密码学组队学习第五期

Friday 15th September, 2023

1 Exercises

1. 令 $\lfloor x \rfloor$ 表示不超过 x 的最大整数。求证 $\lfloor (2+\sqrt{3})^n \rfloor$ 总是奇数，$n \geq 0$ 为整数。提示：考虑 $a_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$

2. 求满足 $\lfloor x/2 \rfloor + \lfloor x/3 \rfloor + \lfloor x/5 \rfloor = x$ 的所有整数 x。

3. 正整数 n 的 Cantor 展开为 $n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1!$，其中 $0 \leq a_j \leq j$ 且 $a_m \neq 0$。求证，每个正整数都有唯一的 Cantor 展开。

4. 令 $p_m > p_{m-1} > \cdots > p_1 > p_0 = 1$ 为严格单调递减的正整数序列。证明每个不超过 $p_m \cdots p_1$ 的正整数 n 都可以唯一表示为 $a_m p_{m-1} \cdots p_0 + a_{m-1} p_{m-2} \cdots p_0 + \cdots + a_1 p_0$ 的形式，其中 $0 \leq a_i < p_i$。

5. 令 a 是 4 位的十进制整数 (即 1000-9999)，不是 1111 的倍数（即其十进制位不全相同）。a' 是将 a 的十进制位从大到小排列得到的数，a'' 是将 a 的十进制位从小到大排列得到的数。定义 $T(a) = a' - a''$。例如 $T(3124) = 4321 - 1234 = 3087$。（1）证明 6174 是 T 的唯一不动点。该不动点也被称为 Kaprekar 常数。（2）证明，对于上述的 a，可以通过不停迭代 T 最终达到该不动点。即 $a, T(a), T(T(a)), \cdots, T^n(a), \cdots$ 最终以 6174 结尾。(3) 编程找出 1000-9999 中（除去 1111，2222 等 9 个数字）按照（2）的方式迭代，首次到达 6174 (即 $T^n(a) = 6174$ 的最小 n) 所需要的最大步数。

6. 证明，$Q_n = n! + 1$ 有大于 n 的素因子。该结论也可以说明素数有无穷多个。

7. 令 p_k 为第 k 个素数。证明 $p_n \le p_1 p_2 \cdots p_{n-1} + 1$ 成立。

8. 求证：如果正整数 n 的最小素因子 $p > \sqrt[3]{n}$，那么 n/p 为素数或者 1。

9. Dirichlet 定理表明，任意算术数列 $an+b, (a>0, n=1,2,\cdots)$ 当 $(a,b)=1$ 时都包含无穷多个素数。请依此证明，（1）对于任意的正整数 n，都存在（十进制表示下）以 n 个 1 结尾的素数。（2）对于任意的正整数 n，都存在（十进制表示下）包含 n 个连续的 1，并以 3 结尾的素数。

10. 验证，多项式 x^2-x+41 的取值在 $0 \le x \le 40$ 时是素数，在 $x=41$ 时是合数。

11. 求证，对于任意的整系数多项式 $f(x)=a_n x^n+\cdots+a_1 x+a_0$，$n \ge 1$，总存在正整数 y 使得 $f(y)$ 是合数。由此可知，不存在只生成素数的一元多项式。实际上存在一些只生成素数的函数，如 Mills 证明了，存在常数 Θ，使得 $\lfloor \Theta^{3^n} \rfloor$ 生成的都是素数，其中 $\Theta \approx 1.3064$。

12. 2013 年，张益唐在孪生素数猜想上取得了重大突破。请证明下面的"三胞胎素数定理"：形如 $(p, p+2, p+4)$ 的素数三元组只有 $(3,5,7)$。

13. 求证，如果 $n>1, k$ 为正整数，$a, a+k, \cdots, a+(n-1)k$ 都是奇素数，那么 k 能被所有小于 n 的素数整除。

14. 证明，$1+\frac{1}{2}+\cdots+\frac{1}{n}$ 对于 $n \ge 2$ 都不是整数。

15. 求 $(a^2+b^2, a+b)$ 所有可能的值。其中，$(a,b)=1$，且 $ab \ne 0$。

16. 如果整数 a,b,c 满足 $(a,b)=1, c|(a+b)$，那么 $(a,c)=(b,c)=1$。

17. 如果 b,c 为互素且都不为 0 的整数，那么 $(a,bc)=(a,b)(a,c)$。

18. 如果 $(a,b)=(a,c)=1$，那么 $(a,bc)=1$。

19. 如果 a,b,c,d 为整数，且 $b,d>0, (a,b)=(c,d)=1$ 且 $\frac{a}{b}+\frac{c}{d}$ 为整数，那么 $b=d$。

