离散数学基础习题答案

Answers to Exercises in Elementary Discrete Mathematics

周晓聪　　乔海燕

中山大学数据科学与计算机学院, 广州 510275

2021 年 1 月 19 日

目录

第四章　证明方法

练习 4.1 对任意整数a, b, c，证明：如果$a \mid b$且$a \mid c$，则$a \mid (b+c)$且$a \mid bc$。你使用的证明方法是直接证明还是间接证明？

证明 若$a \mid b$，即存在k_1使得$b = k_1a$，若$a \mid c$，即存在k_2使得$c = k_2a$，从而$b+c = (k_1+k_2)a$，$bc = (k_1k_2a)a$，因此$a \mid (b+c)$且$a \mid bc$。这里使用的是直接证明。 □

练习* 4.2 对任意整数a, b, c，证明：如果$a \mid b$且$a \mid c$，则对任意的整数s, t有$a \mid bs + ct$。你使用的证明方法是直接证明还是间接证明？

证明 若$a \mid b$，即存在k_1使得$b = k_1a$，若$a \mid c$，即存在k_2使得$c = k_2a$，从而对任意的整数s, t有$bs + ct = sk_1a + tk_2a = (sk_1 + tk_2)a$，因此$a \mid bs + ct$。这里使用的是直接证明。 □

练习 4.3 设n和m是大于1的整数且$n \mid m$，a和b是整数且$a \equiv b (\mod m)$。证明$a \equiv b (\mod n)$。你使用的证明方法是直接证明还是间接证明？

证明 若$n \mid m$，则存在k使得$m = kn$，而$a \equiv b (\mod m)$，则存在整数t使得$a - b = tm$，从而$a - b = tkn$，从而$a \equiv b (\mod n)$。这是直接证明。 □

练习 4.4 设有命题：对任意的实数x和y，$x^2 + xy - 2y^2 = 0$。

(1) 对于该命题，下面的证明有什么错误？

证明 *设x和y等于某个任意的实数r，则有：*

$$x^2 + xy - 2y^2 = r^2 + r \cdot r - 2r^2 = 0$$

既然x和y都是任意的，因此这表明对任意的实数x, y有$x^2 + xy - 2y^2 = 0$。

(2) 上述命题是否成立？给出一个证明或给出一个反例说明你判断的理由。

解答：(1) 证明的错误在于，x和y是任意的实数，它们不一定相等，不能假设它们都是r（都等于r，则x和y并不是任意的实数）。

(2) 这个命题不成立，例如$x = 2, y = 1$，则$x^2 + xy - 2y^2 = 4 + 2 - 2 = 4 \neq 0$。

练习 4.5 设n是整数，证明如果$2 \mid n^3$，则$2 \mid n$。你用的证明方法是直接证明还是间接证明？

证明 若没有$2 \mid n$，则存在整数k使得$n = 2k+1$，从而$n^2 = (2k+1)^3 = 8k^3 + 6k^2 + 12k + 1 = 2t + 1$，这里$t = 4k^3 + 3k^2 + 6k$，从而$n^3$也是奇数，与$2 \mid n^3$矛盾！因此当$2 \mid n^3$时必有$2 \mid n$。这里用的是间接证明法。 □

练习* 4.6 设n是整数，证明如果$3 \mid n^2$，则$3 \mid n$。你用的证明方法是直接证明还是间接证明？

证明 若没有$3 \mid n$，也即存在k使得$n = 3k+1$或$n = 3k+2$。若$n = 3k+1$，则$n^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$，从而不可能有$3 \mid n^2$，矛盾！类似地，若$n = 3k+2$，则$n^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$，也不可能有$3 \mid n^2$，矛盾！总之，当$3 \nmid n$时必有$3 \nmid n^2$，因此若$3 \mid n^2$，则必有$3 \mid n$。这里用的是间接证明法。 □

练习* 4.7 证明$\sqrt{3}$是无理数。

证明 使用反证法。若$\sqrt{3}$不是无理数，即它是有理数，即存在正整数p, q使得$\sqrt{3} = p/q$，且$\gcd(p,q) = 1$。从而$p^2 = 3q^2$，因此$3 \mid p^2$，从而$3 \mid p$，即存在k使得$p = 3k$，从而$9k^2 = 3q^2$，从而$q^2 = 3k^2$，从而$3 \mid q^2$，从而$3 \mid q$，这与$\gcd(p,q) = 1$矛盾！因此$\sqrt{3}$是无理数。 □

练习 4.8 考虑下面的错误"定理"：

错误"定理" *设x和y都是实数且$x + y = 10$，则$x \neq 3$且$y \neq 8$*

(1) 对于该错误"定理"的下面证明有什么错误？

证明 *假设该"定理"的结论不成立，则$x = 3$且$y = 8$，则$x + y = 11$与假设中给出的$x + y = 10$矛盾，因此该定理的结论必然成立。*

(2) 给出一个反例说明上面定理的错误。

解答: (1) 因为假设"定理"的结论不成立是意味着"$x = 3$或$y = 8$"，而非"$x = 3$且$y = 8$"。

(2) 显然当$x + y = 10$时，可取$x = 2$和$y = 8$，则并非"$x \neq 3$且$y \neg 8$"。

练习 4.9 对任意实数x, y，证明$|xy| = |x||y|$。

解答: 我们根据x和y是否大于等于0分情况证明：

(1) 若$x = 0$或$y = 0$，则显然$|xy| = |x||y| = 0$；

(2) 若$x > 0$且$y > 0$，则$|xy| = xy$，而$|x| = x, |y| = y$，因此也有$|x||y| = xy$；

(3) 若$x > 0$且$y < 0$，则$|xy| = -xy$，而$|x| = x, |y| = -y$，因此也有$|x||y| = -xy$；

(4) 若$x < 0$且$y > 0$，则$|xy| = -xy$，而$|x| = -x, |y| = y$，因此也有$|x||y| = -xy$；

(5) 若$x < 0$且$y < 0$，则$|xy| = xy$，而$|x| = -x, |y| = -y$，因此也有$|x||y| = xy$；

综上，总有$|xy| = |x||y|$。

练习 4.10 使用分情况证明法证明：对任意实数x, y，$\min(x,y) + \max(x,y) = x + y$。

证明 对于任意实数x, y，可不失一般性设$x \geq y$，这是$\min(x,y) = y$，而$\max(x,y) = x$，从而$\min(x,y) + \max(x,y) = x + y$。 □

练习 4.11 使用术语"不失一般性"证明对任意实数x, y有：$\min(x,y) = (x+y-|x-y|)/2$且$\max(x,y) = (x+y+|x-y|)/2$。

证明 对于任意实数x, y，可不失一般性设$x \geq y$，这是$\min(x,y) = y$，$\max(x,y) = x$，而$(x+y-|x-y|)/2 = (x+y-(x-y))/2 = y$，且$(x+y+|x-y|)/2 = (x+y+x-y)/2 = x$，因此$\min(x,y) = (x+y-|x-y|)/2$且$\max(x,y) = (x+y+|x-y|)/2$。 □

练习* 4.12 证明不存在有理数r使得$r^3+r+1=0$。

证明 设有有理数r使得$r^3+r+1=0$，则存在互质的两个非零整数a,b使得$r=a/b$，从而有$(a/b)^3+(a/b)+1=0$，从而$a^3+ab^2+b^3=0$。根据a,b的奇偶性分情况讨论：

(1) 如果a是奇数而b是偶数，则a^3是奇数，ab^2是偶数，b^3是偶数，从而必有$a^3+ab^2+b^3$是奇数，与$a^3+ab^2+b^3=0$矛盾！

(2) 如果a是偶数而b是奇数，则a^3是偶数，ab^2是偶数，b^3是奇数，从而也有$a^3+ab^2+b^3$是奇数，与$a^3+ab^2+b^3=0$矛盾！

(3) 如果a是奇数b也是奇数，则a^3,ab^2,b^3都是奇数，从而也有$a^3+ab^2+b^3$是奇数，与$a^3+ab^2+b^3=0$矛盾！

(4) 如果a是偶数，b也是偶数，则与a和b互质矛盾！

综上，无论a,b的奇偶性如何都导出矛盾，因此不存在互质的非零整数a,b使得$r=a/b$且$r^3+r+1=0$，也即使得$r^3+r+1=0$的实数r不是有理数！ □

练习 4.13 设n,m是任意整数，证明$3\mid mn$，则$3\mid m$或$3\mid n$。

使用反证法，假设命题的结论不成立，即设$3\nmid m$且$3\nmid n$，则可能有下面四种情况：

(1) 存在k_1使得$m=3k_1+1$，且存在k_2使得$n=3k_2+1$，这是$mn=3(3k_1k_2+k_1+k_2)+1$，从而有$3\nmid mn$，与$3\mid mn$矛盾！

(2) 存在k_1使得$m=3k_1+1$，且存在k_2使得$n=3k_2+2$，这是$mn=3(3k_1k_2+2k_1+k_2)+2$，从而有$3\nmid mn$，与$3\mid mn$矛盾！

(3) 存在k_1使得$m=3k_1+2$，且存在k_2使得$n=3k_2+1$，这是$mn=3(3k_1k_2+k_1+2k_2)+2$，从而有$3\nmid mn$，与$3\mid mn$矛盾！

(4) 存在k_1使得$m=3k_1+2$，且存在k_2使得$n=3k_2+2$，这是$mn=3(3k_1k_2+k_1+2k_2+1)+1$，从而有$3\nmid mn$，与$3\mid mn$矛盾！

练习 4.14 设m,n是整数，证明若$9\mid(m^2+mn+n^2)$，则$3\mid m$且$3\mid n$（提示：$m^2+mn+n^2=(m-n)^2+3mn$）。

证明 由$9\mid(m^2+mn+n^2)$，从而有$3\mid(m^2+mn+n^2)$，注意到$m^2+mn+n^2=(m-n)^2+3mn$，从而$3\mid((m-n)^2+3mn)$，从而$3\mid(m-n)^2$，从而$3\mid(m-n)$，也即$m\equiv n(\mathrm{mod}\ 3)$。

另一方面由$3\mid(m-n)$有$9\mid(m-n)^2$，从而再由$9\mid((m-n)^2+3mn)$得$9\mid 3mn$，从而$3\mid mn$，由上一题这意味着有$3\mid m$或$3\mid n$，而前面已经证明$m\equiv n(\mathrm{mod}\ 3)$，因此就有$3\mid m$且$3\mid n$。 □

