# Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-01-08

Chapter 3

# BASIC NUMBER THEORY

Basic Notions - Section 3.1.1

# DIVISIBILITY

# Definition

Let $a$ and $b$ be integers ($a, b \in \mathbb{Z}$) with $a \neq 0$.

We say that ***a* divides *b***, written $a|b$, if there exists an integer $k$ such that $b = a\,k$, i.e., $b$ is a multiple of $a$.

<u>Examples</u>:

| | | |
|---|---|---|
| $7 \mid 21$ | since | $21 = 3 \times 7$ |
| $-6 \mid 30$ | since | $30 = -6 \times -5$ |
| $5 \nmid 17$ | since | $17 \neq 5 \times \_\_\_$ |

# Proposition

Let $a, b, c$ integers. For every $a \neq 0$,

$$a \mid 0 \text{ and } a \mid a.$$

Also $1 \mid b$ for every $b$.

**Proof.**

Since $0 = 0 \cdot a$, take $k = 0$.

Since $a = 1 \cdot a$, take $k = 1$.

Since $b = b \cdot 1$, take $k = b$. $\blacksquare$

# Proposition

If $a \mid b$ and $b \mid c$, then $a \mid c$.

**Proof.**

$$a \mid b \implies \exists k_1 \in \mathbb{Z} \text{ s.t. } b = k_1 a$$

"$a$ divides $b$ implies that there exists an integer $k_1$ such that $b$ equals $k_1$ times $a$"

# Proposition

If $a \mid b$ and $b \mid c$, then $a \mid c$.

**Proof.**

$$a \mid b \implies \exists k_1 \in \mathbb{Z} \text{ s.t. } b = k_1 a$$
$$b \mid c \implies \exists k_2 \in \mathbb{Z} \text{ s.t. } c = k_2 b$$

$$c = k_2 b = k_2(k_1 a) = (k_2 k_1) a$$

$$\therefore a \mid c \text{ since } k_2 k_1 \in \mathbb{Z}. \qquad \blacksquare$$

# Proposition

If $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for all integers $s$ and $t$.

**Proof.**

$$a \mid b \implies \exists k_1 \in \mathbb{Z} \text{ s.t. } b = k_1 a$$
$$a \mid c \implies \exists k_2 \in \mathbb{Z} \text{ s.t. } c = k_2 a$$

$$sb + tc = s(k_1 a) + t(k_2 a) = (sk_1 + tk_2)a$$

$$\therefore a \mid (sb + tc) \quad \text{since} \quad sk_1 + tk_2 \in \mathbb{Z}. \quad \blacksquare$$

# Proposition

If $a > 1$ and $b$ are integers, then $a \nmid a\,b + 1$

**Proof.**

Suppose $a \mid a\,b + 1$, i.e., $\exists k \in \mathbb{Z}$ s.t.

$$a\,b + 1 = k\,a$$

which means

$$1 = ka - ba = a\,(k - b).$$

However, $a > 1$ and $(k - b) \in \mathbb{Z}$. $\rightarrow\leftarrow$ $\blacksquare$

Basic Notions - Section 3.1.2

# PRIME NUMBERS

# Definition

- A number $p > 1$ that is divisible by only $1$ and itself is called a **prime number**.
- A number $p > 1$ that is not prime is called **composite**.

<u>Personal Ramblings</u>:

Should the condition that $p > 1$ be dropped and call $-1$ a prime too?

$$-1 = 1 \times -1$$

# Euclid's Lemma (~300BC)

If a prime $p$ divides the product of two integers $a, b > 1$, then $p \mid a$ or $p \mid b$ (or both).

More generally, if $p \mid q_1 q_2 \dots q_k$, then $p$ divides at least one of the factors $q_1, q_2, \dots, q_k$.

# Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ can be represented in exactly one way as a product of prime powers:

$$n = {p_1}^{e_1} {p_2}^{e_2} \ldots {p_k}^{e_k}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and $e_1, e_2, \ldots, e_k$ are positive integers.

**Example:** $3{,}457{,}440 = 2^5 \cdot 3^2 \cdot 5^1 \cdot 7^4$

# Fundamental Theorem of Arithmetic

**Proof.** Two parts:

1. Every integer $n > 1$ can be written as the product of primes.

2. This prime factorization representation is unique.

# Fundamental Theorem of Arithmetic

**Proof.**

1. Let $n$ be the *smallest* integer which is not the product of primes.
   – If $n$ is prime, then $n = n$ (which is a one factor product of primes). $\rightarrow\leftarrow$
   – If $n$ is composite, then $n = a\,b$ for some $1 < a, b < n$.
   – Since $n$ is the smallest integer which is not the product of primes, $a$ and $b$ are the product of primes and their product, $n$, will also be a product of primes. $\rightarrow\leftarrow$

# Fundamental Theorem of Arithmetic

**Proof.**

2. Assume that $n$ can be represented as the product of primes in two distinct ways:
   $$n = {p_1}^{e_1}{p_2}^{e_2} \ldots {p_k}^{e_k} = {q_1}^{d_1}{q_2}^{d_2} \ldots {q_l}^{d_l}.$$
   – Divide out all primes that occur in both prime power representations, e.g., if $p_2 = q_5$.
   – There must now be a prime $p_i$ which does not appear among the remaining $q$s.
   – By Euclid's Lemma, since $p_i \mid n$ it also divides some $q$ in the representation. →← ■

# Proposition

There are an infinite number of primes.

