Some Miscellaneous Number Theory

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

Table of Contents

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that b divides a and write $b|a$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that b divides a and write $b|a$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Lemma 2 (Linear Combinations)

Given $a, b, c \in \mathbb{Z}$, $c|a$ and $c|b$ if and only if $\forall x, y \in \mathbb{Z}$ $c|(ax + by)$.

Proof of Lemma 2

($\Longrightarrow$) If $c|a$ and $c|b$, then $\forall\ x, y,\ \ c|(ax + by)$.

Proof by Definition.

By definition $a = cq_a$ and $b = cq_b$ for some unique q_a and q_b in $\mathbb{Z}$. Therefore,

$$ax + by = cq_a x + cq_b y \tag{1}$$
$$= c(q_a x + q_b y) \tag{2}$$

and by definition of divisibility $\forall\ x, y :\ \ c|(ax + by)$. □

Proof of Lemma 2

($\Longleftarrow$) If $\forall\ x, y,\ c|(ax + by)$, then $c|a$ and $c|b$.

Proof by Specification.

If $x = 1$ and $y = 0$, then $c|a$, and if $x = 0$ and $y = 1$, then $c|b$. $\square$

Divisibility

Definition 1 (Divisibility)

Given $a, b \in \mathbb{Z}$ we say that b divides a and write $b|a$ if and only if $\exists q \in \mathbb{Z}$, unique, such that $a = qb$.

Lemma 2 (Linear Combinations)

Given $a, b, c \in \mathbb{Z}$, $c|a$ and $c|b$ if and only if $\forall x, y \in \mathbb{Z}$ $c|(ax + by)$.

Theorem 3 (Division Algorithm)

Given $a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$, unique, such that $a = qb + r$ and $0 \leq r < |b|$.

Proof of The Division Algorithm (Theorem 3)

Proof of Existence.

Assume that $b > 0$. Let

$$S = \{a - tb | a - tb \geq 0 \text{ and } t \in \mathbb{Z}\};$$

since $t \leq a/b$ implies $a - bt \geq 0$, S is non-empty. Let r be the minimum value in S and q the corresponding coefficient of b so that $r = a - qb$, i.e. $a = qb + r$.

Proof of The Division Algorithm (Theorem 3)

Proof of Existence.

Assume that $b > 0$. Let

$$S = \{a - tb | a - tb \geq 0 \text{ and } t \in \mathbb{Z}\};$$

since $t \leq a/b$ implies $a - bt \geq 0$, S is non-empty. Let r be the minimum value in S and q the corresponding coefficient of b so that $r = a - qb$, i.e. $a = qb + r$. (Why must $r < b$?)

Proof of The Division Algorithm (Theorem 3)

Proof of Existence.

Assume that $b > 0$. Let

$$S = \{a - tb | a - tb \geq 0 \text{ and } t \in \mathbb{Z}\};$$

since $t \leq a/b$ implies $a - bt \geq 0$, S is non-empty. Let r be the minimum value in S and q the corresponding coefficient of b so that $r = a - qb$, i.e. $a = qb + r$. (Why must $r < b$?)

Note that if $b < 0$, then $t \geq a/b$ implies $a - bt \geq 0$ and S is non-empty. The proof then proceeds as before. □

Proof of The Division Algorithm (Theorem 3)

Proof of Uniqueness.

If $a = q_1 b + r_1$ and $a = q_2 b + r_2$, then

$$r_2 - r_1 = (q_1 - q_2)b$$

so that $b|(r_2 - r_1)$.

Proof of The Division Algorithm (Theorem 3)

Proof of Uniqueness.

If $a = q_1 b + r_1$ and $a = q_2 b + r_2$, then

$$r_2 - r_1 = (q_1 - q_2)b$$

so that $b|(r_2 - r_1)$. However, since $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$ we know $0 \leq |r_2 - r_1| < |b|$.

□

Proof of The Division Algorithm (Theorem 3)

Proof of Uniqueness.

