19th January 2012

MA 375

The Euclidean Algorithm

Def If $a, b \in \mathbb{N}$, the greatest common denominator, $\gcd(a,b) = \max\{n \in \mathbb{N} \mid n|a \text{ and } n|b\}$

least common multiple, $\text{lcm}(a,b) = \min\{n \in \mathbb{N} \mid a|n \text{ and } b|n\}$

Remarks:

By unique factorization

$a = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot \ldots \cdot p^{a_p}$ (decomposed of primes)

$b = 2^{b_2} \cdot 3^{b_3} \cdot 5^{b_5} \cdot \ldots \cdot p^{b_p}$

then,

$$\gcd(a,b) = 2^{\min(a_2,b_2)} \cdot 3^{\min(a_3,b_3)} \cdot 5^{\min(a_5,b_5)} \cdot \ldots \cdot p^{\min(a_p,b_p)}$$

$$\text{lcm}(a,b) = 2^{\max(a_2,b_2)} \cdot 3^{\max(a_3,b_3)} \cdot 5^{\max(a_5,b_5)} \cdot \ldots \cdot p^{\max(a_p,b_p)}$$

Problem: How do we find gcd and lcm if no prime factorization is known?

(1) Find factorization for a, b.

(2) Use Euclidean Alogrithm.

Euclidean Algorithm

premise: if $n|a$ and $n|b$, then $n|a-b$, $a \neq b. \wedge\ a-b \neq 0$

Alogorthm:

Input: a, b where $a > b$.

Initialize: $c_0 = a$

$c_1 = b$

Iterate: Divide c_i by c_{i-1}. Keep the remainder. Thus we produce

q = number of copies c_{i-1} fits into c_i and remainder r_i.

$$c_{i+1} = q c_i + r_i \quad \cdot\ q \in \mathbb{N},\ r_i = \text{remainder}$$

Then, assign $c_{i+1} = r_i$

Ex:

1st Iter. $a = c_0 = q \cdot c_1 + r_i$

$c_2 := r_1$, $r_1 < c_1$, $c_0 > c_1 > c_2 \ldots$

2nd Iter. $c_1 = q \cdot c_2 + r_2$

$c_3 := r_2$, $c_2 < c_2$.

We see that,

$C_0 > C_1 > C_2 > \dots$

Since we are in the field of $\mathbb{N}$, this iteration must break, i.e.

when $C_i = 0$, the alogrithm breaks. ($\frac{n}{0}$ = undefined)

Then C_j where j is the last iteration is the gcd(a,b).

Ex

$a = 28 = C_0$

$b = 16 = C_1$

step 1: $28 = 1 \cdot 16 + 12$: $C_2 := r_1 := 12$

$16 = 1 \cdot 12 + 4$: $C_3 := r_2 = 4$

$12 = 3 \cdot 4 + 0$: $C_4 := r_3 = 0$

↑ end of iteration.

Therefore, $\gcd(16, 28) = C_3 = 4$.

$16 - 6 = 10$

Note:

If $d \mid C_0$ and $d \mid C_1$, then $d \mid r_1$.

⇒ Recall .. premise. Since $C_0 - nC_1 = r_1$ .... C_0, C_1, r_1 shares some $d \in \mathbb{N}$.

Reversely, if $d \mid C_1$ and $d \mid r_1$, then $d \mid C_0$

⇒ gcd of C_0 and C_1 is also gcd of C_1 and r_1

hmm... ⇒ gcd of input is no different than gcd of next pairs of Cs. ☆

$\gcd(C_0, C_1) = \gcd(C_1, C_2)$

$= \gcd(C_2, C_3)$

$\vdots$

$= \gcd(C_i, 0)$

$= C_i$

Also,

Note: $16 = 1 \cdot 12 + 4$; $4 = 16 - 1 \cdot 12$

$= 16 - 1 \cdot (28 - 1 \cdot 16)$

$= 2 \cdot 16 - 1 \cdot 28$

⇒ one can express gcd(a,b) as $\mathbb{Z}$ linear combination of a and b. In particular, there is an equation $\gcd(a,b) = \alpha \cdot a + \beta \cdot b$ where $\alpha, \beta \in \mathbb{Z}$

More examples of Euclidean Algorithm

ex. 1

$a = 91 := c_0$

$b = 49 := c_1$

$c_0 = 1 \cdot c_1 + 42 \curvearrowleft := c_2$

$c_1 = 1 \cdot c_2 + 7 \curvearrowleft := c_3$

$c_2 = 7 \cdot c_3 + 0 \implies$ end of iteration

$\gcd(49, 91) = 7$

and: $7 = 2 \cdot 49 - 92$

ex. 2

$a = 13 := c_0$

$b = 8 := c_1$

$c_0 = 13 = 1 \cdot 8 + 5 \curvearrowleft := c_2$

$c_1 = 8 = 1 \cdot c_2 + 3 \curvearrowleft := c_3$

$c_2 = 5 = 1 \cdot c_3 + 2 \curvearrowleft := c_4$

$c_3 = 3 = 2 \cdot c_4 + 1 \curvearrowleft := c_5$

$c_4 = 2 = 2 \cdot c_5 + 0 \implies$ end of iteration

$\gcd(13, 8) = 1 = 8 \cdot 5 - 3 \cdot 13$

Def If $\gcd(a, b) = 1$

we say a and b are relatively prime or coprime

NOTE: If a and b are coprime, then one can write

$1 = \alpha \cdot a + \beta \cdot b$, $a, b \in \mathbb{Z}$

In fact, existence of $\uparrow$ is equivalent to $\gcd(a,b) = 1$

$\implies$ If RHS of equation had a common divisor, then it must also divide the left hand side. Well, then it can only be 1.

