Chapter 4 (book as it is + more)

Divisibility def $m \in \mathbb{Z}$ only positive m (B. DEF)

$m \mid n$ iff $m > 0 \wedge \exists k \in \mathbb{Z}\ (n = mk)$ $n \in \mathbb{Z}$

BOOK NOTATION $m \backslash n$, but I will use STANDARD NOTATION: $m \mid n$

Greatest common divisor of $m, n \in \mathbb{Z}$ BOOK DEF

$$\gcd(m,n) = \max\{k : k \mid m \wedge k \mid n\}$$

missing! $k > 0$ $k \in \mathbb{Z}$

In my ~~dd~~ number theory lecture notes I use symbol (m,n) for $\gcd(m,n)$ i.e

$(m,n) = \gcd(m,n)$ Different DEFINITION

Least common multiple of $m, n \in \mathbb{Z}$ BOOK DEF

$$\operatorname{lcm}(m,n) = \min\{k : k > 0 \wedge m \mid k \wedge n \mid k\}$$

missing $k \in \mathbb{Z}$, $\min > 0$

~~TOGETHER~~ In my number theory l. notes

$\operatorname{lcm}(m,n) = [m,n]$ ← different notation

Lecture notes consider only positive multiples as do the BOOK.

Re-capture definitions (accepting book def. of divisibility)

$$\gcd(m,n) = \max\{k \in \mathbb{Z} : k > 0 \wedge k \mid m \wedge k \mid n\}$$

where $m, n \in \mathbb{Z}$

$$\operatorname{lcm}(m,n) = \min\{k \in \mathbb{Z} : k > 0 \wedge m \mid k \wedge n \mid k\}$$

where $m, n \in \mathbb{Z}^+ = \mathbb{N} - \{0\}$ - because we defined divisibility $m \mid n$ only for $n > 0$

Lecture notes define $\gcd(m,n)$ for any $m, n \in \mathbb{Z}$ and any $k \in \mathbb{Z}$ (as divisibility is defined for any $m, n \in \mathbb{Z}$) so my lecture notes (and classical number theory definitions) are MORE GENERAL than our BOOK DEFNS.

In EUCLID ALGORITH we assumed that $m, n > 0$, and $n \geq m$.

and so DOES the BOOK. lecture notes EUCLID ALGORITHM computes $\gcd(m,n)$ for $m, n > 0$ and $m \leq n$

REMINDER (ch 3)

Let $n, m \in \mathbb{Z}$, $n, m > 0$ (i.e $n, m \in \mathbb{N} - \{0\}$)

$$n = m \left\lfloor \frac{n}{m} \right\rfloor + n \bmod m$$

quotient — remainder

Generalize to any $x, y \in \mathbb{Z}$ — DEFINITION

$$x \bmod y = x - y \left\lfloor \frac{x}{y} \right\rfloor \quad \text{for } y \neq 0$$

$$\bmod \subseteq \mathbb{Z} \times \mathbb{Z} - \{0\}$$

"mod" binary operation

EUCLID ALGORITHM (Recursive def)

Given $n > 0$, $m \geq 0$, $m < n$

$$\gcd(0, n) = n \qquad m = 0$$

$$\gcd(m, n) = \gcd(n \bmod m, m) \qquad m > 0$$

Remark: no such nice formula for $\operatorname{lcm}(m, n)$! hard problem (exercise 2)

HML: prove correctness!

EUCLID ALG FACTONE

For any $n > 0$, $m \geq 0$, $n > m$
there are n', $m' \in \mathbb{Z}$ such that

$$n'n + m'm = \gcd(n, m)$$

we compute n', m'

Take $r = n \bmod m$; i.e

we go back to classical Euclid

$r < m, n$!

$r = n - \lfloor \frac{n}{m} \rfloor m$, of course

$\gcd(r, m) = \gcd(n, m)$

We compute $\gcd(r, m) = \bar{r} r + \bar{m} m$

$= \bar{r}(n - \lfloor \frac{n}{m} \rfloor m) + \bar{m} m$

$= \bar{r} n - \bar{r} \lfloor \frac{n}{m} \rfloor m + \bar{m} m$

$= \left(\bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r}\right) m + \bar{r} n = \gcd(n, m)$

We get

$$m' = \bar{m} - \lfloor \frac{n}{m} \rfloor \bar{r}$$

$$n' = \bar{r}$$

$n = 12$, $n = 18$

$r = 6$

$\gcd(6, 18) = 6$

$= 1 \cdot 6 + 0 \cdot 18$

$\bar{r} = 1$, $\bar{m} = 0$

$n' = 1$, $m' = -1$

$\gcd(12, 18) = 1 \cdot 12 + (-1) 18$

Remark.