If $a = q_1 b + r_1$ and $a = q_2 b + r_2$, then

$$r_2 - r_1 = (q_1 - q_2)b$$

so that $b|(r_2 - r_1)$. However, since $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$ we know $0 \leq |r_2 - r_1| < |b|$. Together these imply that $r_2 - r_1 = 0$ and $r_2 = r_1$. This tells us that $(q_1 - q_2)b = 0$ so that $q_1 = q_2$. Therefore the quotient and remainder are unique. □

Table of Contents

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The greatest common divisor of $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The greatest common divisor of $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Axiom 1 (Well Ordering Principle)

In any non-empty set of positive integers there exists a least element.

Greatest Common Divisor

Definition 4 (Greatest Common Divisor)

The greatest common divisor of $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, written (a, b), is the greatest positive integer d such that $d|a$ and $d|b$.

Axiom 1 (Well Ordering Principle)

In any non-empty set of positive integers there exists a least element.

Theorem 5 (Bezout's Lemma)

Given $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$ if and only if $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$ and it is the least such positive linear combination.

Proof of Theorem 5

Proof using the W.O.P. (Part 1).

Let $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$, and

$$S = \{ax + by | ax + by > 0 \text{ and } x, y \in \mathbb{Z}\}.$$

Proof of Theorem 5

Proof using the W.O.P. (Part 1).

Let $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$, and

$$S = \{ax + by | ax + by > 0 \text{ and } x, y \in \mathbb{Z}\}.$$

Since at least one of a, b, $-a$, or $-b$ must be in S, by the W.O.P. we can let c be the least element in S.

Proof of Theorem 5

Proof using the W.O.P. (Part 1).

Let $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $d = (a, b)$, and

$$S = \{ax + by | ax + by > 0 \text{ and } x, y \in \mathbb{Z}\}.$$

Since at least one of a, b, $-a$, or $-b$ must be in S, by the W.O.P. we can let c be the least element in S. By the definition of S,

$$\exists\, x, y : \ c = ax + by.$$

Lemma 2 guarantees that $d|c$ and so $d \leq c$. □

Proof of Theorem 5

Proof using the W.O.P. (Part 2).

By theorem 3 we know $a = qc + r$ with $0 \leq r < c$. Now

$$\begin{aligned} r &= a - qc && (3)\\ &= a - q(ax + by) && (4)\\ &= a(1 - qx) + b(-qy). && (5) \end{aligned}$$

□

Proof of Theorem 5

Proof using the W.O.P. (Part 2).

By theorem 3 we know $a = qc + r$ with $0 \leq r < c$. Now

$$r = a - qc \tag{3}$$
$$= a - q(ax + by) \tag{4}$$
$$= a(1 - qx) + b(-qy). \tag{5}$$

If $r \neq 0$, then $r \in S$ and this contradicts the assumption that c was the least element, therefore $r = 0$ and $c|a$. By similar proof, $c|b$.

Proof of Theorem 5

Proof using the W.O.P. (Part 2).

By theorem 3 we know $a = qc + r$ with $0 \leq r < c$. Now

$$\begin{aligned} r &= a - qc && (3)\\ &= a - q(ax + by) && (4)\\ &= a(1 - qx) + b(-qy). && (5) \end{aligned}$$

If $r \neq 0$, then $r \in S$ and this contradicts the assumption that c was the least element, therefore $r = 0$ and $c|a$. By similar proof, $c|b$. Since $c|a$ and $c|b$, it is a common divisor so $c \leq d$, and we conclude $c = d$. That is the greatest common divisor is the least positive linear combination. □

Table of Contents

Least Common Multiple

Definition 6 (Least Common Multiple)

The least common multiple of two integers a and b is the smallest positive integer l such that a|l and b|l. We will denote the least common multiple by $[a, b]$.

GCD and LCM

Lemma 7

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}$ is a common multiple of a and b, then $l = [a, b]$ divides m.

GCD and LCM

Lemma 7

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}$ is a common multiple of a and b, then $l = [a, b]$ divides m.

Theorem 8

Given $a, b \in \mathbb{Z}$, let $d = (a, b)$ and $l = [a, b]$, then $dl = |ab|$.

