Number theory summary II

MAT 221, fall 2014

David Pierce

December 22, 2014

http://mat.msgsu.edu.tr/~dpierce/Dersler/

$\mathbb{N} = \{1, 2, 3, \dots\}$, the set of **natural numbers,** and letters will range over this set or else the set $\mathbb{Z}$ of **integers.** In $\mathbb{N}$ or $\mathbb{Z}$, the expression

$$a \mid b$$

means a **divides** b, and b is a **multiple** of a, that is, for some q, $aq = b$. In this case, in $\mathbb{N}$, $a \leqslant b$.

Division Theorem. *If $a \nmid b$, then for some unique q and r,*

$$b = aq + r \quad \& \quad r < a.$$

Since a and b have a common multiple (namely ab), they have a **least common multiple** (by the Well Ordering Theorem), denoted by

$$\operatorname{lcm}(a, b).$$

Since they have a common divisor (namely 1), and all common divisors are less than or equal to $\min\{a, b\}$, the numbers a and b have a **greatest common divisor,** denoted by

$$\gcd(a, b);$$

this can be found by the **Euclidean Algorithm.**

Theorem.

1. *$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$.*
2. *Every common divisor of a and b divides $\gcd(a, b)$.*
3. *$\operatorname{lcm}(a, b)$ divides every common multiple of a and b.*

Euclid's Lemma. *If $a \mid bc$, but $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. By the Euclidean Algorithm, in $\mathbb{Z}$ we can solve

$$ax + by = \gcd(a, b).$$

If $ax + by = 1$ and $a \mid bc$, then $acx + bcy = c$ and so $a \mid c$. □

The letter p always denotes a **prime number.** If $p \mid a$, we may define

$$a(p) = \max\{n \colon p^n \mid a\}.$$

(The existence of this maximum can be proved by contradiction and the Well Ordering Theorem.) If $p \nmid a$, we may let $a(p) = 0$. If always $a(p) \leqslant 1$, then a is **squarefree.**

Fundamental Theorem of Arithmetic. *Every natural number is a product of primes in only one way:*

$$a = \prod_p p^{a(p)}.$$

Proof. By the Strong Induction Theorem, every natural number is a product of primes; by Euclid's Lemma, it is so in only one way. □

Thus

$$\gcd(a, b) = \prod_p p^{\min\{a(p), b(p)\}}, \qquad \operatorname{lcm}(a, b) = \prod_p p^{\max\{a(p), b(p)\}}.$$

A **number-theoretic function** or **arithmetic function** is a function with domain $\mathbb{N}$. We define four of them:

- $\tau(a) = \sum_{d|a} 1$, the number of divisors of a;
- $\sigma(a) = \sum_{d|a} d$, the sum of the divisors of a;
- $\phi(a) = \left|\{x \in \mathbb{N} : x \leqslant n \ \ \& \ \ \gcd(x, n) = 1\}\right|$;
- $\mu(a) = \prod_{p|a}(-1)$, if a is squarefree; otherwise $\mu(a) = 0$.

An arithmetic function F is **multiplicative** if

$$\gcd(a, b) = 1 \implies F(ab) = F(a) \cdot F(b).$$

Theorem. *τ and σ are multiplicative, and*

$$\tau(a) = \prod_{p|a}(a(p) + 1), \qquad \sigma(a) = \prod_{p|a}\sum_{k=0}^{a(p)} p^k = \prod_{p|a} \frac{p^{a(p)+1} - 1}{p - 1}.$$

A number a is **perfect** if $\sigma(a) = 2a$. Examples include 6, 28, 496, and 8128. A **Mersenne prime** is a prime of the form $2^n - 1$, which is $\sum_{k=0}^{n-1} 2^k$. Examples include 3, 7, 31, and 127.

Theorem. *The even perfect numbers are just the numbers $p \cdot (p + 1)/2$, where p is a Mersenne prime.*

Möbius Inversion Theorem. *For arithmetic functions F and G,*

$$G(a) = \sum_{d|a} F(d) \implies F(a) = \sum_{d|a} \mu(d) \cdot G\left(\frac{a}{d}\right).$$

Proof. First prove the special case where $F(a) = \begin{cases} 1, & \text{if } a = 1, \\ 0, & \text{if } a > 1. \end{cases}$ □

Theorem. *ϕ is multiplicative, and*

$$\phi(a) = a \cdot \prod_{p|a}\left(1 - \frac{1}{p}\right) = \prod_{p|a}\left(p^{a(p)} - p^{a(p)-1}\right).$$

In particular, $\phi(p^r) = p^r - p^{r-1}$.

Proof. First show $\sum_{d|a} \phi(d) = a$. Then by Möbius Inversion,

$$\phi(a) = a \cdot \sum_{d|a} \frac{\mu(d)}{d} = a \cdot \sum_{d|p_1\cdots p_r} \frac{\mu(d)}{d},$$

where $p_1 \cdots p_r = \prod_{p|a} p$. By induction on r,

$$\sum_{d|p_1\cdots p_r} \frac{\mu(d)}{d} = \prod_{n=1}^{r} \left(1 - \frac{1}{p_n}\right). \qquad \square$$

For arbitrary *integers* a and b, if $m \in \mathbb{N}$ and $m \mid a - b$, we say a and b are **congruent** to one another, writing

$$a \equiv b \pmod{m}.$$

Fermat's Theorem. $a^p \equiv a \pmod{p}$, *and if* $p \nmid a$, *then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. By induction on a, or as a special case of the following. $\square$

Euler's Theorem. *If* $\gcd(a, m) = 1$, *then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof. If $\{x \in \mathbb{N} \colon x \leqslant m \ \& \ \gcd(x, m) = 1\} = \{b_1, \dots, b_{\phi(m)}\}$, then $\prod_{k=1}^{\phi(m)} (ab_k) \equiv \prod_{k=1}^{\phi(m)} b_k \pmod{m}$. $\square$

Chinese Remainder Theorem. *If* $\gcd(m, n) = 1$, *then every system*

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

is uniquely soluble modulo mn, *every solution being congruent to*

$$anc + bmd,$$

where $nc \equiv 1 \pmod{m}$ *and* $md \equiv 1 \pmod{n}$.