练习* 4.15 对于命题：对任意实数x，如果$|x-3|<3$则$0<x<6$。下面证明是否正确？如果正确，它使用了什么证明策略？如果不正确，能否更正？这个命题是否成立？

证明 设x是任意实数，且$|x-3|<3$。考虑两种情况：

情况一：$x-3\geq 0$，则$|x-3|=x-3$，根据假定有$x-3<3$，因此明显有$x<6$；

情况二：$x-3<0$，则$|x-3|=3-x$，根据假定有$3-x<3$，即$3<3+x$，即$0<x$。

综上证明了$0<x$以及$x<6$，因此我们可得到$0<x<6$。

解答：这个证明是不正确的，因为分两种情况，这两种情况得到的结论并不相同，最后的结论不能将这两个不同的结论进行合取，实际上只能析取，也即按照上面的证明只能得到$x<6$或$0<x$。

符号化来说，就是对于前提$p \vee q$，如果从p可得到r，从q可得到s，则我们实际上只能得到$r \vee s$，也即有$(p \vee q) \wedge (p \to r) \wedge (q \to s) \implies r \vee s$是有效的推理，但从前提$p \vee q, p \to s, q \to r$得到结论$r \wedge s$不是有效的推理。

但这个命题是成立的，只要做一点修改，按照下面的方式证明。

证明 设x是任意实数，且$|x-3|<3$。考虑两种情况：

情况一：$x-3 \geq 0$，则$|x-3| = x-3$，根据假定有$x-3<3$，因此有$x<6$。另一方面由$x-3 \geq 0$有$x \geq 3$，从而$x \geq 0$，从而有$0<x<6$；

情况二：$x-3<0$，则$|x-3| = 3-x$，根据假定有$3-x<3$，即$3<3+x$，即$0<x$。另一方由$x-3<0$有$x<3$，从而$x<6$，从而也有$0<x<6$。

综上就有当$|x-3|<3$时有$0<x<6$。 □

练习 4.16 设a, b是整数，证明存在整数c使得$a \mid c$且$b \mid c$。你的证明是构造性存在证明还是非构造性存在证明？

证明 我们令$c = ab$，则有$a \mid c$且$b \mid c$。这个证明是构造性存在证明。 □

练习* 4.17 证明任意两个有理数之间存在一个无理数。你的证明是构造性存在证明还是非构造性存在证明？

【分析】这个题目我们可以这样思考，首先对于两个整数a, b，如果$a<b$，怎样构造a和b之间的一个无理数呢？显然利用$\sqrt{2}$是无理数，$a<b$意味着$a+1 \leq b$，从而$a+\sqrt{2}/2<b$，显然$a+\sqrt{2}/2$是无理数，因为如果$a+\sqrt{2}/2$是有理数，则由于两个有理数之差仍然是有理数，就会得到$\sqrt{2}/2 = (a+\sqrt{2}/2)-a$也是有理数，这与$\sqrt{2}$是无理数矛盾！

对于整数的情况可推广到对任意的有理数x, y，因为对于x, y，设$x<y$，总可找到整数a, b, c使得$x = a/c$和$y = b/c$，这里$c>0$，且$a<b$，从而$a+1 \leq b$，从而$a/c+1/c \leq b/c$，从而$a/c+\sqrt{2}/(2c) < b/c$，即$a/c+\sqrt{2}/(2c)$是x和y之间的数，而且是无理数，因为若它是有理数，则$(a/c+\sqrt{2}/(2c))-a/c = \sqrt{2}/(2c)$是有理数，这与$\sqrt{2}$是无理数矛盾。由此，我们可得到本题的证明。

证明 设x, y是任意的两个有理数，不失一般性可假定$x<y$。由于x, y是有理数，因此可找到整数a, b, c使得$x = a/c$且$y = b/c$，这里$a<b$且$c>0$。由于$a<b$，因此$a+1 \leq b$，从而$a/c < a/c+\sqrt{2}/(2c) < b/c$，即$x < a/c+\sqrt{2}/(2c) < y$，而且$a/c+\sqrt{2}/(2c)$是无理数，因为若它是有理数，则$(a/c+\sqrt{2}/(2c))-a/c = \sqrt{2}/(2c)$也是有理数，这与$\sqrt{2}$是无理数矛盾。 □

【讨论】这是一个构造性存在证明。

练习 4.18 证明存在有理数a和无理数b使得a^b是无理数。你的证明是构造性存在证明还是非构造性存在证明？

证明 首先我们令$a = 2, b = \sqrt{2}$，如果$a^b = 2^{\sqrt{2}}$是无理数，则已经证明命题。否则，若$2^{\sqrt{2}}$是有理数，则令$a = 2^{\sqrt{2}}$，$b = \sqrt{2}/4$，则$a^b = (2^{\sqrt{2}})^{\sqrt{2}/4} = 2^{\sqrt{2}\cdot\sqrt{2}/4} = 2^{1/2} = \sqrt{2}$是无理数，也即我们得到要么有$a = 2, b = \sqrt{2}$使得$a^b$是无理数，要么有$a = 2^{\sqrt{2}}$，$b = \sqrt{2}/4$使得$a^b$是无理数，因此命题成立。 □

练习* 4.19 试证明形如$4n-1$的质数有无穷多个。

证明 假设形如$4n-1$的质数只有$q_1,q_2,\cdots,q_k$这些，考虑整数$x=4q_1q_2\cdots q_k-1$，这个整数也是$4n-1$形式的整数，如果它是质数，则它就是与$q_1,q_2,\cdots,q_k$都不同的质数。假定它是合数，则根据算术基本定理，它可分解为$x=p_1p_2\cdots p_m$，其中$p_1,p_2,\cdots,p_m$都是质数。而对任意的$1\le i\le m$都有：

$$x\equiv(4q_1q_2\cdots q_k-1)\equiv(-1)\equiv(q_i-1)(\mod q_i)$$

因此对任意的$1\le i\le k$以及任意的$1\le j\le m$都有$q_i\ne p_j$，也即$p_1,p_2,\cdots,p_m$都不在$q_1,q_2,\cdots,q_k$中。注意到所有质数要么是$4n+1$要么是$4n-1$形式，且两个$4n+1$形式的整数的乘积也只能是$4n+1$形式的整数（因为$(4n_1+1)(4n_2+1)=4(4n_1n_2+n_1+n_2)+1$），但$x=p_1p_2\cdots p_m$是$4n-1$形式的整数，所以$p_1,p_2,\cdots,p_m$中至少有一个是$4n-1$形式的质数，且不在$q_1,q_2,\cdots,q_k$这些质数中，因此所有形如$4n-1$的质数就不只是$q_1,q_2,\cdots,q_k$这些，也即形如$4n-1$的质数有无穷多个。 □

练习 4.20 试证明形如$3n-1$的质数有无穷多个。

证明 假设形如$3n-1$的质数只有$q_1,q_2,\cdots,q_k$这些，考虑整数$x=3q_1q_2\cdots q_k-1$，这个整数当然也是$3n-1$ 形式的整数，如果它是质数，则它就是与$q_1,q_2,\cdots,q_k$都不同的质数。假定它是合数，则根据算术基本定理，它可分解为$x=p_1p_2\cdots p_m$，其中$p_1,p_2,\cdots,p_m$都是质数。而对任意的$1\le i\le n$都有：

$$n\equiv(3q_1q_2\cdots q_k-1)\equiv(-1)\equiv(q_i-1)(\mod q_i)$$

因此对任意的$1\le i\le k$以及任意的$1\le j\le m$，都有$q_i\ne p_j$，也即$p_1,p_2,\cdots,p_m$都不在$q_1,q_2,\cdots,q_k$中。注意到所有质数要么是$3n+1$要么是$3n-1$形式，且两个$3n+1$形式的整数的乘积也只能是$3n+1$形式的整数（因为$(3n_1+1)(3n_2+1)=3(3n_1n_2+n_1+n_2)+1$），但$x=p_1p_2\cdots,p_m$是$3n-1$形式的整数，所以$p_1,p_2,\cdots,p_m$中至少有一个是$3n-1$形式的质数，而且不在$q_1,q_2,\cdots,q_k$这些质数中，因此所有形如$3n-1$的质数就不只是$q_1,q_2,\cdots,q_k$这些，也即形如$3n-1$的质数有无穷多个。 □

练习 4.21 设n是整数，证明$15\mid n$当且仅当$3\mid n$且$5\mid n$。

证明 首先，若$15\mid n$时，由于$3\mid 15$且$5\mid 15$，因此显然有$3\mid n$且$5\mid n$。反之，若$3\mid n$且$5\mid n$，则n是3和5的公倍数，因此n是3和5的最小公倍数，即15的倍数，即$15\mid n$。 □

练习 4.22 设有n个整数，它们的积等于n，而它们的和等于0，证明n是4的倍数。

证明 设这n个整数是$a_1,a_2,\cdots,a_n$，则根据题意有$a_1+a_2+\cdots+a_n=0$而$a_1a_2\cdots a_n=n$。我们使用反证法证明这n个整数中至少存在两个偶数。如若不然，即它们之中只有0个或1个偶数：

(1) 若$a_1,a_2,\cdots,a_n$全是奇数，则由于它们的和等于0是偶数，所以必然是偶数个奇数，也即n是偶数，但若$a_1,\cdots,a_n$全是奇数的话，它们的乘积$a_1a_2\cdots a_n$也必是奇数，这与$a_1a_2\cdots a_n=n$是偶数矛盾！

(2) 若$a_1,a_2,\cdots,a_n$中只有一个是偶数，不妨设a_1是偶数，从而$a_2+\cdots+a_n=-a_1$也是偶数，而$a_2,\cdots,a_n$这$n-1$个数都是奇数，因此必有$n-1$是偶数，也即n是奇数，但另一方面，$a_1a_2\cdots a_n=n$，由a_1是偶数，又得到n是偶数，矛盾！

综上，$a_1,a_2,\cdots,a_n$至少有两个偶数，从而由$a_1a_2\cdots a_n=n$可得n是4的倍数。 □

练习 4.23 设$a_1, a_2, \cdots, a_n$是$1, 2, \cdots, n$的某种排列，证明：如果n是奇数，则乘积$(a_1-1)(a_2-2)\cdots(a_n-n)$ 是偶数。