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$
- note $n = a(b/d) = b(a/d) \in \mathbb{N}$, so $l|n$ (by lemma 7) and $l \leq n$

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$
- note $n = a(b/d) = b(a/d) \in \mathbb{N}$, so $l|n$ (by lemma 7) and $l \leq n$
- thus $dl \leq dn = ab$

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$
- note $n = a(b/d) = b(a/d) \in \mathbb{N}$, so $l|n$ (by lemma 7) and $l \leq n$
- thus $dl \leq dn = ab$
- now $ab = ql$, so that $a = q\,(l/b)$ and $b = q\,(l/a)$

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$
- note $n = a(b/d) = b(a/d) \in \mathbb{N}$, so $l|n$ (by lemma 7) and $l \leq n$
- thus $dl \leq dn = ab$
- now $ab = ql$, so that $a = q\,(l/b)$ and $b = q\,(l/a)$
- hence $q|a$, $q|b$, and $q \leq d$

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$
- note $n = a(b/d) = b(a/d) \in \mathbb{N}$, so $l|n$ (by lemma 7) and $l \leq n$
- thus $dl \leq dn = ab$
- now $ab = ql$, so that $a = q\,(l/b)$ and $b = q\,(l/a)$
- hence $q|a$, $q|b$, and $q \leq d$
- thus $ab = ql \leq dl$

Product of GCD and LCM

Proof of Theorem 8.

- assume $a, b > 0$
- note $n = a(b/d) = b(a/d) \in \mathbb{N}$, so $l|n$ (by lemma 7) and $l \leq n$
- thus $dl \leq dn = ab$
- now $ab = ql$, so that $a = q\,(l/b)$ and $b = q\,(l/a)$
- hence $q|a$, $q|b$, and $q \leq d$
- thus $ab = ql \leq dl$
- $\therefore dl \leq ab$, $ab \leq dl$, and we conclude $ab = dl$

Table of Contents

Relations

Definition 9 (Relation)

A relation between two sets R and S is a subset of the Cartesian product $R \times S$.

Relations

Definition 9 (Relation)

A relation between two sets R and S is a subset of the Cartesian product $R \times S$.

Definition 10 (Equivalence Relation)

A relation between a set R and its self is an equivalence relation if it is reflexive, $a \sim a$, symmetric, $a \sim b \Rightarrow b \sim a$, and transitive, $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Relations

Definition 9 (Relation)

A relation between two sets R and S is a subset of the Cartesian product $R \times S$.

Definition 10 (Equivalence Relation)

A relation between a set R and its self is an equivalence relation if it is reflexive, $a \sim a$, symmetric, $a \sim b \Rightarrow b \sim a$, and transitive, $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Definition 11 (Equivalence Classes)

Given an equivalence relation on a set R the equivalence class of a in R is the set of all elements of R which are equivalent to a.

Modular Relations

Definition 12 (Modular Equivalnce)

Two integers a, b are equivalent modulo $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Modular Relations

Definition 12 (Modular Equivalnce)

Two integers a, b are equivalent modulo $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a-b)$.

Theorem 13

Modular equivalence is an equivalence relation.

Proof of Theorem 13

Proof by Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.

Proof of Theorem 13

Proof by Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
Since $a - a = 0$ and $n|0$, $a \equiv a \pmod{n}$ and modular equivalence is reflexive.

Proof of Theorem 13

Proof by Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
If $a \equiv b \pmod{n}$, by definition $n|(a - b)$, and there exists q such that $(a - b) = qn$. Then, $(b - a) = -qn$, $n|(b - a)$, and $b \equiv a \pmod{n}$. Thus modular equivalence is symmetric.

Proof of Theorem 13

Proof by Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $n|(a-b)$ and $n|(b-c)$.
Hence, $(a-b) = q_0 n$, $(b-c) = q_1 n$, and

$$(a-c) = (a-b+b-c) = (q_0 - q_1)n,$$

i.e. $a \equiv c \pmod{n}$ and modular equivalence is transitive.

Proof of Theorem 13

Proof by Satisfying a Definition.

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$.
Since we have shown that modular equivalence is reflexive, symmetric, and transitive, we may conclude that it is an equivalence relation. □

Modular Relations

Definition 12 (Modular Equivalnce)

Two integers a, b are equivalent modulo $n \in \mathbb{N}$, written $a \equiv b \pmod{n}$, if $n|(a - b)$.