The existence of n', m' is really a proof that E.A. produced $\gcd(n,m)$ (look at the proof in the lecture notes!)
Here is a sketch (from the book)
Assume that we computed (by our algorithm) result of ALG $\gcd(m,n) = d$ and $m'm + n'n = d$. Question? Is it true that $m'm + n'n = d$ is the gcd? Let d_1 be a common divisor of m and n, so $d_1 \mid m'm + n'n = d$ i.e $d_1 \mid d$. We easily prove (by use of the algorithm) that $d \mid m$ and $d \mid n$ (d is the divisor) Hence d must be the gcd (as any other divisor divides d)

We can think that EA + FACT provides also a proof of its correctness (NOT A FORMAL PROOF)
Algorithms like that are called

SELF-CERTIFYING.

FACT 2

For any $m, n \geq 2$, $k > 0$

$k \mid m \wedge k \mid n$, iff $k \mid \gcd(m, n)$

Proof $\Rightarrow$

$k \mid m \wedge k \mid n$, so $k \mid \underbrace{n'n + m'm = \gcd(m,n)}_{\text{FACT 1}}$

Assume $\Leftarrow$

$k \mid \gcd(m,n)$; but $\gcd(m,n) \mid m$ and $\gcd(m,n) \mid m$, so $k \mid m$ and $k \mid m$

SUMS

Book (4.8)

FACT 3

$$\sum_{m \mid n} a_m = \sum_k \sum_{m>0} a_m [n = mk]$$

Proof:

$$\sum_{m \mid n} a_m = \sum_m a_m [m \mid n] = \quad [m \mid n] \equiv [n = mk][m > 0]$$

$$= \sum_{m \mid k} a_m [n = mk][m > 0]$$

$$= \sum_k \sum_{m>0} a_m [n = mk]$$

FACT 4 (4.7)

$$\sum_{m \mid n} a_m = \sum_{m} a_{\frac{n}{m}}$$

Book has $m \mid n$ instead of m WRONG!

proof

From fact 3 $\sum_{m \mid n} a_m = \sum_{k} \sum_{m>0} a_m [n = mk]$

Evaluate now

$$\sum_{m} a_{\frac{n}{m}} = \sum_{t} a_t [t = \tfrac{n}{m} \wedge t > 0]$$

$$= \sum_{t} a_t [\underbrace{tm = n}_{t \mid n} \wedge t > 0] \quad \text{(by Fact 3)}$$

$$= \sum_{t=m} a_t [t \mid n] \quad \text{re-name } t \text{ by } m$$

$$= \sum_{m} a_m [m \mid n]$$

Example $n = 12$

$$\sum_{m \mid 12} a_m = \sum_{m \in K} a_m = a_{12} + a_6 + a_4 + a_3 + a_2 + a_1$$

$K = \{m : m \mid 12\} = \{12, 6, 4, 3, 2, 1\}$

$$\sum_{m} a_{\frac{12}{m}} = \sum_{k \in K_1} a_k = a_1 + a_2 + a_3 + a_4 + a_6 + a_{12}$$

$K_1 = \{m : \frac{12}{m}\} = \{1, 2, 3, 4, 6, 12\}$

FACTS

(4.9)

$$\sum_{m \mid n} \sum_{k \mid m} a_{k,m} = \sum_{k \mid n} \sum_{\ell \mid (\frac{n}{k})} a_{k,k\ell}$$

① = ②

① $= \sum_{m \mid n} \sum_{k \mid m} a_{k,m} = \sum_{m} \sum_{k} a_{k,m} [m \mid n][k \mid m]$

$[m \mid n] = [n = mj \wedge m > 0]$

$[k \mid m] = [m = k\ell \wedge k > 0]$

$= \sum_{j} \sum_{m>0} \sum_{\ell} \sum_{k>0} a_{k,m} [n = mj][m = k\ell]$

$= \sum_{\ell, j} \sum_{m,k>0} a_{k,m} [n = mj][m = k\ell]$

$[n = mj][m = k\ell] = [n = jk\ell]$

$m > 0, \; k > 0$
$m = k\ell > 0$
$\Rightarrow \ell > 0$

$= \sum_{j} \sum_{k,\ell>0} a_{k,k\ell} [n = jk\ell]$

$$② = \sum_{k l m} \sum_{\ell \mid \frac{m}{k}} a_{k,k\ell}$$

$$= \sum_{k} \sum_{\ell} a_{k,k\ell} \, [k \mid m] [\ell \mid \tfrac{m}{k}]$$

$$[k \mid n] = [n = kj \wedge k > 0]$$

$$[\ell \mid \tfrac{m}{k}] = [\tfrac{m}{k} = m\ell \wedge \ell > 0] = [m = km\ell \wedge k > 0]$$

