2 Lovasz et al., Sec. 6.7, 第 106-107 页

1. 对于 $12345 \equiv 54321(\text{mod m})$，求最大整数 m。

2. 以下哪些“规则”是正确的?

   (a) $a \equiv b$ (mod c) $\Rightarrow a + x \equiv b + x$ (mod c + x); ✗ $a+x \equiv b+x \pmod c$

   (b) $a \equiv b$ (mod c) $\Rightarrow ax \equiv bx$ (mod cx). ✓ $x \neq 0$

   (c) $\left.\begin{array}{l} a \equiv b(mod\ c) \\ x \equiv y(mod\ z) \end{array}\right\} \Rightarrow a+x \not\equiv b+y(mod\ c+z)$; ✗

   1 3 2 / 7 4 3 / 1+7 3+4 5

   (d) $\left.\begin{array}{l} a \equiv b(mod\ c) \\ x \equiv y(mod\ z) \end{array}\right\} \Rightarrow ax \equiv by(mod\ cz)$. ✗

   1 3 2 / 7 4 3 / 7 12 6

   $ax = by + blz + kcy + kclz$

   $a-b=kc,\ x-y=lz \quad a=b+kc.\ x=y+lz \quad ax-by=blz+kcy+kclz$ 并不能整除 cz

3. 如何定义 $a \equiv b(mod\ 0)$?

4. (a) 找到两个整数 a 和 b，使得 $2a \equiv 2b(\text{mod } 6)$，但 $a \not\equiv b$ (mod 6)。

   4. $a=7$ $b=28$ $2a \equiv 2b \pmod 6 = 2$ $a \pmod 6 = 1 \neq b \pmod 6 = 4$

   (b) 证明：如果 $c \neq 0$ 且 $ac \equiv bc(\text{mod mc})$, 那么 $a \equiv b$ (mod m)。

   设 $ac-bc=k \cdot mc$ $c(a-b)=c \cdot km$

   $c \neq 0$, 则 $a-b=km$, a和b的差是m的倍数,则 $a \equiv b \pmod m$

5. (选做)Let p be a prime. Show that if x, y, u, v are integers such that $x \equiv y$ (mod p), $u, v > 0$, and $u \equiv y$ (mod p-1), then $x^u \equiv y^v$ (mod p)。

3 Lovasz et al.,Sec. 6.10 Review Exercises, 第 122-123 页

必做:

4. 证明：如果 $a \mid b$ 且 $a \mid c$, 那么 $a \mid b^2 + 3c + 2^b c$。

5. 证明每个大于 3 的素数除以 6 的余数为 1 或 -1。

5. 大于3的素数,不会被2.3整除,设$n=6k$, $6k+1 \cdots 6k+5$

   $n=6k$, n是6的倍数,非素数

   $n=6k+2$, 2的倍数,非

   $n=6k+3$, 3的倍数,非

   $n=6k+4$, 2的倍数,非

   $n=6k+1$, $n \equiv 1 \pmod 6$, 有可能是素数

   $n=6k+5=6k-1$, $n \equiv -1 \pmod 6$,有可能为素数,证毕,余数为1或-1

9. 求素因数分解 (a) $\binom{20}{10}$；(b)20!

10. 证明：一个 30 位数的数字素数因子不会超过 100 个。

   10. 30位数, $10^{29} < n < 10^{30}-1$

   素数因子的最大数量用$\log n$估计, $\log n \approx \log 10^{30} = 30\log_2 10$

   $\approx 30 \times 2.3 = 69 < 100$ 证毕

13. 使用欧几里德算法求出 100 和 254 的 g.c.d.。

13、$254 \div 100 = 2 \cdots 54$

$100 \div 54 = 1 \cdots 46$

$54 \div 46 = 1 \cdots 8$

$46 \div 8 = 5 \cdots 6$

$8 \div 6 = 1 \cdots 2$

$6 \div 2 = 3 \cdots 0$

2

$\gcd(100, 254) = 2$

14. (a) 找出欧几里得算法执行 2 次步骤的整数对；

   (b) 找出欧几里得算法执行 6 次步骤的整数对。

$41 = 1 \times 25 + 16$ $16 = 9 \times 1 + 7$ $7 = 3 \times 2 + 1$ $\gcd(25, 41) = 1$