Theorem 13

Modular equivalence is an equivalence relation.

Theorem 14 (Modular Arithmetic)

Given $a, b, c, d, n \in \mathbb{Z}$ with $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$,

$$a \pm c \equiv b \pm d \pmod{n} \text{ and } ac \equiv bd \pmod{n}.$$

Table of Contents

Basic Linear Equation

Lemma 15

If $(a, n) = 1$ for $a, n \in \mathbb{N}$, then a has a multiplicative inverse modulo n.

Basic Linear Equation

Lemma 15

If $(a, n) = 1$ for $a, n \in \mathbb{N}$, then a has a multiplicative inverse modulo n.

- $1 = ax + ny$
- $1 = ax + ny \equiv ax \pmod{n}$

Basic Linear Equation

Lemma 15

If $(a, n) = 1$ for $a, n \in \mathbb{N}$, then a has a multiplicative inverse modulo n.

- $1 = ax + ny$
- $1 = ax + ny \equiv ax \pmod{n}$
- $x \equiv a^{-1} \pmod{n}$

Basic Linear Equation

Lemma 15

If $(a, n) = 1$ for $a, n \in \mathbb{N}$, then a has a multiplicative inverse modulo n.

- $1 = ax + ny$
- $1 = ax + ny \equiv ax \pmod{n}$
- $x \equiv a^{-1} \pmod{n}$

$\therefore$ we can always solve equations of the form $mx + b \equiv a \pmod{n}$ provided $(n, m) = 1$.

Basic Linear Equation

Lemma 15

If $(a, n) = 1$ for $a, n \in \mathbb{N}$, then a has a multiplicative inverse modulo n.

- $1 = ax + ny$
- $1 = ax + ny \equiv ax \pmod{n}$
- $x \equiv a^{-1} \pmod{n}$

$\therefore$ we can always solve equations of the form $mx + b \equiv a \pmod{n}$ provided $(n, m) = 1$.

Basic Linear Equation

Lemma 15

If $(a, n) = 1$ for $a, n \in \mathbb{N}$, then a has a multiplicative inverse modulo n.

Lemma 16

Given $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$, then

$$ax + b \equiv c \pmod{n}$$

has a solution if and only if $d = (a, n)$ divides $c - b$.

Systems of Equations

Theorem 17 (Chinese Remainder Theorem)

The system of equations:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution modulo

$$M = n_1 n_2 n_3 \cdots n_k$$

provided $(n_i, n_j) = 1$ for $i \neq j$.

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

- $M = n_1 n_2 n_3 \cdots n_k$

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

- $M = n_1 n_2 n_3 \cdots n_k$
- $M_i = M/n_i$

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

- $M = n_1 n_2 n_3 \cdots n_k$
- $M_i = M/n_i$
- $\overline{M_i} \equiv M_i^{-1} \pmod{n_i}$

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \quad\quad\quad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

- $M = n_1 n_2 n_3 \cdots n_k$
- $M_i = M/n_i$
- $\overline{M_i} \equiv M_i^{-1} \pmod{n_i}$

- $a_j M_j \overline{M_j} \equiv 0 \pmod{n_i}$ if $j \neq i$

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \quad\quad\quad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

- $M = n_1 n_2 n_3 \cdots n_k$
- $M_i = M/n_i$
- $\overline{M_i} \equiv M_i^{-1} \pmod{n_i}$

- $a_j M_j \overline{M_j} \equiv 0 \pmod{n_i}$ if $j \neq i$
- $a_i M_i \overline{M_i} \equiv a_i \pmod{n_i}$

Systems of Equations

Given:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\vdots \quad\quad\quad \vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

- $M = n_1 n_2 n_3 \cdots n_k$
- $M_i = M/n_i$
- $\overline{M_i} \equiv M_i^{-1} \pmod{n_i}$

- $a_j M_j \overline{M_j} \equiv 0 \pmod{n_i}$ if $j \neq i$
- $a_i M_i \overline{M_i} \equiv a_i \pmod{n_i}$
- $x \equiv \sum_i a_i M_i \overline{M_i} \pmod{M}$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

