Euler’s Theorem

Yan Huang

Objectives

- Exercises on extended Euclidean algorithms
- Exercises on applications of Chinese Remainder Theorem
- Fermat’s little Theorem and Euler’s Theorem
- Mental calculation on modulo arithmetic

Find $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$?

```
egcd :: Int -> Int -> (Int, Int, Int)
egcd a 1 = (0, 1, 1)
egcd a 0 = (1, 0, a)
egcd a b | a < b = let (x, y, d) = egcd b a in (y, x, d)
         | otherwise = let (x, y, d) = egcd b (a `mod` b)
                           q = a `div` b
                       in (y, x-y*q, d)
```

Find integer x, y such that

$$5*x + 7*y = 1$$

3 −2

```
egcd :: Int -> Int -> (Int, Int, Int)
egcd a 1 = (0, 1, 1)
egcd a 0 = (1, 0, a)
egcd a b | a < b = let (x, y, d) = egcd b a in (y, x, d)
         | otherwise = let (x, y, d) = egcd b (a `mod` b)
                           q = a `div` b
                       in (y, x-y*q, d)
```

egcd 5 7 → (x, y, 1)

① egcd 7 5 → (x1, y1, d)

→ ② egcd 5 2 → (x2, y2, d)

→ ③ egcd 2 1 → (x3, y3, d)

→ ④ (0, 1, 1)

$(x_3, y_3) = (1, 0)$

$(x_2, y_2) = (y_3, x_3 - y_3 \cdot (5 \text{ div } 2)) = (0, 1 - 0 \times 2) = (0, 1)$

$(x_1, y_1) = (y_2, x_2 - y_2 \times (7 \text{ div } 5)) = (1, 0 - 1 \times 1) = (1, -1)$

$(x, y) = (y_1, x_1 - y_1 \times q) = (-1, 1 - (-1) \times 1) = (-1, 2)$

Find integer x, y such that

$$12*x + 8*y = 4$$

```
egcd :: Int -> Int -> (Int, Int, Int)
egcd a 1 = (0, 1, 1)
egcd a 0 = (1, 0, a)
egcd a b | a < b = let (x, y, d) = egcd b a in (y, x, d)
         | otherwise = let (x, y, d) = egcd b (a `mod` b)
                           q = a `div` b
                       in (y, x-y*q, d)
```

egcd 12 8

→ egcd 8 4

→ egcd 4 0

→ (1, 0, 4)

= (x, y, d).

$(x_2, y_2) = (1, 0 - (x \cdot q))$

$= (1, 0 - (12 \text{ `div` } 8)) = (1, -1)$

$(x_1, y_1) = (y, x - y \cdot q) = (0, 1 - 0 \cdot q) = (0, 1)$

$8 \cdot x_1 + 4 \cdot y_1 = 4$

$12 x_2 + 8 y_2 = 4.$

Find integer x, y such that

$$27*x + 42*y = \gcd(27, 42)$$

```
egcd :: Int -> Int -> (Int, Int, Int)
egcd a 1 = (0, 1, 1)
egcd a 0 = (1, 0, a)
egcd a b | a < b = let (x, y, d) = egcd b a in (y, x, d)
         | otherwise = let (x, y, d) = egcd b (a `mod` b)
                           q = a `div` b
                       in (y, x-y*q, d)
```

egcd 27 42 → (−3, 2)

egcd 42 27 → (2, −1−2×1) = (2, −3)

egcd 27 15 → (−1, 1−(−1)·(27 `div` 15)) = (−1, 1+1) = (−1, 2)

egcd 15 12 → (1, 0−1×q) = (1, 0−1×(15 `div` 12)) = (1, −1)

egcd 12 3 → (0, 1−0·q) = (0, 1−0·(a `div` b)) = (0, 1)

(a = 12, b = 3; x y)

egcd 3 0 → (1, 0, 3)

Chinese Remainder Theorem

Assume n_1 and n_2 are coprime. Let x be the solution to the following systems of modulo identities

$$x = a_1 \mod n_1$$

$$x = a_2 \mod n_2.$$

$\begin{cases} x = 2 \mod 3 \\ x = 3 \mod 8 \end{cases}$

$x = 11$

Then $x = (X_2 n_2 a_1 + X_1 n_1 a_2) \bmod N$, where $N = n_1 \times n_2$ and $X_1 n_1 + X_2 n_2 = 1$.

$CRT(a_1, n_1, a_2, n_2) \rightarrow x$

$egcd(3, 8) \rightarrow (x_1, x_2)$.

