CSCI 220 | Spring 2022

Discrete Structure

Primes and Greatest Common Divisors

Discrete Mathematics and its Application

Section 4.3

Definition of Prime and Composite

- An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not prime is called *composite*.

prime (p) : its only positive factors are 1 and p.

composite (n) : it has positive factors other than 1 and n.

$n = a \cdot b$, $a, b \neq 1, n,$

$1 < a, b < n$

$2 \leq a, b \leq n-1$.

The Fundamental Theorem of Arithmetic

- Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

$2 = 2$

$3 = 3$

$4 = 2 \cdot 2$

$5 = 5$

$6 = 2 \cdot 3$

$7 = 7$

$8 = 2 \cdot 2 \cdot 2$

$9 = 3 \cdot 3$

$10 = 2 \cdot 5$

Trial Division $\neg(p \to q) \equiv p \wedge \neg q$

- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof by contradiction:

Assume n is composite, all factors of $n > \sqrt{n}$.

$n = a \cdot b$, $1 < a, b < n$ $a > \sqrt{n}$, $b > \sqrt{n}$

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

Trial Division

- If n does not have any prime divisor less than or equal to $\sqrt{n}$, then n is a prime.

Trial Division

- If n does not have any prime divisor less than or equal to $\sqrt{n}$, then n is a prime.
- Is 91 a prime?

① find all primes $\leq \sqrt{91} \approx 9.\ldots$

$2, 3, 5, 7$

$2 \nmid 91$

$3 \nmid 91$

$5 \nmid 91$

$7 \mid 91$ ✓ $\quad 91 = 7(13)$

$$\begin{array}{r} 91 \\ -70 \\ \hline 21 \\ -21 \\ \hline 0 \end{array}$$

91 is not a prime.

it's composite.

Trial Division

- If n does not have any prime divisor less than or equal to $\sqrt{n}$, then n is a prime.
- Is 71 a prime?

primes $\leq \sqrt{71} \approx 8....$

2, 3, 5, 7,

$2 \nmid 71$

$3 \nmid 71$

$5 \nmid 71$

$7 \nmid 71$

71 is a prime.

Infinitude of Prime

- There are infinitely many primes.

Proof by contradiction:

Assume there are finitely many primes.

any # $> P_n$ will be composite.

List out all the primes. (in order) $P_1, P_2, P_3, \cdots P_n$

2 3 5 largest prime.

$L = P_1 \cdot P_2 \cdot P_3 \cdots P_n$ ← product of all primes.

$L+1$ is composite. $\exists P_i$ is prime, $P_i \mid L+1$, $P_i \mid L$ $\Rightarrow$ $P_i \mid (L+1) - L \rightarrow P_i \mid 1$

$P_i = 0$ or 1

they are not prime?

Prime Number Theorem.

- The ratio of $\pi(x)$, the number of primes not exceeding x, and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)
  - Approximating $\pi(x)$ by $x/\ln x$.

2, 3, 5, 7, 11, 13, 17, 19, 23, - - -

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78,498	72,382.4	1.084
10^7	664,579	620,420.7	1.071
10^8	5,761,455	5,428,681.0	1.061
10^9	50,847,534	48,254,942.4	1.054
10^{10}	455,052,512	434,294,481.9	1.048

$\pi(10) = 4$

$\pi(13) = 6$

Definition of Greatest Common Divisors

- Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $gcd(a,b)$. $= (a,b)$

Example of Greatest Common Divisors

- What is the greatest common divisor of 24 and 36?

$$24 = 2 \cdot \underline{2 \cdot 2} \cdot \underline{3} = 2^3 \cdot 3^1$$

$$36 = \underline{2 \cdot 2} \cdot \underline{3} \cdot 3 = 2^2 \cdot 3^2$$

$$\gcd(24, 36) = 2 \cdot 2 \cdot 3 = 12$$

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

Relatively Prime

- The integers $\boldsymbol{a}$ and $\boldsymbol{b}$ are <u>*relatively prime*</u> if their greatest common divisor is 1.

a, b are relatively prime if $\gcd(a,b) = 1$.

in other words, a and b don't share any prime factors.

ex: 4 and 9 are relatively prime

$\gcd(4,9) = 1$.

