$105 = 7 \times 15 = 7 \times 3 \times 5$

$105 = 3 \times 35 = 3 \times 5 \times 7$

Math 214 Foundations of Higher Mathematics C.K. Li

Chapter 11 Number Theory

We practice proof techniques using number theory problems.

A goal: Prove the Fundamental Theorem of Arithmetic. → Every integer larger than 2 is a product of primes, and the list of primes used is unique.

11.1 Divisibility

Definition A positive integer $p \geq 2$ is a prime if 1 and p are the only positiver integer factor (divisor) of p.

A positive integer $n \geq 2$ is a $\boxed{\text{composite number}}$ if it is not a prime., i.e., $n = ab$, $a, b \in \mathbb{Z}$ $1 < a, b < n$

Lemma A positive integer $n \geq 2$ is composite if and only if $n = ab$ with $a, b \in \mathbf{N}$ such that $1 < a < n$ and $1 < b < n$.

Theorem Let a, b, c be integers such that $a \neq 0$.

(1) If $a|b$, then $a|bc$. (2) If $a|b$ and $b|c$, then $a|c$. (3) If $a|b$ and $a|c$, then $a|(b + c)$.

Suppose b is also nonzero.

(a) If $a|b$ and $b|a$, then $a = b$ or $a = -b$. (b) If $a|b$, then $|a| \leq |b|$.

Proof: $a, b, c \in \mathbb{Z}$, $a \neq 0$

(1) If $a|b$, i.e., $b = ak$ for some $k \in \mathbb{Z}$

Then $bc = akc = a\hat{k}$, with $\hat{k} = kc \in \mathbb{Z}$. $\therefore bc = a\hat{k}$.

(2) If $a|b$ and $b|c$, i.e., $b = al$, $c = bm$. $l, m \in \mathbb{Z}$

then $c = bm = (al)m = a(lm)$ $\therefore c = ak$ with $k = lm \in \mathbb{Z}$

(3) If $a|b$ and $a|c$, i.e., $b = al$, $c = am$ $l, m \in \mathbb{Z}$

$\therefore b + c = al + am = a(l + m)$ $\therefore b + c = ak$ $k = l + m \in \mathbb{Z}$

(a) If $a|b$, and $b|a$, $\therefore$ $b = al$, $a = bm$, $l, m \in \mathbb{Z}$.

$\therefore$ $a = bm = alm$

$\therefore$ $1 = lm$. $\therefore$ $(l,m) = (1,1)$ or $(l,m) = (-1,-1)$ $\Big\}$ otherwise $|lm| > 1$.

$\therefore$ $a = b$ or $a = -b$.

(b) If $a|b$, then $b = ak$

So $|b| = |a||k| \geq |a|$ $\because$ $|k| \geq 1$.

$\therefore$ $|a| \leq |b|$

$b = aq_1 + r_1$, $b = aq_2 + r_2$

11.2 Division Algorithm

Theorem Suppose $a, b \in \mathbf{N}$. Then there are unique integers a and r such that $b = aq + r$ with $0 \le r < a$.

Proof. Consider $S = \{b - ax : x \in \mathbf{Z}, b - ax \ge 0\}$. Then ....

Corollary (General form of the Division Algorithm) Suppose $a, b \in \mathbf{Z}$ and $a \ne 0$. Then there exist unique integers q and r such that $\boxed{b = aq + r \text{ with } 0 \le r < |a|}$.

Partition of integers in remainder classes

Definition/notation Let $n \ge 2$ be a positive integers.

$$\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

with $[k] = \{nx + k : x \in \mathbf{Z}\}$ is a partition of $\mathbf{Z}$. We say that

$$a \equiv b \pmod{n} \qquad \text{if} \qquad a - b \text{ is divisible by } n.$$

$\mathbb{Z}_{12} = \{[0], [1], \ldots [11]\}$

$[0] = \{12x : x \in \mathbb{Z}\}$

$= \{\ldots, -12, 0, 12, 24, \ldots\}$

$[1] = \{\ldots, -11, 1, 13, 25, \ldots\}$

$= \{12x + 1 : x \in \mathbb{Z}\}$

$\vdots$

$[11] = \{12x + 11 : x \in \mathbb{Z}\}$.

$S = \{b - ax : x \in \mathbb{Z}, b - ax \ge 0\}$

$b = aq + r$

$r \le |a|$

Example.

$b = -7$

$a = 2$

$-7 = 2 \times (-4) + 1$

$b = -7$

$a = \cancel{-9}\ -2$

$-7 = (-2)\boxed{4} + 1$

To prove that $\cancel{b = aq_1 + r_1 \ \& \ b = aq_2 + r_2}$.

① there are q, r such that $b = aq + r$
with $q \in \mathbb{Z}$, $r \in \{0, 1, \dots, a-1\}$.

② if $b = aq_2 + r_2$ with $q_2 \in \mathbb{Z}$, $r_2 \in \{0, 1, \dots, a-1\}$
then $q_2 = q$, $r_2 = r$.

Proof. ① Consider $S = \{b - ax : x \in \mathbb{Z}, b - ax \geq 0\}$
$\subseteq \mathbb{N} \cup \{0\}$.

$S \neq \phi$ because for $x = -1$, $b - ax = b + a > 0$.