$25 = 1 \times 16 + 9$ $9 = 1 \times 7 + 2$ $2 = 2 \times 1 + 0$

17. 求整数 x 和 y，使得 $25x + 41y = 1$。

$1 = 7 - 3 \times 2 = 7 - 3 \times (9 - 1 \times 7) = 4 \times 7 - 3 \times 9 = 4 \times (16-9) - 3 \times 9 = 4 \times 16 - 7 \times 9$

$= 4 \times 16 - 7 \times (25-16) = 11 \times 16 - 7 \times 25 = 11 \times (41-25) - 7 \times 25$

$= 11 \times 41 - 18 \cdot 25$

$\therefore \begin{cases} x = -18 \\ y = 11 \end{cases}$

18. 求整数 x 和 y，使得 $2x + y \equiv 4$ (mod 17), $5x - 5y \equiv 9$ (mod 17).

$3^{-1} \equiv 6 \pmod{17}$

$5^{-1} \equiv 7 \pmod{17}$ $5(x-y) \cdot 5^{-1} \equiv 9 \cdot 5^{-1} \pmod{17} = x - y \equiv 63 \pmod{17}$ $\rightarrow 12 \pmod{17}$

即 $x - y \equiv 12 \pmod{17}$, $2x + y \equiv 4 \pmod{17}$ $3x \equiv 16 \pmod{17}$ $x \equiv 11 \pmod{17}$ $y \equiv 16 \pmod{17}$

20. 证明费马定理的两种形式定理 6.5.1 和 (6.1) 是等价的。

   (a) 定理 6.5.1: 若 p 是一个素数, 且 a 是一个整数，则 $p \mid a^p - a$。

   (b) 定理 (6.1): 若 p 是一个素数, 且 a 是不可被 p 整除的一个整数, 则 $p \mid a^{p-1} - 1$。

选做:

6. Let $a > 1$, and $k, n > 0$. Prove that $a^k - 1 \mid a^n - 1$ if and only if $k \mid n$.

8. How many integers are there that are not divisible by any prime larger than 20 and not divisible by the square of any prime?

12. Find the number of (positive) divisors of n, for $1 \leq n \leq 20$ (example: 6 has 4 divisors: 1, 2, 3, 6). Which of these numbers have an odd number of divisors? Formulate a conjecture and prove it.

Discrete Mathematics homework 1.3

---

1 Lang, Sec. I.5, 第13-15页

必做：

4. 设n为整数且$n \geq 2$。
   (a)证明任意整数x与唯一一个整数m对模n同余，其中$0 < m \leq n$。
   (b)证明任意与n互素的整数$x \neq 0$同与n 互素的唯一整数m同余，其中$0 < m < n$。
   (c)设$\varphi(n)$为 与n互 素 的 整 数m的 个 数， 其 中$0 < m < n$。我们称φ为欧拉phi函数，同时定义$\varphi(1) = 1$，如果$n = p$是素数，那么$\varphi(p)$是什么？
   (d)$1 \leq n \leq 10$, 确定每个整数n 的$\varphi(n)$。

6. 设a, b为非0整数且互素，证明$1/ab$可以被写为如下带有整数x, y的形式：

$$\frac{1}{ab} = \frac{x}{a} + \frac{y}{b}$$

9. 对于所有整数x, y 和所有素数p, 证明$(x + y)^p = x^p + y^p$ (mod p)。

$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k$　$\binom{p}{k} = C_p^k = \frac{p!}{k!(p-k)!}$，所有$\binom{p}{k}$都能被$p$整除，$1 \leq k \leq p-1$，$\binom{p}{k} \equiv 0 \pmod p$

