明: 2^d 被 a 整除后, 所可能取到的不同的最小非负余数有 d_0 个.

证明. 由于 $a \mid 2^{d_0} - 1$, 那么对于所有 $1 \le d < d_0$, 都有 $a \nmid 2^d - 1$, 否则不满足 d_0 是满足要求的最小正整数.

接下来要说明, 由 $2^d - 1$ $(d = 1, 2, \ldots, d_0)$ 组成的序列中, 每个数除以 a 得到的余数两两不相同. 假设存在正整数 $1 \le i < j \le d_0$ 使得 $2^i - 1$ 和 $2^j - 1$ 除以 a 得到的余数都为 r $(0 \le r < a)$. 也就是 $2^i - 1 = aq_1 + r$, $2^j - 1 = aq_2 + r$. 将两式相减, 得到 $2^j - 2^i = a(q_2 - q_1)$, 即 $a \mid 2^j - 2^i = 2^{j-i}(2^i - 1)$. 由于 $a \nmid 2^i - 1$, 这说明 $a \mid 2^{j-i}$, 进而 a 是偶数. 我们知道 $a \mid 2^{d_0} - 1$, 但是偶数不能整除奇数, 这造成了矛盾.

另外, 我们可以发现

$$
\begin{aligned}
2^{d+d_0} - 1 &= 2^d 2^{d_0} - 1 \\
&= 2^d 2^{d_0} - 2^d + 2^d - 1 \\
&= 2^d (2^{d_0} - 1) + 2^d - 1 \\
&= aN + 2^d - 1,
\end{aligned}
$$

其中 N 是某个整数. 这可以说明对于所有正整数 d, 都有 a 整除 $2^d - 1$ 的余数和 a 整除 $2^{d+d_0} - 1$ 的余数相同. 所以数列 $2^d - 1$ $(d = 1, 2, \ldots, d_0)$ 中每个数除以 a 得到的余数就是所有可能取到的 d_0 个余数. □

例 8. 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:

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

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

例 9. 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. 经变换得 $pn^2=m^2$. 根据整除的定义, 有 $p\mid m^2$. 因为 p 是素数, 又有 $p\mid m$, 即存在整数 k, 使得 $m=pk$. 将 $m=pk$ 代入 $pn^2=m^2$ 得到 $n^2=pk^2$. 重复上述步骤, 可以发现 $p\mid n$.

这说明 m 与 n 都有质因数 p, 与 m,n 互质矛盾. 所以假设有误, 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 10. 设整数 $a>b>0$, $n>1$. 证明: $a^n-b^n\nmid a^n+b^n$.

证明. 假设 $a^n-b^n\mid a^n+b^n$. 那么

$$\frac{a^n+b^n}{a^n-b^n}=1+\frac{2b^n}{a^n-b^n}=1+\frac{2}{(a/b)^n-1}.$$

这说明了 $(a/b)^n$ 只能取 2 或 3. 但这在 $n>1$ 时不可能成立, 与假设矛盾. □