CSCI 220 Lecture 4 Note   Tuesday, 02/15/2022

Announcement

- The Lecture Recordings will be available on the following YouTube Playlists
  Link: https://youtube.com/playlist?list=PLZaTmV9UMKliRBuEs0-dL968iQqE0qwpc

Primes and Greatest Common Divisors

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.
    i.e., $n = a \cdot b$, where $a, b \neq 1, n$,
    which $1 < a, b < n$, or $2 \leq a, b \leq n - 1$.

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.
  - We will proof this later when we do induction, the proof of this theorem involved induction.
  - Let's look at some examples:
    $2 = 2$, 2 is a prime.
    $3 = 3$, 3 is a prime.
    $4 = 2 \cdot 2$
    $5 = 5$, 5 is a prime.
    $6 = 2 \cdot 3$
    $7 = 7$, 7 is a prime.
    $8 = 2 \cdot 2 \cdot 2$
    $9 = 3 \cdot 3$
    $10 = 2 \cdot 5$
    and so on …

Trial Division

- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
  - Proof by contradiction: $\neg(p \to q) \equiv p \wedge \neg q$
  - Assume n is a composite integer, and n does not have a prime divisor less than or equal to $\sqrt{n}$, which all factors of n will be greater than $\sqrt{n}$.
  - Then, we have $n = a \cdot b$, where $a, b \neq 1, n$, since n is composite.
    Since all factors of n will be greater than $\sqrt{n}$, $a > \sqrt{n}$ and $b > \sqrt{n}$.
  - Then, $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. Contradiction! $n \ngtr n$.
- If n does not have any prime divisor less than or equal to $\sqrt{n}$, then n is a prime.
  - This is contrapositive of the previous statement. So, they are equivalent. We can use this statement to show whether a number is a prime.
  - Without this statement, you will want to show none of the number between 2 and $n - 1$ divides n, to show its only positive factors is 1 and n, thus, it's a prime.
    With this statement, you can check a lot less number.

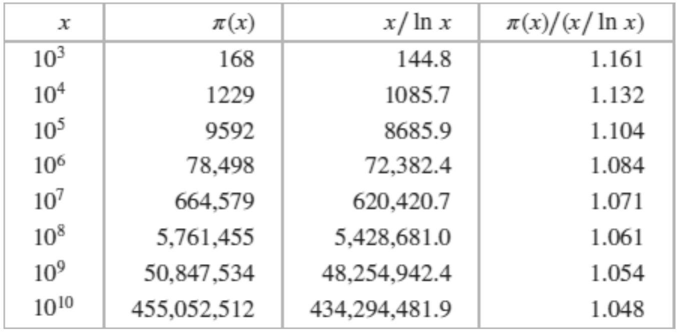
- Let's look at the following example:
  - Is 91 a prime?
    - List all the primes $\leq \sqrt{91} = 9\ldots.$: 2, 3, 5, 7
    - $2 \nmid 91,\ 3 \nmid 91,\ 5 \nmid 91,\ 7|91$
    - $91 = 7 \cdot 13$. 91 is not a prime, it's a composite.
  - Is 71 a prime?
    - List all the primes $\leq \sqrt{71} = 8\ldots.$: 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.
  - Then we can list out all the primes in order:
    $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots, p_n = largest\ prime$.
    Any number greater than p_n will be composite, since p_n is the last/largest prime.
  - Let's make a very large number, call it L, and we make it by multiplying all the primes, $L = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n$.
  - And let's make a larger number, $L+1$. $L+1$ must be a composite, since it's larger then p_n. Then, there exists a prime p_i such that $p_i|L+1$.
  - $p_i|L$ is also true, since L is the product of all primes.
  - Then $p_i|(L+1) - L$ → $p_i|1$, then p_i can only be 1.
    Contradiction! 1 is NOT a 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 $x/\ln x$.



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

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 $gcd(a,b)$.

- What is the greatest common divisor of 24 and 36?
  - $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$ and $36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$
    They have two 2 and one 3 in common,
    so the $\gcd(24{,}36) = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3 = 12$.
  - If you look at the exponent of the prime factorization, you can take the minimum exponents of each prime base in a and b.

- 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 $lcm(a, b)$.
    - To find $\text{lcm}(a, b)$:
      $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$ and $36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$
      You need to have all the factors in a and b, so it need to have at least three 2 and two 3, then $\text{lcm}(24{,}36) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 = 72$.
    - If you look at the exponent of the prime factorization, you can take the maximum exponents of each prime base in a and b.