20. 证明下面的几个等式：

$$(a,b)=\begin{cases} a & a=b \\ 2(a/2,b/2) & a,b\text{都是偶数} \\ (a/2,b) & a\text{是偶数},b\text{是奇数} \\ (a-b,b) & a,b\text{都是奇数，且}a>b \end{cases}$$

根据上面的结论，设计一个只用到减法，奇偶性判定和除以 2 操作（移位）的最大公因子算法。该算法称为 Binary-GCD 算法。尝试将其推广到其他进制下（如三进制等）。

21. Fibonacci 数列：$F_n=F_{n-1}+F_{n-2},F_1=F_2=1$。已知 Fibonacci 数列的通项公式具有形式 $F_n=\alpha(\frac{1+\sqrt{5}}{2})^2+\beta(\frac{1-\sqrt{5}}{2})^2$，求常数 α 和 β。

22. 定义 $F_0=0$。证明：
    - $F_{n+3}+F_n=2F_{n+2}$，$F_{n+3}-F_n=2F_{n+1}$。
    - $F_{2n}=F_n^2+2F_{n-1}F_n$，$F_{n-2}+F_{n+2}=3F_n$。
    - $F_{2n+1}^2=F_{n+1}^2+F_n^2$，$F_{2n}=F_{n+1}^2-F_{n-1}^2$。

    关于 Fibonacci 数列，有许多非常有意思的性质和应用。大家可以网上去搜一下。

23. 下面两图是 $F_4=3,F_5=5,F_6=8$ 为边长的图形组成的。左图的面积为 $F_6^2=64$, 右图的面积为 $F_5(F_6+F_5)=F_5F_7=65$。请问多出来的面积是哪里来的?（提示：右图中的那些小图形，真的能覆盖这个长方形的区域吗?）证明 $F_{n-1}F_{n+1}-F_n^2=(-1)^n$，并依此不等式构造一些类似的例子。

24. 证明，利用欧几里得算法求 (F_{n+1},F_{n+2}) 恰好需要 n 步。并据此分析欧几里得算法的时间复杂度。

25. 证明，$(F_m,F_n)=F_{(m,n)}$。

26. 证明，$n!$ 中包含素数 p 的幂次为 $\lfloor\frac{n}{p}\rfloor+\lfloor\frac{n}{p^2}\rfloor+\lfloor\frac{n}{p^3}\rfloor+\cdots$。

27. 求 100000! 十进制表示中末尾的连续 0 的个数。

28. 求所有的正整数 n，满足 n 能被所有不超过 $\sqrt{n}$ 的正整数整除。

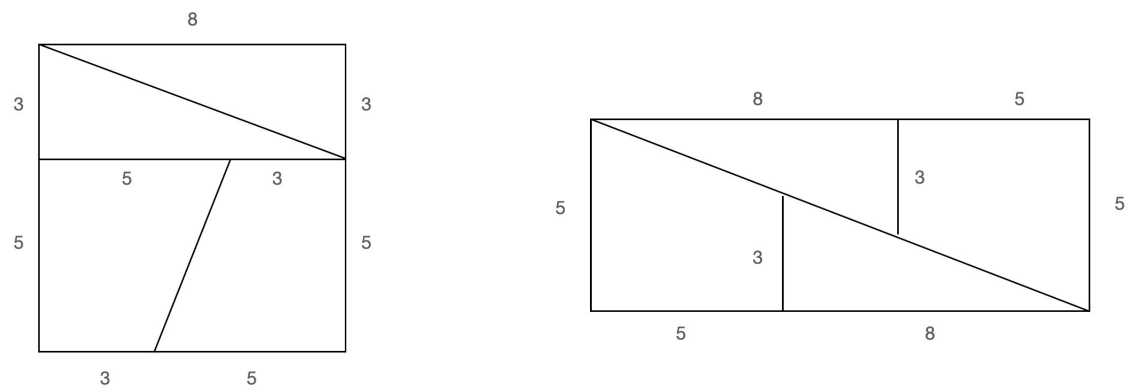

图 1: 23 题图

29. 令 n 为正整数。有多少对正整数 a, b 满足 a, b 的最小公倍数为 n。

30. 对于给定的正整数 a 和 b，考虑其对应的算术数列 $a, a+b, a+2b, \cdots$。证明，对任意的正整数 n，存在连续的 n 个数 $a+lb, a+(l+1)b, \cdots, a+(l+n-1)b$，这些数都是合数。