Isomorphism

Let $\mathbb{G}, \mathbb{H}$ be groups with respect to the operations $\star_{\mathbb{G}}$ and $\star_{\mathbb{H}}$. A function $f: \mathbb{G} \to \mathbb{H}$ is an isomorphism if

1. f is a bijection, and
2. For all $g_1, g_2 \in \mathbb{G}$, $f(g_1 \star_{\mathbb{G}} g_2) = f(g_1) \star_{\mathbb{H}} f(g_2)$.

If there exists an isomorphism between $\mathbb{G}$ and $\mathbb{H}$, we say $\mathbb{G}$ and $\mathbb{H}$ are *isomorphic* and write $\mathbb{G} \simeq \mathbb{H}$.

The Isomorphism

$(i_1, j_1) \in \mathbb{Z}_p \times \mathbb{Z}_q$.

(i_2, j_2)

$(i_1, j_1) + (i_2, j_2) = ((i_1 + i_2) \bmod p,$

$(j_1 + j_2) \bmod p)$.

$\mathbb{Z}_{pq}$ $\xrightarrow{f(a) = (a \bmod p, a \bmod q)}$ $\mathbb{Z}_p \times \mathbb{Z}_q$

a $\longrightarrow$ $(a \bmod p, a \bmod q)$.

$\longleftarrow$

$f^{-1} = CRT(i, p, j, q)$ $(i \bmod p, j \bmod p)$

Using CRT to Simplify Modulo Computations

- Calculate

3299 mod 24

$24 = 3 \times 8$.

$\xrightarrow{f(3299)} (3299 \bmod 3,\ 3299 \bmod 8)$

$= (2, 3) \in \mathbb{Z}_3 \times \mathbb{Z}_8$.

$\xrightarrow{CRT(2,3,3,8)}$ 11

Using CRT to Simplify Modulo Computations

- Calculate

12345*12345 mod 35

$35 = 5 \times 7$

$$\begin{cases} x \equiv 0 \bmod 5 \\ x \equiv 2 \bmod 7. \end{cases}$$

$x \equiv 30$

$= (12345 \bmod 35)^2$.

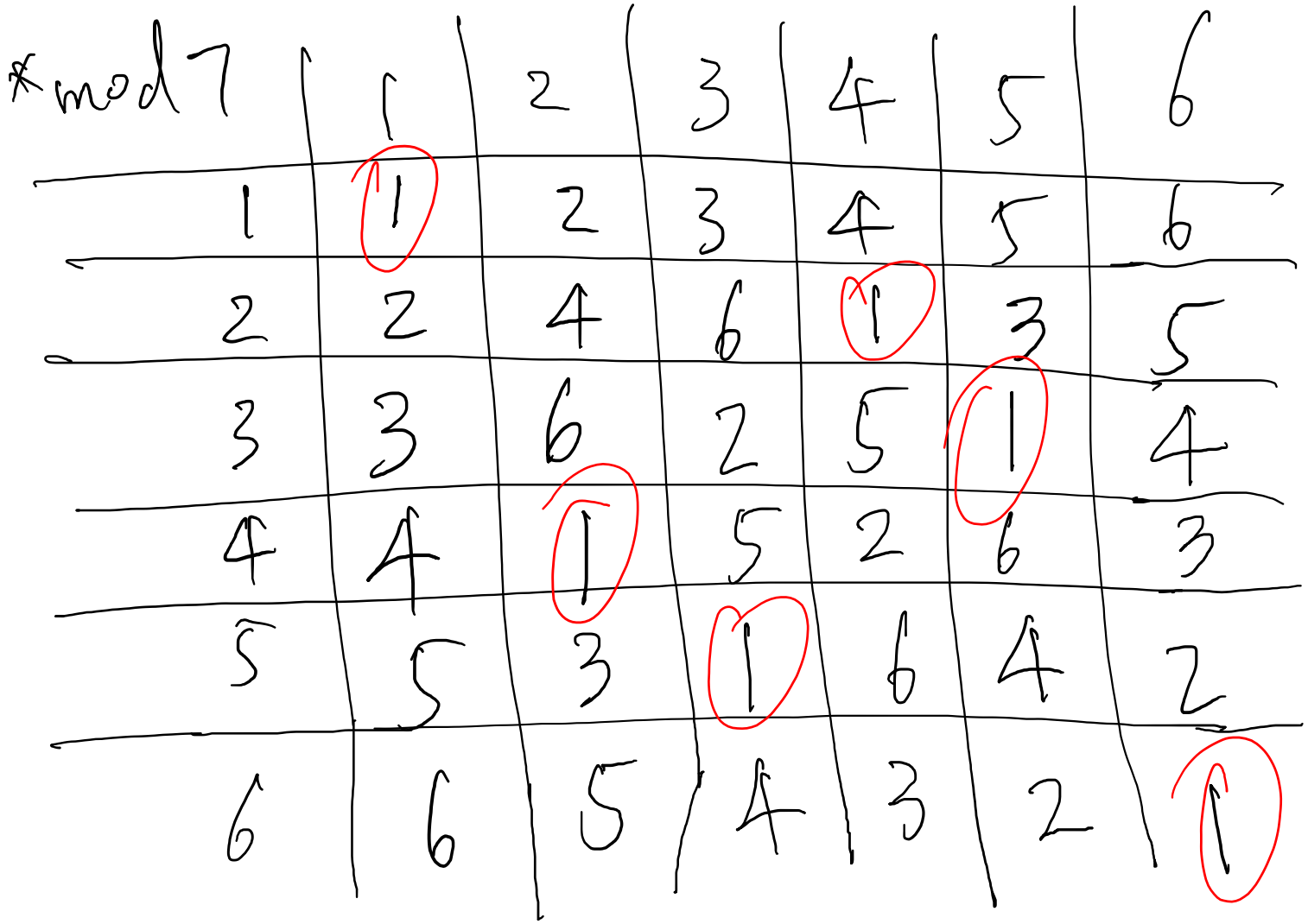
$\downarrow \rightarrow (12345 \bmod 5, 12345 \bmod 7)^2$

