第一章

1. （1）若$a\mid b$且$c\mid d$，则$ac\mid bd$；

（2）若$a\mid b_1,\cdots,a\mid b_k$，则对任意整数$x_1,\cdots,x_k$有$a\mid b_1x_1+\cdots+b_kx_k$。

证明：（1）$a\mid b$且$c\mid d\Rightarrow b=k_1a,d=k_2c$，因此有$bd=k_1k_2ac\Rightarrow ac\mid bd$。

（2）$a\mid b_1,\cdots,a\mid b_k\Rightarrow b_1=l_1a,\cdots,b_k=l_ka$，则

$$\begin{aligned}b_1x_1+\cdots+b_kx_k&=l_1x_1a+\cdots+l_kx_ka\\&=(l_1x_1+\cdots+l_kx_k)a\end{aligned}$$

因此有$a\mid b_1x_1+\cdots+b_kx_k$。

2. 若$x^2+ax+b=0$有整数根$x_0\neq 0$，则$x_0\mid b$。一般地，若$x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$有整数根$x_0\neq 0$，则$x_0\mid a_0$。

证明：$x_0^2+ax_0+b=0\Rightarrow b=-x_0^2-ax_0=(-x_0-a)x_0$，所以有$x_0\mid b$。$x_0\mid a_0$同理可证。

3. 若$5\mid n$且$17\mid n$，则$85\mid n$。

证明：由于$5\times 7-17\times 2=1$，所以有$5\times 7n-17\times 2n=n$，又因为$5\mid n$且$17\mid n$，所以$5\times 17\mid 5\times 7n$且$5\times 17\mid 17\times 2n$，因此$85\mid 5\times 7n-17\times 2n=n$。

4. 若$2\mid n$，$5\mid n$及$7\mid n$，则$70\mid n$。

提示：类似于上一题，可先根据$2\mid n$，$5\mid n$证$10\mid n$，然后再根据$10\mid n$及$7\mid n$去证$70\mid n$。

5. 设a,b,n满足$a\mid bn,ax+by=1,x,y$是两个整数。证明：$a\mid n$。

证明：$ax+by=1\Rightarrow anx+bny=n$，又$a\mid bn$，所以$a\mid anx,a\mid bny\Rightarrow a\mid anx+bny=n$。

6. （1）若$2\mid ab$，则$2\mid a,2\mid b$至少有一个成立。

（2）若$7\mid ab$，则$7\mid a,7\mid b$至少有一个成立。

（3）若$14\mid ab$，试问$14\mid a$或$14\mid b$必有一个成立吗？

证明：（1）若$2\nmid a$，则a是奇数，不妨设$a=2k+1$，则有

$$a-2k=1$$

两边同乘以 b，可得

$$ab-2kb=b$$

由于$2\mid ab$，所以 2 整除上述等式的左边，因此$2\mid b$。

（2）若$7\nmid a$，则$\gcd(7,a)=1$，即存在整数u,v使得$ua+7v=1$，

两边同乘以 b，可得

$$uab+7vb=b$$

由于$7\mid ab$，所以 2 整除上述等式的左边，因此$7\mid b$。

（3）不一定。例如$a=2,b=7$，有$14\mid ab$，但 14 不整除 2 和 7。

7. 证明：对任意整数n有

（1）$6\mid n(n+1)(n+2)$；

证明：三个连续整数中，至少有一个被 2 整除，也至少有一个被 3 整除。

若 n，n+1，n+2 中有一个既能被 2 整除又能被 3 整除，则该数能被 6 整除，结论成立；

若 2 和 3 分别整除不同的两个数，不妨设$2\mid n$，$3\mid n+1$，则有$6\mid n(n+1)(n+2)$，结论也成立。

（2）$8\mid n(n+1)(n+2)(n+3)$；

证明：三个连续整数中，一定存在两个连续偶数不妨设为 n 和 n+2。两个连续偶数中必有一个被 4 整除，设$2\mid n,\quad 4\mid n+2$，则有$8\mid n(n+2)$，即$8\mid n(n+1)(n+2)(n+3)$。同理可证，当 n+1 和 n+3 是两个连续偶数的时候，结论同样成立。

