Discrete Mathematics homework 1.1

---

1. 下述几种情况, a分别意味着什么?
   (a) $2|a$; a是2的倍数
   (b) $2\nmid a$; a不是2的倍数
   (c) $0|a$. 0整除a, 无意义, 0不能整除任何数

2. 证明:
   (a) 若$a|b$且$b|c$, 则有$a|c$; $b=am, m\in N, c=bn, n\in N$, 则$c=bn=amn$, $a|c$成立
   (b) 若$a|b$且$a|c$, 则有$a|(b+c)$且$a|(b-c)$; $b=am, c=an, b+c=(m+n)a, b-c=(m-n)a$, $a|(b+c)$, $a|(b-c)$成立
   (c) 若$a,b>0$且$a|b$, 则有$a\le b$; $a|b, b=ak, k\in N^+$, 有$b=ak\ge a$, $b\ge a$
   (d) 若$a|b$且$b|a$, 则有$a=b$或$a=-b$. $b=am, a=bn, m,n\in N, a=amn$, 且$a\neq 0$, $mn=1$, 且$m,n\in N$, $\begin{cases} m=1 \\ n=1 \end{cases}$ 或 $\begin{cases} m=-1 \\ n=-1 \end{cases}$ $\therefore \begin{cases} a=b \\ a=-b \end{cases}$

3. 设r是除式$b\div a$的余数, 假设$c|a$, $c|b$, 证明$c|r$. 3. $b=aq+r$, $a=cn, b=cm$ 代入 $cm=cnq+r$, $c(m-nq)=r$, 有$c|r$

4. 假设$a|b$, 且$a,b>0$, 令r是除式$c\div a$的余数, 令s是除式$c\div b$的余数, 除式$s\div a$的余数是多少? 4. $c=aq_1+r$, $c=bq_2+s$. $b=am$ $b>a$, $a>r$, $b>s$
   有$s=c-bq_2=aq_1+r-bq_2=a(q_1-mq_2)+r$. $q_1-mq_2>0$, 余数是r

5. 假设a 与b 均为一个整数, 并且$a\mid b$. 同时假设p 为一个素数, 并且有$p\mid b$ 及$p\nmid a$. 证明p 是比值b/a 的一个约数. 5. $b=ak, b=pm, ak=pm, k=\frac{pm}{a}$, $p\nmid a$, p, a互质, $\gcd(p,a)=1$
   $\frac{b}{a}=k=\frac{pm}{a}, k\in N, k=p\frac{m}{a}$. 则$p|k$, $p|\frac{b}{a}$. 则证毕

6. 证明: 一个数字n 的素因数分解最多包含$\log_2 n$ 个因子.

7. 请通过例子证明: 如果放弃p 是素数的假设, 则费马小定理及其引理将都不成立.
   (a)费马小定理: 若p 是一个素数且a 是一个整数, 则$p\mid a^p-a$.
   (b)引理: 若p 是一个素数且$0<k<p$, 则$p\mid\binom{p}{k}$.
   (a) $p=4, a=2, a^p-a=16-2=14$
   4不整除14, 不成立
   (b) $p=4, k=2, 0<2<p$, $\binom{4}{2}=6$, 4不整除6, 不成立

8. 证明: 课件14页Bezout定理.(提示:参考最大公约数的存在性证明)

9. 证明: 素因数分解的存在性.(提示: 归纳法) 9. 证明$n\ge 2$都可被分解为素因数乘积
   $n=2$, 2为素数, 成立
   令$n=k$, $k\ge 2$, 假设该数可以被分解为素数乘积
   当$n=k+1$时, $\begin{cases} k+1\text{为素数, 素因数为本身} \\ k+1\text{非素数}, k+1=a\times b, a,b<k+1 \end{cases}$
   由前文归纳假设, k以内的数都可以素因数分解
   $\therefore a, b$可以被分解为素因数乘积, 即$k+1$被分解为素因数乘积
   证毕, 素因数分解对任意整数$n\ge 2$成立

10. 补充阅读(如有兴趣): Sec. I.4末尾, pp. 10–12小字部分.