- The integers a and b are *relatively prime* if their greatest common divisor is 1.
    - a and b doesn't need to be prime from them to be relatively prime. For example, 4 and 6 are relatively prime, since $\gcd(4, 9) = 1$. But neither 4 nor 6 is prime.
    - If two number are relatively prime or have GCD of 1, it also implies that they don't share common factor (beside 1).

- The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
    - For example, $\{5, 6, 7, 11, 13\}$ are pairwise relatively prime.
    - But, if you add 15 to the list, $\{5, 6, 7, 11, 13, 15\}$ are not pairwise relatively prime. Since $\gcd(5{,}15) = 5$ and $\gcd(6{,}15) = 3$.

- Let a and b be positive integers. Then $ab = gcd(a, b) \cdot lcm(a, b)$.
    - Proof:
        - Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$.
        - $$\begin{aligned}
\gcd(a, b) &= p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\beta_n)} \\
\text{lcm}(a, b) &= p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\beta_n)} \\
\gcd(a, b) \cdot \text{lcm}(a, b) &= \left(p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\beta_n)}\right)\left(p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\beta_n)}\right) \\
&= \left(p_1^{\min(\alpha_1,\beta_1)} \cdot p_1^{\max(\alpha_1,\beta_1)}\right)\left(p_2^{\min(\alpha_2,\beta_2)} \cdot p_2^{\max(\alpha_2,\beta_2)}\right) \ldots \left(p_n^{\min(\alpha_n,\beta_n)} \cdot p_n^{\max(\alpha_n,\beta_n)}\right) \\
&= p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)+\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\beta_n)+\max(\alpha_n,\beta_n)} \\
&= p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot \ldots \cdot p_n^{\alpha_n+\beta_n} = p_1^{\alpha_1} p_1^{\beta_1} \cdot p_2^{\alpha_2} p_2^{\beta_2} \cdot \ldots \cdot p_n^{\alpha_n} p_n^{\beta_n} \\
&= \left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}\right)\left(p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}\right) = ab
\end{aligned}$$

Exercises on Greatest Common Divisors

- Find $\gcd(16, 20)$. $= 4$
- Find $\gcd(0, 100)$. $= 100$
    - Any number divides 0, and the largest number divides 100 is 100.
    - For any non-zero n, $\gcd(0, n) = n$.
- Find $\gcd(2014, 2067)$.
    - If you try to factor 2014 and 2067, you can factor a 2 from 2014, and a 3 from 2067. $2014 = 2 \cdot 1007$ and $2067 = 3 \cdot 689$. Then it's hard to factor 1007 and 689 by hand.
    - So, we want to find a better way to solve for gcd than factoring.
- Find $\gcd(2014, 2067)$ without factoring.
    - Let made $\gcd(2014, 2067) = d$.
      Then by definition, d is the largest number that $d|2014$ and $d|2067$.
      $d|2067 - 2014$ will also hold, which we have $d|53$.
      Now, d become the largest number that divides 2014, 2067, and 53,

which $\gcd(2014, 2067) = \gcd(53, 2014)$.
Then $d|2014 - 53k$ is true, and we can subtract 53 38-times from 2014 with a remainder 0. $d|2014 - 53(38) \rightarrow d|0$.
Now, we have d is the largest number that divides 2014, 2067, 53, and 0, which $\gcd(2014, 2067) = \gcd(53, 2014) = \gcd(0, 53) = 53$.

- We can derive the Euclidean Algorithm from what we just did here. Instead of using the division here, we can put them in the division algorithm form, which lead us to the Euclidean Algorithm:

$$2067 = 2014(1) + 53$$
$$2014 = 53(38) + 0$$

  Once we hit the remainder 0, gcd will be the remainder of the previous line, 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 $r_1 = b$.
    $r_0 = r_1 q_1 + r_2$, $0 \leq r_2 < r_1$;
    $r_1 = r_2 q_2 + r_3$, $0 \leq r_3 < r_2$;
    $\dots$
    $r_{n-2} = r_{n-1} q_{n-1} + r_n$, $0 \leq r_n < r_{n-1}$;
    $r_{n-1} = r_n q_n$.
  - Then $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$
    $= \gcd(r_n, 0) = r_n$.
- Find $\gcd(414, 662)$ using Euclidean Algorithm.

$$662 = 414(1) + 248$$
$$414 = 248(1) + 166$$
$$166 = 82\,(2) + 2$$
$$82 = 2(41) + 0$$

  - $\gcd(414, 662) = 2$.

What to expect or prepare for the next class:

- BEZOUT'S THEOREM
- Solving Linear Congruences

Suggested Problems (You don't need to hand in.)

- Discrete Mathematics and its Application 4.3 # 1, 17, 25, 33
- zyBook Additional Exercises #1.6.1 (follow the Euclidean Algorithm we did in class.)