（3）$24\mid n(n+1)(n+2)(n+3)$；

证明：根据第（2）小题结论，有$8\mid n(n+1)(n+2)(n+3)$，又因为四个连续整数中，至少有一个被 3 整除，因此有$3\mid n(n+1)(n+2)(n+3)$。又$(3,8)=1$，所以有$24\mid n(n+1)(n+2)(n+3)$。

（4）若$2\nmid n$，则$8\mid n^2-1$及$24\mid n(n^2-1)$；

证明：因为$2\nmid n$，所以$n-1,n+1$为两个连续偶数，两个连续偶数中必有一个被 4 整除，不妨设$2\mid n-1,\quad 4\mid n+1$，则有$8\mid (n-1)(n+1)$，即$8\mid n^2-1$

对于三个连续$n-1,n,n+1$，必有一个被 3 整除，所以$3\mid n(n^2-1)$，又

$8\mid n^2-1\Rightarrow 8\mid n(n^2-1)$，由于$(3,8)=1$，根据推论 1.2.2（2）可得$24\mid n(n^2-1)$。

（5）若$2\nmid n,3\nmid n$，则$24\mid n^2+23$；

证明：$2\nmid n$，则根据第（4）小题结论有$8\mid n^2-1$。对于三个连续$n-1,n,n+1$，必

有一个被 3 整除，所以$3\mid n(n^2-1)$，而$3\nmid n$，所以$3\mid n^2-1$，由于$(3,8)=1$，根据

推论 1.2.2（2）可得$24\mid n^2-1$。因此有$24\mid (n^2-1+24)=n^2+23$。

（6）$6\mid n^3-n$；

证明：$n^3-n=(n-1)n(n+1)$是 3 个连续整数的乘积，类似于第（1）小题，可证。

（7）$30\mid n^5-n$；

证明：$n^5-n=(n-1)n(n+1)(n^2+1)$，由第（6）小题结论可知$6\mid n^3-n$。如果$n-1,n,n+1$有 5 的倍数，则结论得证，若没有，则 n 必然是 5k+2 和 5k+3 两种形

式，可将其代入n^2+1，可知n^2+1一定是 5 的倍数，即$5|(n^2+1)$。结论得证。

（8）$42|n^7-n$；

证明：$n^7-n=(n-1)n(n+1)(n^2-n+1)(n^2+n+1)$。由第（6）小题结论可知$6|(n-1)n(n+1)$。如果$n-1,n,n+1$有 7 的倍数，则结论得证，若没有，则 n 必然是 7k+2、7k+3、7k+4、7k+5 四种形式，可将其代入$(n^2-n+1)(n^2+n+1)$，可知$(n^2-n+1)(n^2+n+1)$一定是 7 的倍数，即$7|(n^2-n+1)(n^2+n+1)$。结论得证。

（9）证明对任意整数n，$\frac{1}{5}n^5+\frac{1}{3}n^3+\frac{7}{15}n$是整数。

证明：

$$\begin{aligned}\frac{1}{5}n^5+\frac{1}{3}n^3+\frac{7}{15}n&=\frac{1}{15}n(3n^4+5n^2+7)\\&=\frac{1}{15}n(3n^4-10n^2+7+15n^2)\\&=\frac{1}{15}n((3n^2-7)(n^2-1)+15n^2)\\&=\frac{(n-1)n(n+1)(3n^2-7)}{15}+n^3\end{aligned}$$

由于$n-1,n,n+1$中必有一个是 3 的倍数，如果$n-1,n,n+1$有 5 的倍数，则结论得证，若没有，则 n 必然是 5k+2 和 5k+3 两种形式，可将其代入$(3n^2-7)$，可知$(3n^2-7)$一定是 5 的倍数。结论得证。