MODULAR ARITHMATIC

If $n \in \mathbb{Z}$: write $n\mathbb{Z}$ for set of all multiples of n.

e.g. let $n = 6$: ~~OR~~

One can calculate, with remainders,:

$3 + 6\mathbb{Z}$:= a set of all numbers, which, when divided by 6, gives remainder of 3.

Operations

$+$: $(3 + 6\mathbb{Z}) + (2 + 6\mathbb{Z}) = 5 + 6\mathbb{Z}$

$\cdot$: $(2 + 6\mathbb{Z}) + (5 + 6\mathbb{Z}) = 10 + 6\mathbb{Z}$

eg.

$9 + 8 = 17 = 2 \cdot 6 + 5$

$8 \cdot 5 = 40 = 10 + 6 \cdot 5$

Def pick $n \in \mathbb{Z}$

write $a + n\mathbb{Z}$ for $\{a + bn, b \in \mathbb{Z}\}$ (alternately a mod n

then, ~~elements of the~~ sets are (called) cosets

arithmatic of cosets

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z}$$
$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}$$

Def: $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n-1 + n\mathbb{Z}\}$

eg. $n = 6$

$\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, \ldots, 5 + 6\mathbb{Z}\}$

→ once n is implicity understood, we denote $a + n\mathbb{Z}$ as $\bar{a}$.

→ for instance, we calculate

$\bar{2} \cdot \bar{1} = \bar{2}$ $\quad \bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ $\quad \bar{2} \cdot \bar{5} = \bar{10} = \bar{4}$

$\bar{2} \cdot \bar{2} = \bar{4}$ $\quad \bar{2} \cdot \bar{4} = \bar{8} = \bar{2}$ $\quad \bar{2} \cdot \bar{0} = \bar{0}$

⇒ observe that some results return $\bar{0}$

Def a <u>zero divisor</u> in $\mathbb{Z}/n\mathbb{Z}$ is a coset $a + n\mathbb{Z}$ for which there exists a coset $b + n\mathbb{Z}$ such that

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = \bar{0}$$

Q: which numbers a give zero divisors in $\mathbb{Z}/n\mathbb{Z}$?

A: Exactly those for which $\gcd(a,n) \neq 1$

i) If $\gcd(a,n) \neq 1$, then let $d = \gcd(n,a)$

⇒ $\exists d, e \in \mathbb{N}$, $n = d \cdot e$

⇒ ae is a multiple of $ed = n$

⇒ $(a + n\mathbb{Z}) \cdot (e + n\mathbb{Z}) = ae + n\mathbb{Z} = 0 + n\mathbb{Z}$

so a is a zero divisor

ii) if $\gcd(a,n) = 1$

Then, there are $\alpha, \beta \in \mathbb{Z}$, with $1 = \alpha \cdot a + \beta \cdot n$

Thm The number a for which multiplication by a is bijective on $\mathbb{Z}/n\mathbb{Z}$ are exactly those a with $\gcd(a,n) = 1$

ex: if $n = 6$

$\{1, 5\} + 6\mathbb{Z}$

We say these special cosets are units in $\mathbb{Z}/n\mathbb{Z}$: To be a unit means that multiplication is reversible?

ex $7=n$

$\bar{1}\cdot\bar{1}=\bar{1}$

$\bar{2}\cdot\bar{4}=\bar{1}$ → $\gcd(7,2) = (-1)\cdot 7 + 4\cdot 2 = 1$

$\bar{3}\cdot\bar{5}=\bar{1}$ → $\gcd(7,3) = (1)\cdot 7 - 2(3) = 1$

$\bar{4}\cdot\bar{2}=\bar{1}$

$\bar{5}\cdot\bar{3}=\bar{1}$

$\bar{6}\cdot\bar{6}=\bar{1}$

Def Let $p(n)$ = # of cosets in $\mathbb{Z}/n\mathbb{Z}$ for which multiplication is invertible.

= # {numbers in $\{0,\dots,n-1\}$ whose gcd w/ n is 1}

$p(n)$ = Euler p-function

ex If n = prime

$p(n) = n-1$ (since n is prime ↓)

Fact: If $n=ab$ with $\gcd(a,b)=1$, then $p(n) = p(a)\cdot p(b)$

e.g. $p(4)=2$ $\quad p(4) \neq p(2)\cdot p(2)$

$p(2)=1$