证明 由于n是奇数，考虑$a_1-1, a_2-2, \cdots, a_n-n$这$n$个数的和：

$$(a_1-1)+(a_2-2)+\cdots+(a_n-n)=(a_1+\cdots+a_n)-(1+2+\cdots+n)$$

由于$a_1, \cdots, a_n$是$1, 2\cdots, n$的某种排列，因此这n个数的和等于0，而n是奇数，所以$a_1-1, a_2-2, \cdots, a_n-n$这$n$个数不可能全是奇数（否则奇数个奇数的和仍是奇数），也即这n个数存在偶数，从而它们的乘积$(a_1-1)(a_2-2)\cdots(a_n-n)$是偶数。 □

练习 4.24 证明对任意$n\in\mathbb{N}$，$0^3+1^3+2^3+\cdots+n^3=[n(n+1)/2]^2$。

证明 我们对自然数n实施数学归纳法：

(1) **归纳基**：当$n=0$时待证等式两边都是0，等式成立；

(2) **归纳步**：假设$n=k$时待证等式成立，即有：

$$0^3+1^3+2^3+\cdots+k^3=[k(k+1)/2]^2$$

考虑$n=k+1$：

$$\begin{aligned}0^3+1^3+2^3+\cdots+k^3+(k+1)^3 &= [k(k+1)/2]^2+(k+1)^3\\ &= [(k+1)/2]^2(k^2+4(k+1))\\ &= [(k+1)/2]^2(k+2)^2=[(k+1)(k+2)/2]^2\end{aligned}$$

即对$n=k+1$，待证等式也成立。 □

练习* 4.25 证明对任意的正整数n，$1\cdot 1!+2\cdot 2!+\cdots+n\cdot n!=(n+1)!-1$。

证明 对正整数n做数学归纳法：

归纳基：当$n=1$，显然有$1\cdot 1!=1=2!-1$，因此等式成立。

归纳步：设当$n=k$时等式成立，即有$1\cdot 1!+2\cdot 2!+\cdots+k\cdot k!=(k+1)!-1$。考虑$n=k+1$，我们有：

$$\begin{aligned}& 1\cdots 1!+2\cdot 2!+\cdots+k\cdot k!+(k+1)\cdot(k+1)!\\ =\ & (k+1)!-1+(k+1)\cdot(k+1)!\\ =\ & (k+1)!(k+1+1)-1=(k+2)!-1\end{aligned}$$

因此对$n=k+1$时等式也成立，从而根据数学归纳法有待证等式成立。 □

练习 4.26 证明对任意的正整数n，$\sum_{k=1}^{n} k2^k=(n-1)2^{n+1}+2$。

证明 对正整数n实施数学归纳法：

归纳基：当$n=1$时，待证等式两边都是1，所以等式成立。

归纳步：设当$n=p$时等式成立，即有：$\sum_{k=1}^{p} k2^k = (p-1)2^{p+1}+2$。考虑$n=p+1$，

$$\begin{aligned}\sum_{k=1}^{p+1} k2^k &= \sum_{k=1}^{p} k2^k + (p+1)2^{p+1} = (p-1)2^{p+1}+2+(p+1)2^{p+1} \\ &= 2^{p+1}(p-1+p+1)+2 = p2^{p+2}+2\end{aligned}$$

因此对$n=p+1$时等式也成立。 □

练习* 4.27 证明对任意的正整数n，

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}} > 2(\sqrt{n+1}-1)$$

证明 我们对正整数n进行数学归纳法证明该不等式：

归纳基：若$n=1$，我们有：

$$9>8 \implies 9>4\cdot(1+1) \implies 3>2(\sqrt{1+1}) \implies 1>2(\sqrt{1+1}-1)$$

因此该不等式对于$n=1$成立。

归纳步：假定不等式对于$n=k$时成立（归纳假设），也即对于$k\geq 1$有：

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}} > 2(\sqrt{k+1}-1)$$

我们需要证明有不等式对于$n=k+1$也成立，即要证明有：

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}} > 2(\sqrt{k+2}-1)$$

根据归纳假设我们有：

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}} > 2(\sqrt{k+1}-1)+\frac{1}{\sqrt{k+1}}$$

注意到$k\geq 1$，我们有：

$$\begin{aligned}& 4k^2+12k+9 > 4k^2+12k+8 \\ \implies & 4k^2+12k+9 > 4(k+2)(k+1) \\ \implies & (2k+3)^2 > (2\sqrt{k+2}\sqrt{k+1})^2 \\ \implies & 2k+3 > 2\sqrt{k+2}\sqrt{k+1} \\ \implies & 2(k+1)+1 > 2\sqrt{k+2}\sqrt{k+1} \\ \implies & 2\sqrt{k+1}\sqrt{k+1}+1 > 2\sqrt{k+2}\sqrt{k+1} \\ \implies & 2\sqrt{k+1}+\frac{1}{\sqrt{k+1}} > 2\sqrt{k+2} \\ \implies & 2(\sqrt{k+1}-1)+\frac{1}{\sqrt{k+1}} > 2(\sqrt{k+2}-1)\end{aligned}$$

也即我们有：

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}>2(\sqrt{k+1}-1)+\frac{1}{\sqrt{k+1}}>2(\sqrt{k+2}-1)$$

这就完成了归纳步的证明，因此由数学归纳原理，所要证的不等式成立。 □

练习 4.28 证明对任意的$n>6$，$3^n<n!$。

证明 对自然数n实施数学归纳法：

(1) **归纳基**：当$n=7$，$3^7=2187$，$7!=5040$，因此有$3^7<7!$；

(2) **归纳步**：设当$n=k$时成立，即有$3^k<k!$，这里$k\geq 7$，考虑$n=k+1$，显然有：

$$3^{k+1}=3\cdot 3^{k+1}<3\cdot k!<(k+1)!$$

因此当$n=k+1$时也有$3^n<n!$。 □

练习 4.29 证明对任意的$n\geq 10$，$2^n>n^3$。

证明 对自然数n实施数学归纳法：

(1) **归纳基**：当$n=10$，$2^{10}=1024$，$10^3=100$，因此有$2^{10}>n^3$；

(2) **归纳步**：设当$n=k$时成立，即有$2^k>k^3$，这里$k\geq 10$，考虑$n=k+1$，由于$k>10$，因此$k^3>10k^2$，从而$k^3>3k^2+3k+1$，从而$2\cdot k^3>k^3+3k^2+3k+1=(k+1)^3$，从而

$$2^{k+1}=2\cdot 2^k>2\cdot k^3>(k+1)^3$$

因此当$n=k+1$时也有$2^n>n^3$。 □

练习 4.30 证明对任意自然数n，$6\mid(n^3-n)$。

证明 对自然数n实施数学归纳法：

(1) **归纳基**：当$n=0,1,2$时，(n^3-n)分别等于$0,0,6$，因此都有$6\mid(n^3-n)$；

(2) **归纳步**：设当$n=k$时成立，即有$6\mid(k^3-k)$，这里$k\geq 2$，考虑$n=k+1$，由$(k+1)^3=k^3+3k^2+3k+1$，从而

$$(k+1)^3-(k+1)=k^3+3k^2+3k+1-k-1=(k^3-k)+3k^2+3k=(k^3-k)+3k(k+1)$$

根据归纳假设$6\mid(k^3-k)$，而k和$k+1$总有一个数是偶数，因此$6\mid 3k(k+1)$，因此当$n=k+1$时也有$6\mid((k+1)^3-(k+1))$。 □

练习 4.31 证明对任意自然数n，$9\mid(4^n+6n-1)$。

证明 对自然数n实施数学归纳法：

(1) **归纳基**：当$n=0,1$时，(4^n+6n-1)分别等于$0,9$，因此都有$9\mid(4^n+6n-1)$；

(2) **归纳步**：设当$n=k$时成立，即有$9\mid(4^k+6k-1)$，这里$k\geq 1$，考虑$n=k+1$，我们有：

$$4^{k+1}+6(k+1)-1=4\cdot 4^k+6k+6-1=4^k+6k-1+3\cdot 4^k+6=4^k+6k-1+3(4^k+2)$$

根据归纳假设$9 \mid 9 \mid (4^k+6k-1)$，不难使用数学归纳法证明对任意自然数k都有$3 \mid (4^k+2)$，因此$9 \mid (4^{k+1}+6(k+1)-1)$。

我们可补充证明，对任意自然数n有$3 \mid (4^n+2)$，显然当$n=0$时成立，假设$n=k$时成立，即$3 \mid (4^k+2)$，则对于$n=k+1$，我们有$4^{k+1}+2=4^k+2+3\cdot 4^k$，因此显然有$3 \mid (4^{k+1}+2)$。 □

练习 4.32 证明对任意的正整数n，$21 \mid 4^{n+1}+5^{2n-1}$。

证明 对自然数n实施数学归纳法：

(1) 归纳基：当$n=1$时，$4^{n+1}+5^{2n-1}=21$，因此有$21 \mid (4^{n+1}+5^{2n-1})$；

(2) 归纳步：设当$n=k$时成立，即有$21 \mid (4^{k+1}+5^{2k-1})$，这里$k \geq 1$，考虑$n=k+1$，我们有：

$$4^{k+1+1}+5^{2(k+1)-1}=4\cdot 4^{k+1}+25\cdot 5^{2k-1}=4\cdot(4^{k+1}+5^{2k-1})+21\cdot 5^{2k-1}$$

根据归纳假设$21 \mid (4^{k+1}+5^{2k-1})$，而显然$21 \mid 21\cdot 5^{2k-1}$，因此$21 \mid (4^{k+1+1}+5^{2(k+1)-1})$。 □

练习 4.33 下面的“证明”哪里有错？

“定理”：对任意正整数n，如果x和y是正整数且$\max(x,y)=n$，则$x=y$。

归纳基：设$n=1$，如果$\max(x,y)=1$且x和y都是正整数，我们有$x=1$且$y=1$。

归纳步：设k是正整数，假设当$\max(x,y)=k$且x和y是正整数时$x=y$。令$\max(x,y)=k+1$，这里x和y是正整数，则$\max(x-1,y-1)=k$，根据归纳假设$x-1=y-1$，即$x=y$。归纳步证明完毕。

解答：上述“证明”的错误在于归纳步的证明：当x和y是正整数时，$x-1$和$y-1$不一定是正整数，而要证明的命题是$P(n)$：若x和y是正整数且$\max(x,y)=n$，则$x=y$。当$x-1$和$y-1$不是正整数时，就不能由归纳假设$P(k)$成立得到$x-1=y-1$，这时的$P(k)$成立是说，若x和y是正整数且$\max(x,y)=k-1$时，$x=y$，从而当$x-1$和$y-1$不是正整数时，不能由$\max(x-1,y-1)=k-1$得到$x-1=y-1$。

