Problem Solving with Algorithms

Sarah M. Li

I. Euclidean Algorithm

If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$

The greatest common factor of two numbers does not change if the larger number is replaced by its difference with the smallest number.

Example 1: $\gcd(252, 105) = 21$ $\begin{cases} 252 = 21 \times 12 \\ 105 = 21 \times 5 \end{cases}$

$\gcd(252-105, 105) = \gcd(147, 105) = 21$ $\begin{cases} 147 = 21 \times 7 \\ 105 = 21 \times 5 \end{cases}$

$\gcd(147-105, 105) = \gcd(42, 105) = 21$ $\begin{cases} 42 = 21 \times 2 \\ 105 = 21 \times 5 \end{cases}$

$\gcd(105-42, 42) = \gcd(63, 42) = 21$ $\begin{cases} 63 = 21 \times 3 \\ 42 = 21 \times 2 \end{cases}$

$\gcd(63-42, 42) = \gcd(21, 42) = 21$ $\begin{cases} 21 = 21 \times 1 \\ 42 = 21 \times 2 \end{cases}$

$\gcd(42-21, 21) = \gcd(21, 21) = 1$

Intuition: Since the replacement above reduces the larger of the two numbers, repeating this process gives successively smaller pairs of numbers until the two numbers become equal. When that occurs, they are the gcd of the original two numbers.

Example 2: $\gcd(2322, 654) = *$ $a = 2322$ $b = 654$ $a = bq + r$

$2322 = 654 \cdot \underline{3} + \underline{360}$

$* = \gcd(654, 360)$

$654 = 360 \cdot \underline{1} + \underline{294}$

$* = \gcd(360, 294)$

$360 = 294 \cdot \underline{1} + \underline{66}$

$* = \gcd(294, 66)$

$294 = 66 \cdot \underline{4} + \underline{30}$

$* = \gcd(66, 30)$

$66 = 30 \cdot \underline{2} + \underline{6}$

$* = \gcd(30, 6)$

$30 = 6 \cdot \underline{5}$

Hence $\gcd(2322, 654) = 6$.

Q: Why does the Euclidean Algorithm work?

Claim: If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

In other words $a = bq + r$ WTS **$\gcd(a,b) = d$ iff $\gcd(b,r) = d$**

Proof ($\Rightarrow$) Let $d = \gcd(a,b)$
$d \mid a$ and $d \mid b$, then $d \mid (a - qb)$.

Hence $r = a - bq$. Thus $d \mid r$. This means d is a common factor of b and r.

Suppose towards contradiction that $\exists d' > d$ s.t. $d' \mid r$ and $d' \mid r$.

Then $d' \mid (bq + r)$. Then $d' \mid a$. Then $\gcd(a,b) = d' > d$. This yields a contradiction.

Hence $\gcd(b,r) = d$.

($\Leftarrow$) Let $d = \gcd(b,r)$
$d \mid b$ and $d \mid r$, then $d \mid (bq + r)$ Hence $d \mid a$.

Reasoning analogously as before, $\gcd(a,b) = d$.

II. The Extended Euclidean Algorithm

Example 3 $\gcd(888, 54) = 6$ (The last non-zero remainder in the repeated fraction)

$888 = 54 \cdot 16 + \boxed{24}$ $\quad \therefore 6 = 54 \cdot 33 + 888 \cdot (-2)$

$54 = 24 \cdot 2 + \boxed{6}$ $\quad 6 = 54 + (888 - 54 \cdot 16) \cdot (-2) = 54 + 888 \cdot (-2) + 54 \cdot 32 = 888 \cdot (-2) + 54 \cdot 33$

$24 = 6 \cdot 4 + 0$ $\quad 6 = 54 - 24 \cdot 2 = 54 + 24 \cdot (-2)$

Intuition: Write $\gcd(888, 54)$ as a linear combination of 888 and 54

Example 4 Use Euclidean Algorithm to find gcd (1180, 482) = 2.

Then write 2 as a linear combination of 1180 and 482.