Because $\mathbb{N} \cup \{0\}$ is well-ordered, there is a smallest element for S, say r.
Then there is $x = q$ such that
$r = b - ax = b - aq$.

$\therefore$ $b = aq + r$, $q \in \mathbb{Z}$, $r \in \{0, \dots, a-1\}$

Note that $r \in \{0, \dots, a-1\}$.
If not: $r - a = \hat{r}$ with $0 \leq \hat{r} < r$
and $b - aq - a = r - a = \hat{r} \in S$
as $b - aq - a = b - (q+1)a \in S$

---

② Suppose $b = aq_2 + r_2$, $q_2 \in \mathbb{Z}$, $r_2 \in \{0, 1, \dots, a-1\}$

Then $r_2 = b - aq_2 \in S$, $\therefore$ $r \leq r_2$.

If $r_2 > r$,

$0 < r_2 - r = (b - aq_2) - (b - aq) = a(q - q_2)$

Because $r, r_2 \in \{0, \dots, a-1\}$. $\therefore$ $r_2 - r < a$

$\therefore$ $r_2 - r = a(q - q_2)$ implies $q = q_2$.

Then $r_2 = b - q_2 = b - q = r$, which is a contradiction

$\therefore$ $\cancel{q_2 = q}$, $r_2 = r$. $\therefore$ $q_2 = q$

11.3 Greatest common divisors

Definition Suppose $a, b \in \mathbf{Z}$ are not both zero. Then their greatest common divisor is the largest common divisor of a and b.

~~The greatest common divisor~~ of a, b is the number $d = \gcd(a,b)$ such that

(1) $d \mid a \wedge d \mid b$

and

(2) if $\hat{d}$ s.t. $\hat{d} \mid a \wedge \hat{d} \mid b$

then $d \geq \hat{d}$

$\Updownarrow$

(2') $\hat{d} \mid d$

Theorem Let $a, b \in \mathbf{Z}$ are not both zero. Then the following condition are equivalent.

(1) d is the greatest common divisor of a and b.

(2) d is the smallest element in the set

$$S = \{ax + by : x, y \in \mathbf{Z}, ax + by \in \mathbf{N}\}.$$

(3) d is a common divisor of a and b, and $c \mid d$ for any common divisor c of a and b.

11.4 Euclidean Algorithm

Lemma Let $a, b \in \mathbf{N}$. If $b = aq + r$ with $0 \le r < a$, then $\gcd(a,b) = \gcd(r,a)$.

Consequently, there are positive integers $r_1 > r_2 > r_3 \cdots > r_{n-1}$ such that

$$\gcd(a,b) = \gcd(r_1, a) = \gcd(r_1, r_2) = \cdots = \gcd(0, r_{n-1}) = r_{n-1}.$$

Example: $\gcd(374, 946) =$

RSA scheme

$n = \underline{p}\,\underline{q}$

$$\begin{aligned}
&\gcd(374, 946) \\
&= \gcd(374, 198) \\
&= \gcd(176, 198) \\
&= \gcd(176, 22) \\
&= \gcd(22, 0) \\
&= 22
\end{aligned}$$

$\underline{22} = 374x + 946y$

$(x, y) = (-5, 2)$

$946 = 374 \cdot 2 + 198$

$\boxed{198 = 946 - 2 \times 374}$

$374 = 198 \cdot 1 + 176$

$\boxed{176 = 374 - 1 \times 198}$

$198 = 176 \cdot 1 + 22$

$\boxed{22 = 198 - 1 \times 176}$

$$\begin{array}{r} 2 \\ 374 \overline{)946} \\ \underline{748} \\ 198 \end{array} \qquad \begin{array}{r} 1 \\ 198 \overline{)374} \\ \underline{198} \\ 176 \end{array} \qquad \begin{array}{r} 8 \\ 22 \overline{)176} \\ \underline{176} \\ 0 \end{array}$$

$$\begin{aligned}
22 &= \cancel{176 \cdot 1 \; 198} \\
&= 198 - \cancel{176}\; 1 \times (176) \\
&= 198 - 1 \times (374 - 1 \times 198) \\
&= 2 \times 198 - 1 \times 374 \\
&= 2 \times (946 - 2 \times 374) - 1 \times 374 \\
&= 2 \times 946 + (-5) \times 374
\end{aligned}$$

Proof of Lemma: Use the fact: $\gcd(a,b) = \min\{ax+by : x, y \in \mathbb{Z},\ ax+by > 0\}$.

Then

$$\underline{\gcd(a,b) = \min\{ax+by : x, y \in \mathbb{Z},\ ax+by > 0\}}$$

~~gcd (~~ Let $b = aq + r_1$.

Then

$$\gcd(a, r_1)$$

$$= \min\{ax + r_1 z : x, z \in \mathbb{Z},\ ax + r_1 z > 0\}$$

$$= \min\{ax + (b-aq)z : x, z \in \mathbb{Z},\ ax + (b-aq)z > 0\}$$

$$= \min\{a(x-qz) + bz : x-qz,\ z \in \mathbb{Z},\ a(x-qz)+bz > 0\}$$

$$= \min\{ay + bz : y, z \in \mathbb{Z},\ ay+bz > 0\}$$

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