$$= \sum_{k>0} \sum_{j} \sum_{\ell>0} \sum_{m} a_{k,k\ell} \, [n = kj] [n = km\ell]$$

$$= \sum_{j} \sum_{m} \sum_{k,\ell>0} a_{k,k\ell} \, [j = \tfrac{m}{k}] [n = km\ell]$$

$$= \sum_{j} \sum_{m} \sum_{k,\ell>0} a_{k,k\ell} \, [n = mk\ell]$$

evaluate $\sum_{j=\frac{m}{k}} S$

$$\sum_{j=\frac{m}{k}} S = S \sum_{j=\frac{n}{k}} 1 = S \cdot 1 = S$$

$$② = \sum_{m} \sum_{k,\ell>0} a_{k,k\ell} \, [n = mk\ell] = ①$$

?

ONE more step!

We moved

$$② = \sum_{m} \sum_{k,l>0} a_{k,kl}\,[n = mlk]$$

Re-name m by j i.e $m = j$

$$② = \sum_{j} \sum_{k,l>0} a_{k,kl}\,[n = jlk] = ①$$

end

PRIMES - PRIME NUMBERS

A positive integer is called PRIME if it has only two divisors 1 and itself. We assume (CONVENTION) that 1 is not prime.

DEF: PRIME

$p \in \text{PRIMES}$ iff $p \in \mathbb{N}$, $p > 1$ and $p \in P$

$$\forall k \,(k \mid p \Rightarrow k = 1 \vee k = p)$$

SOME PRIMES: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...

Is 91 prime? NO! $91 = 7 \cdot 13$!!

COMPOSITE (def)

$n \in \mathbb{Z}$ is COMPOSITE iff $\exists m \in \mathbb{Z}$ $m \mid n$ and $m \neq 1, m \neq n$

COMPOSITE numbers have more than TWO DIVISORS

Directly from by definition we get

FACT

$\forall n \in \mathbb{Z}$ $n \in PRIMES \vee n \in COMPOSITE$

and $PRIMES \cap COMPOSITE = \emptyset$

2 is ONLY even prime !!

PRIMES and DIVISIBILITY

P - set of PRIME numbers

FACT 1

$\forall p \in P \; \forall n \in \mathbb{N}$ $p \perp n$ or $p \mid n$

Follows from $\gcd(p, n) = 1$ or p

DEF $n \perp m$ iff $\gcd(n, m) = 1$

→ Bool notation

n, m are called RELATIVELY PRIME

FACT 2

A product of two numbers is divisible by a prime p only when p divides one of the factors.

Formally:

$$\forall_{p \in P} \forall_{n,m \in \mathbb{Z}} \left(p \mid mn \Rightarrow p \mid m \vee p \mid n \right)$$

Assume not true, ie there is p, m, n such that

$$p \mid m \cdot n \wedge p \nmid m \wedge p \nmid n.$$

$p \nmid m$, so by FACT 1 $p \perp m$. Now when $p \mid m \cdot n$ and $p \perp m$, we get $p \mid n$. (contradiction with $p \nmid n$.

FACT 3

A product $q_1 q_2 \cdots q_n$ of prime numbers (factors) q_i is divisible by a prime p only when $p = q_i$, for some q_i.

FACT 3 (Formal)

$$\forall_{p,2_1,\dots 2_n \in P}\left(p \mid \prod_{k=1}^{n} 2_k \Rightarrow \exists_{1 \le i \le n}\,(p = 2_i)\right)$$

Proof. Let $p \mid \prod_{k=1}^{n} 2_k$. By lemma 2 $p \mid 2_i$ for some 2_i. But $p > 1$, $p, 2 \in P$, so $p = 2_i$

$1 \notin P$

FACT 4 FORMAL

$$\forall_{n \in N}(n > 1 \Rightarrow \exists_{p \in P}\ p \mid n)$$ i.e

Every natural number n, $n > 1$ is divisible by some prime.

When $n \in P$, this is evident (n|n). When n is composite, it can be factored $n = n_1 n_2$, where $n_1 > 1$. The smallest possible one of these divisors n_1 must be prime.

PRIME

FACT 5 MAIN FACTORIZATION THEOREM

Every composite number can be factored UNIQUELY into prime factors.