31. 求所有满足 $m^n = n^m$ 的整数解（注意，除非特别说明，0^0 是无意义的）。

32. 令 a, b 是互素的正整数。求使得 $ax + by = n$ 没有非负整数解 $x \geq 0, y \geq 0$ 的最大正整数 n 。该问题被称为 Frobenius 问题，是一个经典的困难问题。Frobenius 问题和格中的深洞 (deep hole) 问题有联系。

33. 我国古代数学家张丘建在《算经》一书中曾提出过著名的"百钱买百鸡"问题：鸡翁一，值钱五；鸡母一，值钱三；鸡雏三，值钱一。百钱买百鸡，则翁、母、雏各几何？请解答。

34. p 是奇素数。求证 $(a+b)^p \equiv a^p + b^p \mod p$。

35. 证明，对任意的正整数 m，总存在无穷多个 Fibonacci 数 F_n 能被 m 整除。

36. 利用中国剩余定理，证明存在任意长度的连续正整数，使得其中每个都有大于 1 的完全平方因子。即，对于任意的正整数 k，存在正整数 n，对任意的 $0 \leq l < k$，都存在整数 r，使得 $r^2 | n + l$。

37. a, b, c 是整数，且 $(a, b) = 1$。证明，存在整数 n，使得 $(an + b, c) = 1$。

38. 将中国剩余定理扩展到模数不是两两互素的情形。对于两个方程的情形，考虑下面的计算过程是否正确。如果正确，请证明。如果不正确，请指出问题在哪里。

    - $\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \end{cases}$
    - 令 $d = (m_1, m_2), m_1' = m_1/d, m_2' = m_2/d$。
    - 得到 $\begin{cases} x \equiv a_1 \mod m_1' \\ x \equiv a_2 \mod m_2' \\ x \equiv a_1 \mod d \\ x \equiv a_2 \mod d \end{cases}$
    - 如果最后两个式子不兼容，即 $a_1 \not\equiv a_2 \mod d$，则判定方程无解。否则，根据 $\begin{cases} x \equiv a_1 \mod m_1' \\ x \equiv a_1 \mod d \end{cases}$ 得到 $x \equiv a_1 \mod [m_1', d]$。类似地得到 $x \equiv a_2 \mod [m_2', d]$。即 $\begin{cases} x \equiv a_1 \mod [m_1', d] \\ x \equiv a_2 \mod [m_2', d] \end{cases}$
    - 虽然这时候两个模数仍然是不互素的，但是其乘积 $[m_1', d][m_2', d] < m_1 m_2 = m_1' m_2' d^2$，从而 $\frac{m_1 m_2}{[m_1', d][m_2', d]} \geq 2$。因此该过程是收敛的，且最多迭代 $\log_2(d)$ 次。实际上每次都迭代过程，都消耗掉最少 d 的一个素因子。因此经过一定步数之后，两个模数就互素了。此时再利用中国剩余定理求解。

39. 中国剩余定理中，如果模数不是两两互素的，但是每个模数的素因子分解是已知的，请给出一个高效的求解算法。

40. 证明，如果 $n > 4$ 是合数，那么 $(n-1)! \equiv 0 \mod n$。

41. 证明：如果 $(a, 42) = 1$，则 $168 | (a^6 - 1)$。

42. 如果 p 是素数，$p \nmid ab$，且 $a^p \equiv b^p \mod p$，那么 $a^p \equiv b^p \mod p^2$。

43. 如果素数 $p > 3$，那么 $2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \mod p$。

44. 对于哪些 n, $n^4 + 4^n$ 是素数？（答案是“不存在这样的 n”，试证明之）

45. 证明，对于正整数 $n \geq 2$，$n \nmid (2^n - 1)$。

46. 如果 p 是奇素数，证明 $((p-1)!)^{p^{n-1}} \equiv -1 \mod p^n$。

47. 如果 $(a,n)=1$，且 $n>1$，则 n 是素数当且仅当 $(x-a)^n$ 与 $x^n - a$ 作为多项式模 n 同余（即两个多项式的同次项的系数都是同余的）。这个是 AKS（素性判定）算法的出发点。

48. 求 $(n!+1,(n+1)!)$。

49. 求 $7^{987654321}$（十进制表示下）的倒数第 6 位数字。

50. 设 $n = p_1 p_2 \cdots p_k$ 是不同的奇素数 $p_1, \cdots, p_k$ 的乘积。证明 $a^{\varphi(n)+1} \equiv a \mod n$。

51. 证明中国剩余定理的解还可以写成 $x \equiv a_1 M_1^{\varphi(m_1)} + a_2 M_2^{\varphi(m_2)} + \cdots + a_r M_r^{\varphi(m_r)} \mod M$。