8. 证明：形如$6k-1$的素数有无穷多个。
证明：首先证明形如$6k-1$的整数必有一个形如$6k-1$的素因子。
设$n=6k-1$，（1）若 n 是素数，则结论成立。
（2）若 n 是合数，则 n 一定是奇数，因此 n 的素因子为 6k+1 和 6k-1 的形式。若 n 没有形如 6k-1 的素因子，则 n 的素因子都为 6k+1 的形式，那么 n 的形式也一定是 6k+1，与 n 的形式为 6k-1 矛盾。因此，n 必有一个形如$6k-1$的素因子。
假设形如$6k-1$的素数有有限个，不妨设为$q_1,q_2,\ldots,q_t$，令

$$M=6(q_1q_2\ldots q_t)-1$$

则 M 必有一个形如 6k-1 的素因子 q，由于形如$6k-1$的素数有有限个$q_1,q_2,\ldots,q_t$，因此 q 必为$q_1,q_2,\ldots,q_t$中的 1 个，因而有 q|M，$q|6(q_1q_2\ldots q_t)$，即 q|1，矛盾。所以形如$6k-1$的素数有无穷多个。

9. 若$(a,b)=1,c|a+b$，则$(c,a)=(c,b)=1$。
证明：设$(c,a)=d$，则由$d|c$，$c|a+b$，可知$d|a+b$，又因为$d|a$，根据整除的性质有$d|a+b-a=b$，因此有$d|(a,b)=1$，即$d=1$。同理可证$(c,b)=1$。

10. 设a,b是正整数，且有整数x,y使得$ax+by=1$。证明：

（1）$[a,b]=ab$；（2）$(ac,b)=(c,b)$。

证明：由$ax+by=1$可知$(a,b)=1$

（1）设 m 为 a，b 的任意公倍数即 a|m，b|m。存在整数 k 使得 m=ak。由 b|m，可知 b|ak，又 a，b 互素，由推论 1.2.2 可知 b|k。因此存在整数 t 使得 k=bt，所以 m=abt。故 ab|m。由此可知 ab 是 a，b 的公倍数中的最小正整数，即[a，b]=ab。

（2）很显然$(c,b)\mid(ac,b)$。下证$(ac,b)\mid(c,b)$。

令$d=(ac,b)$，则$d\mid ac$，且$d\mid b$，而$(a,b)=1$，所以$(a,d)=1$。根据整除性质，$d\mid c$。因此$(ac,b)\mid(c,b)$。

综上，$(ac,b)=(c,b)$

11. 判断以下结论是否成立，对的给出证明，错的举出反例。

（1）若$\gcd(a,b)=\gcd(a,c)$，则$lcm[a,b]=lcm[a,c]$；

答：错。提示：a=6，b=8，c=10

（2）若$\gcd(a,b)=\gcd(a,c)$，则$\gcd(a,b,c)=\gcd(a,b)$；

答：正确。提示：左右互相整除。

证明：$\gcd(a,b,c)\mid a,\gcd(a,b,c)\mid b\Rightarrow\gcd(a,b,c)\mid\gcd(a,b)$

$\gcd(a,b)=\gcd(a,c)\Rightarrow\gcd(a,b)\mid c\Rightarrow\gcd(a,b)\mid\gcd(a,b,c)$

（3）若$d\mid a,d\mid a^2+b^2$，则$d\mid b$；

答：错。提示：d=4，a=8，b=10

（4）若$a^4\mid b^3$，则$a\mid b$；

答：正确。

证明：设$a=p_1^{e_1}p_2^{e_2}\cdots p_l^{e_l},b=p_1^{r_1}p_2^{r_2}\cdots p_l^{r_l}$。$a=2^3\cdot3^4\cdot5^0,b=2^4\cdot3^4\cdot5$，由$a^4\mid b^3$可知$4e_i\le3r_i$，$1\le i\le l$，因此有$e_i\le\frac{3}{4}r_i\le r_i$，$1\le i\le l$。因此有$a\mid b$。

（5）若$a^2\mid b^3$，则$a\mid b$；

答：错误。例如$a=2^6,b=2^5$，则有$a^2=2^{12}\mid2^{15}=b^3$，而$a\nmid b$。

（6）若$a^2\mid b^2$，则$a\mid b$；

答：正确。

证明：$a=p_1^{e_1}p_2^{e_2}\cdots p_l^{e_l},b=p_1^{n_1}p_2^{n_2}\cdots p_l^{n_l}$，则$a^2=p_1^{2e_1}p_2^{2e_2}\cdots p_l^{2e_l}$，$b^2=p_1^{2n_1}p_2^{2n_2}\cdots p_l^{2n_l}$。因为$a^2\mid b^2$，所以$\forall 1\le i\le l$，有$2e_i\le2n_i$。因此有$e_i\le n_i$，即有$a\mid b$。