Pairwise Relatively Prime

- The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

$5, 6, 7, 11, 13, \cancel{15}$

$gcd(5, 15) = 5$

Definition of Least Common Multiple

- The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $lcm(a,b)$. $= [a,b]$

$lcm(24,36)$

$24 = 2\cdot 2\cdot 2\cdot 3 = 2^3\cdot 3$

$36 = 2\cdot 2\cdot 3\cdot 3 = 2^2\cdot 3^2$

$lcm(24,36) = 2\cdot 2\cdot 2\cdot 3\cdot 3 = 2^3\cdot 3^2 = 72$

Theorem regarding GCD and LCM

- Let a and b be positive integers.
  Then $ab = gcd(a,b) \cdot lcm(a,b)$.

Theorem regarding GCD and LCM

- Let a and b be positive integers.
  Then $ab = gcd(a, b) \cdot lcm(a, b)$.
  - Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$.
  - $\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \dots \cdot p_n^{\min(\alpha_n,\beta_n)}$
    $\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \dots \cdot p_n^{\max(\alpha_n,\beta_n)}$

$a = 2^3 \cdot 3 \cdot 7^2 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^2$

$b = 3^2 \cdot 5^3 \cdot 7 = 2^0 \cdot 3^2 \cdot 5^3 \cdot 7^1$

Theorem regarding GCD and LCM

- Let a and b be positive integers. Then $ab = gcd(a, b) \cdot lcm(a, b)$.
  - Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_n^{\beta_n}$.
  - $\gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \cdots \cdot p_n^{\min(\alpha_n,\beta_n)}$
    $\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \cdots \cdot p_n^{\max(\alpha_n,\beta_n)}$

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

$$= \left(p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \cdots \cdot p_n^{\min(\alpha_n,\beta_n)}\right)\left(p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \cdots \cdot p_n^{\max(\alpha_n,\beta_n)}\right)$$

$$= p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)+\max(\alpha_2,\beta_2)} \cdot \cdots \cdot p_n^{\min(\alpha_n,\beta_n)+\max(\alpha_n,\beta_n)}$$

$$= p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot \cdots \cdot p_n^{\alpha_n+\beta_n} = p_1^{\alpha_1}p_1^{\beta_1} \cdot p_2^{\alpha_2}p_2^{\beta_2} \cdot \cdots \cdot p_n^{\alpha_n}p_n^{\beta_n}$$

$$= \left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_n^{\alpha_n}\right)\left(p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_n^{\beta_n}\right) = ab$$

Examples of Greatest Common Divisors

- Find $\gcd(16, 20)$. $= 4$

$$\gcd(0, n) = n$$
$$n \neq 0$$

- Find $\gcd(0, 100)$. $= 100$

- Find $\gcd(2014, 2067)$. $= 53$

$2014 = 2 \cdot 1007$, $1007 = 53 \cdot 19$

$2067 = 3 \cdot 689$, $689 = 53 \cdot 13$

Example of Greatest Common Divisors

- Find $\gcd(2014, 2067) = d$ without factoring.

$d \mid 2014$

$d \mid 2067$ $\Rightarrow$ $d \mid 2067 - 2014 = 53$

$d \mid 53$ $\qquad$ $d \mid 2014 - 53(38) = 0$

$d \mid 0$

$2067 = 2014(1) + 53$

$2014 = 53(38) + 0$

$\gcd(2014, 2067)$

$= \gcd(53, 2014)$

$= \gcd(0, 53)$

$= 53$

Euclidean Algorithm

- Lemma: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.
  - Let $r_0 = a$ and $r_1 = b$.

    $r_0 = r_1 q_1 + r_2, \quad 0 \le r_2 < r_1;$

    $r_1 = r_2 q_2 + r_3, \quad 0 \le r_3 < r_2;$

    …

    $r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 \le r_n < r_{n-1};$

    $r_{n-1} = r_n q_n. + 0$
  - Then $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})$

    $= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$

Example of Euclidean Algorithm

- Find $\gcd(414, 662)$ using Euclidean Algorithm.

$662 = 414(1) + 248$

$414 = 248(1) + 166$

$248 = 166(1) + 82$

$166 = 82(2) + 2$ ← gcd,

$82 = 2(41) + 0$

$\gcd(248, 414)$

$= \gcd(166, 248)$

$= \gcd(82, 166)$

$= \gcd(2, 82)$

$= \gcd(0, 2)$

$= 2$

BEZOUT'S THEOREM

- If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Example of BEZOUT'S THEOREM

- Find linear combination of $414s + 662t = \gcd(414, 662)$.