The IDEA of FACT 5, as all lemma 1-5 we use to prove it is Found in EUCLID'S Elements in Books VII and IX

Proof of the MAIN THEOREM

STEP ONE. We show that every composite number $n > 1$ is the product of prime factors. By the FACT 4, there is $p_1 \in P$ such that $n = p_1 n_1$. If n_1 is composite, $n_1 = p_2 n_2$ ($p_2 \in P$) again by FACT 4. We continue this process with decreasing number $n, n_1, n_2, \ldots$ until some n_k becomes a prime and get $n = p_1 p_2 \cdots p_k$ ($p_k = n_k$)

STEP TWO. Now we have to prove UNIQUENESS Assume that we have TWO different prime factorizations

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \quad (*) \quad p_i \neq q_i$$

Each $p_i \mid n$, so each $p_i \mid \prod_{k=1}^{\ell} q_k$, so by FACT 3 $p_i = q_j$ for some j.
Conversely, $q_i \mid n$, so $q_i = p_k$, some k.
This proves that both sides of $(*)$ contain the same primes. The only difference might be that a prime p could occur a greater number of times on one side then on the other. In this case we CANCEL p sufficient number of times and get equation with p on one side, not on other. CONTRAD. from FACT 3.

MAIN PRIME FACTORIZATION THEOREM

Real representation (formal)

For any $n > 1$, $n \in \mathbb{N}$ there are $\alpha_i \geq 1$ $p_1 < \dots < p_r \in \mathbb{P}$ such that

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} = \prod_{k=1}^{r} p_k^{\alpha_k}$$

and the representation is unique

p_i's are different PRIME FACTORS of n

α_i is the MULTIPLICITY, i.e the number of times p_i occurs in the prime factorization

We write it shortly as

BOOK STATEMENT

MORE GENERAL FORM

$$n = \prod_{p} p^{\alpha_p} \qquad \alpha_p \geq 0$$

This is infinite product; but for particular n, all but few exponents $\alpha_p = 0$ ($p^0 = 1$). Hence for a given n it is really a finite product.

We know, by MAIN PRIME FAC. TH that for any $n > 1$ is represented UNIQUELY as

$$n = \prod_p p^{n_p} \qquad n_p \geq 0, \ p \in P \qquad d = n$$

so we can think of the sequence

$\langle n_1, n_2, n_3, \ldots n_p \ldots \rangle$ as a NUMBER SYSTEM for positive integers.

We assume P is ordered by $\leq$

$p_1 \leq p_2 < p_3 < \ldots$

$2 < 3 < 5 < 7 < 11 < 13 < \ldots$

$$n = \prod_{\substack{p_i \\ i \geq 1}} p_i^{n_i} \qquad n_i \geq 0$$

$n = \langle n_1, n_2, \ldots \rangle$

Example

$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$, so

$12 = \langle 2, 1, 0, 0, 0 \ldots \rangle = \langle 2, 1 \rangle$

$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$

$18 = \langle 1, 2, 0, 0 \ldots \rangle = \langle 1, 2 \rangle$

General

$$m = \prod_p p^{m_p}, \qquad n = \prod_p p^{n_p}$$

$$k = m \cdot n = \prod_p p^{m_p} \cdot \prod_p p^{n_p} = \prod_p p^{(m_p + n_p)}$$

FACTS

$k = m \cdot n$ iff $k_p = m_p + n_p$ for all p

FACT 7

$$m = \prod_p p^{m_p}, \quad n = \prod_p p^{n_p}$$

$m \mid n$ iff $m_p \le n_p$

$m \mid n$ iff there is k, $n = m \cdot k$, by FACT 6

iff $n_p = m_p + k_p$ iff $m_p \le n_p$

FACT 8

$k = \gcd(m,n)$ iff $k_p = \min(m_p, n_p)$

$k = \operatorname{lcm}(m,n)$ iff $k_p = \max(m_p, k_p)$

Directly from FACT 7

Example

① $12 = 2^2 3^1$, $18 = 2^1 \cdot 3^2$

$\gcd(12,18) = 2^{\min(2,1)} \cdot 3^{\min(1,2)} = 2^1 \cdot 3^1 = 6$

$\operatorname{lcm}(12,18) = 2^{\max(2,1)} \cdot 3^{\max(2,1)} = 2^2 \cdot 3^2 = 36$

② $m = 2^6 \cdot 3^2 \cdot 5 \cdot 7^0$ $n = 2^5 \cdot 3^3 \cdot 7 \cdot 5^0 \cdot 7^1$

$\gcd(m,n) = 2^5 \cdot 3^2$ $\operatorname{lcm}(m,n) = 2^6 \cdot 3^3 \cdot 5 \cdot 7$