52. 证明 $a^m \equiv a^{m-\varphi(m)} \mod m$ 对任意的正整数 $m > 1$ 和 a 成立。

53. 求所有满足下面条件的正整数 n：

    - $\varphi(n) = 6, 14, 24$。
    - $\varphi(3n) = 3\varphi(n)$。
    - $\varphi(n) = n/2$。
    - $\varphi(n) | n$。
    - $\varphi(n) = 2^k$。
    - $\varphi(n^k) = n^{k-1}\varphi(n)$，$k$ 是正整数。

54. 如果 n 是合数，且 $\varphi(n)|(n-1)$，则 n 无平方因子且是至少三个不同素数的乘积。

55. 如果 $(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1$，证明 $\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\mathrm{ord}_n(b)$。

56. 假设 p 是费马数 $(2^{2^n}+1)$ 的一个素因子。证明：$\mathrm{ord}_p(2) = 2^{n+1}$，从而 $2^{n+1}|(p-1)$，即 p 必为形如 $2^{n+1}k+1$ 的素数。

57. 令 $m = a^n - 1$，证明 $\mathrm{ord}_m(a) = n$，于是 $n|\varphi(m) = \varphi(a^n - 1)$。

58. 请写出所有 $x^n + y^n = z^n, n \geq 2$ 的非平凡整数解 $xyz \neq 0$ 。

59. 请证明，$\mathrm{ord}_{2^k}(3) = 2^{k-2}, k \geq 3$。

60. 假定 $n = p_1^{e_1} \cdots p_r^{e_r}$ 是 n 的素因子分解，其中 $e_i > 0$，p_i 为互不相同的素数。请利用中国剩余定理证明 $\varphi(n) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r})$。

61. 假如 p 是大于 7 的素数。请证明 (提示：用原根的存在性，或者以后要讲到的 Legendre 符号)：

    1. 总存在 $a \neq 0$ 使得 $x^2 \equiv a \mod p$ 且 $y^2 \equiv a+1 \mod p$ 同时有解 (x,y)。
    2. 总存在 $a \neq 0$ 使得 $x^2 \equiv a \mod p$ 且 $y^2 \equiv a+2 \mod p$ 同时有解 (x,y)。
    3. 总存在 $a \neq 0$ 使得 $x^2 \equiv a \mod p$ 且 $y^2 \equiv a+3 \mod p$ 同时有解 (x,y)。

2 数学游戏

以下是几个数论游戏，大家可以挑战一下。

1. Nim. 有若干堆石子，每堆石子的数量有限。两个人轮流取石子，每次只能从一堆石子中取，至少取走一颗石子。取到最后一颗石子的人获胜。假设有 r 堆石子，每堆石子的数目分别是 $n_1, \cdots, n_r$。A 先取，B 后取。哪些情况下，A 有必胜策略？哪些情况下，B 有必胜策略？例如，假设有两堆石子，各有 n 颗石子，那么 B 有必胜策略。因为 A 不论怎么取，B 都可以保证自己取完后，两堆剩下的石子数目是一样的，直到游戏结束。

2. The Game of Euclid. 给定两个正整数，以下的操作称为是一次移动：将其中较大的数，减去较小数的某个整数倍 (保证结果仍然是非负的)，用得到的数替换原来那个较大的数。换句话说，$\{x,y\} \to \{x-ty, y\}$，其中 $x \geq y, x-ty \geq 0$，$t \geq 1$ 是正整数。A 和 B 轮流进行上述操作（A 先开始）。当某个玩家不能再进行移动时候，则判定该玩家输（显然，当某个玩家通过一次移动，将其中某个数变成 0 时候，则该玩家获胜，游戏结束）。假定游戏以正整数 a, b 开局，哪些情况下，A 有必胜策略？哪些情况下，B 有必胜策略。例如，当 $a = b$

时候，A 有必胜策略，因为显然 A 只有一种走法，$(a, a) \to (0, a)$。$S(n) = \sum_{1 \le a, b \le n,\ \text{A 有必胜策略的开局状态}(a,b)} (a+b)$。请编程计算 $S(10^8)$。

3. Taxman. 给定整数 n，你和收税人按照如下规则取走 $1 \sim n$ 之间的数字：

   - 每当你取一个数字，收税人取它所有剩下（还没有被取走）的因子。
   - 当你取某个数的时候，必须保证收税人能够取走至少一个数字，否则你不能取走这个数。
   - 当你没有数字可以取的时候，收税人取走所有剩下没被取走的数字。

   你和收税人的得分就是你们各自取走的数字之和。得分高的人获胜。你能打败收税人吗?在线试一试:https://www.cryptool.org/en/cto/taxman