**Proof.**

Assume that there are exactly $n$ primes:

$$p_1, p_2, \dots, p_n$$

Where $p_1 < p_2$ and $p_2 < p_3$ etc. Consider

$$s = p_1 p_2 \dots p_n + 1\,.$$

None of the primes $p_1, p_2, \dots, p_n$ divide $s$, so s must be prime and $p_n < s$. $\rightarrow\leftarrow$ $\blacksquare$

# Prime Number Theorem (~1797)

Let $\pi(x)$ be the number of primes *less than or equal to* $x$. Then

$$\pi(x) \sim \frac{x}{\ln x},$$

i.e.,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1\,.$$

# Prime Number Theorem (~1797)

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, …

$$\vdots$$

$$\pi(22) = 8,$$

$$\pi(23) = 9,$$

$$\pi(24) = 9,$$

$$\vdots$$

# Prime Number Theorem (~1797)

| $x$ | $\pi(x)$ | $\frac{x}{\ln x}$ | $\frac{\pi(x)}{x/\ln x}$ |
|---:|---:|---:|---:|
| 10 | 4 | 4.3 | 0.92103 |
| 100 | 25 | 21.7 | 1.15129 |
| 1,000 | 168 | 144.8 | 1.16050 |
| 10,000 | 1,229 | 1,085.7 | 1.13195 |
| 100,000 | 9,592 | 8,685.9 | 1.10432 |
| 1,000,000 | 78,498 | 72,382.4 | 1.08449 |
| 10,000,000 | 664,579 | 620,421.0 | 1.07117 |
| 100,000,000 | 5,761,455 | 5,428,681.0 | 1.06130 |
| 1,000,000,000 | 50,847,534 | 48,254,942.4 | 1.05373 |

# Prime Number Theorem (~1797)

- Rough estimate of the size of the $n^{\text{th}}$ prime:

$$p_n \sim n \ln n \ .$$

- Rough estimate of the number of primes in an interval:

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}}$$

$$\approx 3.9 \times 10^{97}$$

Basic Notions - Section 3.1.3

# GREATEST COMMON DIVISOR

# Definition

The **greatest common divisor** of $a \neq 0$ and $b$ is the largest positive integer dividing both $a$ and $b$, and denoted $\gcd(a, b)$ or $(a, b)$.

**Example:**

| | | |
|---|---|---|
| 30 | Pos. Divisors: | **1**,**2**,**3**,5,**6**,10,15,30 |
| 42 | Pos. Divisors: | **1**,**2**,**3**,**6**,7,14,21,42 |

$$\gcd(30,42) = 6$$

# Definition

We say that $a$ and $b$ are **relatively prime** if $\gcd(a,b) = 1$.

Two ways to find GCD:

1. Factor both integers and compare primes
   - $\left.\begin{aligned} 30 &= 2 \cdot 3 \cdot 5 \\ 42 &= 2 \cdot 3 \cdot 7 \end{aligned}\right\} \Longrightarrow \gcd(30, 42) = 2 \cdot 3 = 6$
2. Use the Euclidean Algorithm

# Euclidean Algorithm

- **Compute** $\mathbf{gcd(252, 600)}$
  - Use “long” division algorithm to divide the bigger number by the smaller number:
    - $600 = 2 \cdot 252 + 96$

      quotient remainder

      divisor
  - Use the division algorithm again on the **divisor** and **remainder**
    - $252 = 2 \cdot 96 + 60$

# Euclidean Algorithm

– Continue until you get a remainder of 0:

$$600 = 2 \cdot 252 + 96$$

$$252 = 2 \cdot 96 + 60$$

$$96 = 1 \cdot 60 + 36$$

$$60 = 1 \cdot 36 + 24$$

$$36 = 1 \cdot 24 + 12$$

$$24 = 2 \cdot \underline{\mathbf{12}} + 0$$

$$\gcd(600, 252) = 12$$

# Euclidean Algorithm

$$\gcd(600,252)$$

$$600 = 2 \cdot 252 + 96 \qquad = \gcd(252,96)$$

$$252 = 2 \cdot 96 + 60 \qquad = \gcd(96,60)$$

$$96 = 1 \cdot 60 + 36 \qquad = \gcd(60,36)$$

$$60 = 1 \cdot 36 + 24 \qquad = \gcd(36,24)$$

$$36 = 1 \cdot 24 + 12 \qquad = \gcd(24,12)$$

$$24 = 2 \cdot 12 + 0 \qquad = \gcd(12,0) = 12$$

# Division Algorithm

If $a$ and $b$ are integers such that $b > 0$, then there are unique integers $q$ and $r$ such that

$$a = q\,b + r$$

with $0 \leq r < b$.

# Euclidean Algorithm

Let $r_0 = a$ and $r_1 = b$ be integers such that $a \geq b > 0$. If the division algorithm is successively applied to

$$r_j = q_{j+1} r_{j+1} + r_{j+2},$$

with $0 < r_{j+2} < r_{j+1}$ for $j = 0, 1, 2, \ldots, n-2$ and $r_{n+1} = 0$, then

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

the last nonzero remainder.

# Theorem

Let $a$ and $b$ be two integers, with at least one of $a, b$ nonzero, and let $d = \gcd(a, b)$. Then there exists integers $x, y$ such that

$$ax + by = d\,.$$

In particular, if $a$ and $b$ are relatively prime, then there exists integers $x, y$ with

$$ax + by = 1\,.$$

# Corollary (Euclid's Lemma)

If $p$ is a prime and $p$ divides a product of integers $ab$, then either $p|a$ or $p|b$.

Proof.

- If $p \mid a$, then done. Assume $p \nmid a$ .
- $p$ is prime, so $\gcd(a, p) = 1$ or $p$ (not $p$).
- There exist integers $x, y$ such that
$$ax + py = 1 \quad \Longrightarrow \quad bax + bpy = b$$
- Since $p \mid ab$ and $p \mid p$, $p \mid (bax + bpy) = b$. ∎