MATH 381 Section 4.3

Prof. Olivia Dumitrescu

22 March 2024

Section 4.3 Primes and GCDs

Recall for any $n \in \mathbb{N}$, $1 \mid n$, $n \mid n$.

Definition Let p be an integer where $p \geq 2$.
p is prime if its only positive factors are 1 and p.
An integer greater than 1 is called composite if it's not prime.
Note: 1 is neither prime nor composite.

Theorem 0.1 *Fundamental Theorem of Arithmetic*
Every integer greater than 1 is either prime or uniquely a product of primes.

Theorem 0.2 *If n is a composite integer, then it has a prime factor less than or equal to $\sqrt{n}$.*

Proof n is composite

$$\begin{aligned} 1 < a < n \\ n = a \cdot b \end{aligned} \implies 1 < b < n$$

Claim is false if $a > \sqrt{n} \wedge b > \sqrt{n}$.

$$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \implies n > n$$

Therefore, claim is true by contradiction.

Example Find prime factorization of 7007.

Theorem 0.3 *There are infiinitely many primes.*

Proof Assume by contradiction this is not the case and we have finitely many primes.

$$\{p_1, \dots, p_n\}$$
$$q := p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$$

1. has a unique prime factorization

2. or is a prime number

$$\exists 1 \leq j \leq n (p_j \mid q)$$
$$p_j \mid p_1 \cdot p_2 \cdot \dots \cdot p_n + 1 \implies p_j \mid 1$$

i.e. there is no prime number dividing q. Therefore q has to be prime $q > p_n$ so it is not on the list. Therefore, there are infinitely many primes by contradiction.

Theorem 0.4 *The ratio of $\pi(x)$ (the number of primes, not exceeding x), and $\dfrac{x}{\ln x}$ approaches 1 when x gets larger and larger.*

Proposition 0.5 *Goldbach's conjecture*
1742 Goldbach wrote to Euler: Every odd integer is a sum of 3 primes $n > 5$
Euler simplified it: Every even integer is a sum of 2 primes.
True for all positive numbers up to $4 \cdot 10^{18}$

Definition Let a and b be some integers not both zero.

1. The largest d so that $d \mid a$ and $d \mid b$. The largest d so that $d \mid a$ and $d \mid b$ is the greatest common divisor of a and b. (We denote it $\gcd(a, b)$.)

2. The least common multiple of positive integers a and b is the smallest positive integer divisible by both a and b ($\mathrm{lcm}(a, b)$).

1. $$\gcd(a, b) \mid a$$
   $$\gcd(a, b) \mid b$$

   Moreover, if d is any other common divisor for a and b:

   $$\begin{matrix} d \mid a \\ d \mid b \end{matrix} \implies d \mid \gcd(a, b)$$

2.

$$\begin{aligned} a &\mid \operatorname{lcm}(a,b) \\ b &\mid \gcd(a,b) \end{aligned}$$

Moreover, if k is any other common multiple for a and b:

$$\begin{matrix} a \mid k \\ b \mid k \end{matrix} \implies \operatorname{lcm}(a,b) \mid k$$

Theorem 0.6 $a, b \in \mathbb{N}$

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b$$

Example What is the $\gcd(24, 36)$?

$$\begin{aligned} &\{d \mid d \mid 24\} = \{1,2,3,4,6,8,12,24\} \\ &\{d \mid d \mid 36\} = \{1,2,3,4,6,9,12,18,36\} \\ &\gcd(24,36) = 12 \end{aligned}$$

Definition

1. We say that a and b are relatively prime (or coprime) if their greatest common divisor is 1.

2. The integers $a_1, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for any $1 \le i \le n$ and $1 \le j \le n$.

Example 1. 10, 17, and 21 are pairwise relatively prime

2. 10, 19, and 24 are not pairwise relatively prime because $\gcd(10, 24) \neq 1$.