$\gcd(414, 662)$
$\gcd(248, 414)$
$= \gcd(166, 248)$
$= \gcd(82, 166)$
$= \gcd(2, 82)$
$= \gcd(0, 2)$
$= 2$

$662 = 414(1) + 248$

$414 = 248(1) + 166$

$248 = 166(1) + \boxed{82}$

$166 = 82(2) + 2$ ← gcd.

$82 = 2(41) + 0$

$2 = 166 - 82(2) = 166(1) + \boxed{82}(-2)$

$= 166(1) + [248(1) + 166(-1)](-2)$

$2 = 166(3) + 248(-2)$

$= [414(1) + 248(-1)](3) + 248(-2)$

$2 = 248(-5) + 414(3)$

$= [662(1) + 414(-1)](-5) + 414(3)$

$2 = 414(\underset{s}{8}) + 662(\underset{t}{-5})$

Example of BEZOUT'S THEOREM

- Find $\gcd(198, 252)$ using Euclidean Algorithm.
- Find linear combination of $198s + 252t = \gcd(198, 252)$.

$$252 = 198(1) + 54$$
$$198 = 54(3) + 36$$
$$54 = 36(1) + 18$$
$$36 = 18(2) + 0$$

$$\gcd(198, 252) = 18$$

$$\begin{aligned}
18 &= 54(1) + \underline{36}(-1) \\
&= 54(1) + [198(1) + 54(-3)](-1) \\
&= 54(4) + 198(-1) \\
&= \underbrace{[252(1) + 198(-1)]}(4) + 198(-1)
\end{aligned}$$

$$18 = 198(\underset{s}{-5}) + 252(\underset{t}{4})$$

Lemma regarding GCD and Division

- If a, b, and c are positive integers such that $\gcd(a,b)=1$ and $a|bc$, then $a|c$.

$a \nmid b$, $a | bc$ $\rightarrow$ $a|c$.

$4 \nmid 7$ $4 | 7\cdot 8$ $\rightarrow$ $4|8$

$\gcd(4,7)=1$,

$4 \nmid 6$, $4 | 6\cdot 10$ $\rightarrow$ $4 \nmid 10$

$\gcd(4,6)=2$

Lemma regarding GCD and Division

- If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof : $\gcd(a,b) = 1$

by Bezout's Thm, $\exists s,t \in \mathbb{Z}.$ $as + bt = 1$

multiply c, $asc + btc = c$

$a | asc$ $\quad a | btc$ $\rightarrow a | asc + btc = c$

since $a|a$, $a|bc$ $\quad \rightarrow a|c$

$\square$.

Lemma regarding GCD and Division

- If p is a prime and $p | a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p | a_i$ for some i.

$\gcd(p, a_i) = 1$ or p.

when a_i is multiple of p.

$\rightarrow p | a_i$

Theorem about Division on Modular

- Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc\ (mod\ m)$ and $gcd(c, m) = 1$, then $a \equiv b\ (mod\ m)$.

$$\frac{8}{2} \equiv \frac{18}{2} \pmod{5}$$

$$4 \equiv 9 \pmod{5} \quad ✓$$

$$\gcd(2, 5) = 1$$

$$\frac{8}{2} \equiv \frac{18}{2} \pmod{10}$$

$$4 \equiv 9 \pmod{10} \quad ✗$$

$$\gcd(2, 10) = 2$$

$$4 \equiv 9 \left(\mathrm{mod}\ \frac{10}{\underbrace{\gcd(2,10)}_{=2}}\right)$$

$$4 \equiv 9 \pmod{5} \quad ✓$$

Theorem about Division on Modular

- Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

$m \mid ac - bc \rightarrow m \mid c(a-b) \rightarrow m \mid a-b$

$gcd(m, c) = 1$ $\qquad a \equiv b \pmod{m}$

$gcd(c, m) = d$

$d \mid c$, $c = dc'$

$d \mid m$, $m = dm'$

$adc' \equiv bdc' \pmod{dm'}$

$adc' = bdc' + dm'k$

$ac' = bc' + m'k \rightarrow ac' \equiv bc' \pmod{m'}$