- $M = 17 \cdot 23 = 391$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

- $M = 17 \cdot 23 = 391$
- $M_1 = 23$ and $M_2 = 17$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

- $M = 17 \cdot 23 = 391$
- $M_1 = 23$ and $M_2 = 17$
- $\overline{M_1} \equiv 23^{-1} \pmod{17} = 3$ and $\overline{M_2} \equiv 17^{-1} \pmod{23} = 19$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

- $M = 17 \cdot 23 = 391$
- $M_1 = 23$ and $M_2 = 17$
- $\overline{M_1} \equiv 23^{-1} \pmod{17} = 3$ and $\overline{M_2} \equiv 17^{-1} \pmod{23} = 19$
- $8 \cdot 23 \cdot 3 = 552 \equiv 161 \pmod{391}$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

- $M = 17 \cdot 23 = 391$
- $M_1 = 23$ and $M_2 = 17$
- $\overline{M_1} \equiv 23^{-1} \pmod{17} = 3$ and $\overline{M_2} \equiv 17^{-1} \pmod{23} = 19$
- $8 \cdot 23 \cdot 3 = 552 \equiv 161 \pmod{391}$
- $10 \cdot 17 \cdot 19 = 3230 \equiv 102 \pmod{391}$

Example of the CRT

Given:

$$\begin{aligned} x &\equiv 8 \pmod{17} \\ x &\equiv 10 \pmod{23} \end{aligned}$$

- $M = 17 \cdot 23 = 391$
- $M_1 = 23$ and $M_2 = 17$
- $\overline{M_1} \equiv 23^{-1} \pmod{17} = 3$ and $\overline{M_2} \equiv 17^{-1} \pmod{23} = 19$
- $8 \cdot 23 \cdot 3 = 552 \equiv 161 \pmod{391}$
- $10 \cdot 17 \cdot 19 = 3230 \equiv 102 \pmod{391}$
- $x \equiv 161 + 102 \equiv 263 \pmod{391}$

Table of Contents

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$
- $\phi(6) = 2$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$
- $\phi(6) = 2$
- $\phi(7) = 6$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$
- $\phi(6) = 2$
- $\phi(7) = 6$
- $\phi(8) = 4$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$
- $\phi(6) = 2$
- $\phi(7) = 6$
- $\phi(8) = 4$
- $\phi(9) = 6$

Definitions

Definition 18 (Relatively Prime)

Given $a, b \in \mathbb{Z}$, if $(a, b) = 1$ then we say that they are relatively prime.

Definition 19 (Euler's ϕ-Function)

Given $a \in \mathbb{N}$ define $\phi(a)$ to be the number of positive integers less than or equal to a which are relatively prime to a.

- $\phi(1) = 1$
- $\phi(2) = 1$
- $\phi(3) = 2$
- $\phi(4) = 2$
- $\phi(5) = 4$
- $\phi(6) = 2$
- $\phi(7) = 6$
- $\phi(8) = 4$
- $\phi(9) = 6$
- $\phi(10) = 4$

Some Results

Lemma 20

If $p \in \mathbb{N}$ is prime, then $\phi(p^k) = (p-1) \cdot p^k$.

Some Results

Lemma 20

If $p \in \mathbb{N}$ is prime, then $\phi(p^k) = (p-1) \cdot p^k$.

Theorem 21

If $m, n \in \mathbb{N}$ are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Residue Classes

Definition 24 (Complete Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a complete residue system for n if for every integer a there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Typically the class representatives are $0, 1, 2, \ldots, (n-1)$ and we assume there are no duplicates.

Residue Classes

Definition 24 (Complete Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a complete residue system for n if for every integer a there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Typically the class representatives are $0, 1, 2, \ldots, (n-1)$ and we assume there are no duplicates.

Lemma 25

If S is a complete residue system modulo n and a is relatively prime to n, then the sets

$$aS = \{as | s \in S\}$$

and

$$aS + r = \{as + r | s \in S \text{ and } r \in \mathbb{Z} \text{ is given}\}$$

are both complete residue systems modulo n.