$1180 = 482 \cdot 2 + \boxed{216}$ $\quad \therefore \; 2 = 1180 \times (-29) + 482 \times 71$

$482 = 216 \cdot 2 + \boxed{50}$ $\quad 2 = 482 \times 13 + (1180 - 482 \times 2) \times (-29) = 1180 \times (-29) + 482 \times 71$

$216 = 50 \cdot 4 + \boxed{16}$ $\quad 2 = 216 \times (-3) + (482 - 216 \times 2) \times 13 = 482 \times 13 + 216 \times (-29)$

$50 = 16 \cdot 3 + \boxed{2}$ $\quad 2 = 50 + (216 - 50 \cdot 4) \cdot (-3) = 50 + 216 \cdot (-3) + 50 \cdot 12 = 216 \times (-3) + 50 \times 13$

$16 = 2 \cdot 8 + 0$ $\quad 2 = 50 - 16 \cdot 3 = 50 + 16 \cdot (-3)$

III Continued Fraction [300 BC, around the time of Euclid's]

A way of expressing a number as an integer plus a series of nested fractions.

Type 1 Finite continued fractions

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

$a_1, \cdots, a_n \in \mathbb{N}^0$, $a_0 \in \mathbb{N}$

$[a_0; a_1, \cdots, a_n]$

Represent a rational number

Example 5 : $[1; 2, 3, 2] = \frac{23}{16}$

$$1 + \cfrac{1}{2 + \cfrac{1}{3 + \frac{1}{2}}} = 1 + \cfrac{1}{2 + \frac{1}{\frac{7}{2}}} = 1 + \cfrac{1}{2 + \frac{2}{7}} = 1 + \cfrac{1}{\frac{16}{7}} = 1 + \frac{7}{16} = \frac{23}{16}$$

Type 2 Infinite continued fractions.

$x_n = [a_0; a_1, \cdots] = \lim_{n \to \infty} x_n = a + b\sqrt{c}$, $a, b \in \mathbb{Q}$, $c \in \mathbb{Z}$.

This sequence goes infinitely.

Represent an irrational number

Example 6: $\frac{89}{37} = [2; 2, 2, 7]$

Euclidean Algorithm

$89 = 37 \times 2 + 15$

$37 = 15 \times 2 + 7$

$15 = 7 \times 2 + 1$

$$\frac{89}{37} = 2 + \frac{15}{37} = 2 + \cfrac{1}{\frac{37}{15}} = 2 + \cfrac{1}{2 + \frac{7}{15}} = 2 + \cfrac{1}{2 + \cfrac{1}{\frac{15}{7}}} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{7}}}$$

→ Terminate Here!

Example 7 $[1,2,1,2,1,2,\cdots] = [1,\overline{2}]$

Let $[\overline{1,2}] = x = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2+\ddots}}}$ (*) $\boxed{x>0}$

This part looks the same as the whole thing (*)

Hence: $x = 1 + \cfrac{1}{2+\frac{1}{x}} = 1 + \cfrac{1}{\frac{2x+1}{x}} = 1 + \cfrac{x}{2x+1} = \cfrac{3x+1}{2x+1}$

This means $2x^2 + x = 3x+1 \Leftrightarrow 2x^2 - 2x - 1 = 0$. (A)

Solving (A) yields $x = \cfrac{2 \pm \sqrt{4+8}}{4} = \cfrac{2 \pm 2\sqrt{3}}{4} = \cfrac{1 \pm \sqrt{3}}{2}$

But $x>0$, thus $x = \cfrac{1+\sqrt{3}}{2}$

Example 8 $\sqrt{2} = [1;2,2,\cdots] = [1;\overline{2}]$

$\sqrt{2} = 1 + \sqrt{2} - 1$

$= 1 + \cfrac{(\sqrt{2}-1)(\sqrt{2}+1)}{\sqrt{2}+1}$

$\therefore \sqrt{2} = 1 + \cfrac{1}{\sqrt{2}+1} = 1 + \cfrac{1}{1+1+\frac{1}{\sqrt{2}+1}} = 1 + \cfrac{1}{2+\frac{1}{1+\sqrt{2}}} = 1 + \cfrac{1}{2+\frac{1}{1+1+\frac{1}{1+\sqrt{2}}}} = 1 + \cfrac{1}{2+\frac{1}{2+\frac{1}{1+\sqrt{2}}}} = \cdots$

↑ Replace $\sqrt{2}$ by $1 + \frac{1}{\sqrt{2}+1}$

↑ Replace $\sqrt{2}$ by $1 + \frac{1}{\sqrt{2}+1}$

Example 9 $\frac{72}{19} = [3;1,3,1,3]$

$72 = 19 \times 3 + 15$

$19 = 15 \times 1 + 4$

$15 = 4 \times 3 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

IV. RSA Cryptosystem

Encryption: $(\overset{e}{5}, 14)$ locks . they are public

Text: B → 2

$2^5 \pmod{14} = 32 \pmod{14} = 4 \pmod{14}$

Ciphertext: D → 4 The original message is encrypted.