练习* 4.34 证明对任意的正奇数n，$8 \mid n^2-1$。

证明 我们使用强归纳法证明，令$P(n)$是：如果n是正奇数，则$8 \mid n^2-1$。我们证明$P(n)$对任意自然数成立：

(1) 归纳基：显然$P(0),P(1),P(2),P(3)$都成立；

(2) 归纳步：对任意$k \geq 3$，归纳假设是$P(0),P(1),\cdots,P(k)$成立，我们要证明$P(k+1)$成立。如果$k+1$不是正奇数，则命题$P(k+1)$平凡成立。若$k+1$是正奇数时，则$k-1$也是正奇数，而且由于$k \geq 3$，所以$k-1 \geq 1$，所以按照归纳假设有$P(k-1)$成立，也即若$k-1$是正奇数，则$8 \mid (k-1)^2-1$，而

$$(k+1)^2-1=k^2+2k+1-1=(k-1)^2-1+4k$$

由于$k+1$是正奇数，从而k是偶数，从而有$8 \mid 4k$，而由归纳假设$8 \mid (k-1)^2-1$，因此也有$8 \mid (k+1)^2-1$。

综上，根据强归纳法这就证明了，对任意正奇数n，$8 \mid n^2-1$。 □

练习* 4.35 分别使用第一数学归纳法和第二数学归纳法证明：任意大于12分的邮资可由若干4分和5分的邮票支付。

证明 令命题$P(n)$是“n分邮资可由若干4分和5分的邮票支付”。要证明$\forall(n \geq 12)P(n)$为真。

(1) 首先使用第一数学归纳法证明：

(i) 归纳基：$P(12)$显然成立，因为$12 = 3 \cdot 4$；

(ii) 归纳步：设$k \geq 12$，归纳假设是$P(k)$成立，要证明$P(k+1)$成立。由于$P(k)$成立，也即k分邮资可由若干4分和5 分的邮票支付，分两种情况：(a) 若支付k分邮资的邮票中至少包含一张4分邮票，这将这张4分邮票替换为5分邮票就可以支付$k+1$分邮资，即这时由$P(k)$成立可得到$P(k+1)$成立；(b) 若支付k分邮资的邮票中没有任何4分邮票，那么由于$k \geq 12$，因此其中至少有3张5分邮票，从而将这3张5分邮票替换为4张4分邮票，则可支付$k+1$分邮资，因此这时由$P(k)$成立也可得到$P(k+1)$成立。

综上，根据第一数学归纳法有$\forall(n \geq 12)P(n)$为真。

(2) 然后使用第二数学归纳法证明：

(i) 归纳基：$P(12), P(13), P(14), P(15)$都成立，因为$12 = 3 \cdot 4, 13 = 2 \cdot 4 + 5, 14 = 4 + 2 \cdot 5, 15 = 3 \cdot 5$。

(ii) 归纳步：设$k \geq 15$，归纳假设是$P(12), \cdots, P(k)$成立，要证明$P(k+1)$成立。由于$k \geq 15$，因此$k-3 \geq 12$，因此根据归纳假设有$P(k-3)$成立，即$k-3$分邮资可由若干4分和5分邮票支付，从而对于$k+1$分邮资，只要在支付$k-3$分邮资的基础上增加一张4分邮资就可支付，因此$P(k+1)$成立。

综上，根据第二数学归纳法有$\forall(n \geq 12)P(n)$为真。 □

练习 4.36 证明任意大于12分的邮资可由3分和7分的邮票支付。

证明 令命题$P(n)$是“n分邮资可由若干3分和7分的邮票支付”。要证明$\forall(n \geq 12)P(n)$为真。我们使用第二数学归纳法证明：

(i) 归纳基：$P(12), P(13), P(14)$都成立，因为$12 = 4 \cdot 3, 13 = 2 \cdot 3 + 7, 14 = 2 \cdot 7$。

(ii) 归纳步：设$k \geq 15$，归纳假设是$P(12), \cdots, P(k)$成立，要证明$P(k+1)$成立。由于$k \geq 14$，因此$k-2 \geq 12$，因此根据归纳假设有$P(k-2)$成立，即$k-2$分邮资可由若干3分和7分邮票支付，从而对于$k+1$分邮资，只要在支付$k-2$分邮资的基础上增加一张3分邮资就可支付，因此$P(k+1)$成立。

综上，根据第二数学归纳法有$\forall(n \geq 12)P(n)$为真。 □

【**讨论**】我们也可使用第一数学归纳法证明$\forall(n \geq 12)P(n)$：

(i) 归纳基：$P(12)$显然成立，因为$12 = 4 \cdot 3$；

(ii) 归纳步：设$k \geq 12$，归纳假设是$P(k)$成立，要证明$P(k+1)$成立。由于$P(k)$成立，也即k分邮资可由若干3分和7 分的邮票支付，分两种情况：(a) 若支付k分邮资的邮票中至少包含2张3分邮票，这将这2张3分邮票替换为7分邮票就可以支付$k+1$分邮资，即这时由$P(k)$成立可得到$P(k+1)$成立；(b) 若支付k分邮资的邮票至多只有1张3分邮票，那么由于$k \geq 12$，因此其中至少有2张7分邮票，从而将这2张7分邮票替换为5张3分邮票，则可支付$k+1$分邮资，因此这时由$P(k)$成立也可得到$P(k+1)$成立。

综上，根据第一数学归纳法有$\forall(n \geq 12)P(n)$为真。

练习* 4.37 对于任意的自然数a和正整数b：(1) 使用强归纳法证明存在唯一的自然数q和r使得$a = bq + r$且$0 \leq r < b$。(2) 使用自然数的良序性质证明存在唯一的自然数q和r使得$a = bq + r$且$0 \leq r < b$。

解答：(1) 首先我们使用强归纳法进行证明。

证明 我们针对自然数a使用强归纳法证明。令$P(a)$是：对任意正整数b，存在唯一的整数q和r使得$a = bq + r$且$0 \leq r < b$，即$P(a)$是 $\forall b \exists q \exists r (a = bq + r \wedge 0 \leq r < b)$。

(i) 归纳基：显然$P(0)$成立，因为对任意正整数b，$0 = b \cdot 0 + 0$；

(ii) 归纳步：对任意自然数$k \geq 1$，归纳假设是$P(0), \cdots, P(k)$成立，我们要证明$P(k+1)$也成立。对任意正整数b，若$k+1 < b$，则有$k+1 = b \cdot 0 + k + 1$，也即$k+1 = bq + r$，这里$q = 0, r = k+1$，这时$0 \leq r < b$。显然这时q和r是唯一的（因为若$q > 0$，这时不可能存在小于$k+1$的r使得$k+1 = bq + r$）。因此当$k+1 < b$时总有$P(k+1)$成立（这种情况没有用到归纳假设）。

下面考虑$k+1 \geq b$的情况，这时$k+1-b \geq 0$，根据归纳假设有$P(k+1-b)$成立，从而对整数b，存在唯一的自然数q'和r'使得$k+1-b = bq' + r'$且$0 \leq r' < b$，这样我们就得到$k+1 = b(q'+1) + r$且$0 \leq r' < b$，也即存在$q' = q+1$，$r = r'$使得$k+1 = bq + r$且$0 \leq r < b$。容易看到使得$k+1 = bq + r$的q和r是唯一的，因此$P(k+1)$成立。

综上总有$P(k+1)$成立，根据强归纳法，对任意自然数$P(a)$成立。 □

(2) 其次我们使用自然数集的良序性质证明。

证明 对任意自然数a和正整数b，令集合$S = \{a - bq \in \mathbb{N} \mid q \in \mathbb{N}\}$，显然$S$非空，因为至少有$a \in S$（这时对应$q = 0$），即$S$是自然数集的非空子集，根据良序原理，它存在最小的自然数，设为r，也即$r = a - bq$，且是S中最小的自然数。由于$r = a - bq$且属于S，是自然数，即$r \geq 0$，因此我们只需证明$r < b$。

我们使用反证法，若$r \geq b$，在令$r' = r - b$，从而$r' \geq 0$，即$r' = a - bq - b = a - b(q-1) \geq 0$，从而$r' \in S$，且由于$b$是正整数，所以$r' < r$，这与$r$是$S$的最小自然数，矛盾！所以必有$r < b$。

显然对任意自然数a和正整数b，使得$a = bq + r$且$0 \leq r < b$的自然数q和r是唯一的。因为若还存在自然数q', r'使得$a = bq' + r'$且$0 \leq r' < b$，则$bq + r = bq' + r'$，若$r \neq r'$，不妨设$r > r'$，从而$r - r' = b(q' - q) > 0$，从而$b \mid (r - r')$，但是因为$0 \leq r < b$且$0 \leq r' < b$，因此$r - r' < b$，比b小又是b的倍数的自然数只有0，因此$r - r' = 0$，也即这时必有$r' = r$，从而也必有$q' = q$。 □

【**讨论**】在证明了对任意自然数a和正整数b存在唯一的自然数q和r使得$a = bq + r$且$0 \leq r < b$之后，不难将结论推广为：对任意整数a和正整数b存在唯一的整数q和r使得$a = bq + r$且$0 \leq r < b$，因为当$a < 0$时，可先考虑$-a$。

练习 4.38 基于两个整数的最大公因子能表示成这两个整数的线性组合这个定理，证明对任意的正整数a, b，如果$\gcd(a, b) = 1$，则对任意大于等于$ab - a - b + 1$的整数n，都存在非负整数s, t使得$n = as + bt$。

证明 对任意正整数a, b，如果$a = 1$或$b = 1$，则命题显然成立，所以下面只考虑$a \geq 2$且$b \geq 2$的情况，而且我们不妨设$b > a$（注意，由于$\gcd(a, b) = 1$，因此这时不可能有$a = b$）。

我们首先证明：对正整数a, b，不失一般性设$b > a$，若$\gcd(a, b) = 1$，则对任意既不是a的倍数又不是b的倍数的正整数k，总存在满足$(a-1) \geq q \geq 1$且$p \geq 1 - b$的整数p, q使得$ap + bq = k$。

因为由$\gcd(a,b)=1$，则存在整数p',q'使得$ap'+bq'=1$，从而对任意正整数k，就有$akp'+bkq'=k$，即存在整数$p=kp',q=kq'$使得$ap+bq=k$。而当k不是a的倍数，也不是b的倍数时，则有$p\neq 0$且$q\neq 0$。

