ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

Bài tập tuần 1

Tính chất chia hết trên vành số nguyên

Môn học: Nhập môn mã hóa mật mã

CSC15005_22MMT

Sinh viên:
Nguyễn Hồ Đăng Duy
22127085
22MMT

Giảng viên hướng dẫn:
Nguyễn Đình Thúc
Trần Hà Sơn
Nguyễn Văn Quang Huy

Ngày 14 tháng 10 năm 2024

Mục lục

1 Bài 1 **2**

2 Bài 2 **3**

3 Bài 3 **4**

4 Bài 4 **6**

5 Bài 5 **7**

6 Bài 6 **8**

7 Bài 7 **9**

1 Bài 1

Hãy chứng minh rằng mọi hợp số n đều có ước nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$

Vì n là hợp số nên tồn tại a và b sao cho $n = a.b$ $(1 < a \leqslant b < n)$.
Giả sử cả a và b đều lớn hơn $\sqrt{n}$. Điều này có nghĩa là:

$$a > \sqrt{n} \text{ và } b > \sqrt{n}$$

Khi đó, ta có:

$$a.b > \sqrt{n}.\sqrt{n} = n$$

Điều này mâu thuẫn với dữ kiện $n = a.b$. Do đó, giả thiết ban đầu sai. Nghĩa là ít nhất một trong 2 số a hoặc b phải nhỏ hơn hoặc bằng $\sqrt{n}$.
Nếu $a \leqslant \sqrt{n}$ thì a có thể là một số nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$. Nếu a không phải là một số nguyên tố, ta có thể phân tích tiếp a thành tích của các số nguyên tố và chắc chắn một trong các ước nguyên tố này của a sẽ nhỏ hơn hoặc bằng $\sqrt{n}$
Kết luận: Mọi hợp số n đều có ít nhất một ước nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$

2 Bài 2

Áp dụng thuật toán Euclide, hãy tìm ước chung lớn nhất của các cặp số sau:

a) a = 252, b = 198

$$\begin{aligned} 252 &= 198.1 + 54 \\ 198 &= 54.3 + 36 \\ 54 &= 36.1 + +18 \\ 36 &= 18.2 + 0 \end{aligned}$$

Suy ra, $gcd(252, 198) = 18$

b) a = 16261, b = 85652

$$\begin{aligned} 85652 &= 16261.5 + 4347 \\ 16261 &= 4347.3 + 3220 \\ 4347 &= 3220.1 + +1127 \\ 3220 &= 1127.2 + 966 \\ 1127 &= 966.1 + 161 \\ 966 &= 161.6 + 0 \end{aligned}$$

Suy ra, $gcd(16261, 85652) = 161$

c) a = 139024789, b = 93278890

$$\begin{aligned} 139024789 &= 93278890.1 + 45745899 \\ 93278890 &= 45745899.2 + 1787092 \\ 45745899 &= 1787092.25 + +1068599 \\ 1787092 &= 1068599.1 + 718493 \\ 1068599 &= 718493.1 + 350106 \\ 718493 &= 350106.2 + 18281 \\ 350106 &= 18281.19 + 2767 \\ 18281 &= 2767.6 + 1679 \\ 2767 &= 1679.1 + 1088 \\ 1679 &= 1088.1 + 591 \\ 1088 &= 591.1 + 497 \\ 591 &= 497.1 + 94 \\ 497 &= 94.5 + 27 \\ 94 &= 27.3 + 13 \\ 27 &= 13.2 + 1 \\ 13 &= 1.13 + 0 \end{aligned}$$

Suy ra, $gcd(139024789, 93278890) = 1$

3 Bài 3

Áp dụng thuật toán Eudlide mở rộng, với các cặp số (a, b) ở bài tập 2, hãy tìm một cặp số (x, y) thỏa

$$ax + by = d,$$

trong đó d là ước chung lớn nhất của a và b.

a) a = 252, b = 198

Từ kết quả bài 2, ta có $d = 18$.
Gán $(x_0, y_0, r_0) = (1, 0, 252)$ và $(x_1, y_1, r_1) = (0, 1, 198)$
Ta có:

$$\begin{aligned}(1,0,252) - 1.(0,1,198) &= (1,-1,54)\\ (0,1,198) - 3.(1,-1,54) &= (-3,4,36)\\ (1,-1,54) - 1.(-3,4,36) &= (4,-5,18)\\ (-3,4,36) - 2.(4,-5,18) &= (-11,14,0)\end{aligned}$$