ϕ is Multiplicative

$$\phi(15) = \phi(3)\phi(5)$$

$$\left.\begin{array}{ccccc} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \\ 3 & 6 & 9 & 12 & 15 \end{array}\right\} q3 + r$$

$$q = 0, \ldots, 4 \text{ and } r = 0, \ldots, 3$$

ϕ is Multiplicative

$$\phi(15) = \phi(3)\phi(5)$$

$$\left.\begin{array}{ccccc} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \\ 3 & 6 & 9 & 12 & 15 \end{array}\right\} q3 + r$$

$$q = 0, \ldots, 4 \text{ and } r = 0, \ldots, 3$$

$\phi(3)$ rows are relatively prime to 3

ϕ is Multiplicative

$$\phi(15) = \phi(3)\phi(5)$$

$$\left.\begin{array}{ccccc} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \\ 3 & 6 & 9 & 12 & 15 \end{array}\right\} q3 + r$$

$$q = 0, \ldots, 4 \text{ and } r = 0, \ldots, 3$$

$\phi(5)$ entries per row are relatively prime to 5

ϕ is Multiplicative

$$\phi(15) = \phi(3)\phi(5)$$

$$\left.\begin{array}{ccccc} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \\ 3 & 6 & 9 & 12 & 15 \end{array}\right\} q3 + r$$

$$q = 0, \ldots, 4 \text{ and } r = 0, \ldots, 3$$

$\phi(15) = \phi(3)\phi(5)$ are relatively prime to 15

Some Results

Lemma 20

If $p \in \mathbb{N}$ is prime, then $\phi(p^k) = (p-1) \cdot p^k$.

Theorem 21

If $m, n \in \mathbb{N}$ are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Theorem 22 (Euler's Theorem)

If $a, n \in \mathbb{N}$ and $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proving Euler's Theorem

Definition 26 (Reduced Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a reduced residue system for n if for every integer a relatively prime to n there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Note that $|S| = \phi(n)$.

Proving Euler's Theorem

Definition 26 (Reduced Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a reduced residue system for n if for every integer a relatively prime to n there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Note that $|S| = \phi(n)$.

- let S be a reduced residue system

Proving Euler's Theorem

Definition 26 (Reduced Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a reduced residue system for n if for every integer a relatively prime to n there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Note that $|S| = \phi(n)$.

- let S be a reduced residue system
- then $aS = \{as | s \in S\}$ is also a reduced residue system

Proving Euler's Theorem

Definition 26 (Reduced Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a reduced residue system for n if for every integer a relatively prime to n there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Note that $|S| = \phi(n)$.

- let S be a reduced residue system
- then $aS = \{as | s \in S\}$ is also a reduced residue system
- $$\prod_{s \in S} s \equiv \prod_{s \in S} as \equiv a^{\phi(n)} \prod_{s \in S} s \pmod{n}$$

Proving Euler's Theorem

Definition 26 (Reduced Residue System)

Given $n \in \mathbb{N}$ we say that a set S is a reduced residue system for n if for every integer a relatively prime to n there exists an element $s \in S$ such that $a \equiv s \pmod{n}$. Note that $|S| = \phi(n)$.

- let S be a reduced residue system
- then $aS = \{as | s \in S\}$ is also a reduced residue system
- $$\prod_{s \in S} s \equiv \prod_{s \in S} as \equiv a^{\phi(n)} \prod_{s \in S} s \pmod{n}$$
- $a^{\phi(n)} \equiv 1 \pmod{n}$

Some Results

Lemma 20

If $p \in \mathbb{N}$ is prime, then $\phi(p^k) = (p-1) \cdot p^k$.

Theorem 21

If $m, n \in \mathbb{N}$ are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Theorem 22 (Euler's Theorem)

If $a, n \in \mathbb{N}$ and $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 23 (Fermat's Little Theorem)

If $a, p \in \mathbb{N}$, p prime, and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Table of Contents

Miscellaneous Proofs

Claim (A False Conjecture)

There exist infinitely many $n \in \mathbb{N}$ such that $n^2 + 4n - 5$ is prime.

Miscellaneous Proofs

Claim (A False Conjecture)

There exist infinitely many $n \in \mathbb{N}$ such that $n^2 + 4n - 5$ is prime.

Counter Claim.