10. 设n 为整数且$n \geq 2$。举例说明对于$1 \leq k \leq p^n - 1$, 二项式系数$\binom{p^n}{k}$ 不一定被p^n 整除。

即除了x^p和y^p之外都有$\binom{p}{k}$系数的项都被p整除
$\therefore (x+y)^p = x^p + \binom{p}{1} x^{p-1} y^1 + \cdots + \binom{p}{p-1} x^1 y^{p-1} + y^p$
$\equiv x^p + y^p \pmod p$

选做：

1. Let n, d be positive integers and assume $1 < d < n$. Show that n can be written in the form

$$n = c_0 + c_1 d + ... + c_k d^k$$

   with integers c_i, such that $0 \leq c_i < d$, and that these integers c_i are uniquely determined.
   [Hint: For the existence, write $n = qd + c_0$ by the Euclidean algorithm, and then use induction. For the uniqueness, use induction, assuming $c_0, ..., c_r$ are uniquely determined; show that c_{r+1} is then uniquely determined.]

7. Show that any rational number $a \neq 0$ can be written in the form

$$a = \frac{x_1}{p_1^{r_1}} + ... + \frac{x_n}{p_n^{r_n}}$$

   where $x_1, ..., x_n$ are integers, $p_1, ..., p_n$ are distinct prime numbers, and $r_1, ..., r_n$ are integers ≥ 0.

11. (a) Prove that a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
    (b) Prove that it is divisible by 9 if and only if the sum of its digits is divisible by 9.
    (c) Prove that it is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. In other words, let the integer be $n = a_k a_{k-1} ... a_0 = a_0 + a_1 10 + a_2 10^2 + ... + a_k 10^k, 0 \neq a_i \neq 9$.
    Then n is divisible by 11 if and only if $a_0 - a_1 + a_2 - a_3 + ... + (-1)^k a_k$ is divisible by 11.

2 Hardy & Wright, Sec. 5.4, 课件ch2第53页

1. 使用定理56证明定理57的特殊情况(即d = 1)。
   $kx \equiv l \pmod m$, $(k,m)=1$, $1 | l$, $k^{-1} \cdot (kx) \equiv k^{-1} l \pmod m$. $x \equiv k^{-1} l \pmod m$
   由定理56, $x - k^{-1} l \equiv 0 \pmod m$. 成立除非 $x = k^{-1} l$, 即只有一个
2. 验证从$kx \equiv \ell \pmod m$到$k'x \equiv \ell' \pmod{m'}$的消去率。

3 Hardy & Wright, Sec.5.5

1. 课件ch2幻灯片55页和56页示例。
   $\gcd(a,m)=1$, $\gcd(a+km, m)=1$, 即$a+km$与m互质
   最大公因数有$\gcd(a+km, m) = \gcd(a,m)$. $a+km$看作$a+m$的倍数, 即$\gcd(a+km, m)=1$
2. 课件ch2幻灯片57-58页，证明：
   $a_1' m + a_1 m' \equiv a_2' m + a_2 m' (mod\ mm') \implies a_1 m' \equiv a_2 m' (mod\ m)$.
   $(m,m')=1$, $(mm', m) = m$; $a_1' m \equiv 0 \pmod m$, $a_2' m \equiv 0 \pmod m$
   $a_1' m + a_1 m' \equiv a_2' m + a_2 m' \pmod m$, 左右消去$a_1' m$, $a_2' m$, 即$a_1 m' \equiv a_2 m' \pmod m$
3. 课件ch2幻灯片62页示例。

4. 课件ch2幻灯片63页，证明：$\phi(p^c) = p^c - p^{c-1}$.

选做：

(Hardy & Wright, Sec. 8.1 ,课件ch2第66页)