Decryption $(\overset{d}{11}, 14)$ To recover the message

↑ secret

$4^{11} \pmod{14} = 4194304 \pmod{14} = 2 \pmod{14} \rightarrow B.$

Q: How does it work?

① Pick two prime numbers: $p=2$ $q=7$ In real life, p, q have to be enormous.

② $N = pq = 14$, the **modulus** in the encryption key and decryption key.

⇓

★ Become public

③ $\phi(N) = (p-1)(q-1)$ # of numbers in $\mathbb{Z}_N$ that are coprime with N.

"phi function" this is the formula (Math reason behind)

$= 1 \times 6 = 6$

coprime with 14
1
✓
3
5
✓
9
11
13

④ Choose e $\begin{cases} 1 < e < \phi(N) \\ \text{coprime with } N, \phi(N) \end{cases}$

↓ coprime with 14

$e = 3, 5$

↓ coprime with 6

$e = 5$

Lock (5, 14) hand to everyone

⑤ Choose d: $de \overset{5}{\overset{\|}{}} \bmod \phi(N) \overset{6}{\overset{\|}{}} = 1$

$5d \pmod 6 = 1 \quad \therefore d = 5, 11, 17, \ldots$ ✓

	mod 6
5	5
10	4
15	3
20	2
25	1 ✓
30	0 The 6th multiple of 5.
⋮	

Appendix: Continued Fraction of $\sqrt{n}$.

The continued fraction of x

1). Let $x_0 = x$, and $a_0 = \lfloor x_0 \rfloor$ e.g., $\lfloor \pi \rfloor = \lfloor 3.14\cdots \rfloor = 3$

2). Let $x_1 = \frac{1}{x_0 - a_0}$, $a_1 = \lfloor x_1 \rfloor$

3). Let $x_2 = \frac{1}{x_1 - a_1}$, $a_2 = \lfloor x_2 \rfloor$

4). Continue until a pattern is spotted * We don't know if there is a pattern for π.

$$x = [a_0; a_1, a_2, \cdots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$$

Ex 10: $x = \sqrt{2} = [1; \overline{2}]$

$x_0 = \sqrt{2}$, $a_0 = \lfloor \sqrt{2} \rfloor = \lfloor 1.4\cdots \rfloor = 1$

$x_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$, $a_1 = \lfloor x_1 \rfloor = \lfloor 2.4\cdots \rfloor = 2$

$x_2 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$ ($= x_1$), $a_2 = \lfloor x_2 \rfloor = \lfloor 2.4\cdots \rfloor = 2$ ($= a_1$)

$x_3 = x_2 = x_1$, $a_3 = \lfloor x_3 \rfloor = \lfloor x_2 \rfloor = \lfloor x_1 \rfloor = a_1$

Hence, we could see that $a_n = a_1 = 2$ for $n \geq 1$.

Thus $\sqrt{2} = [1; 2, 2, \cdots] = [1; \overline{2}]$ ← goes on forever

Ex 11: $x = \sqrt{5} = [2; \overline{4}]$

$x_0 = \sqrt{5}$, $a_0 = \lfloor x_0 \rfloor = \lfloor \sqrt{5} \rfloor = \lfloor 2\cdots \rfloor = 2$

$x_1 = \frac{1}{\sqrt{5}-2} = \frac{\sqrt{5}+2}{(\sqrt{5}-2)(\sqrt{5}+2)} = \sqrt{5}+2$ $a_1 = \lfloor x_1 \rfloor = \lfloor 4.\cdots \rfloor = 4$

$x_2 = \frac{1}{\sqrt{5}-2} = x_1$, hence $a_2 = \lfloor x_2 \rfloor = \lfloor x_1 \rfloor = a_1 = 4$.

$x_3 = \frac{1}{x_2 - a_2} = \frac{1}{x_1 - a_1} = x_2$, hence $a_3 = \lfloor x_3 \rfloor = \lfloor x_2 \rfloor = \lfloor x_1 \rfloor = a_1 = 4$.

Reasoning analogously, $a_n = a_1 = 4$ for $n \geq 1$.

Hence $\sqrt{5} = [2; 4, 4, \cdots] = [2; \overline{4}] = 2 + \cfrac{1}{4 + \cfrac{1}{4 + \ddots}}$