Proof for **Theorem 0.6**
Nautral numbers a and b enjoy a unique prime factorization.

$$\begin{gathered} a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \\ b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n} \\ p_i \text{ are prime numbers} \\ 0 \le a_i, b_i \in \mathbb{N} \\ \gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)} \\ \operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)} \end{gathered}$$

For any 2 numbers a, b

$$\min(a,b) + \max(a,b) = a + b$$

$$\begin{gathered}
\gcd(a,b) \cdot \operatorname{lcm}(a,b) \\
\left(p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}\right) \left(p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}\right) \\
p_1^{\min(a_1,b_1)+\max(a_1,b_1)} p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \dots p_n^{\min(a_n,b_n+\max(a_n,b_n))} \\
p_1^{a_1+b_1} p_2^{a_2+b_2} \dots p_n^{a_n+b_n} = a \cdot b \quad \blacksquare
\end{gathered}$$

Lemma 0.7 *Let* $a = b \cdot q + r \quad a, b \in \mathbb{Z}$*.*

$$\begin{gathered}
q, r \in \mathbb{Z} \qquad 0 \leq r < b \\
\gcd(a,b) = \gcd(b,r)
\end{gathered}$$

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

1.

$$\begin{cases} a = b \cdot q + r \\ d \mid a \\ d \mid b \end{cases} \qquad \implies d \mid a - b \cdot q = r$$

$$\begin{gathered}
\therefore d \mid r \\
\implies \gcd(a,b) \mid b \wedge \gcd(a,b) \mid r \\
\implies \gcd(a,b) \mid \gcd(b,r)
\end{gathered}$$

2. *Take* $k = \gcd(b,r)$

$$\begin{cases} k \mid b \\ k \mid r \end{cases} \quad \implies k \mid b \cdot q + r = a$$

but $a = b \cdot q + r \implies k \mid a$*.*
Therefore, $k \mid a$ *and* $k \mid b$
so $k \mid \gcd(a,b) \implies \gcd(b,r) \mid \gcd(a,b)$

1. *Part 1* $\implies \gcd(a,b) \mid \gcd(b,r)$

2. *Part 2* $\implies \gcd(b,r) \mid \gcd(a,b)$

$$\left.\begin{array}{r} x \mid y \\ y \mid x \end{array}\right\} \quad x = y$$

$$x, y \in \mathbb{Z}$$
$$x, y \neq 0$$

$$\begin{array}{r} y = ax \\ x = by \end{array} \implies a, b \in \{\pm 1\}$$

$$\begin{array}{r} x = abx \\ x(1-ab) = 0 \end{array} \implies a \cdot b = 1$$

There are three ways to compute $\gcd(a, b)$.

1. List factors
2. Find prime factorization
3. Euclidean Algorithm

Corollary 0.8 *Euclidean Algorithm*
Knowing $\gcd(a, b)$*, you know* $\operatorname{lcm}(a, b)$*. Suppose we have $a, b \in \mathbb{Z}$ such that $a \geq b$. Apply division algorithm $\implies q_i \in \mathbb{Z}$.*

$$\begin{array}{rll} r_0 = a & r_0 = r_1 \cdot q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = b & r_1 = r_2 \cdot q_2 + r_3 & 0 \leq r_3 < r_2 \\ & \vdots & \\ & r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n & \\ & r_{n-1} = r_n \cdot q_n & \end{array}$$

$a, b \in \mathbb{N}$

$$\gcd(a, b) = r_n$$

Proof Lemma 0.7 + Relations 3

$$\begin{aligned} \rightarrow \gcd(a, b) &= \gcd(r_0, r_1) \\ &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) \\ &= \gcd(r_n, 0) = r_n \end{aligned}$$

Theorem 0.9 *Bézout theorem*
If $a, b \in \mathbb{Z}_+$, then there exist integers s and t so that $a \cdot s + b \cdot t = \gcd(a, b)$.

Corollary 0.10 *If $a, b \in \mathbb{N}$ are coprime, then $\gcd(a, b) = 1$.*
$\implies$ *s and t so that $\in \mathbb{Z}$*

$$a \cdot s + b \cdot t = 1$$

Lemma 0.11 *If $a, b, c \in \mathbb{Z}_+$ such that*

$$\begin{cases} a \mid b \cdot c \\ \gcd(a, b) = 1 \end{cases}$$

Then $a \mid c$.

Proof By Bézout's theorem, $\gcd(a, b) = 1 \implies \exists m, n \in \mathbb{Z}$ such that

$$am + bn = 1$$
$$amc + bnc = c$$
$$\begin{matrix} a \mid amc \\ a \mid bc \end{matrix} \quad \implies \quad a \mid amc + bnc = c \quad \blacksquare$$

Corollary 0.12 *p is prime and*

$$p \mid a_1 a_2 \dots a_n \qquad a_i \in \mathbb{Z}$$

Then $\exists i = \overline{1, n}$ so that $p \mid a_i$

$$\begin{matrix} p \mid b \cdot c \\ p \nmid b \iff \gcd(p, b) = 1 \end{matrix} \qquad \textit{then} \quad p \mid c$$