Discrete Mathematics homework 1.2

1 Lovasz et al., Sec. 6.6, 第 100-103 页

必做：

1. 证明：如果 a 和 b 是正整数，且 $a \mid b$，则 $gcd(a, b) = a$。$a|b$，设 $b=k\cdot a$，$k\in N^*$，$gcd(a,b)$ 取所有公约数中最大的，且 b 为 a 的 k 倍，∴ a 是最大公约数
2. (a) 证明：$gcd(a, b) = gcd(a, b—a)$。(a) 设 $d=gcd(a,b)$，$d|a$，$d|b$，令 $r=b-a$ 则 $d|(b-a)$，$d|r$，$gcd(a,b)=gcd(a,b-a)$
   (b) 证明：设 r 为 b 除以 a 的余数，则 $gcd(a\ b) = gcd(a\ r)$。(b) 令 $gcd(a,b)=d$，$b>a$，$b=ad+r$，$r=b-ad$ $d|b$，$d|a$，且 $d|b-ad$，则 $d|r$，$gcd(a,r)=d=gcd(a,b)$ 证毕
3. (a) 证明：如果 a 为偶数且 b 为奇数，则 $gcd(a, b) = gcd(a/2, b)$。(a) 设 $d=gcd(a,b)$，$d\neq 2$，则 d 不受 2 影响，$gcd(a,b)=gcd(a/2,b)$
   (b) 证明：如果 a 和 b 都是偶数，则 $gcd(a, b) = 2gcd(a/2, b/2)$。$a,b$ 为偶数，则 $gcd(a,b)$ 至少包含因数 2，把 a,b 除以 2 后，求出 $a/2$，$b/2$ 的 gcd 再补上 2 仍成立，$gcd(a,b)=2gcd(a/2,b/2)$
4. 如果知道了两个整数的素因数分解，该如何表示它们的最小公倍数？$72=3^2\times 2^3$ $60=3^1\times 2^2\times 5^1$ $gcd=3^1\times 2^2=12$ 取相同指数后，再取指数的最小次方 $a=m_1^{a_1}\times\cdots\times m_n^{a_n}$ $b=m_1^{b_1}\times\cdots\times m_n^{b_n}$ $gcd(a,b)=m_1^{a_1}m_2^{b_2}\cdots(a_1<b_1, b_2<a_2\cdots)$
8. 证明对于某些任意大的正整数，即使其 g.c.d. 为 1，欧几里德算法 (Euclidean algorithm)) 也可以在两步终止（找一个大整数的例子使得辗转相除法可以在两次循环返回结果，包括 gcd 为 1 的情形）。

选做：

5. Suppose that you are given two integers, and you know the prime factorization of one of them. Describe a way of computing the greatest common divisor of these numbers.

6. Prove that for any two integers a and b, $gcd(a, b)lcm(a, b) = ab$.

7. Three integers a, b, and c form a Pythagorean triple if $a^2 + b^2 = c^2$.
   (a) Choose any three integers x, y, and z, and let $a = 2xyz$, $b = (x^2 - y^2)z$, $c = (x^2 + y^2)z$. Check that (a, b, c) is a Pythagorean triple.
   (b) Prove that all Pythagorean triples arise this way: If a, b, c are integers such that $a^2 + b^2 = c^2$, then there are other integers x, y, and z such thata, b, and c can be expressed by the formulas above.
   [Hint: First, show that the problem can be reduced to the case where $gcd(a, b, c) = 1$, a is even, and b, c are odd. Second, write $a^2 = (b—c)(b + c)$ and use this to argue that $(b + c)/2 and b—c)/2$ are squares.]

9. Describe the Euclidean Algorithm applied to two consecutive Fibonacci numbers. Use your description to show that the Euclidean Algorithm can take arbitrarily many steps.

11. Consider the following version of the Euclidean Algorithm to compute $gcd(a, b)$: (1) Swap the numbers if necessary to have $a \le b$; (2) if $a = 0$, then return b; (3) if $a \neq 0$, then replace b by $b—a$ and go to (1).
    (a) Carry out this algorithm to compute $gcd(19, 2)$.
    (b) Show that the modified Euclidean Algorithm always terminates with the right answer.
    (c) How long does this algorithm take, in the worst case, when applied to two 100-digit integers?