（7）$ab\mid[a^2,b^2]$；

答：正确。

证明：设 $d=\gcd(a,b)$， $a=k_1d,b=k_2d$，则

$$lcm[a^2,b^2]=\frac{a^2b^2}{\gcd(a^2,b^2)}=\frac{k_1^2d^2k_2^2d^2}{d^2}=k_1^2d^2k_2^2=k_1k_2ab$$

所以 $ab\,|\,[a^2,b^2]$

（8）$[a^2,ab,b^2]=[a^2,b^2]$；

略。(同 9)

（9）$(a^2,ab,b^2)=(a^2,b^2)$；

正确，设 $a=p_1^{e_1}p_2^{e_2}\cdots p_l^{e_l}, b=p_1^{r_1}p_2^{r_2}\cdots p_l^{r_l}$。

则，$(a^2,b^2)=p_1^{2\min(e_1,r_1)}p_2^{2\min(e_2,r_2)}\cdots p_l^{2\min(e_l,r_l)}$

又，$ab=p_1^{e_1+r_1}p_2^{e_2+r_2}\cdots p_l^{e_l+r_l}$ 且 $e_i+r_i\geq 2\min(e_i,r_i)$

故，$(a^2,ab,b^2)=(a^2,b^2)$

（10）$(a,b,c)=((a,b),(a,c))$；

正确。因 $(a,b,c)|(a,b),(a,b,c)|(a,c)$， 故 $(a,b,c)|((a,b),(a,c))$

任意 $t|((a,b),(a,c))$,有 $t|(a,b),t|(a,c)$,因此，$t|a,t|b),t|c$， 故有 $t|(a,b,c)$.

因此，$\big((a,b),(a,c)\big)|(a,b,c)$.

（11）若 $d\,|\,a^2+1$，则 $d\,|\,a^4+1$；

答：不正确。例如 d=13，a=5，$13|5^2+1=26$，但是 $13\nmid 5^4+1=626$。

（12）若 $d\,|\,a^2-1$，则 $d\,|\,a^4-1$。

答：正确。

证明：$d|a^2-1\Rightarrow d|(a^2-1)(a^2+1)=a^4-1$。

12. 设 $(a,b)=1$。证明：$(d,ab)=(d,a)(d,b)$。

证明：令 $d_1=(d,ab)$， $d_2=(d,a)$， $d_3=(d,b)$

显然有 $d_2\,|\,d_1, d_3\,|\,d_1$，又 $(a,b)=1$，所以 $(d_2,d_3)=1$，因此有 $d_2d_3\,|\,d_1$。

反之，设 $a=d_2t$，$b=d_3s$，由 $d_1=(d,ab)$ 可知 $(d_1,t)=1$，$(d_1,s)=1$，所以 $(d_1,st)=1$。又 $d_1\mid ab=d_2d_3st$，所以 $d_1\mid d_2d_3$。

综上，$d_1=d_2d_3$，即 $(d,ab)=(d,a)(d,b)$。

13. 用扩展的欧几里得算法求以下数组的最大公约数，并把它表为这些数的整系数线性组合:

（1）1819,3587;（2）2947,3997;（3）-1109,4999。

（1）1819,3587

3587=1×1819+1768　　　　17=51-1×（1768-34×51）

1819=1×1768+51　　　　　=-1×1768+35×51

1768=34×51+34
51=1×34+17
34=2×17
（1819,3587）=17

=-1×1768+35×（1819-1×1768）
=-36×1768+35×1819
=-36×（3587-1×1819）+35×1819
=-36×3587+71×1819
(1819,3587)= -36×3587+71×1819

(2)2947,3997
3997=1×2947+1050
2947=2×1050+847
1050=1×847+203
847=4×203+35
203=5×35+28
35=1×28+7
28=4×7
(2947,3997)=7

7=35-1×（203-5×35）
=118×2947-87×3997
（2947,3997）=118×2947-87×3997

(3)-1109,4999
4999=4×1109+563
1109=1×563+546
563=1×546+17
546=32×17+2
17=8×2+1
(-1109,4999)=1

1=17-8×（547-32×17）
=522×4999-2353×1109
(-1109,4999) =522×4999-2353×1109