进一步，在所有使得$ap+bq=k$的整数对p,q中，我们总可使得$(a-1)\geq q\geq 1$，因为若$q<1$，则可令$q'=q+a$，$p'=p-b$仍有$ap'+bq'=k$，如果q'还小于1，则可继续这个过程，直到b的系数q大于等于1。而若$q>(a-1)$，即$q\geq a$，则可令$q'=q-a$，$p'=p+b$仍有$ap'+bq'=1$，如果q'还大于a，则可继续这个过程，直到b的系数q小于等于$a-1$。注意，在这个过程中，由于我们假定k不是a的倍数，因此总有$q\neq 0$。

因此在使得$ap+bq=k$的整数对p,q中，总存在满足$(a-1)\geq q\geq 1$的p,q。而当进一步假定$b>a$时，总有$p\geq 1-b$，因为若$p<1-b$，则有：

$$ap+bq<a(1-b)+bq\leq a(1-b)+b(a-1)=a-b<0$$

这与$ap+bq=k$是正整数矛盾，因此这时必有$p\geq 1-b$。

到此我们证明了，对任意正整数b,a，不妨设$b>a$，若$\gcd(a,b)=1$，则对任意不是a的倍数又不是b的倍数的正整数k，都存在满足$(a-1)\geq q\geq 1$且$p\geq 1-b$的整数p,q使得$ap+bq=k$。特别地，当$k=1$时，存在满足$(a-1)\geq 1\geq 1$且$p\geq 1-b$的整数p,q使得$ap+bq=1$。显然当k是a的倍数时，则存在$p\geq 1,q=0$使得$k=pa$，而当k是b的倍数时，则存在$q\geq 1,p=1$使得$k=qb$。

从而对大于等于$ab-a-b+1$的自然数$n=ab-a-b+k$，这里$k\geq 1$，要么$k=ap$，从而$n=b(a-1)+a(p-1)$，或$k=bq$，从而$n=a(b-1)+b(q-1)$，要么存在$p\geq 1-b$且$q\geq 1$使得$k=ap+bq$，从而：

$$n=ab-a-b+k=ab-a-b+ap+bq=a(b+p-1)+b(q-1)$$

而$b+p-1\geq 0$且$q-1\geq 0$，即也存在非负整数$s=b+p-1,t=q-1$使得$n=ab-a-b+k=as+bt$。这就证明了对任意大于等于$ab-a-b+1$的自然数n，都存在非负整数s,t使得$n=as+bt$。 □

【讨论】由于我们不知道a,b的具体值，因此这一题很难使用第一数学归纳法，或强归纳法进行证明，只能利用贝祖系数的性质直接构造使得$n=as+bt$的非负整数s和t。

练习 4.39 找出下面“证明”$a^n=1$的错误，这里n是任意非负整数，a是非零实数。

归纳基：根据定义$a^0=1$。

归纳步：假设对任意的非负整数$j\leq k$有$a^j=1$，注意到：

$$a^{k+1}=\frac{a^k\cdot a^k}{a^{k-1}}=\frac{1\cdot 1}{1}=1$$

即有$a^{k+1}=1$，这就完成了归纳步的证明。

解答：上述“证明”的错误之处在于归纳步的证明中，归纳假设是对任意的非负整数$j\leq k$有$a^j=1$，而这时$k\geq 0$，从而$k-1$不是非负整数，不能引用归纳假设得到$a^{k-1}=1$。

练习 4.40 基于自然数的良序性质说明下面的方式都可证明对任意正整数n,k有$P(n,k)$为真：

a) $P(1,1)$为真，而且对任意的正整数n,k有$P(n,k)\to[P(n+1,k)\wedge P(n,k+1)]$为真；

b) 对任意的正整数k有$P(1,k)$为真，而且对任意的正整数n,k有$P(n,k)\to P(n+1,k)$为真；

c) 对任意的正整数n有$P(n,1)$为真，而且对任意的正整数n,k有$P(n,k)\to P(n,k+1)$为真。

解答：a) 令$S=\{s\mid$ 存在正整数n,k使得$n+k=s$且$P(n,k)$不为真$\}$。若存在正整数n,k使得$P(n,k)$不为真，则S是非空集。从而根据良序原理，S存在最小的正整数s，使得存在n,k有$n+k=s$且$P(n,k)$不为真。但显然$s\neq 2$，因为$P(1,1)$为真，从而$s\geq 2$，从而使得$P(n,k)$不为真的n,k有$n>1$或$k>1$。若$n>1$，则由于$n-1+k=s-1\notin S$，从而$P(n-1,k)$为真，但a)的归纳步表明$P(n,k)$为真，矛盾！若$k>1$，则由于$n+k-1=s-1\notin S$，从而$P(n,k-1)$为真，但a)的归纳步同样表明$P(n,k)$为真，矛盾！因此S必为空集，即对任意正整数n,k都有$P(n,k)$为真。

b) 令$S=\{n\mid$存在正整数k使得$P(n,k)$不为真$\}$。若存在正整数n,k使得$P(n,k)$不为真，则S是非空集。从而根据良序原理，S存在最小的正整数n，使得存在k有$P(n,k)$不为真。但显然$n>1$，因为对任意正整数k有$P(1,k)$为真。从而$n-1$是正整数且不属于S，因此$P(n-1,k)$为真，但b)的归纳步表明$P(n,k)$为真，矛盾！因此S必为空集，即对任意正整数n,k都有$P(n,k)$为真。

c) 令$S=\{k\mid$存在正整数n使得$P(n,k)$不为真$\}$。若存在正整数n,k使得$P(n,k)$不为真，则S是非空集。从而根据良序原理，S存在最小的正整数k，使得存在n有$P(n,k)$不为真。但显然$k>1$，因为对任意正整数n有$P(n,1)$为真。从而$k-1$是正整数且不属于S，因此$P(n,k-1)$为真，但b)的归纳步表明$P(n,k)$为真，矛盾！因此S必为空集，即对任意正整数n,k都有$P(n,k)$为真。

练习 4.41 证明：对任意的正整数n,k有：

$$\sum_{j=1}^{n}[j(j+1)(j+2)\cdots(j+k-1)]=\frac{n(n+1)(n+2)\cdots(n+k)}{(k+1)}$$

【**分析**】这一题有两个正整数n,k，因此需要用到上一题给出的证明策略，但到底用哪个策略呢？我们来观察一下$P(1,1)$, $P(1,k)$和$P(n,1)$，这里$P(n,k)$代表上述等式：

$$\begin{aligned}
P(1,1) &: \sum_{j=1}^{1}1=\frac{1\cdot(1+1)}{(1+1)}\\
P(1,k) &: \sum_{j=1}^{1}[j(j+1)(j+2)\cdot(j+k-1)]=1\cdot 2\cdot k=\frac{1\cdot 2\cdots(k+1)}{(k+1)}\\
P(n,1) &: \sum_{j=1}^{n}j=\frac{n(n+1)}{2}
\end{aligned}$$

我们发现这几个等式的成立都很显然。我们再比较$P(n+1,k)$和$P(n,k+1)$这两个等式的左边：

$$\begin{aligned}
P(n+1,k) &: \sum_{j=1}^{n+1}[j(j+1)(j+2)\cdots(j+k-1)]\\
&= \sum_{j=1}^{n}[j(j+1)(j+2)\cdots(j+k-1)]+(n+1)(n+2)\cdots(n+k)
\end{aligned}$$

$$P(n,k+1) \quad : \quad \sum_{j=1}^{n}[j(j+1)(j+2)\cdots(j+k-1)(j+k)]$$

显然$P(n+1,k)$更容易使用$P(n,k)$表示，因此我们的策略应该是证明，对任意的正整数k有$P(1,k)$，以及对任意的正整数n,k有$P(n,k)\to P(n+1,k)$。

【证明】我们对正整数n进行数学归纳法证明上述等式。

归纳基：注意到，对任意的正整数k有：

$$\sum_{j=1}^{1}[j(j+1)(j+2)\cdot(j+k-1)] = 1\cdot 2\cdot k = \frac{1\cdot 2\cdots(k+1)}{(k+1)}$$

归纳步：假定对任意的正整数n,k有等式成立（归纳假设），也即对任意正整数n,k有：

$$\sum_{j=1}^{n}[j(j+1)(j+2)\cdots(j+k-1)] = \frac{n(n+1)(n+2)\cdots(n+k)}{(k+1)}$$

注意到：

$$\begin{aligned}
& \sum_{j=1}^{n+1}[j(j+1)(j+2)\cdots(j+k-1)] \\
= & \sum_{j=1}^{n}[j(j+1)(j+2)\cdots(j+k-1)] + (n+1)(n+2)\cdots(n+k) \qquad // \text{ 由归纳假设} \\
= & \frac{n(n+1)(n+2)\cdots(n+k)}{(k+1)} + (n+1)(n+2)\cdots(n+k) \\
= & (n+1)(n+2)\cdots(n+k)\left(\frac{n}{(k+1)}+1\right) \\
= & \frac{(n+1)((n+1)+1)\cdots((n+1)+(k-1))((n+1)+k)}{(k+1)}
\end{aligned}$$

这就完成了归纳步的证明。综上，由数学归纳法原理，上述等式对任意的正整数n,k都成立。

【讨论】如果知道组合数$C(n,k)$的计算公式：

$$C(n,k) = \frac{n!}{k!(n-k)!}$$

那么上述等式通过简单的变换后实际上是：

$$\sum_{j=1}^{n} C(k+j-1,j-1) = \sum_{i=0}^{n-1} C(k+i,i) = C(n+k,n-1)$$

实际上，在后面第八章我们可使用组合证明或数学归纳法证明下面的等式：

$$\sum_{i=0}^{r} C(m+i,i) = C(m+r+1,r)$$

取$m = k, r = n-1$则得到这一题要证明的等式。

练习* 4.42 归纳定义整数集的子集S：(1) 归纳基：$5 \in S$；(2) 归纳步：对任意整数x, y，如果$x \in S, y \in S$，则$x+y \in S$且$x-y \in S$。

(1) 证明对任意的整数$s \in S$都有$5 \mid s$。

(2) 设$A = \{5k \in \mathbb{Z} \mid k \in \mathbb{Z}\}$，证明$S = A$。（提示：在证明$A \subseteq S$时，因为对于整数$k < 0$，由$5|k| \in S$时也有$5k \in S$。因此只要对任意自然数$k$，有$5k \in S$即可）