$= (0, 4)^2 = (0, 16 \bmod 7) = (0, 2)$

$CRT(0, 5, 2, 7) \longrightarrow 30$

Recall: $\mathbb{Z}_7^* = (\{1, \ldots, 6\}, *_{\mathbf{mod}\ 7})$

- Closure
- Identity
- Inverse
- Associativity



Iterative multiplications

$a = 2 \mod 7$

$a^2 = 4 \mod 7$

$a^3 = 8 \mod 7 = 1$

$a^4 = 2 \mod 7$

$a^5 = 4$

$a^6 = 1$

$a = 3 \mod 7$

$a^2 = 9 \mod 7 = 2$

$a^3 = 27 \mod 7 = 6$

$a^4 = 18 \mod 7 = 4$

$a^5 = 12 = 5 \mod 7$

$a^6 = 15 = 1 \mod 7$

Fermat's Little Theorem

If p is prime, then for all $a \in \mathbb{Z}_p^*$

$$a^{p-1} = 1 \mod p$$

$x = q(p-1) + r$

$a^x \bmod p = a^{q(p-1)+r} \bmod p = \left(a^{(p-1)\cdot q} \bmod p\right)\left(a^r \bmod p\right)$

$= a^r \bmod p$

- p = 7, a =5

$$5^{7-1} = 5^6 = (25)^3 \equiv 4^3 = 16 \times 4 \bmod 7$$

$$\equiv 2 \times 4 \bmod 7$$

$$\equiv 1$$

$\bmod 7$

- p =11, a =2

$$2^{p-1} \bmod p = 2^{10} \bmod 11 = 1024 \bmod 11 = 1$$

$$2^{20} \bmod p = 2^{10} \cdot 2^{10} \bmod 11 = 1$$

$$2^{12} \bmod p = 2^{10} \cdot 2^{2} \bmod 11 = 1 \times 4 \bmod 11 = 4.$$

Euler's Theorem

If n and a are coprime, then

$$a^{\phi(n)} = 1 \pmod{n}$$

where $\phi(n) = n\Pi_{p|n}(1 - \frac{1}{p})$ is called Euler's totient function.

$\prod_{p|n} (1 - \frac{1}{p})$.

$p|n$ if p divides n.

$\phi(15) = (1 - \frac{1}{3})(1 - \frac{1}{5}) \times 15$

$= 8$

$\phi(8) = (1 - \frac{1}{2}) \cdot 8 = 4$

$n = 15, a = 11$

$$a^{\phi(15)} = 11^{8} \bmod 15 = 1$$

Some Magic You can Play Now

- $11^{17} \bmod 3$

Apply Fermat's little theorem.

$p=3$. $p-1=2$. $17 \bmod 2 = 1$. $11^2 \bmod 3 = 1$. by Fermat.

$11^{17} = 11^{8\times 2+1} = (11^2)^8 \cdot 11 = 11 = 2 \bmod 3$.

Some Magic You can Play Now

- $11^{2016} \bmod 15$

$15 = 3 \times 5$

$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 5 \end{cases}$

$x \equiv 1$

$\xrightarrow{f} (11^{2016} \bmod 3,\ 11^{2016} \bmod 5) = (1, 1) \xrightarrow{CRT} 1$

$11^{2016} \bmod 3 = 1$ because $2016 \bmod (3-1) = 0$.

$11^{2016} \bmod 5 = 1$ $2016 \bmod (5-1) = 0$.