Vậy $(x, y) = (4, -5)$ thì $252.4 + 198.(-5) = 18$

b) a = 16261, b = 85652

Từ kết quả bài 2, ta có $d = 161$.
Gán $(x_0, y_0, r_0) = (1, 0, 85652)$ và $(x_1, y_1, r_1) = (0, 1, 16261)$
Ta có:

$$\begin{aligned}(1,0,85652) - 5.(0,1,16261) &= (1,-5,4347)\\ (0,1,16261) - 3.(1,-5,4347) &= (-3,16,3220)\\ (1,-5,4347) - 1.(-3,16,3220) &= (4,-21,1127)\\ (-3,16,3220) - 2.(4,-21,1127) &= (-11,58,966)\\ (4,-21,1127) - 1.(-11,58,966) &= (15,-79,161)\\ (-11,58,966) - 6.(15,-79,161) &= (-101,532,0)\end{aligned}$$

Vậy $(x, y) = (-79, 15)$ thì $16261.(-79) + 85652.15 = 161$

c) a = 139024789, b = 93278890

Từ kết quả bài 2, ta có $d = 1$.
Gán $(x_0, y_0, r_0) = (1, 0, 139024789)$ và $(x_1, y_1, r_1) = (0, 1, 93278890)$

Ta có:

$$\begin{aligned}
(1, 0, 139024789) - 1.(0, 1, 93278890) &= (1, -1, 45745899) \\
(0, 1, 93278890) - 2.(1, -1, 45745899) &= (-2, 3, 1787092) \\
(1, -1, 45745899) - 25.(-2, 3, 1787092) &= (51, -76, 1068599) \\
(-2, 3, 1787092) - 1.(51, -76, 1068599) &= (-53, 79, 718493) \\
(51, -76, 1068599) - 1.(-53, 79, 718493) &= (104, -155, 350106) \\
(-53, 79, 718493) - 2.(104, -155, 350106) &= (-261, 389, 18281) \\
(104, -155, 350106) - 19.(-261, 389, 18281) &= (5063, -7546, 2767) \\
(-261, 389, 18281) - 6.(5063, -7546, 2767) &= (-30639, 45665, 1679) \\
(5063, -7546, 2767) - 1.(-30639, 45665, 1679) &= (35702, -53211, 1088) \\
(-30639, 45665, 1679) - 1.(35702, -53211, 1088) &= (-66341, 98876, 591) \\
(35702, -53211, 1088) - 1.(-66341, 98876, 591) &= (102043, -152087, 497) \\
(-66341, 98876, 591) - 1.(102043, -152087, 497) &= (-168384, 250963, 94) \\
(102043, -152087, 497) - 5.(-168384, 250963, 94) &= (943963, -1406902, 27) \\
(-168384, 250963, 94) - 3.(943963, -1406902, 27) &= (-3000273, 4471669, 13) \\
(943963, -1406902, 27) - 2.(-3000273, 4471669, 13) &= (6944509, -10350240, 1) \\
(-3000273, 4471669, 13) - 13.(6944509, -10350240, 1) &= (-93278890, 139024789, 0)
\end{aligned}$$

Vậy $(x, y) = (6944509, -10350240)$ thì $139024789.6944509 + 93278890.(-10350240) = 1$

4 Bài 4

Từ bài tập số 2, hãy chứng minh rằng giả sử có hai số nguyên a < b, khi đó số các phép tính bit cần thiết để thực hiện thuật toán Euclide là $O((log_2 a)^3)$.

Đầu tiên, ta chứng minh:
(1) Trong mỗi bước của thuật toán Euclid, số lớn sẽ giảm đi ít nhất một nửa.
Giả sử, sau bước đầu tiên ta có

$$b = a.q + r \ (0 \leqslant r < a) \text{ hay } r = b - a.q$$

Vì q là số nguyên, ta có thể viết $r < a$
Nếu $q \geqslant 2$ thì

$$r = b - a.q \leqslant b - 2.a$$

Điều này cho thấy nếu a không quá lớn so với a thì trong trường hợp xấu nhất, số lớn (b) sẽ giảm đi ít nhất một nửa. Do đó, trong mọi trường hợp, sau mỗi bước lặp lại của thuật toán Euclid, số lớn sẽ giảm đi ít nhất một nửa.
(2) Chi phí của một phép chia 2 số n bit là $O(n^2)$
Thuật toán chia bit gồm các phép toán như sau:

- **So sánh:** So sánh số bị chia với số chia → Chi phí cho mỗi lần lặp $O(n)$.
- **Trừ:** Nếu số bị chia lớn hơn hoặc bằng số chia, thực hiện phép trừ và ghi lại một chữ số vào thương → Chi phí cho mỗi lần lặp $O(n)$.
- **Nhân::** Nhân số chia với chữ số vừa ghi vào thương → Chi phí cho mỗi lần lặp $O(n)$.
- **Lặp lại:** Tiếp tục các bước trên cho đến khi số bị chia nhỏ hơn số chia.

Số lần lặp của thuật toán phụ thuộc vào độ lớn của số bị chia so với số chia. Trong trường hợp xấu nhất, số lần lặp có thể lên đến n lần, với n là số bit của số bị chia.
Trong mỗi lần lặp, chúng ta thực hiện một phép so sánh, một phép trừ và một phép nhân. Do đó chi phí của mỗi lần lặp là $O(n)$.
Vì có tối đa n lần lặp ⇒ Tổng chi phí của phép chia là $O(n) * O(n) = O(n^2)$

Chứng minh đề bài
Từ **(1)**, giả sử a có n bit. Để a giảm xuống còn 1, cần tối đa $log_2 a$ bước. Mỗi bước chia, ta thực hiện phép chia 2 số có độ dài bit tối đa là n. Từ **(2)**, ta biết một phép chia 2 số n bit có chi phí là $O(n^2)$.
Vậy tổng sô phép tính bit là:

- Tối đa $log_2 a$ bước.
- Mỗi bước có chi phí $O(n^2)$.

Do đó, tổng chi phí là $O(n^2 * log_2 a$. Mà $n = log_2 a$ nên tổng chi phí là $O((log_2 a)^3)$

5 Bài 5

Hãy chứng minh rằng có thể tìm ước chung lớn nhất của hai số nguyên dương bằng thuật toán sau:

$$(\mathbf{a},\mathbf{b}) = \begin{cases} \mathbf{a} & \textbf{nếu a = b}, \\ \mathbf{2 \cdot gcd(a/2, b/2)} & \textbf{nếu a và b chẵn}, \\ \mathbf{gcd(a/2, b)} & \textbf{nếu a chẵn, b lẻ}, \\ \mathbf{gcd(a - b, b)} & \textbf{nếu a và b lẻ}. \end{cases}$$

Khi $a = b$ thì thuật toán sẽ trả về a. Điều này hiển nhiên đúng vì a chính là ước chung lớn nhất của a và b trong trường hợp này.
Giả sử thuật toán đúng với mọi cặp số (a', b') mà $a' + b' < a + b$.
Ta tiến hành xét các trường hợp của thuật toán như sau:
a) a, b đều chẵn
Đặt $a' = a/2, b' = b/2$. Theo giả thiết quy nạp, thuật toán tìm đúng $gcd(a', b')$
Mặt khác, ta có quan hệ giữa $gcd(a, b)$ và $gcd(a', b')$ như sau:

1. *Mọi ước chung của a và b cũng là ước chung của a' và b':*
   - Nếu d là ước chung của a và b, tức là $a = dx, b = dy$ (với x, y là các số nguyên).
   - Khi đó, $a' = a/2 = dx/2, b' = b/2 = dy/2$
   - Điều này có nghĩa là d cũng là ước của a' và b' (vì a, b chẵn)
2. *Ngược lại, mọi ước chung của a' và b' khi nhân với 2 sẽ là ước chung của a và b*
   - Nếu d' là ước chung của a' và b', tức là $a' = d'x', b' = d'y'$ (với x', y' là các số nguyên).
   - Khi đó, $a = 2a' = 2d'x', b = 2b' = 2d'y'$
   - Điều này có nghĩa là $2'd$ cũng là ước của a và b

Từ hai quan sát trên, ta thấy rằng tập hợp các ước chung của a và b chỉ khác tập hợp các ước chung của a' và b' ở chỗ mỗi phần tử trong tập hợp thứ hai được nhân thêm 2. Do đó, $gcd(a, b) = 2gcd(a', b')$
b) a chẵn, b lẻ
Tương tự đặt $a' = a/2$. Theo giả thiết quy nạp, thuật toán tìm đúng $gcd(a', b)$. Vì các ước chung của a và b cũng là ước chung của a' và b nên $gcd(a, b) = gcd(a', b)$
c) a, b đều lẻ
Đặt $a' = a - b$. Theo giả thiết quy nạp, thuật toán tìm đúng $gcd(a', b)$.
Giả sử d là một ước chung của a và b, tức là a chia hết cho d và b cũng chia hết cho d. Vì $a' = a - b$ nến a' cũng chia hết cho d. Do đó, d là ước chung cả cả a' và b.
Chứng minh tương tự ta có kết quả mọi ước chung của a' và b cũng là ước của a và b.
Vì 2 tập hợp ước chung giống nhau nên ước chung lớn nhất của chúng cũng giống nhau. Do đó $gcd(a, b) = gcd(a', b)$.

Từ các chứng minh trên, ta có thể kết luận thuật toán đề bài là đúng.

6 Bài 6

Hãy cài đặt thuật toán Euclide mở rộng bằng C/C + +, Java hoặc Python. Kiểm tra chương trình với các cặp số (a, b) ở bài tập 2.

Thuật toán sau đây được cài đặt dựa trên slide **Quan hệ chia hết trên tập số nguyên**, gồm có các bước sau

- **Bước 1:** Gán $(x_0, y_0, r_0) = (1, 0, a)$ và $(x_1, y_1, r_1) = (0, 1, b)$
- **Bước k:** Gán $(x_k, y_k, r_k) = (x_{k-2} - x_{k-1} * q_{k-1}, y_{k-2} - y_{k-1} * q_{k-1}, r_{k-2} - r_{k-1} * q_{k-1})$ trong đó $q_{k-1} = \left[\frac{r_{k-2}}{r_{k-1}}\right]$

```python
def extended_gcd_iterative(a, b):
    x0, y0, r0 = 1, 0, a
    x1, y1, r1 = 0, 1, b

    while r1 != 0:
        q = r0 // r1

        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
        r0, r1 = r1, r0 - q * r1

    return r0, x0, y0
```

Sau khi thử lại với các cặp số (a,b) ở bài tập 2:

```python
# a) a = 252, b = 198
a = 252
b = 198
gcd, x, y = extended_gcd_iterative(a, b)
print(f"a) gcd({a},{b}) = {gcd}, x = {x}, y = {y}")

# b) a = 16261, b = 85652
a = 16261
b = 85652
gcd, x, y = extended_gcd_iterative(a, b)
print(f"b) gcd({a},{b}) = {gcd}, x = {x}, y = {y}")

# c) a = 139024789, b = 93278890
a = 139024789
b = 93278890
gcd, x, y = extended_gcd_iterative(a, b)
print(f"c) gcd({a},{b}) = {gcd}, x = {x}, y = {y}")
```

Thu được kết quả:

```
a) gcd(252,198) = 18, x = 4, y = -5
b) gcd(16261,85652) = 161, x = -79, y = 15
c) gcd(139024789,93278890) = 1, x = 6944509, y = -10350240
```

7 Bài 7

Hãy sửa đổi chương trình ở Bài 6 để nó trả về một số x > 0 (ax + by = gcd(a, b)) và x nhỏ nhất có thể.

Vì phương trình $a.x + b.y = gcd(a, b)$ vẫn đúng nếu chúng ta điều chỉnh x và y theo một cách nhất định nên ta có thể tìm một giá trị khác của x sao cho x trở thành số dương nhỏ nhất.
Nếu (x, y) là một nghiệm của phương trình, thì tất cả các nghiệm khác có thể được biểu diễn dưới dạng:

$$x' = x + k.(\frac{b}{gcd(a,b)}) \text{ và } y' = y - k.(\frac{a}{gcd(a,b)})$$

Với k là một số nguyên bất kỳ. Điều này có nghĩa là ta có thể thay đổi x bằng cách cộng thêm một số bội của $\frac{b}{gcd(a,b)}$ và điều chỉnh y tương ứng, mà vẫn giữ được phương trình ban đầu.
Để tìm k sao cho x' là số dương nhỏ nhất, ta đặt thêm điều kiện

$$x + k.(\frac{b}{gcd(a,b)}) > 0 \Leftrightarrow k(\frac{b}{gcd(a,b)}) > -x \Leftrightarrow k > \frac{-x}{(\frac{b}{gcd(a,b)})}$$

Từ đó, vì k là số nguyên, ta lấy giá trị k như sau để đảm bảo x' dương:

$$k = \left\lceil \frac{-x}{\frac{b}{gcd(a,b)}} \right\rceil = (\frac{-x}{\frac{b}{gcd(a,b)}}) + 1$$

Từ đó, có thể triển khai thuật toán như sau:

```
def find_min_x(a, b):
    gcd, x, y = extended_gcd_iterative(a, b)
    if x <= 0:
        k = (-x // (b // gcd)) + 1
        x += k * (b // gcd)
        y -= k * (a // gcd)
    return x
```

Sau khi thử lại với các ví dụ ở câu 2, thu được kết quả như sau

```
a) x = 4
b) x = 453
c) x = 6944509
```