HW8

4.2Exercise

26

26. Use Algorithm 5 to find $11^{644} \bmod 645$.

answer

$644 = (1010000100)_2$
$11 \equiv 11 \pmod{645}$
$11^2 \equiv 121 \pmod{645}$
$11^4 \equiv 451 \pmod{645}$
$11^8 \equiv 226 \pmod{645}$
$11^{16} \equiv 121 \pmod{645}$
$11^{32} \equiv 451 \pmod{645}$
$11^{64} \equiv 226 \pmod{645}$
$11^{128} \equiv 121 \pmod{645}$
$11^{256} \equiv 451 \pmod{645}$
$11^{512} \equiv 226 \pmod{645}$

$11^{644} \equiv 226 * 121 * 451 \pmod{645}$
$11^{644} \equiv 1 \pmod{645}$

55

$*$ 55. Describe an algorithm that finds the Cantor expansion of an integer.

answer

```
answer = 0
fact = 1
for i from 1 to n:
    answer = answer + a[i] * fact
    fact = fact * i
```

64

$*$ 64. Show that Algorithm 5 uses $O((\log m)^2 \log n)$ bit operations to find $b^n \bmod m$.

answer

```
procedure modular_exponentiation(b, n, m)
    x = 1
    power = b mod m

    for i = 0 to k-1 do
        if a[i] = 1 then
            x = (x * power) mod m
        endif
        power = (power * power) mod m
    return x
```

$$n = (a_{k-1}a_{k-2}...a_1a_0)_2$$
$$k = \lceil \log n \rceil$$

so Algorithm 5 is $O(\log n)$

note

这里的解答不完整。
实际上是对m取模运算的bit operation的操作的复杂度大致是$O((\log m)^2)$
数字位数：
如果两个数各有 L 位（其中 $L = O(\log m)$），那么它们的乘积最多会有 $2L$ 位。

普通乘法复杂度：
采用传统的乘法算法（如"长乘法"），计算两个 L 位数的乘积需要大约 $O(L^2)$ 位运算。也就是说，乘法的复杂度为 $O((\log m)^2)$。

模乘运算：
模乘运算通常包括两步：

计算乘积 $a \times b$，复杂度为 $O((\log m)^2)$ 位运算。

对乘积取模（通常通过除法运算实现），这部分复杂度一般不会超过乘法的复杂度，也大致为 $O((\log m)^2)$ 位运算。

因此，总的来说，每次模乘运算的位运算复杂度是 $O((\log m)^2)$。
所以最终复杂度是$O((\log m)^2 \log n)$

4.3Exercise

13

$*$ 13. Prove or disprove that there are three consecutive odd positive integers that are primes, that is, odd primes of the form p, $p+2$, and $p+4$.

answer

$3, 5, 7$

Q.E.D

21

The value of the Euler ϕ-function at the positive integer n is defined to be the number of positive integers **less than or equal to** n that are **relatively prime** to n. For instance, $\phi(6)=2$ because of the positive integers less or equal to 6, only 1 and 5 are relatively prime to 6. [Note: ϕ is the Greek letter phi.] 21. Find these values of the Euler ϕ-function.

- a) $\phi(4)$
- b) $\phi(10)$

- c) $\phi(13)$

answer

- a) $\phi(4) = 2$
- b) $\phi(10) = 4$
- c) $\phi(13) = 12$

57

$*$ 57. Prove that the set of positive rational numbers is countable by showing that the function K is a one-to-one correspondence between the set of positive rational numbers and the set of positive integers if
$K(m/n) = p_1^{2a_1} p_2^{2a_2} \cdot \ldots \cdot p_s^{2a_s} q_1^{2b_1-1} q_2^{2b_2-1} \cdot \ldots \cdot q_t^{2b_t-1}$,
where $\gcd(m, n) = 1$ and the prime-power factorizations of m and n are
$m = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}$ and $n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$.

answer

- injective: if $\frac{m_1}{n_1} \neq \frac{m_2}{n_2}$, then $K(\frac{m_1}{n_1}) \neq K(\frac{m_2}{n_2})$
  Pf: By contrapositive, we show that if $K(\frac{m_1}{n_1}) = K(\frac{m_2}{n_2})$, then $\frac{m_1}{n_1} = \frac{m_2}{n_2}$
  We note that $K(\frac{m_1}{n_1}) = K(\frac{m_2}{n_2}) = k$.
  By prime factorization， $k = p_{k_1}^{a_1} p_{k_2}^{a_2} p_{k_3}^{a_3} ... p_{k_n}^{a_n}$
  we classify p_{k_i} by the rule that p_{m_i} (a_i is even) and p_{n_i} (a_i is odd).
  then $m_1 = m_2 = p_{m_1}^{a_{m_1}/2} p_{m_2}^{a_{m_2}/2} ... p_{m_{n_m}}^{a_{m_{n_m}}/2}$
  then $n_1 = n_2 = p_{n_1}^{(a_{n_1}+1)/2} p_{n_2}^{(a_{n_2}+1)/2} ... p_{n_{n_n}}^{(a_{n_{n_n}}+1)/2}$
  so $\frac{m_1}{n_1} \neq \frac{m_2}{n_2}$
- surjective: For any positive integer k, there exist n, m, $k = K(\frac{m}{n})$
  Pf:
  By prime factorization， $k = p_{k_1}^{a_1} p_{k_2}^{a_2} p_{k_3}^{a_3} ... p_{k_n}^{a_n}$
  we classify p_{k_i} by the rule that p_{m_i} (a_i is even) and p_{n_i} (a_i is odd).
  then $m = p_{m_1}^{a_{m_1}/2} p_{m_2}^{a_{m_2}/2} ... p_{m_{n_m}}^{a_{m_{n_m}}/2}$
  then $n = p_{n_1}^{(a_{n_1}+1)/2} p_{n_2}^{(a_{n_2}+1)/2} ... p_{n_{n_n}}^{(a_{n_{n_n}}+1)/2}$
  so $k = K(m/n)$
  Q.E.D

4.4Exercise

9

9. Solve the congruence $4x \equiv 5 \pmod{9}$ using the inverse of 4 modulo 9 found in part (a) of Exercise 5.

answer

$4 \equiv 7^{-1} \pmod{9}$
$7 * 4x \equiv 7 * 5 \pmod{9}$
$x \equiv 8 \pmod{9}$

21

21. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences

- $x \equiv 1 \pmod{2}$
- $x \equiv 2 \pmod{3}$
- $x \equiv 3 \pmod{5}$
- $x \equiv 4 \pmod{11}$.

answer

$M = 2 * 3 * 5 * 11 = 330$
$M_1 = 165$
$M_2 = 110$
$M_3 = 66$
$M_4 = 30$

$M_1 y_1 \equiv 1 \pmod{2}$
$M_2 y_2 \equiv 1 \pmod{3}$
$M_3 y_3 \equiv 1 \pmod{5}$
$M_4 y_4 \equiv 1 \pmod{11}$

$y_1 = 1$
$y_2 = 2$

$y_3 = 1$
$y_4 = 7$

$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 = 1643$
$x \equiv 323 \pmod{330}$

27

$*$ 27. Find all solutions, if any, to the system of congruences $x \equiv 7 \pmod 9$, $x \equiv 4 \pmod{12}$, and $x \equiv 16 \pmod{21}$.

answer

$x = 9x_1 + 7 = 12x_2 + 4 = 21x_3 + 16$
So $9x_1 = 6 = 12x_2 + 3 = 21x_3 + 15$
So $3x_1 + 2 = 4x_2 + 1 = 7x_3 + 5$
So there exist y
$y \equiv 2 \pmod 3$
$y \equiv 1 \pmod 4$
$y \equiv 5 \pmod 7$
$x = 3y + 1$

Then by chinese remainder theorem,
$y = 257 + 84n$
$x = 772 + 252n$
So
$x \equiv 16 \pmod{252}$

33

33. Use Fermat's little theorem to find $7^{121} \bmod 13$.

answer

$7^{12} \equiv 1 \pmod{13}$
$7^{120} \equiv 1 \pmod{13}$

$$7^{121} \equiv 7 \pmod{13}$$