解答：

(1) 由于S是归纳定义的，因此我们可针对S的元素s做结构归纳，证明$5 \mid s$。

证明　令$P(s)$是：$5 \mid s$，我们证明$\forall s \in S P(s)$，对s的结构做归纳证明：

(i) 归纳基：s是S的归纳定义的归纳基给出的元素5，显然有$P(5)$成立；

(ii) 归纳步：存在x和y使得$s = x + y$，则归纳假设是$P(x)$成立且$P(y)$成立，显然$P(s) = P(x+y)$也成立；或者存在x和y使得$s = x - y$，则归纳假设也是$P(x)$成立且$P(y)$成立，显然$P(s) = P(x-y)$也成立。

综上，根据结构归纳法，对任意$s \in S$有$P(s)$成立。 □

(2) 对于$S = A$，实际上(1)已经证明对任意$s \in S$有$5 \mid S$，也即对任意$s \in S$存在$k \in \mathbb{Z}$使得$s = 5k$，因此有$s \in A$，也即有$S \subseteq A$。因此只需再证明$A \subseteq S$即可。对于$A \subseteq S$，对于整数$k < 0$，若$5|k| \in S$，即$-5k \in S$，则根据S的归纳定义，显然有$0 \in S$，从而$0 - (-5k) = 5k \in S$。所以我们只要证明对任意自然数k有$5k \in S$即可，这可对k实施归纳法即可。

证明　由(1)有$S \subseteq A$，所以我们只需证明$A \subseteq S$，即对任意整数k有$5k \in S$。为此我们先使用数学归纳法证明，对任意自然数n有$5n \in S$，即令$P(n)$是$5n \in S$，我们证明$\forall n \in \mathbb{Z} P(n)$成立。

(i) 归纳基：显然$P(0)$成立，因为$0 \in S$；

(ii) 归纳步：对任意$k \geq 0$，假定$P(k)$成立，即$5k \in S$，我们要证明$P(k+1)$成立，因为$5(k+1) = 5k+5$，而$5 \in S$，根据S的归纳步，显然有$5k+5 \in S$，因此$P(k+1)$确实成立。

综上根据数学归纳法有，对任意自然数k有$5k \in S$。从而对任意整数k，若$k \geq 0$，则有$5k \in S$，而若$k < 0$，则有$-5k \in S$，而$0 \in S$，从而根据S的归纳步有$5k = 0 - (-5k) \in S$。这就这名了对任意整数k，有$5k \in S$，即$A \subseteq S$。综上就有$S = A$。 □

练习 4.43 固定整数a, b，归纳定义整数子集S_a^b：(1) 归纳基：$a \in S_a^b, b \in S_a^b$；(2) 归纳步：对任意整数x, y，如果$x \in S_a^b, y \in S_a^b$，则$x + y \in S_a^b$且$x - y \in S_a^b$。令集合A定义为：

$$A = \{c \in \mathbb{Z} \mid \exists s, t \in \mathbb{Z}, c = as + bt\}$$

证明$A \subseteq S$。

证明　我们首先使用归纳法证明，对任意自然数k，有$ka \in S_a^b$。

归纳基：当$k = 0$时，由于$a \in S_a^b$，所以$a - a \in S_a^b$，即$0 \in S_a^b$。显然当$k = 1$时有$a \in S_a^b$；

归纳步：假设当$k = p$时有$pa \in S_a^b$，则由$a \in S_a^b$，及S_a^b的归纳定义有$pa + a = (p+1)a \in S_a^b$。

这就证明了对任意自然数k有$ka \in S_a^b$，而由于$0 \in S_a^b$，因此也有$-ka \in S_a^b$，也即对任意整数k有$ka \in S_a^b$。

类似地可证明对任意的整数k有$kb \in S_a^b$。从而对任意整数s, t，有$sa \in S_a^b$和$tb \in S_a^b$，从而由S_a^b的归纳定义就有$sa + tb \in S_a^b$，这就证明了$A \subseteq S$。 □

练习* 4.44 设S是所有整数对集的一个子集，即$S \subseteq \mathbb{Z} \times \mathbb{Z}$，$S$由以下句子递归定义：
归纳基：$(0, 0) \in S$；
归纳步：如果$(a, b) \in S$，则$(a, b+1) \in S, (a+1, b+1) \in S, (a+2, b+1) \in S$。
a) 给出前四次使用归纳定义能够得到的S的元素；
b) 对归纳步的应用次数使用强归纳法，证明对任意的整数a, b，若$(a, b) \in S$则$a \leq 2b$；
c) 使用结构归纳法证明对任意的整数a, b，若$(a, b) \in S$则$a \leq 2b$。

解答：这一题给出集合的归纳定义，并分别使用强归纳法和结构归纳法证明集合元素的性质，学生由此可进一步了解强归纳法和结构归纳法的不同运用。

a) 严格地说应该是前四次使用归纳定义中的归纳步能够得到的S的元素：

至少1次使用归纳步： $(0, 1)$ $(1, 1)$ $(2, 1)$
至少2次使用归纳步： $(0, 2)$ $(1, 2)$ $(2, 2)$ $(3, 2)$ $(4, 2)$
至少3次使用归纳步： $(0, 3)$ $(1, 3)$ $(2, 3)$ $(3, 3)$ $(4, 3)$ $(5, 3)$ $(6, 3)$
至少4次使用归纳步： $(0, 4)$ $(1, 4)$ $(2, 4)$ $(3, 4)$ $(4, 4)$ $(5, 4)$ $(6, 4)$ $(7, 4)$ $(8, 4)$

b) 对归纳步的应用次数使用强归纳法，意味着我们要证明的命题$P(n)$是：对任意的非负整数n，以及任意的整数a, b，若(a, b)是应用n次归纳步得到的S的元素，则$a \leq 2b$。

归纳基：当$n = 0$时，则意味着不使用归纳步得到的S的元素，这个元素只能是$(0, 0)$，因此只要有$0 \leq 2 \cdot 0$，则命题$P(0)$成立；

归纳步：假设对于$k \geq 0$，对任意的$0 \leq j \leq k$时命题$P(j)$成立。也即，对任意的整数a, b，若(a, b)是应用少于等于k次归纳步得到的S的元素，则$a \leq 2b$（这时归纳假设）。考类$n = k + 1$，对于任意的整数a, b，若(a, b)是应用$k + 1$次归纳步得到的S的元素，那么（根据最小化规则）存在整数c, d，(c, d)是应用k次或更少次归纳步得到的S的元素，且$a = c, b = d+1$，或者$a = c+1, b = d+1$，或者$a = c + 2, b = d + 1$。由于(c, d)是应用k次或更少次归纳步得到的S的元素，因此根据归纳假设$c \leq 2d$，分情况讨论(a, b)：

(1) 若$a = c, b = d + 1$，则由$c \leq 2d$，得到$a = c \leq 2d < 2(d + 1) = 2b$；

(2) 若$a = c + 1, b = d + 1$，则由$c \leq 2d$，得到$a = c + 1 \leq 2d + 1 < 2(d + 1) = 2b$；

(3) 若$a = c + 2, b = d + 1$，则由$c \leq 2d$，得到$a = c + 2 \leq 2d + 2 = 2(d + 1) = 2b$。

因此总有$a \leq 2b$，这就完成了归纳步的证明。综上根据强归纳法，对任意的非负整数n有$P(n)$为真，也即对任意的整数a, b有，若$(a, b) \in S$，则$a \leq 2b$。

c) 使用结构归纳法证明：对任意的整数a, b有若$(a, b) \in S$则$a \leq 2b$：

归纳基：对于$(0, 0) \in S$，显然有$0 \leq 2 \cdot 0$；

归纳步：对任意的整数a, b，假定$(a, b) \in S$且$a \leq 2b$，根据S的定义的归纳步，我们只需证明也有$a \leq 2(b+1)$，$(a + 1) \leq 2(b + 1)$以及$(a + 2) \leq 2(b + 1)$即可，而由$a \leq 2b$不难得到这些不等式都成立。这就完成了归纳步的证明。

综上根据结构归纳法有：对任意整数a, b，若$(a, b) \in S$，则$a \leq 2b$。

【讨论】比较上面强归纳法和结构归纳法的证明，显然结构归纳法的证明更为简单直接。实际上，本质上可针对归纳步的应用次数做强归纳法而证明结构归纳法本身的正确性。

练习 4.45 归纳定义正整数对集的子集S：(1) 归纳基：$\langle 1,1\rangle \in S, \langle 2,2\rangle \in S$；(2) 归纳步：对任意正整数$a,b$，若$\langle a,b\rangle \in S$，则$\langle a+2,b\rangle \in S$且$\langle a,b+2\rangle \in S$。证明：对任意正整数$a,b$，$\langle a,b\rangle \in S$当且仅当$2 \mid (a+b)$。

证明　我们首先证明对任意的正整数a,b，若$(a,b) \in S$，则$a+b$是偶数。使用结构归纳法证明：对于任意的正整数a,b，若$(a,b) \in S$，则：

归纳基：根据S的归纳定义的归纳基有两种情况：(i) $(a,b) = (1,1)$，这时有$1+1 = 2$是偶数；或(ii) $(a,b) = (2,2)$，这时有$2+2 = 4$是偶数；

归纳步：根据S的归纳定义中的归纳步有两种情况：

(i) 存在正整数c和d，$(c,d) \in S$，且$a = c+2, b = d$，这时的归纳假设是$c+d$是偶数，显然也有$a+b = c+2+d$也是偶数；

(ii) 存在正整数c和d，$(c,d) \in S$，且$a = c, b = d+2$，这时的归纳假设是$c+d$是偶数，显然也有$a+b = c+d+2$也是偶数。

综上，根据结构归纳法，对任意的正整数a,b，若$(a,b) \in S$，则$a+b$是偶数。

其次我们证明对任意的正整数a,b，若$a+b$是偶数，则$(a,b) \in S$。对任意正整数n，定义命题$P(n)$：

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+[(a+b=n) \wedge (a+b \text{ 是偶数}) \ \to \ (a,b) \in S]$$

即我们要证明命题$P(n)$对任意的正整数n为真。我们对n进行强归纳法：

归纳基：$P(1)$成立（因为不存在正整数a,b使得$a+b = 1$）；$P(2)$成立，因为只有正整数$a = 1, b = 1$使得$a+b = 2$（且$a+b$是偶数），而$(1,1) \in S$；$P(3)$成立，因为不存在正整数a,b使得$a+b = 3$且$a+b$是偶数；$P(4)$成立，因为只有正整数$a = 2, b = 2$，或者$a = 1, b = 3$，或者$a = 3, b = 1$使得$a+b = 4$且$a+b$是偶数，而$(2,2) \in S$（S的归纳定义的归纳基），以及$(1,3),(3,1) \in S$（因为$(1,1) \in S$）。

归纳步：对于任意的正整数$k \geq 4$，假定对整数$1 \leq j \leq k$有$P(j)$成立（归纳假设），也即对任意的$1 \leq j \leq k$有，对任意正整数a,b，若$a+b = j$且$a+b$是偶数，则$(a,b) \in S$。按照强归纳法，我们需要证明有$P(k+1)$成立，即要证明对任意正整数a,b，若$a+b = k+1$且$a+b$是偶数，则也有$(a,b) \in S$。这可证明如下：

对任意的正整数a,b，设$a+b$是偶数且$a+b = k+1$，由于$k \geq 4$，因此$k+1 \geq 5$，因此a,b之中必存在一个数大于2（因为若两个数都小于等于2，则它们的和小于等于4），不妨设$a > 2$，从而$a-2 > 0$也是正整数，且$1 \leq (a-2)+b = k-1 \leq k$，根据归纳假设有$P(k-1)$成立，因此由$a-2+b$是偶数（因为$a+b$是偶数）且$a-2+b = k-1$，得$(a-2,b) \in S$，根据$S$的归纳定义的归纳步，由$(a-2,b) \in S$也有$(a,b) \in S$。

这就完成了归纳步的证明，综上，根据强归纳法，对任意正整数n，$P(n)$成立，也即对任意正整数a,b，若$a+b$是偶数，则$(a,b) \in S$。 □

【讨论】对任意正整数a,b，若$(a,b) \in S$，则$a+b$是偶数，可利用S是归纳定义的使用结构归纳法证明，因为这实质上是要证明对任意的属于S的元素(a,b)都满足性质$a+b$是偶数。但反之对任意正整数a,b，若$a+b$是偶数，要证明$(a,b) \in T$，则只能针对$a+b$进行强归纳法证明。

练习 4.46 归纳定义正整数对集的子集S：(1) **归纳基**：$\langle 1,1\rangle\in S,\langle 1,2\rangle\in S,\langle 2,1\rangle\in S$；(2) **归纳步**：对任意正整数$a,b$，若$\langle a,b\rangle\in S$，则$\langle a+2,b\rangle\in S$且$\langle a,b+2\rangle\in S$。证明：对任意正整数$a,b$，如果$\langle a,b\rangle\in S$，则$a$或$b$是奇数。

证明　使用结构归纳法证明：对于任意的正整数a,b，若$(a,b)\in S$，则：

归纳基：根据S的归纳定义的归纳基有三种情况：(i) $(a,b)=(1,1)$；或(ii) $(a,b)=(1,2)$；或(iii) $(a,b)=(2,1)$，显然这三种情况都有a或b是奇数；

归纳步：根据S的归纳定义中的归纳步有两种情况：

(i) 存在正整数c和d，$(c,d)\in S$，且$a=c+2,b=d$，这时的归纳假设是c或d是奇数，显然也有$a=c+2$或$b=d$是奇数；

(ii) 存在正整数c和d，$(c,d)\in S$，且$a=c,b=d+2$，这时的归纳假设是c或d是奇数，显然也有$a=c$或$b=d+2$是奇数。

综上，根据结构归纳法，对任意的正整数a,b，若$(a,b)\in S$，则a或b是奇数。 □

练习 4.47 归纳定义正整数对集的子集S：(1) **归纳基**：$\langle 1,6\rangle\in S,\langle 2,3\rangle\in S$；(2) **归纳步**：对任意正整数$a,b$，若$\langle a,b\rangle\in S$，则$\langle a+2,b\rangle\in S$且$\langle a,b+6\rangle\in S$。证明：对任意正整数$a,b$，如果$\langle a,b\rangle\in S$，则$a+b$是奇数且$3\mid b$。

证明　使用结构归纳法证明：对于任意的正整数a,b，若$(a,b)\in S$，则：

归纳基：根据T的归纳定义的归纳基有两种情况：(i) $(a,b)=(1,6)$，这时有$1+6=7$是奇数且$3\mid 6$；或(ii) $(a,b)=(2,3)$，这时有$2+3=5$是奇数，且$3\mid 3$；

归纳步：根据S的归纳定义中的归纳步有两种情况：

(i) 存在正整数c和d，$(c,d)\in S$，且$a=c+2,b=d$，这时的归纳假设是$c+d$是奇数且$3\mid d$，显然也有$a+b=c+2+d$也是奇数，且$3\mid b$；

(ii) 存在正整数c和d，$(c,d)\in S$，且$a=c,b=d+6$，这时的归纳假设是$c+d$是奇数且$3\mid d$，显然也有$a+b=c+d+6$也是奇数，且由$3\mid d$显然有$3\mid(d+6)$。

综上，根据结构归纳法，对任意的正整数a,b，若$(a,b)\in S$，则$a+b$是奇数，且$3\mid b$。 □

练习 4.48 基于字符串集的归纳定义，以及字符串连接的递归定义，证明空串是字符串连接运算的单位元，即对任意字符串w，有$\lambda\circ w=w=w\circ\lambda$。

证明　$w\circ\lambda=w$是串连接的定义的一部分，而对于$\lambda\circ w=w$，只要对w做结构归纳法：

归纳基：若$w=\lambda$，则根据串连接运算的定义有$\lambda\circ\lambda=\lambda$；

归纳步：若存在$u\in\Sigma^*$和$a\in\Sigma$使得$w=ua$，则根据归纳假设有$\lambda\circ u=u$，从而根据连接运算的定义有$\lambda\circ(ua)=(\lambda\circ u)a=ua=w$。 □

练习 4.49 基于字符串集的归纳定义，以及字符串连接的递归定义，证明字符串连接运算满足结合律，即对任意字符串u,v,w，有$u\circ(v\circ w)=(u\circ v)\circ w$。

证明　这对w做结构归纳法证明（注意，为简单起见，下面省略了连接运算符$\circ$）：

归纳基：若$w=\lambda$，则由λ是串连接的单位元有$u(v\lambda)=uv$及$(uv)\lambda=uv$；

归纳步：若存在$s\in\Sigma^*$和$a\in\Sigma$使得$w=sa$，则根据归纳假设有$u(vs)=(uv)s$，从而根据串连接的定义有：$u(vw)\;=\;u(v(sa))=u((vs)a)=(u(vs))a=((uv)s)a=(uv)(sa)=(uv)w$。 □

练习* 4.50 字符串的逆(reversal)由这个串中的字母根据逆序构成，例如字符串“abcabc”的逆是“cbacba”。字符串w的逆记为w^R。

(1) 给出字符串的逆运算的递归定义；

(2) 使用结构归纳法证明对任意两个字符串u, w有$(u \circ w)^R = w^R \circ u^R$。

解答：

(1) 为了给出串逆w^R的归纳定义，我们对w进行归纳：

归纳基：若$w = \lambda$，则$\lambda^R = \lambda$，空串的逆还是空串；

归纳步：若存在$u \in \Sigma^*, a \in \Sigma$使得$w = ua$，则$w^R = (ua)^R = a \cdot u^R$，即$ua$的逆等于$a$（作为单个符号的串）连接$u$的逆。

(2) 为证明对任意的两个串$w_1, w_2 \in \Sigma$，有w_1, w_2有$(w_1w_2)^R = w_2^R w_1^R$。我们对w_2做结构归纳：

归纳基：若$w_2 = \lambda$，则由λ是连接的单位元有$(w_1w_2)^R = (w_1\lambda)^R = w_1^R$，且$w_2^R w_1^R = \lambda^R w_1^R = \lambda w_1^R = w_1^R$，因而要证的等式成立；

归纳步：若存在$u \in \Sigma^*, a \in \Sigma$使得$w_2 = ua$，则根据归纳假设有对任意的串$w_1$有$(w_1u)^R = u^R w_1^R$，从而根据串连接和串逆的定义，以及归纳假设和串连接的结合律有：

$$(w_1w_2)^R = (w_1(ua))^R = ((w_1u)a)^R = a(w_1u)^R = a(u^R w_1^R) = (au^R)w_1^R = (ua)^R w_1^R = w_2^R w_1^R$$

这就完成了归纳步的证明，综上根据结构归纳法有对任意的串w_1, w_2，$(w_1w_2)^R = w_2^R w_1^R$。

练习 4.51 序列$a_0, a_1, a_2, \cdots$递归地定义如下：

$$\begin{aligned} a_0 &= 0 \\ a_{n+1} &= 2a_n + n, \qquad \forall n \in \mathbb{N} \end{aligned}$$

证明对任意$n \in \mathbb{N}$，$a_n = 2^n - n - 1$。

证明　对自然数n实施数学归纳法即可。

(1) 归纳基：当$n = 0$时，有$a_0 = 2^0 - 0 - 1 = 0$；

(2) 归纳步：设$n = k$时，$a_k = 2^k - k - 1$。考虑$n = k + 1$，则：

$$a_{k+1} = 2(a_k) + k = 2(2^k - k - 1) + k = 2^{k+1} - k - 2 = 2^{k+1} - (k+1) - 1$$

也即当$n = k + 1$时也成立，因此对任意自然数n，有$a_n = 2^n - n - 1$。 □

练习 4.52 设F_n是第n个斐波拉契数，下面题目中所有的n都是自然数。

(1) 证明对任意的n，$\sum_{i=0}^n F_i = F_{n+2} - 1$；

(2) 证明对任意的n，$\sum_{i=0}^n F_{2i+1} = F_{2n+2}$；

(3) 为$\sum_{i=0}^n F_{2i}$找到一个公式，并证明其正确性。

证明　(1) 对自然数n实施归纳法。

归纳基：当$n = 0$时，$\sum_{i=0}^0 F_i = F_0 = 0, F_2 - 1 = 0$，等式成立；

归纳步：假设$n=k$时等式成立，则当$n=k+1$时，

$$\sum_{i=0}^{k+1} F_i \ = \ \sum_{i=0}^{k} F_i + F_{k+1} = F_{k+2} - 1 + F_{k+1} = F_{k+3} - 1$$

因此当$n=k+1$时等式也成立。

(2) 对自然数n实施归纳法。

归纳基：当$n=0$时，$\sum_{i=0}^{0} F_{2i+1} = F_1 = 1, F_2 = 1$，等式成立；

归纳步：假设$n=k$时等式成立，则当$n=k+1$时，

$$\sum_{i=0}^{k+1} F_{2i+1} \ = \ \sum_{i=0}^{k} F_{2i+1} + F_{2(k+1)+1} = F_{2k+2} + F_{2(k+1)+1} = F_{2k+4}$$

因此当$n=k+1$时等式也成立。 □

(3) 不难看到：

$$\begin{aligned}\sum_{i=0}^{n} F_{2i} \ &= \ F_0 + F_2 + F_4 + \cdots + F_{2n} \\ &= \ F_0 + F_0 + F_1 + F_2 + F_3 + \cdots + F_{2n-2} + F_{2n-1} = F_0 + \sum_{i=0}^{2n-1} F_i\end{aligned}$$

而根据(1)有$\sum_{i=0}^{2n-1} F_i = F_{2n-1+2} - 1 = F_{2n+1} - 1$。因此我们使用数学归纳法证明，对任意自然数$n$，

$$\sum_{i=0}^{n} F_{2i} = F_{2n+1} - 1$$

归纳基：当$n=0$时，$\sum_{i=0}^{0} F_{2i} = F_0 = 0, F_1 - 1 = 0$，等式成立；

归纳步：假设$n=k$时等式成立，则当$n=k+1$时，

$$\sum_{i=0}^{k+1} F_{2i} \ = \ \sum_{i=0}^{k} F_{2i} + F_{2k+2} = F_{2k+1} - 1 + F_{2k+2} = F_{2(k+1)+1} - 1$$

因此当$n=k+1$时等式也成立。

练习 4.53 设F_n是第n个斐波那契数，下面题目中所有的n都是自然数。

(1) 证明对所有的$m \geq 1$和所有n，$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$；

(2) 证明对所有的$m \geq 1$和所有$n \geq 1$，$F_{m+n} = F_{m+1}F_{n+1} - F_{m-1}F_{n-1}$；

(3) 证明对所有的n，$(F_n)^2 + (F_{n+1})^2 = F_{2n+1}$以及$(F_{n+2})^2 - (F_n)^2 = F_{2n+2}$；

(4) 对所有自然数m, n，如果$m \mid n$，则$F_m \mid F_n$。

证明 (1) 令命题$P(n)$为：对所有$m \geq 1$有$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$。我们要证明对任意自然数$n$有$P(n)$成立，对$n$实施强归纳法：

归纳基：当$n=0$时，显然对任意$m \geq 1$都有$F_m = F_{m-1}F_0 + F_mF_1$；而当$n=1$时有$F_{m+1} = F_{m-1}F_1 + F_mF_1$，因此$P(0)$和$P(1)$成立。

归纳步：对任意$k \geq 1$，假定$P(0), P(1), \cdots, P(k)$成立，考虑$n = k+1$，由于$k \geq 1$，因此$k-1 \geq 0$，从而按归纳假设有$P(k)$和$P(k-1)$成立，从而有：对任意$m \geq 1$，

$$\begin{aligned} F_{m+k+1} &= F_{m+k} + F_{m+k-1} = F_{m-1}F_k + F_mF_{k+1} + F_{m-1}F_{k-1} + F_mF_k \\ &= F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k) = F_{m-1}F_{k+1} + F_mF_{k+2} \end{aligned}$$

即有$P(k+1)$成立。

(2) 令命题$P(n)$为：对所有$m \geq 1$有$F_{m+n} = F_{m+1}F_{n+1} - F_{m-1}F_{n-1}$。我们要证明对任意正整数$n$有$P(n)$成立，对$n$实施强归纳法：

归纳基：当$n = 1$时，显然对任意$m \geq 1$都有$F_{m+1} = F_{m+1}F_2 - F_{m-1}F_0$；而当$n = 2$时有

$$\begin{aligned} F_{m+1}F_3 - F_{m-1}F_1 &= 2F_{m+1} - F_{m-1} = F_{m+1} + F_{m+1} - F_{m-1} \\ &= F_{m+1} + F_m + F_{m-1} - F_{m-1} = F_{m+1} + F_m = F_{m+2} \end{aligned}$$

因此$P(1)$和$P(2)$成立。

归纳步：对任意$k \geq 2$，假定$P(1), P(2), \cdots, P(k)$成立，考虑$n = k+1$，由于$k \geq 2$，因此$k-1 \geq 1$，从而按归纳假设有$P(k)$和$P(k-1)$成立，从而有：对任意$m \geq 1$，

$$\begin{aligned} F_{m+k+1} &= F_{m+k} + F_{m+k-1} = F_{m+1}F_{k+1} - F_{m-1}F_{k-1} + F_{m+1}F_k - F_{m-1}F_{k-2} \\ &= F_{m+1}(F_{k+1} + F_k) - F_{m-1}(F_{k-1} + F_{k-2}) = F_{m+1}F_{k+2} - F_{m-1}F_k \end{aligned}$$

即有$P(k+1)$成立。

(3) 对(1)取$m = n+1$，则有$(F_n)^2 + (F_{n+1})^2 = F_{2n+1}$，而由(2)有对任意正整数$m, k$，$F_{m+k} = F_{m+1}F_{k+1} - F_{m-1}F_{k-1}$，从而对任意自然数$n$，取$m = n+1, k = n+1$，而有$F_{2n+2} = F_{n+2}F_{n+2} - F_nF_n$，即$F_{2n+2} = (F_{n+2})^2 - (F_n)^2$。

(4) 令命题$P(k)$表示，对所有正整数$m \geq 1$，有$F_m \mid F_{km}$。我们使用数学归纳法证明$P(k)$对所有自然数k成立。

归纳基：当$k = 0$时，因为$F_0 = 0$，而总有$F_m \mid F_0$，因此$P(0)$成立，当$k = 1$时，显然也有$P(1)$成立。

归纳步：对$t \geq 1$，假设$P(t)$成立，即对所有证整数$m \geq 1$，有$F_m \mid F_{tm}$，考虑$P(t+1)$。注意到根据上面证明的(1)有：

$$F_{(t+1)m} = F_{m+tm} = F_{m-1}F_{tm} + F_mF_{tm+1}$$

根据归纳假设$F_m \mid F_{tm}$，因此也有$F_m \mid F_{(t+1)m}$，即$P(t+1)$成立。

这就证明了对所有正整数$m \geq 1$和自然数$k \geq 0$，有$F_m \mid F_{km}$，从而对所有自然数m, n，若$m \mid n$，则$m \geq 1$，且存在自然数k使得$n = km$，从而$F_m \mid F_{km}$，即$F_m \mid F_n$。 □

【**讨论**】对于上面的(4)，直接针对m或n使用归纳法证明，对若$m \mid n$则$F_m \mid F_n$有一定难度，但利用已经证明的(1)则可比较容易地证明。

练习* 4.54 证明对于非负整数a和b，且$a < b$时，下面计算$gcd(a, b)$的算法是正确的。

```
1   function gcd(a, b : nonnegative integers with a < b)
2       if (a == 0) then return b
3       else return gcd(b mod a, a)
4   end
```

证明 我们令$P(a)$是命题：对任意非负整数b，若$a < b$则上述算法是正确的，即能正确计算$gcd(a, b)$的值。我们使用强归纳法证明，对任意非负整数a，有$P(a)$成立。

(1) 归纳基：对于$P(0)$，上述算法对任意$b > a$，当$a = 0$时$gcd(a, b) = b$，也即上述算法能正确计算$gcd(a, b)$的值，即$P(0)$成立；

(2) 归纳步：对任意$k \geq 0$，假定$P(0), P(1), \cdots, P(k)$成立，我们要证明$P(k+1)$成立。对任意非负整数b，若$b > k+1 \geq 1$，则有$0 \leq b \ \mathbf{mod} (k+1) < (k+1)$，从而由归纳假设有$P(b \ \mathbf{mod} (k+1))$成立，也即对任意非负整数$a$，若$b \ \mathbf{mod} (k+1) < a$，则上述算法能正确计算$gcd(b \ \mathbf{mod} (k+1), a)$，特别地，对于$k+1$，上述算法能正确计算$gcd(b \ \mathbf{mod} (k+1), k+1)$，也就是说，上述算法第3行等式右边的递归调用能得到正确的$gcd(b \ \mathbf{mod} (k+1), k+1)$，而根据最大公因数的性质，即对任意非负整数$m, n, m < n$，确实有$\gcd(m, n) = \gcd(n\%m, m)$，因此上述算法的第3行左边得到的$gcd(k+1, b)$也是正确的，从而上述算法对任意非负整数$b$，能正确计算$gcd(k+1, b)$，也即有$P(k+1)$成立。

综上，对任意非负整数a有$P(a)$成立，也即上述算法是正确的。 □

练习 4.55 给出一个递归算法计算下面定义的序列的第n项：$a_0 = 1, a_1 = 3, a_2 = 5$，且$a_n = a_{n-1} + a_{n-2}^2 + a_{n-3}^3$，并证明你给出的算法的正确性。

解答：根据序列的递归定义，可直接给出递归算法如下：

```
1   Procedure recursivelyCalSeq(n : nonnegative integer) begin
2       if (n < 3) return 2n − 1;
3       else begin
4           x := recursivelyCalSeq(n − 1);
5           y := recursivelyCalSeq(n − 2);
6           z := recursivelyCalSeq(n − 3);
7           return x + y · y + z · z · z;
8       end
9   end
```

【**证明**】下面证明上述算法的正确性，令$P(n)$是命题$recursivelyCallSeq(n) = a_n$，则要证明$\forall n \geq 0 (P(n))$。针对$n$进行归纳证明：

(1) **归纳基**：当$n = 0$时，算法只执行第2行，返回1，等于a_0；当$n = 1$时，算法只执行第2行，返回3，等于a_1。当$n = 2$时，算法也只执行第2行，返回5，等于a_2，因此$P(0), P(1)$和$P(2)$成立；

(2) **归纳步**：对任意的$k \geq 3$，假定$P(0), P(1), \cdots, P(k-1)$成立。由于$k \geq 3$，以$k$为输入执行算法将执行第4, 5, 6, 7行，这时根据归纳假设有$P(k-1), P(k-2)$和$P(k-3)$成立，也即$x = recursivelyCalSeq(k-1) = a_{k-1}$，$y = recursivelyCalSeq(k-2) = a_{k-2}$，$z = recursivelyCalSeq(k-3) = a_{k-3}$，从而算法会在第7行返回$x + y \cdot y + z \cdot z \cdot z$，即$a_{k-1} + a_{k-2}^2 + a_{k-3}^3$，这根据数列$a_n$的定义，这等于$a_k$，也即$P(k)$成立。

综上，根据强归纳证明法，对任意自然数n有$P(n)$成立，即对任意n，以n为输入执行算法$recursivelyCalSeq(n)$将得到数列的第n项a_n。