Note that $n^2 + 4n - 5 = (n+5)(n-1)$, if $n = 1$ this is 0, if $n = 2$ this is 7 (which is prime), and if $n > 2$ this is composite. So,

$$\forall n \in \mathbb{N},\ \text{if } n > 2, \text{then } n^2 + 4n - 5 = (n+5)(n-1) \text{ is composite.}$$

Miscellaneous Proofs

Definition 27 (Lots of Ones Sequence)

For $n = 0$ let $a_0 = 12$, and for $n > 0$ let $a_n = 10 \cdot a_{n-1} + 1$, so that

$$a_0 = 12,\ a_1 = 121,\ a_2 = 1211,\ a_3 = 12111,\ \ldots$$

Miscellaneous Proofs

Definition 27 (Lots of Ones Sequence)

For $n = 0$ let $a_0 = 12$, and for $n > 0$ let $a_n = 10 \cdot a_{n-1} + 1$, so that

$$a_0 = 12,\ a_1 = 121,\ a_2 = 1211,\ a_3 = 12111,\ \ldots$$

Theorem 28

For all n the term a_{3n} is divisible by 3.

Miscellaneous Proofs

Proof by Induction.

If $n = 0$, then $a_{3n} = a_0 = 12 = 3 \cdot 4$, and so by definition $3 | a_{3n}$.

Miscellaneous Proofs

Proof by Induction.

If $n = 0$, then $a_{3n} = a_0 = 12 = 3 \cdot 4$, and so by definition $3|a_{3n}$.
Suppose that $3|a_{3n}$ for some n and consider $a_{3(n+1)}$. By the definition of the sequence

$$a_{3(n+1)} = a_{3n+3} = 10^3 \cdot a_{3n} + 111.$$

Miscellaneous Proofs

Proof by Induction.

If $n = 0$, then $a_{3n} = a_0 = 12 = 3 \cdot 4$, and so by definition $3|a_{3n}$.
Suppose that $3|a_{3n}$ for some n and consider $a_{3(n+1)}$. By the definition of the sequence

$$a_{3(n+1)} = a_{3n+3} = 10^3 \cdot a_{3n} + 111.$$

Note that $111 = 3 \cdot 37$ and by the induction assumption $a_{3n} = 3 \cdot m$ for some m. Therefore

$$a_{3(n+1)} = 10^3 \cdot 3 \cdot m + 3 \cdot 37 = 3 \cdot (10^3 \cdot m + 37),$$

which means that, by the definition of divisibility, $3|a_{3(n+1)}$.

□

Miscellaneous Proofs

Proof by Induction.

If $n = 0$, then $a_{3n} = a_0 = 12 = 3 \cdot 4$, and so by definition $3|a_{3n}$.
Suppose that $3|a_{3n}$ for some n and consider $a_{3(n+1)}$. By the definition of the sequence

$$a_{3(n+1)} = a_{3n+3} = 10^3 \cdot a_{3n} + 111.$$

Note that $111 = 3 \cdot 37$ and by the induction assumption $a_{3n} = 3 \cdot m$ for some m. Therefore

$$a_{3(n+1)} = 10^3 \cdot 3 \cdot m + 3 \cdot 37 = 3 \cdot (10^3 \cdot m + 37),$$

which means that, by the definition of divisibility, $3|a_{3(n+1)}$. Thus, by the principle of mathematical induction $3|a_{3n}$ for all n. □

Miscellaneous Proofs

Definition 27 (Lots of Ones Sequence)

For $n = 0$ let $a_0 = 12$, and for $n > 0$ let $a_n = 10 \cdot a_{n-1} + 1$, so that

$$a_0 = 12,\ a_1 = 121,\ a_2 = 1211,\ a_3 = 12111,\ \ldots$$

Claim (Another False Conjecture)

For all values of n, a_n as defined in definition 27 is composite.

Miscellaneous Proofs

Claim (Another False Conjecture)

For all values of n, a_n as defined in definition 27 is composite.

Counter Example.

Running the code:

```
[> a=12
[> for n in range(200):
      if is_prime(a):
          print "a_",n,"is prime"
      a=10*a+1
```

we get the output `a_136 is prime` and `a_184 is prime`.

Some Miscellaneous Number Theory

Dr. Chuck Rocca
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES