MAT2120 Number Theory
Lecture Notes

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

1 Divisibility Theory

1.1 September 5th

(Class missed; all principles mentioned in class are written below at September 5th lecture notes.)

1.2 September 10th

1. **Well Ordering Principle**(WOP). Every nonempty set of positive integers has a least element.
2. **Principle of Mathematical Induction**. Let S be a set of positive integers. If S satisfies the following two conditions
   (a) $1 \in S$
   (b) $n \in S \Rightarrow n+1 \in S$
   then S is the set of all positive integers.
3. **Archimedean property**. $\forall a, b \in \mathbb{N}$, then $\exists n \in \mathbb{N}$ such that $na > b$.

Remark 1. $1 \Leftrightarrow 2 \Rightarrow 3$.

Definition 1. *If $a, b \in \mathbb{Z}$, then a* ***divides*** *b, denoted by $a \mid b$, if $c \in \mathbb{Z}$ such that $b = ac$.*

We write $a \nmid b$ if a does not divide b.

Theorem 1 (The Division Algorithm). *If $a, b \in \mathbb{Z}$, $b > 0$, then there are unique integers q and r such that*

$$a = bq + r$$

where $0 \leq r < b$.

Proof. Consider

$$S = \{a - bk \mid k \in \mathbb{Z}\}.$$

Let T be the set of all nonnegative integers in S. Since $T \neq \emptyset$, it follows the WOP, thus T has a least element of $r = a - bq$, and it is clear that $r \geq 0$.

We will claim that $r < b$. Suppose $r \geq b$. then

$$\begin{aligned} r &> r - b \\ &= a - bq - b \\ &= a - (q+1)b \geq 0. \end{aligned}$$

This contradicts to the choice of r: which is that r is the minimum element of S. Hence, $r < b$.

We will claim that q and r are unique. Suppose that $a = bq_1 + r_1 = bq_2 + r_2$, where $0 \leq r_1, r_2 < b$. Note that

$$\begin{aligned} 0 &= b(q_1 - q_2) + (r_1 - r_2) \\ \Rightarrow r_2 = r_1 &= b(q_1 - q_2), \end{aligned}$$

thus $b \mid (r_2 - r_1)$.

Since $0 \leq r_1, r_2 < b$, we have $-1 < r_2 - r_1 < b$. Thus $r_2 - r_1 = 0$, i. e. $r_1 = r_2$. Since $bq_1 + r_1 = bq_2 + r_2$, $q_1 = q_2$. □

Remark 2. 1. If $a, b \in \mathbb{Z}$, $b \neq 0$ then $a = bq + r$, where $0 \leq r < |b|$.
2. If $f(x) = g(x)q(x) + r(x)$, then $0 \leq \deg r(x) < \deg g(x)$.

Theorem 2 (Greatest Common Divisor). *Suppose $a, b \in \mathbb{Z}$, where $a \neq 0$ and $b \neq 0$. Then $\exists! d \in \mathbb{Z}$ satisfying the followings:*

1. $d > 0$.
2. $d \mid a$, $d \mid b$.
3. $k \mid a$, $k \mid b \Rightarrow k \mid d$.

Proof. By WOP, we may choose d to be the least positive integer of the form[1]

$$d = ax + by \qquad x, y \in \mathbb{Z}.$$

It is clear that $d > 0$, and if $k \mid a$, $k \mid d$ then $k \mid (ax + by) = d$.

Note that by the division algorithm, $\exists t, u \in \mathbb{Z}$ such that $a = dt + u$ where $0 \leq u < d$. Then

$$\begin{aligned} dt + u &= (ax + by)t + u \\ &= axt + byt + u, \end{aligned}$$

and so

$$a(1 - xt) + b(-yt) = u.$$

Since $u < d$, it follows the minimality of d that $u = 0$, thus $d \mid a$. Similarily we can show that $d \mid b$.

Remains to show the uniqueness of d. Suppose that d' satifies above conditions. then $d \mid d'$ and $d' \mid d$. Hence $d = d'$, because $d, d' > 0$.

Definition 2 (Greatest Common Divisor). $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$.

The unique positive integer d given by the theorem above is called the ***greatest common divisor*** *of a and b. It is denoted by* $\gcd(a, b)$, *or* (a, b).

[1] Consider $S = \{ax + by \mid x, y \in \mathbb{Z}\} \supset T = \{s \in S \mid s > 0\} \neq \emptyset$. By WOP, $\exists d \in T$.

Remark 3. 1. $(a,0) = |a|$, $(0,0) := 0$.
2. $7 = (14, 21)$.

Theorem 3. *For any $m \in \mathbb{Z}$,*

$$m\mathbb{Z} := \{mx \mid x \in \mathbb{Z}\}$$

is closed under $+$ and $-$.[2]

Conversely, if a nonempty subset S of $\mathbb{Z}$ is closed under $+$ and $-$, then $\exists! m \geq 0 \in \mathbb{Z}$ such that $S = m\mathbb{Z}$.

1.3 September 19th

Proof. $S \subset \mathbb{Z} \Rightarrow S = m\mathbb{Z}$

Since $S \neq \emptyset$, $\exists a \in S$

Since S is closed under $+, -$, $0 \in S$. We may assume that $S \neq \{0\}$. (if $S = \{0\}$, then $S = 0 \cdot \mathbb{Z}$)

Take any $n \in S$. Then $0 - n = -n \in S$. Thus we may also assume that S has a positive integer.

In all, WLOG[3], we may assume that S has a positive integer.

$A = B \Rightarrow A \subset B$ and $B \subset A$
$A \subset B \Rightarrow$ if $x \in A$ then $x \in B$

By WOP, S has a least positive integer m. We want to show that $S = m\mathbb{Z}$.

1. $m\mathbb{Z} \subset S$
   $m \in S$ and S is closed under $+, -$. So S must have all multiples of m.
2. $S \subset m\mathbb{Z}$
   Take any $a \in S$. By division algorithm, $\exists q, r \in \mathbb{Z}$ such that $a = qm + r$ where $0 \leq r < m$. Since $mq \in S$ and $a \in S$,

$$r = a - mq \in S$$

[3] Without loss of generality

. Thus $r = 0$ by the minimality of m. Hence $a = mq \in m\mathbb{Z}$.

Remains to show the uniqueness of m. Suppose $m\mathbb{Z} = S = m'\mathbb{Z}$. Then $m = \pm m'$. Since $m, m' > 0$, $m = m'$.

Theorem 4. *Let $d = (a, b)$. Then $d = ax + by$ for some $x, y \in \mathbb{Z}$ and $\{ax + by \mid x, y \in \mathbb{Z}\}$ is the set of all multiples of d. i. e. $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$.*

Proof. We knew that $d = ax + by$ for some $x, y \in \mathbb{Z}$. (by the theorem in the last class)

Define $S := a\mathbb{Z} + b\mathbb{Z}$. Then $a\mathbb{Z} \subset S$ and $b\mathbb{Z} \subset S$. Since S is closed under $+$, $-$, it follows the previous theorem that

$$\exists m \geq 0 \in \mathbb{Z} \text{ such that } S = m\mathbb{Z}.$$

We want to show that $m = d$. Since $a, b \in S = m\mathbb{Z}$, $m \mid a$, $m \mid b$. If $e \mid a$ and $e \mid b$, then $e \mid m$. ($\because m + as + bt$ for some $s, t \in \mathbb{Z}$)

By the definition of GCD, $m = d$.

Remark 4. The GCD of a and b (not both 0) is the least positive integer that is a linear combination of a and b.

Theorem 5 (Euclidean Algorithm). *$a, b \in \mathbb{Z}$, $a \neq 0$. Using the division algorithm,*

$$b = aq_1 + r_1, \text{ where } 0 < r_1 < |a|.$$

If $r_1 = 0$, terminate process.

Repeating process,

$$\begin{aligned} a &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

Then $(a, b) = r_n$.

Proof. Clearly, $r_n > 0$. Note that

$$\begin{aligned} r_n \mid r_{n-1}, r_n \mid r_n &\Rightarrow r_n \mid r_{n-2} \\ r_n \mid r_{n-2}, r_n \mid r_{n-1} &\Rightarrow r_n \mid r_{n-3} \\ &\vdots \\ r_n \mid r_1, r_n \mid r_2 &\Rightarrow r_n \mid a \\ r_n \mid a, r_n \mid r_1 &\Rightarrow r_n \mid b \end{aligned}$$

Note also that if

$$\begin{aligned} k \mid a, k \mid b &\Rightarrow k \mid r_1 \\ k \mid r_1, k \mid a &\Rightarrow k \mid r_2 \\ &\vdots \\ k \mid r_n, k \mid r_{n-1} &\Rightarrow k \mid r_n \end{aligned}$$

Hence we conclude that $r_n = (a, b)$.

Proof (Alternate proof).

$$b = aq + r \Rightarrow (a, b) = (a, r) \qquad r = a(-q) + b, b = aq + r$$

Note that $e \mid a$, $e \mid b$ iff $e \mid r$, $e \mid a$. Thus $(a, b) \mid (a, b)$ and $(a, k) \mid (a, b)$.

Hence $(a, b) = (a, r)$, since $(a, b) > 0$ and $(a, k) > 0$. Therefore we can see that

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

Example

$$\begin{aligned} (68, 710) &= 2 \\ 710 &= 68 \cdot 10 + 30 \\ 68 &= 30 \cdot 2 + 8 \\ 30 &= 8 \cdot 3 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 \end{aligned}$$

$$\begin{aligned} 2 &= 8 - 6 \cdot 1 \\ &= 8 - (30 - 8 \cdot 3) \\ &= 8 \cdot 4 + 30 \cdot (-1) \\ &= (68 - 30 \cdot 2) \cdot 4 + 30 \cdot (-1) \\ &= 68 \cdot 4 + 30 \cdot (-1) \\ &= 68 \cdot 4 + (710 - 68 \cdot 10) \cdot (-9) \\ &= 68 \cdot 94 + 710 \cdot (-9) \end{aligned}$$

Definition 3 (Diophantine Equation). *A **Diophantine equation** is a polynomial equation that allows two or more variables to take integer values only.*

e. g.

$$ax + by = c$$

$$x^n + y^n = z^n$$

$$x^2 - dy^2 = 1$$

Theorem 6. *$a \neq 0$, $b \neq 0$.*

1. *The equation $ax + by = c$ has integer solutions if and only if $(a, b) \mid c$.*
2. *Suppose that $(a, b) \mid c$. Then the general solution of the equation $ax + by = c$ has form the of*
$$\left\{x_0 + \frac{b}{(a, b)}t,\, y_0 - \frac{a}{(a, b)}t\right\}$$
where $t \in \mathbb{Z}$ and (x_0, y_0) is an arbitrary solution of the equation.

General solution for $y'' - 4y' + 3y = 0$?
$\Rightarrow c_1 e^x + c_2 e^{3x}$
– 2 bases

1.4 September 24th

Proof. Note that

$$\begin{aligned} &a \mid b, a \mid c \Rightarrow a \mid (bx + cy) \qquad \forall x, y \in \mathbb{Z} \\ &m \mid ab, (m, a) = 1 \Rightarrow m \mid b \qquad \because (m, a) = 1, \exists s, t \in \mathbb{Z} \qquad as + mt = 1 \end{aligned}$$

Then $bas + bmt = b$.

Since $m \mid ab$, it follows that $m \mid b$.

1. $(\Rightarrow)$ $(a, b) \mid a$, $(a, b) \mid b \Rightarrow (a, b) \mid (ax + by) = c$
   $(\Leftarrow)$ Let $(a, b) = d$ and $c = c_1 d$. Then $\exists s, t \in \mathbb{Z}$ such that $as + bt = d$. thus
   $$\begin{aligned} c = c_1 d &= c_1 (as + bt) \\ &= ac_1 s + bc_1 t \end{aligned}$$
   hence $(c_1 s, c_1 t)$ is a solution.

2. Note that

$$
\begin{aligned}
& a\left(x_0+\frac{b}{d}t\right)+b\left(y_0-\frac{a}{d}t\right)\\
=& ax_0+\frac{ab}{d}t+by_0-\frac{ba}{d}t\\
=& ax_0+by_0=c
\end{aligned}
$$

Suppose that (x, y) is an arbitrary solution of $ax+by=c$. Since $ax+by=c=ax_0+by_0$, we have

$$a(x-x_0)=b(y_0-y).$$

Let $a=a_1d$, $b=b_1d$, where $d=(a, b)$. Then

$$a_1(x-x_0)=b_1(y_0-y).$$

Since $(a, b)=1$, $b_1 \mid (x-x_0)$. Then $\exists t\in\mathbb{Z}$ such that $x-x_0=b_1t$, and similarily $y_0-y=a_1t$. Hence

$$x=x_0+\frac{b}{(a, b)}t, y=y_0-\frac{a}{(a, b)}t.$$

Example

$$710x+68y=6$$

[4] Recall

$$
\begin{aligned}
710\cdot(-9)+68\cdot 94=2\\
710\cdot(-9\times 3)+68\cdot(94\times 3)=2\times 3=6
\end{aligned}
$$

Hence

$$
\begin{aligned}
x=-27+\frac{68}{2}t=-27+34t\\
x=282-\frac{710}{2}t=282-355t
\end{aligned}
$$

[4] Maybe an eaxm problem?

Definition 4 (Least Common Multiple). *The* ***least common multiple*** *of two nonzero integers a and b, denoted* $[a, b]$ *or* $\operatorname{lcm}(a, b)$ *is the integer l satisfying the followings:*

1. $l > 0$.
2. $a \mid l$, $b \mid l$.
3. $a \mid c$, $b \mid c \Rightarrow l \mid c$.

Theorem 7. *For* $a \neq 0, b \neq 0 \in \mathbb{Z}$, $[a, b]$ *uniquely exists. Moreover,* $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}$.

Proof. Let $S = a\mathbb{Z} \cap b\mathbb{Z}$. Since $ab \in S$, $S \neq \emptyset$. Clearly, S is closed under $+, -$.

By theorem, $\exists l$ such that $S = l\mathbb{Z}$.

We want to show that $l = [a, b]$. Since $l \in S$, $a \mid l$, $b \mid l$. If $a \mid c$, $b \mid c$, then $c \in S = l\mathbb{Z}$ and $l \mid c$.

Remains to show the uniqueness of l. Suppose l_1 and l_2 are both the LCMs of a and b. Then $l_1 \mid l_2$ and $l_2 \mid l_1$. By (2), (3), $l_1 = l_2$, since $l_1 > 0$, $l_2 > 0$.

Remark 5.

$$(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

Recall

1. $(0, 0) := 0$
2. $(a, 0) := |a|$
3. $[0, 0] := 0$
4. $[a, 0] := 0$

Theorem 8. *For $a > 0, b > 0 \in \mathbb{Z}$,*

$$(a, b)\,[a, b] = ab.$$

Proof. (Proof left for homework – due September 26th.)

Theorem 9. *Let b be a positive integer with $b > 1$. Then every positive integer n can be expressed in unique form of*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0$$

where $a_i \in \mathbb{Z}$, $0 \leq a_i \leq b-1$ for $i = 0, 1, \cdots, k$ and $a_k \neq 0$.

$b \Rightarrow$ base.

Proof. We use the division algorithm. (Proof left for homework – due September 26th.)

Definition 5 (Prime Numbers). *A **prime** is an integer p such that*

1. $p > 1$.
2. $a \mid p \Rightarrow a = \pm 1$ *or* $\pm p$.

Remark 6. p is prime.

1. $\forall a \in \mathbb{Z}$, $(a, p) = 1$ or $(a, p) = p$. (iff p is prime)
2. $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. (iff p is prime)

Theorem 10 (Infinitude of Primes). *There exists infinitely many primes.*

Proof (Euclid's).

Lemma 1. *Every positive integer $n \geq 2$ has a prime factor.*

Proof. Consider the set $S = \{m \mid m \text{ is a divisor of } n\}$. Then $S \neq \emptyset$.

By WOP, $\exists$ least positive integer $p \in S$. Note that every divisor of p is also a divisor of n. Thus p is a prime number by the minimality of p.

Suppose there exists finitely many primes

$$p_1, p_2, \cdots, p_k.$$

Let

$$n := p_1 p_2 \times \cdots \times p_k.$$

Then $n > 1$ and $\exists$ prime p such that $p \mid n$ by Lemma 1.

Thus $p = p_i$ for some $1 \leq i \leq k$, hence $p \mid p_1 p_2 \times \cdots \times p_k$, thus

$$p \mid (n - p_1 p_2 \times \cdots \times p_k) \Rightarrow p \mid 1.$$

Which is a contradiction to the definition of prime numbers. Thus there exists infinitely many primes.

Theorem 11. *There are arbitrary large gaps between successive primes. i. e. For any positive integer n, there exists at least n consecutive composite positive integers.*

Proof. Consider n consecutive integers

$$(n+1)!+2,\,(n+1)!+3,\,\cdots,\,(n+1)!+(n+1)\,.$$

For $2 \le j \le n+1$, it is clear that $j \bigm| (n+1)!$. Thus $j \bigm| ((n+1)!+j)$.

Hence $\exists n$ consecutive integers which are all composites.

Definition 6 (Mersenne Primes). *A* ***Mersenne prime*** *is a Mersenne number*[5] *which is also prime.*

e. g. $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_5 = 2^5 - 1 = 31$, $M_7 = 2^7 - 1 = 127$, $\cdots$ but $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$

1.5 September 26th

It can be seen that

1. If $2^n - 1$ is prime, then n is prime.
2. If a and p are positive integers such that $a^p - 1$ is prime, then $a = 2$ or $p = 1$. [6]

The converse of 1. does not hold. (e. g. $2^{11} - 1 = 23 \times 89$)

Question Are there infinitely many Mersenne primes? $\Rightarrow$ yet unknown! **O**nly **G**od **K**nows

Remark 7. Using Mersenne numbers and some theorem of groups[7], we can show the infinitude of primes.

[6] Proof exists at Wikipedia
[7] Lagrange theorem

Example $2^{11213}-1$ is prime (1963)

$2^{82589933}-1$ is prime (2018)

Definition 7 (Fermat Primes). *A* ***Fermat prime*** *is a Fermat number*[8] *which is also prime.*

e.g. $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$: the only known Fermat primes.

Theorem 12. *If 2^m+1 is an odd prime, then m is a power of 2.*

Proof. If m is a positive integer and is not a power of 2, then

$$m=rs$$

where $1\le r, s<m$ and s is odd. Note that for any $n\in\mathbb{Z}^+$,

$$(a-b)\mid\left(a^l-b^l\right).$$

Put $a=2^r$, $b=-1$, $l=s$. Then

$$(2^r+1)\mid(2^{rs}+1)\Rightarrow(2^r+1)\mid(2^m+1).$$

Since $1<2^r+1<2^m+1$, it follows that 2^m+1 is not prime. $\rightarrow\leftarrow$

Theorem 13. *A regular polygon of n sides can be constructed using an unmarked ruler and compass if and only if*

$$n=2^m \qquad \text{or} \qquad n=2^r p_1 p_2\times\cdots\times p_k$$

where $m\ge 2$, $r\ge 0$ and $p_1, p_2, \cdots, p_k$ are distinct Fermat primes.

e. g.

$$
\begin{aligned}
3 &= 2^{2^0}+1 && \text{: constructive}\\
5 &= 2^{2^1}+1 && \text{: constructive}\\
7 & && \text{: not constructive}\\
17 &= 2^{2^2}+1 && \text{: constructive}
\end{aligned}
$$

Theorem 14.

$$(F_m, F_n) = 1$$

if $m \neq n \in \mathbb{Z}^+ \cup \{0\}$.

Proof. **Claim** $F_n = F_0F_1 \times \cdots \times F_{n-1} + 2$ where $n \geq 1$.

$n=1$. $F_1 = 5$; $F_0 + 2 = 3 + 2 = 5$.
$n=2$. $F_2 = 17$; $F_0F_1 + 2 = 3 \times 5 + 2 = 17$.
Inductive step. Assume that the claim is true for $s \leq k$. Then

$$
\begin{aligned}
&F_0F_1 \times \cdots \times F_k + 2\\
=&\left(F_0F_1 \times \cdots \times F_{k-1}\right)F_k + 2\\
=&\left(F_k+2\right)F_k + 2\\
=&F_k^2 - 2F_k + 2\\
=&\left(F_k-1\right)^2 + 1\\
=&2^{2^{k+1}} + 1 = F_{k+1}.
\end{aligned}
$$

Note that for $i = 0, 1, \cdots, n-1$,

$$F_n \div F_i = \left(F_0F_1 \times \cdots \times F_{n-1} + 2\right) \div F_i$$

leaves the remainder of 2. i. e. $F_n = qF_i + 2$.

Thus if $m \mid F_n$, then $m \mid 2$, and so $m = 1$ or $m = 2$. Since F_n and F_i are odd, it follows that $m = 1$.

Corollary 1. *There are infinitely many primes.*

Proof. It follows immediately by the following statements.

1. $\{F_n \mid n \geq 0\}$ is an infinite set.
2. F_n has a prime factor of p_n.
3. $(F_m, F_n) = 1$ if $m \neq n$.

Remark 8. 1. Fermat conjectured all Fermat numbers are primes, but it's not true:

$$F_5 = 4294967297 = 641 \times 6700417.$$

2. Open questions remains:
   (a) Are there infinitely many Fermat primes?
   (b) Are there infinitely many composite Fermat numbers?
   (c) Is it true that F_n is composite for all $n > 4$?

Theorem 15 (Prime Number Theorem). *If*

$$\pi(x) := (\textit{number of primes less than or equal to } x)$$

Then

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

e. g. $\pi(10) = 4$.

It was conjectured by Gauss and Legendre; proved by Hadamad and Poisson independently using complex analysis.

Theorem 16. *If n is a positive composite integer, then n has a prime factor not exceeding* $\sqrt{n}$.

i. e. $\exists$ *prime factor* p *such that* $p \mid n$ *and* $p \leq \sqrt{n}$.

Corollary 2. *If n has no prime factors not exceeding $\sqrt{n}$, then n is prime.*

Proof (by the contrapositive of the theorem above). (Proof left for students.)

Theorem 17 (Fundamental Theorem of Arithmetic). *Let $n > 1$ be an integer. Then n can be expressed as a product of prime factors in an unique way, except for the order of factors. i. e. $\mathbb{Z}$ is an unique factorization domain[9].*

Proof. (Using WOP; see the book.)

2 Congrugences

2.1 October 1st

Definition 8. $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$

a is ***congrugent*** *to b modulo m if* $m \mid (a-b)$.

Theorem 18. *1.* $a \equiv a \pmod{m}$

2. $a \equiv b \Rightarrow b \equiv a$
3. $a \equiv b, b \equiv c \Rightarrow a \equiv c$
4. $a \equiv b, c \equiv d \Rightarrow a \pm c \equiv b \pm d, ac \equiv bd$.

$4\frac{1}{2}$. $1 \leq i \leq n$. *Then* $a_i \equiv b_i \Rightarrow \sum_1^n a_i \equiv \sum_1^n b_i, \prod_1^n a_i \equiv \prod_1^n b_i$

5. *Let* $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_nx^n$, *where* $a_i, b_i \in \mathbb{Z}$. *Suppose* $a_i \equiv b_i \pmod{m}$. *If* $a \equiv b$, *then* $f(a) \equiv g(b)$.

Example 1. $10 \equiv 1 \pmod 3$.

$10 \equiv 1 \pmod 9$.

$10 \equiv -1 \pmod{11}$.

Let $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$. Then

$$\begin{aligned} a &\equiv a_0 + a_1 + \cdots + a_n \pmod 3 \\ &\equiv a_0 + a_1 + \cdots + a_n \pmod 9 \\ &\equiv a_0 - a_1 + \cdots + (-1)^n a_n \pmod{11} \end{aligned}$$

$\because$ If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, then

$$\begin{aligned} f(10) &\equiv f(1) \pmod 3 \\ f(10) &\equiv f(1) \pmod 9 \\ f(10) &\equiv f(-1) \pmod{11} \end{aligned}$$

e. g.

$$\begin{aligned} 26384 &\equiv 2+6+3+8+4 \equiv 2 \pmod 3 \\ 26384 &\equiv 2+6+3+8+4 \equiv 5 \pmod 9 \\ 26384 &\equiv 2-6+3-8+4 \equiv 6 \pmod{11} \end{aligned}$$

Example 2. $41 \mid \left(2^{20} - 1\right)$?

Note that

$$2^5 \equiv -9 \pmod{41}.$$

Thus

$$\begin{aligned} \left(2^5\right)^4 &\equiv (-9)^4 \\ &\equiv 81 \times 81 \end{aligned}$$

Since $81 \equiv -1 \pmod{41}$, $81 \times 81 \equiv 1 \pmod{41}$. Hence

$$\begin{aligned} 2^{20} - 1 &\equiv \left(2^5 - 4\right) - 1 \\ &\equiv (-9)^4 - 1 \\ &\equiv 1 - 1 \equiv 0 \pmod{41}. \end{aligned}$$

Note that $7 \times 2 \equiv 4 \times 2 \pmod 6$, but $7 \not\equiv 4 \pmod 6$, also $7 \equiv 4 \pmod 3$.

Theorem 19. $a, b, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $d = (c, m)$.

If $ac \equiv bc \pmod m$, *then* $a \equiv b \pmod{\frac{m}{d}}$.

Proof. Since $ac \equiv bc \pmod m$,

$$m \mid (ac - bc).$$

Thus $\exists k \in \mathbb{Z}$ such that $c(a-b) = km$, and so

$$\frac{c}{d}(a-b) = k\frac{m}{d}.$$

Since $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$, it follows that

$$\frac{m}{d} \mid (a-b).$$

□

Question. $2^{1137} \equiv\ ? \pmod{17}$

Theorem 20. *Let* $m \in \mathbb{Z}^+$. *For any* $a \in \mathbb{Z}$, $\exists! r \in \mathbb{Z}$ *such that*

$$a \equiv r \pmod m$$

where $0 \le r \le m - 1$.

Proof. Use the division algorithm.

Definition 9. *A **complete system of residues** modulo m is the set of integers such that every integers is congrugent modulo m to exactly one integer of the set.*

e. g.

1. $\{0, 1, 2, \cdots, m-1\}$ is a complete system of residues modulo m.[10]
2. If m is odd, $\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$ is also a complete system of residues modulo m.

Theorem 21. *If $\{r_1, r_2, \cdots, r_m\}$ is a complete system of residues modulo m and if $a \in \mathbb{Z}^+$ with $\underline{(a, m) = 1}$, then for any integer b,*

$$\{ar_1 + b, ar_2 + b, \cdots, ar_m + b\}$$

is a complete system of residues modulo m.

e. g. $m = 4 \Rightarrow \{0, 1, 2, 3\}, \{0, 3, 6, 9\}, \{1, 2, 3, 4\}, \cdots$

but $\{0, 2, 4, 6\}$ is not a complete system of residues modulo 4.

Proof. Note that a set of m incongrugent integers modulo m will always form a complete system of residues modulo m.

Thus it suffices to show that no two integers $ar_1 + b, \cdots, ar_m + b$ are congrugent modulo m.

Suppose that

$$ar_j + b \equiv ar_k + b.$$

[10] The least nonnegative residues modulo m

then

$$ar_j \equiv ar_k.$$

Since $(a, m) = 1$, $r_j \equiv r_k$. Hence $j = k$. $\square$

Theorem 22. *$a, b \in \mathbb{Z}^+$, $m \in \mathbb{Z}^+$, $d = (a, m)$.*

If $d \nmid b$, then $ax \equiv b \pmod{m}$ has no solutions.

If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d incongrugent solutions modulo m as follows:

$$x = x_0 + \frac{m}{d}t \qquad t = 0, 1, 2, \cdots, d-1$$

where x_0 is a particular solution of $ax \equiv b \pmod{m}$.

Example 3. $9x \equiv 12 \pmod{15}$?

Note that $(9, 15) = 3 \mid 12$, by theorem, $\exists$ exactly 3 incongrugent solutions modulo 15.

To find a particular solution, consider $9x + 15y = 12$. Note that

$$\begin{aligned} 15 &= 9 \times 1 + 6 \\ 9 &= 6 \times 1 + 3 \\ 6 &= 3 \times 2 + 0 \\ 3 &= 9 - 6 = 9 \times 2 - 15. \end{aligned}$$

Thus $9 \times 8 + 15 \times (-4) = 12$.

Hence the general solution is given by

$$\begin{aligned} x &= x_0 \equiv 8 \pmod{15} \\ x &= x_0 + \frac{15}{3} \times 1 \equiv 13 \pmod{15} \\ x &= x_0 + \frac{15}{3} \times 2 = 18 \equiv 3 \pmod{15}. \end{aligned}$$

Proof. (Proof left for homework – due October 3rd.)

Remark 9. Consider $ax \equiv 1 \pmod{m}$. By the previous theorem, $\exists$ solutions of this congrugence if and only if $(a, m) = 1$.

Definition 10. $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $(a, m) = 1$.

*A solution of $ax \equiv 1 \pmod{m}$ is called an **inverse** of a modulo m.*

e. g. $7x \equiv 1 \pmod{31} \Rightarrow x = 9 \pmod{31}$. Thus 9 and all integers congrugent to 9 are inverses of 7 modulo 31.

e. g. $7x \equiv 22 \pmod{31} \Rightarrow 9 \times 7x \equiv 9 \times 22 \pmod{31} \Rightarrow 1 \times x \equiv 12 \pmod{31}$

Remark 10. $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$. $(\mathbb{Z}_n^*, *)$ is a group.

$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

e. g. $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

2.2 October 8th

Definition 11 (Euler ϕ Function). *Let $n \in \mathbb{Z}^+$. The **Euler ϕ–function** $\phi(n)$ is defined to be the count of positive integers not exceeding n which are relatively prime to n.*

e. g. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(8) = 4$, $\phi(12) = 4$

In general, if p is prime, then $\phi(p) = p - 1$.

Question. How to compute $\phi(n)$? Goal: $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$, i. e. ϕ is multiplicative.

> **Definition 12 (Reduced Residue System).** *A **reduced residue system** modulo n is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n and no two distinct elements of the set are congrugent modulo n.*

e. g. $n = 8 \Rightarrow \{1, 3, 5, 7\}$: a reduced residue system modulo 8.

Lemma 2. *If $\left\{r_1, r_2, \cdots, r_{\phi(n)}\right\}$ is a reduced residue system modulo n and if $a \in \mathbb{Z}^+$ with $(a, n) = 1$ then $\left\{ar_1, ar_2, \cdots, ar_{\phi(n)}\right\}$ is also a reduced residue system modulo n.*

Only multiplication holds; addition does not hold.

Proof. (See the textbook.)

Theorem 23 (Euler's Theorem). *If $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with $(a, m) = 1$ then*

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

Proof. Let $\left\{r_1, r_2, \cdots, r_{\phi(m)}\right\}$ be a reduced residue system modulo m. Since $(a, m) = 1$, the set $\left\{ar_1, ar_2, \cdots, ar_{\phi(m)}\right\}$ is a reduced residue system modulo m by Lemma.

Then

$$ar_1 \times ar_2 \times \cdots \times ar_{\phi(m)} \equiv r_1 \times r_2 \times \cdots \times r_{\phi(m)} \pmod{m}$$

and so

$$a^{\phi(m)} \times r_1 \times r_2 \times \cdots \times r_{\phi(m)} = r_1 \times r_2 \times \cdots \times r_{\phi(m)} \pmod{m}.$$

Hence $a^{\phi(m)} \equiv 1 \pmod{m}$.[11] □

Corollary 3 (Fermat's Little Theorem). *If p is prime and $p \nmid a$ ($\Rightarrow (a, p) = 1$), then*

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

[11] Note that $\left(r_1 r_2 \times \cdots \times r_{\phi(m)}, m\right) = 1$

Corollary 4. *Let p : prime. Then*

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

Proof. If $a \equiv 0 \pmod{p}$, then $a^p \equiv 0 \equiv a \pmod{p}$.

If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$ thus $a^{p-1} \equiv a \pmod{p}$. □

Example 4. $2^{1137} \pmod{17}$?

By Euler's theorem, $2^{16} \equiv 1 \pmod{17}$. Thus

$$2^{1137} = \left(2^{16}\right)^{71} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{17}.$$

Example 5. Show that 117 is not a prime.

Suppose 117 is prime. then

$$2^{117} \equiv 2 \pmod{117}.$$

Note that

$$2^7 \equiv 128 \equiv 11 \pmod{117}.$$

Thus

$$\begin{aligned} 2^{117} &\equiv \left(2^7\right)^{16} \cdot 2^5 \\ &\equiv 11^{16} \cdot 2^5 \\ &\equiv 121^8 \cdot 2^5 \\ &\equiv 4^8 \cdot 2^5 \\ &\equiv 2^{21} \equiv 11^3 \not\equiv 2 \pmod{17}. \end{aligned}$$

Example 6. Solve $x^{35} + 5x^{19} + 11x^3 \equiv 0 \pmod{17}$.

By Fermat's little theorem,

$$x^{17} \equiv x \pmod{17}.$$

Then

$$x^{35} = x\left(x^{17}\right)^2 \equiv x^3$$
$$x^{19} = x^2\left(x^{17}\right) \equiv x^3$$

Thus

$$x^{35} + 5x^{19} + 11x^3 \equiv (1+5+11)x^3 \equiv 0 \cdot x^3 \equiv 0 \pmod{17}.$$

Hence x can be any integer.

Theorem 24 (Wilson's Theorem). *If p is a prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Was conjectured by Wilson; and proved by Lagrange.

Lemma 3. *Let p be prime. a is self-invertible modulo p, i. e. $a \cdot a \equiv 1 \pmod{p}$, if and only if $a \equiv \pm 1 \pmod{p}$.*

Proof (of lemma). ($\Leftarrow$) It's trivial.

($\Rightarrow$) Note that

$$a^2 \equiv 1 \pmod{p}$$

and so $p \mid (a-1)(a+1)$.

Since p is prime, $p \mid (a-1)$ or $p \mid (a+1)$. Thus $a \equiv 1$ or $a \equiv -1 \pmod{p}$. $\square$

Proof (of theorem). If $p = 2$, then $(p-1)! = 1 \equiv -1 \pmod{2}$.

Consider for $p > 2$. Note that $\{1, 2, \cdots, p-1\}$ is a reduced residue system modulo p. By lemma, 1 and $p-1$ are self-invertible. Thus we can group the remaining $p-3$ residues $\frac{p-3}{2}$ pair of inverses a and b such that $ab \equiv 1 \pmod{p}$.

Hence

$$\begin{aligned}(p-1)! &= 1\cdot[2\cdot 3\times\cdots\times(p-2)]\,(p-1)\\ &\equiv 1\cdot 1\times\cdots\times 1\,(p-1)\\ &\equiv p-1\equiv -1 \pmod{p}.\end{aligned}$$

□

e. g. $(6-1)!+1=121\not\equiv 0 \pmod{6}$, thus 6 is not prime.

In fact, the converse of Wilson's theorem also holds, but is inefficient to test primality.

Theorem 25. *If $n\in\mathbb{Z}^+$ and*

$$(n-1)!\equiv -1 \pmod{m},$$

then n is prime.

Proof. Suppose that n is composite. Then $n=ab$ where $1<a<n$ and $1<b<n$. Since $a<n$, $a \mid (n-1)!$. Since $(n-1)\equiv -1 \pmod{n}$,

$$n \mid [(n-1)!+1].$$

Thus $a \mid [(n-1)!+1]$, hence $a \mid 1$, which is a contradiction.

Remark 11. p is prime if and only if $(p-1)!\equiv -1 \pmod{p}$, and also $(p-2)!\equiv 1 \pmod{p}$.

Applications of Euler's and Wilson's theorem.

1. p is odd prime. Then

$$[1\cdot 3\cdot 5\times\cdots\times(p-2)]^2\equiv[2\cdot 4\cdot 6\times\cdots\times(p-1)]^2\equiv(-1)^{\frac{p+1}{2}} \pmod{p}.$$

2. p is odd prime. Then $x^2\equiv -1 \pmod{p}$ has a solution if and only if $p\equiv 1 \pmod{4}$.

2.3 October 10th

Proof. 1. As x runs through $\frac{p-1}{2}$ even integers from 2 to $p-1$, then $p-x$ runs through odd integers from $p-2$ down to 1. Then

$$(2\cdot 4\cdot 6\times\cdots\times(p-1))\equiv(-1)^{\frac{p-1}{2}}(1\cdot 3\cdot 5\times\cdots\times(p-2))\pmod p$$

and so

$$(2\cdot 4\cdot 6\times\cdots\times(p-1))^2\equiv(1\cdot 3\cdot 5\times\cdots\times(p-2))^2\pmod p.$$

By Wilson's theorem,

$$-1\equiv(p-1)!=(1\cdot 3\cdot 5\times\cdots\times(p-2))(2\cdot 4\cdot 6\times\cdots\times(p-1))\pmod p.$$

Thus

$$(-1)^{\frac{p-1}{2}}(1\cdot 3\cdot 5\times\cdots\times(p-2))^2\equiv -1\pmod p,$$

hence

$$(1\cdot 3\cdot 5\times\cdots\times(p-2))^2\equiv(-1)^{\frac{p+1}{2}}\pmod p.$$

$\square$

2. ($\Rightarrow$) Suppose $x_0^2\equiv -1\pmod p$ for some $x\in\mathbb{Z}$. Then

$$x_0^{p-1}=\left(x_0^2\right)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}.$$

On the other hand, by Euler's theorem, $x_0^{p-1}\equiv 1\pmod p$.[12] Thus $(-1)^{\frac{p-1}{2}}\equiv 1\pmod p$; i. e.

$$p\,\Big|\,\left[1-(-1)^{\frac{p-1}{2}}\right].$$

Hence $1-(-1)^{\frac{p-1}{2}}=0$.[13] Therefore $\frac{p-1}{2}$ is even and so $p\equiv 1\pmod 4$.

($\Leftarrow$) Note that

$$\begin{aligned}(p-1)!&=\left(1\cdot 2\cdot 3\times\cdots\times\frac{p-1}{2}\right)\left((p-1)(p-2)(p-3)\times\cdots\times\frac{p+1}{2}\right)\\&\equiv\left(1\cdot 2\cdot 3\times\cdots\times\frac{p-1}{2}\right)\left((-1)(-2)(-3)\times\cdots\times\frac{-(p-1)}{2}\right)\pmod p\\&\equiv(-1)^{\frac{p-1}{2}}\times 1^2\cdot 2^2\cdot 3^2\times\cdots\times\left(\frac{p+1}{2}\right)^2\pmod p\end{aligned}$$

[12] Note that $x_0^2\equiv -1\pmod p$, thus $(x_0,p)\mid 1$, and so $(x_0,p)=1$; i. e. $p\nmid x_0$.

[13] If $1-(-1)^{\frac{p-1}{2}}=2\neq 0$, then $p\mid 2$. $\rightarrow\leftarrow$

Thus

$$-1 \equiv (p-1)! \equiv \left(1 \cdot 2 \cdot 3 \times \cdots \times \frac{p-1}{2}\right)^2 \pmod{p}.$$

Put $x_0 = 1 \cdot 2 \cdot 3 \times \cdots \times \frac{p-1}{2}$. Then $x_0^2 \equiv -1 \pmod{p}$. □

Theorem 26. *Let p be a prime number and $e \in \mathbb{Z}^+$. Then*

$$\phi(p^e) = p^e - p^{e-1}.$$

Proof. Note that

$$\begin{aligned}\phi\left(p^2\right) &= (\text{the number of positive integers} \le p^e \text{ which are relatively prime to } p^e) \\ &= p^e - (\text{the number of positive integers} \le p^e \text{ which are NOT relatively prime to } p^e)\end{aligned}$$

while the positive integers $\le p^e$ which are NOT relatively prime to p^e are

$$p, 2p, 3p, \cdots, \left(p^{e-1}\right)p.$$

□

Remark 12. 1. $\phi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$.
2. Let $n = p_1^{e_1} p_2^{e_2} \times \cdots \times p_k^{e_k}$. Then

$$\begin{aligned}\phi(n) &= \phi(p_1^{e_1})\,\phi(p_2^{e_2}) \times \cdots \times \phi\left(p_k^{e_k}\right) \\ &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \times \cdots \times p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\ &= \left[p_1^{e_1} p_2^{e_2} \times \cdots \times p_k^{e_k}\right] \times \left[\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right)\right] \\ &= n\left[\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right)\right].\end{aligned}$$

Note 1. $m = 4, n = 7$ ($(m,n) = 1$)

$$\phi(mn) = \phi(28) = 12 = 2 \times 6 = \phi(4)\,\phi(7).$$

Lemma 4. *If* $m, n \in \mathbb{Z}^+$, $r \in \mathbb{Z}$, $(m, n) = 1$, *then the integers* $r, m+r, 2m+r, \cdots, (m-1)m+r$ *are congrufent to* $0, 1, 2, \cdots, n-1$ *modulo n.*

Proof. Suffies to show that no two integers in the list are congrugent modulo n.

Suppose that $km + r \equiv lm + r \pmod{n}$ where $0 \le k, l < n$. Then $km \equiv lm \pmod{n}$. Since $(m, n) = 1$, hence $k \equiv l \pmod{n}$. Since $0 \le k, l < n$, $k = l$. □

Theorem 27. $\phi(mn) = \phi(m)\phi(n)$ *if* $(m, n) = 1$.

Proof. Consider

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & nm \end{array}$$

Let $r \le m$ be a positive integer with $(r, m) > 1$. Let $d = (r, m)$. Then $d \mid r$, $d \mid m$, and so $d \mid (km + r)$ for any $k \in \mathbb{Z}$; i. e. d is a factor of every element in the r^{th} row.

Thus no element in the r^{th} row is relatively prime to m and hence to mn if $(r, m) > 1$. Hence, there are $\phi(m)$ rows satisfying $(r, m) = 1$.

Consider now the r^{th} row where $(r, m) = 1$.

$$r, m+r, 2m+r, \cdots, (n-1)m+r$$

By Lemma, exactly $\phi(n)$ elements in the r^{th} row are relatively prime to n, and hence to mn. Hence we conclude that $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$. □

Note 2. $n = 28$, $d = n$. $C_d :=$ (the class of positive integers $m \le n$ satisfying $(m, n) = d$). Then

$$C_1 = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\} \qquad 12 = \phi(28) = \phi\left(\frac{28}{1}\right)$$

$$C_2 = \{2, 6, 10, 18, 22, 26\} \qquad 6 = \phi(14) = \phi\left(\frac{28}{2}\right)$$

$$C_4 = \{4, 8, 12, 20, 24, 28\} \qquad 6 = \phi(7) = \phi\left(\frac{28}{4}\right)$$

$$C_7 = \{7, 21\} \qquad 2 = \phi(4) = \phi\left(\frac{28}{7}\right)$$

$$C_{14} = \{14\} \qquad 1 = \phi(2) = \phi\left(\frac{28}{14}\right)$$

$$C_{28} = \{28\} \qquad 1 = \phi(1) = \phi\left(\frac{28}{28}\right)$$

$$12+6+6+2+1+1 = 28.$$

Theorem 28. *For $n \in \mathbb{Z}^+$,*

$$n = \sum_{d \mid n} \phi(d) = \sum_{d \mid n} \phi\left(\frac{n}{d}\right).$$

Proof. Let $m \in \mathbb{Z}^+$ such that $m \leq n$. Then $m \in C_d$ if and only if $(m, n) = d$, if and only if $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Thus the number of positive integers $\leq \frac{n}{d}$ which are relatively prime to $\frac{n}{d}$ is equlal to the number og elements m in C_d. Hence each class C_d has $\phi\left(\frac{n}{d}\right)$ elements.

Since there is a class corresponding to elery factor d of n and every integer $m \leq n$ belongs to exactly one class, it follows that the sum of the count of elements in various classes is n; i. e. $\sum_{d \mid n} \phi\left(\frac{n}{d}\right) = n$.

As d runs over the divisors of n, so does $\frac{n}{d}$. Hence $\sum_{d \mid n} \phi(d) = n$. $\square$

Theorem 29 (Chinese Remainder Theorem). *Let $m_1, m_2, \cdots, m_r$ are pairwise relatively prime positive integers. Then the system of congrugences*

$$\begin{cases} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \\ & \vdots \\ x \equiv a_r & \pmod{m_r} \end{cases}$$

where $a_i \in \mathbb{Z}$, has a unique solution modulo $M = m_1 m_2 \times \cdots \times m_r$.

Proof. (Proof left for homework – due October 15th.)

Example 7. 1.

$$\begin{cases} x \equiv 1 & \pmod{4} \\ x \equiv 3 & \pmod{5} \\ x \equiv 2 & \pmod{7} \end{cases}$$

$$\begin{aligned} 35 \times \underline{?}_3 &\equiv 1 && \pmod{4} \\ 28 \times \underline{?}_2 &\equiv 3 && \pmod{5} \\ 20 \times \underline{?}_6 &\equiv 2 && \pmod{7} \end{aligned}$$

Note that

$$\begin{aligned} M = 4 \cdot 5 \cdot 7 &= 35 \cdot 4 = M_1 m_1 \\ &= 28 \cdot 5 = M_2 m_2 \\ &= 20 \cdot 7 = M_3 m_3 \end{aligned}$$

thus $x = 1 \cdot 35 \cdot 3 + 3 \cdot 28 \cdot 2 + 2 \cdot 20 \cdot 6 = 93 \pmod{140}$

2.

$$\begin{cases} 8x \equiv 4 & \pmod{14} \\ 5x \equiv 3 & \pmod{11} \end{cases}$$
$$\Leftrightarrow \begin{cases} 4x \equiv 2 & \pmod{7} \\ 5x \equiv 3 & \pmod{11} \end{cases}$$
$$\Leftrightarrow \begin{cases} x \equiv 4 & \pmod{7} \\ x \equiv 5 & \pmod{11} \end{cases}$$

By CRT, $x = 4 \cdot 11 \cdot 2 + 5 \cdot 7 \cdot 8 \equiv 368 \equiv 60 \pmod{77}$
Note that $x \equiv 60 \pmod{77} \Leftrightarrow x \equiv 60, x \equiv 137 \pmod{154}$.

3 Primitive Roots

3.1 October 15th

Recall By Euler, $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$. Thus $\exists$ at least one positive integer x such that $a^x \equiv 1 \pmod{m}$. By WOP, $\exists$ a least posivite integer x satisfying $a^x \equiv 1 \pmod{m}$.

Definition 13. $a, m \in \mathbb{Z}^+$, $(a, m) = 1$. *The least positive integer x such that $a^x \equiv 1 \pmod{m}$ is called the **order** of a modulo m.*

We denote this as $\text{order}_m a$, *or* $\text{ord}_m a$.

e. g. $\text{ord}_7 2 = 3$, $\text{ord}_7 3 = 6$

Remark 13. 1. $a \equiv b \pmod{m}$, then $\text{ord}_m a = \text{ord}_m b$. ($\because b^{\text{ord}_m a} \equiv a^{\text{ord}_m a} \equiv 1 \Rightarrow \text{ord}_m b \leq \text{ord}_m a$)
2. Suppose $(a, m) \neq 1$. Then $a^x \equiv 1 \pmod{m}$ has no solution. Thus $a^k \not\equiv 1 \pmod{m}$ $\forall k \in \mathbb{Z}^+$.

Theorem 30. $(a, m) = 1$. *A positive integer x is a solution of $a^x \equiv 1 \pmod{m}$ if and only if $\operatorname{ord}_m a \mid x$.*

Proof. ($\Rightarrow$) By division algorithm,

$$x = q \operatorname{ord}_m a + r \qquad 0 \le r < \operatorname{ord}_m a.$$

Then

$$\begin{aligned} a^x &= a^{q \operatorname{ord}_m a + r} \\ &= \left(a^{\operatorname{ord}_m a}\right)^q a^r \\ &\equiv a^r \pmod{m}. \end{aligned}$$

Since $a^x \equiv 1$, $a^r \equiv 1$. Since $0 \le r < \operatorname{ord}_m a$, it follows that $r = 0$. Hence $a = q \operatorname{ord}_m a$ and so $\operatorname{ord}_m a \mid x$.

($\Leftarrow$) Since $\operatorname{ord}_m a \mid x$, $x = k \operatorname{ord}_m a$ for some $k \in \mathbb{Z}^+$. Then $x^a \equiv x^{k \operatorname{ord}_m a} \equiv \left(a^{\operatorname{ord}_m a}\right)^k \equiv 1^k \equiv 1 \pmod{m}$.

Corollary 5.

$$\begin{aligned} &(a, m) = 1 \\ &\Rightarrow \operatorname{ord}_m a \mid \phi(m). \end{aligned}$$

e. g. $\operatorname{ord}_{17} 5 = 16$, $\phi(17) = 16$.

Recall $m = 7$, then $\operatorname{ord}_7 2 = 3$, $\operatorname{ord}_7 3 = 6$.

$m = 12$, then $\phi(12) = 4$: so there is no positive integer a such that $\operatorname{ord}_m a = 4$.

Definition 14 (Primitive root). *$r, m \in \mathbb{Z}^+$ and $(r, m) = 1$. If $\operatorname{ord}_m r = \phi(m)$, then r is called a **primitive root** modulo m.*

e. g.

1. 3 is a primitive root modulo 7.
2. There are no primitive roots modulo 12.

Theorem 31. $(r, m) \in \mathbb{Z}^+$, $(r, m) = 1$. *If r is a primitive root modulo m, then the integers $r, r^2, \cdots, r^{\phi(m)}$ form a reduced residue system modulo m.*

e. g. 2 is a primitive root modulo 9; $\phi(9) = 6$.

$$\begin{aligned} 2 &\equiv 2 \\ 2^2 &\equiv 4 \\ 2^3 &\equiv 8 \\ 2^4 &\equiv 7 \\ 2^5 &\equiv 5 \\ 2^6 &\equiv 1 \end{aligned}$$

Proof. Suffices to show that the first $\phi(m)$ powers of r are all relatively prime to m and that no two are congrugent modulo m.

Since $(r, m) = 1$, $\left(r^k, m\right) = 1$ for any $k \in \mathbb{Z}^+$. Thus $r, r^2, \cdots, r^{\phi(m)}$ are all relatively prime to m.

Assume that $r^i \equiv r^j \pmod{m}$. Since $1 \leq i, j \leq \phi(m)$, we have $i = j$, since $i \equiv j \pmod{\phi(m)}$ by the next theorem.

Theorem 32. $a, m \in \mathbb{Z}^+$, $(a, m) = 1$. $a^i \equiv a^j \pmod{m}$ *if and only if* $i \equiv j \pmod{\mathrm{ord}_m a}$ *where* $i, j \in \mathbb{Z}^+ \cup \{0\}$.

Proof. ($\Rightarrow$) Suppose $a^i \equiv a^j \pmod{m}$ where $i \geq j$. Since $(a, m) = 1$, $\left(a^j, m\right) = 1$. Then

$$a^j a^{i-j} \equiv a^i \equiv a^j \pmod{m}.$$

Since $\left(a^j, m\right) = 1$, $a^{i-j} \equiv 1 \pmod{m}$. Thus $\operatorname{ord}_m a \mid (i-j)$, therefore $i \equiv j \pmod{\operatorname{ord}_m a}$.

($\Leftarrow$) Proof left for students.

Theorem 33. $r, m \in \mathbb{Z}^+$, $(r, m) = 1$. *Suppose r is a primitive root modulo m. Then r^n is also a primitive root modulo m if and only if $(n, \phi(m)) = 1$.*

Corollary 6. *If a positive integer m has a primitive root, then it has a total of $\underline{\phi(\phi(m))}$ incongrugent primitive roots.*

e. g. $m = 11$

By Corollary, 11 has $\phi(\phi(11)) = 4$ incongrugent primitive roots – of 2, 6, 7, 8.

Lemma 5. *If* $\operatorname{ord}_m a = t$, *then*

$$\operatorname{ord}_m(a^u) = \frac{\operatorname{ord}_m a}{(\operatorname{ord}_m a, u)} = \frac{t}{(t, u)}.$$

Proof (of lemma). Let $s := \operatorname{ord}_m(a^u)$ and $v := (t, u)$. Then $t = t_1 v$, $u = u_1 v$ where $(t_1, u_1) = 1$.

Note that

$$(a^u)^{t_1} \equiv (a^{uv})^{t_1} \equiv \left(a^t\right)^{u_1} \equiv 1^{u_1} \equiv 1.$$

Thus $s \mid t_1$.

On the other handm since $1 \equiv (a^u)^s = a^{us}$, we have $t \mid us$. Then $t = \underline{t_1 v} \mid us = \underline{u_1 v s}$, and so, $t_1 \mid u_1 s$.

Since $(t_1, u_1) = 1$, $t_1 \mid s$. Hence $s = t_1 = \frac{t}{v} = \frac{t}{(t,u)}$.

Proof (of theorem). By Lemma,

$$\begin{aligned}\operatorname{ord}_m(r^n) &= \frac{\operatorname{ord}_m r}{(\operatorname{ord}_m r, n)} \\ &= \frac{\phi(m)}{(\phi(m), n)}.\end{aligned}$$

End of midterm.

4 Index (or Discrete Logarithm)

4.1 October 15th

Note 3. Let r be a primitive root modulo m. Then $\left\{r, r^2, \cdots, r^{\phi(m)}\right\}$ is a reduced residue system.

Thus if a is an integer such that $(a, m) = 1$, then $\exists!$ integer x with $1 \le x \le \phi(m)$ such that $r^x \equiv a \pmod{m}$.

4.2 October 17th

(Class missed; but this class was a Q&A session, so no notes here.)

4.3 October 29th

Theorem 34. *A positive integer m possess a primitive root if and only if* $m = 2, 4, p^t$ *or* $2p^t$ *where p is odd prime and* $t \in \mathbb{Z}^+$.

Definition 15 (Index). *Let m be a positive integer with primitive root r. If a is an integer with* $(a, m) = 1$*, then* $\exists! x$ *with* $1 \le x \le \phi(m)$ *and* $r^x \equiv a \pmod{m}$.

We call x as the ***index*** *or the* ***discrete logarithm*** *of a to the base r modulo m. We denote this by* $\mathrm{ind}_r\, a$.

Remark 14. 1. $r^{\mathrm{ind}_r a} \equiv a \pmod{m}$.[14]
2. $(a, m) = 1, (b, m) = 1, a \equiv b \pmod{m} \Rightarrow \mathrm{ind}_r\, a = \mathrm{ind}_r\, b$.

[14] Please don't do such things like $\cancel{a}^{\log_{\cancel{a}} b} = b$, or $\cancel{\sqrt{2^{\cancel{2}}}} = 2$. It ruins mathematics!

Theorem 35. *Let m be a positive integer with primitive root r, and a be an integer with* $(a, m) = 1$. *Then,*

1. $\operatorname{ind}_r 1 \equiv 0 \pmod{\phi(m)}$.
2. $\operatorname{ind}_r ab \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(m)}$.
3. $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \pmod{\phi(m)}$, *where* $k \in \mathbb{Z}^+$.

Proof. 1. By Euler's theorem, $r^{\phi(m)} \equiv 1 \pmod{m}$. Since r is a primitive root modulo m, no small positive power of r is congruent to 1 modulo m. Hence $\operatorname{ind}_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$.

2. Note that

$$r^{\operatorname{ind}_r ab} \equiv ab \pmod{m},$$

and

$$r^{\operatorname{ind}_r a + \operatorname{ind}_r b} = r^{\operatorname{ind}_r a} r^{\operatorname{ind}_r b} \equiv ab \pmod{m}.$$

Thus $r^{\operatorname{ind}_r ab} \equiv r^{\operatorname{ind}_r a + \operatorname{ind}_r b}$, hence $\operatorname{ind}_r ab \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(m)}$.

3. Note that

$$r^{\operatorname{ind}_r a^k} \equiv a^k \pmod{m}$$
$$r^{k \operatorname{ind}_r a} = \left(a^{\operatorname{ind}_r a}\right)^k \equiv a^k \pmod{m}$$

thus $r^{\operatorname{ind}_r a^k} \equiv r^{k \operatorname{ind}_r a} \pmod{m}$, hence $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \pmod{\phi(m)}$.

Example 8. $6x^{12} \equiv 11 \pmod{17}$?

Note that 3 is a primitive root of 17.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_r a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Taking ind_3 on $6x^2 \equiv 11 \pmod{17}$, we have [15]

$$\operatorname{ind}_3\left(6x^{12}\right) \equiv \operatorname{ind}_3 11 \pmod{16}.$$

Thus

$$\begin{aligned}
\operatorname{ind}_3 6 + \operatorname{ind}_3 x^{12} &\equiv \operatorname{ind}_3 11 \pmod{16} \\
\Leftrightarrow 15 + 12 \operatorname{ind}_3 x &\equiv 7 \pmod{16} \\
\Leftrightarrow 12 \operatorname{ind}_3 x &\equiv -8 \equiv 24 \pmod{16} \\
\Leftrightarrow \operatorname{ind}_3 x &\equiv 2 \pmod{4}.
\end{aligned}$$

Hence $\operatorname{ind}_3 x \equiv 2, 6, 10, 14 \pmod{16}$, therefore, $x \equiv 9, 15, 8, 2 \pmod{17}$.

Since each step in the computation is reversible, there are four incongrugent solutions to the original equation.

c.f. If we take another primitive root then we still have the same solution.

Theorem 36. $(a, m) = 1$. *Suppose that m has a primitive root of r. Then the following statements are equivalent.*

1. $x^n \equiv a \pmod{m}$ *has a solution.*
2. $(n, \phi(m)) \mid \operatorname{ind}_r a$.
3. $a^{\frac{\phi(m)}{(n,\phi(m))}} \equiv 1 \pmod{m}$ *has* $(n, \phi(m))$ *solutions.*

Proof. $1 \Leftrightarrow 2$. Note that

$$x^n \equiv a \pmod{m} \Leftrightarrow n \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(m)}.$$

15

$$\begin{aligned}
&\because 6x^2 \equiv 11 \pmod{17} \\
&\Leftrightarrow 3^{\operatorname{ind}_3 6x^2} \equiv 3^{\operatorname{ind}_3 11} \pmod{17} \\
&\Leftrightarrow \operatorname{ind}_3 6x^2 \equiv \operatorname{ind}_3 11 \pmod{\phi(17)}
\end{aligned}$$

Recall that $ax \equiv b \pmod{m}$ has a solution if and only if $(a, m) \mid b$. If it has a solution, then it has (a, m) solutions.

$2 \Leftrightarrow 3$. Let $c = \phi(m)$ and $d = (n, \phi(m)) = (n, c)$. Then, $c = dc_1$ for some c_1.
Note that[16]

$$\begin{aligned} a^{\frac{c}{d}} = a^{c_1} &\equiv 1 \pmod{m} \\ \Leftrightarrow c_1 \operatorname{ind}_r a &\equiv 0 \pmod{\phi(m)} \\ \Leftrightarrow c_1 d &\mid c_1 \operatorname{ind}_r a \\ \Leftrightarrow d &\mid \operatorname{ind}_r a. \end{aligned}$$

Note 4. Suppose that m has two primitive roots r and s. Let $(a, m) = 1$. Then

$$\operatorname{ind}_s a \equiv \operatorname{ind}_s r \cdot \operatorname{ind}_r a \pmod{\phi(m)}.$$

Proof. Put $i = \operatorname{ind}_s a,\ j = \operatorname{ind}_s r,\ k = \operatorname{ind}_r a$. Then

$$s^i \equiv a \quad s^j \equiv r \quad r^k \equiv a \pmod{m},$$

thus

$$s^i \equiv a \equiv r^k \equiv \left(s^j\right)^k \equiv s^{jk} \pmod{m},$$

and so

$$i \equiv jk \pmod{\phi(m)}.$$

□

Theorem 37 (Euler Criterion). *Let p be an odd prime, and $(a, p) = 1$. Then $x^2 \equiv a \pmod{p}$*

1. *has a solution if and only if $p^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*
2. *has no solutions if and only if $p^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

[16] e. g. $x^3 \equiv 4 \pmod{13}$ has no solution.

Proof. By Euler's theorem, $a^{p-1} \equiv 1 \pmod p$. Then

$$\begin{aligned} a^{p-1} - 1 &\equiv 0 \pmod p \\ \Leftrightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) &\equiv 0 \pmod p. \end{aligned}$$

Note that $1 \not\equiv -1 \pmod p$ since p is odd prime. By the previous theorem, $x^2 \equiv a \pmod p$ has a solution if and only if $a^{\frac{p-1}{(2,p-1)}} = a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

5 Quadratic Residue

5.1 October 29th

Consider $ax + b \equiv 0 \pmod p$ where p is prime and $p \nmid a$.[17] Note that this is always solvable.[18]

Now consider $ax^2 + bx + c \equiv 0 \pmod p$. Recall $ax^2 + bx + c = 0$ – put $x = y + \lambda$. Then

$$\begin{aligned} a(y+\lambda)^2 + b(y+\lambda) + c &= 0 \\ \Rightarrow ay^2 + 2a\lambda y + a\lambda^2 + by + b\lambda + c &= 0 \\ \Rightarrow ay^2 + (2a\lambda + b)y + a\lambda^2 + b\lambda + c &= 0. \end{aligned}$$

Put $\lambda = -\frac{b}{2a}$. Then

$$\begin{aligned} ay^2 &= -a\lambda^2 - b\lambda - c \\ &= -a\left(-\frac{b}{2a}\right)^2 - b\left(-\frac{b}{2a}\right) - c \\ &= \frac{b^2 - 4ac}{4a}. \end{aligned}$$

Thus

$$\begin{aligned} y^2 &= \frac{b^2 - 4ac}{4a^2} \\ \Rightarrow y &= \pm\frac{\sqrt{b^2 - 4ac}}{2a}, \end{aligned}$$

[17] If $p \mid a$, then $b \equiv 0 \pmod p$.
[18] Since $(a, p) = 1$, $ax + b \equiv 0 \Rightarrow x \equiv a^{p-2}(-b) \pmod p$.

hence

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Return to $ax^2 + bx + c \equiv 0 \pmod{p}$. We may assume that $p \nmid a$ and $p \neq 2$. [19] Since $p \nmid a$, we can find an inverse of a, say a^*, i. e. $a \cdot a^* \equiv 1 \pmod{p}$. Then

$$ax^2 + bx + c \equiv a\left(x^2 + a^* bx + a^* c\right) \pmod{p}.$$

Since $p \neq 2$, we can find an inverse $2^* = \frac{p+1}{2}$ for 2 modulo p. Thus

$$\begin{aligned} & x^2 + a^* bx + a^* c \\ & \equiv (x + 2^* a^* b)^2 + a^* c - (2^*)^2 (a^*)^2 b^2 \pmod{p} \end{aligned}$$

5.2 October 31st

Put $y = x + 2^* a^* b$ and $d = (2^*)^2 (a^*)^2 b^2 - a^* c$. Hence

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad \text{if and only if} \quad y^2 \equiv d \pmod{p}.$$

Remark 15. $ax^2 + bx + c \equiv 0 \pmod{p}$, p is odd prime, $p \nmid a$. Since p is odd and $p \nmid a$, $p \nmid 4a$. Thus

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad \text{if and only if} \quad 4a\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Note that

$$\begin{aligned} & 4a\left(ax^2 + bx + c\right) \\ & = 4a^2x^2 + 4abx + 4ac \\ & = (2ax + b)^2 - \left(b^2 - 4ac\right). \end{aligned}$$

Thus

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad \text{if and only if} \quad y^2 \equiv A \pmod{p}$$

where $y = 2ax + b$ and $A = b^2 - 4ac$.

[19] If $p \mid a$, then $ax^2 + bx + c \equiv 0 \Leftrightarrow bx + c \equiv 0 \pmod{p}$.
If $p = 2$, then $ax^2 + bx + c \equiv 0 \pmod{2}$ is too easy.

Example 9. $3x^2 - 4x + 7 \equiv 0 \pmod{13}$?

1. (calculation left for students.)
2. $4a = 4 \cdot 3 = 12$. We solve $12\left(3x^2 - 4x + 7\right) \equiv 0 \pmod{13}$. Then

$$\begin{aligned}(6x-4)^2 &\equiv 16 - 84 \pmod{13}\\ &\equiv 10 \pmod{13}\end{aligned}$$

Put $y = 6x - 4$. Then $t^2 \equiv 10 \pmod{13}$. It can be seen that $\exists$ two solutions $y \equiv 6$ or $7 \pmod{13}$.[20] Note that

$$\begin{aligned}6x - 4 &\equiv 6 \pmod{13}\\ 6x - 4 &\equiv 7 \pmod{13}\end{aligned}$$

Hence $x \equiv 6$ or $x \equiv 4 \pmod{13}$.

Definition 16 (Quadratic Residue). $m \in \mathbb{Z}^+$, $(a, m) = 1$. *We say that a is a* ***quadratic residue*** *of m if*

$$x^2 \equiv a \pmod{m}$$

has a solution.

Remark 16. $x^2 \equiv a \pmod{p}$ and p is prime. If $(p, a) = 1$, i. e. $(i, p) \neq 1$, then $x \equiv 0$ is the only solution.[21]

[20] $2\,\mathrm{ind}_6\, y \equiv \mathrm{ind}_6\, 10 \pmod{12} \Rightarrow \mathrm{ind}_6\, y \equiv 1$ or $7 \pmod{12}$

[21] Since $p \mid a$, $a \equiv 0 \pmod{p}$. Then $x^2 \equiv a \equiv 0 \pmod{p}$.
If x_0 is a solution, then $p \mid x_0^2$ and so $p \mid x_0$, thus $x_0 \equiv 0 \pmod{p}$.

Example 10. $p = 13$. Note that

$$\begin{aligned} 1^2 &\equiv 1 \equiv 12^2 \pmod{13} \\ 2^2 &\equiv 4 \equiv 11^2 \pmod{13} \\ 3^2 &\equiv 9 \equiv 10^2 \pmod{13} \\ 4^2 &\equiv 3 \equiv 9^2 \pmod{13} \\ 5^2 &\equiv 12 \equiv 8^2 \pmod{13} \\ 6^2 &\equiv 10 \equiv 7^2 \pmod{13} \end{aligned}$$

Thus 13 has exactly 6 quadratic residues, namely 1, 3, 4, 9, 10, 12, and 6 quadratic non-residues, 2, 5, 6, 7, 8, 11.[22]

Lemma 6. *p : odd prime, $p \nmid a$. Then $x^2 \equiv a \pmod{p}$ has either no solutions, or exactly 2 incongrugent solutions modulo p.*

Proof. If $x^2 \equiv a \pmod{p}$ has a solution, say $x = x_0$. Then $x \equiv -x_0 \equiv p - x_0$ is also a solution.

Note that $x_0 \not\equiv -x_0 \pmod{p}$.[23] To show that there are no more than 2 incongrugent solutions, assume that $x \equiv x_0$ and $x \equiv x_1$ are both somutions of $x^2 \equiv a \pmod{p}$. Note that

$$x_0^2 \equiv x_1^2 \equiv a \quad \text{and so} \quad 0 \equiv x_0^2 - x_1^2 \equiv (x_0 - x_1)(x_0 + x_1).$$

This $p \mid (x_0 - x_1)$ or $p \mid (x_0 + x_1)$, hence $x_0 \equiv x_1 \pmod{p}$ or $x_0 \equiv -x_1 \pmod{p}$. □

Theorem 38. *Every odd prime p has exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues.*

Proof. (Using Lemma; See the book.)

[22] FYI: In 1973, R. H. Hudson proved that 13 is the only prime p that has more than $\sqrt{p}$ consecutive quadratic non-residues.

[23] If $x_0 \equiv -x_0$, then $2x_0 \equiv 0$. Note that $x_0^2 \equiv a \Rightarrow p \nmid x_0$, $p \nmid 2 \Rightarrow p \nmid 2x_0$.

Definition 17 (Legendre Symbol). *p : odd prime, $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{otherwise} \end{cases}$$

e. g.

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$
$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

Question: $\left(\frac{713}{1009}\right) =?$

$x^2 \equiv 713 \pmod{1009}$?

Recall Euler's criterion

p : odd prime, $p \nmid a$. $x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Theorem 39 (Euler Criterion). *p : odd prime, $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

e. g.

$$\begin{aligned}\left(\frac{5}{23}\right) &\equiv 5^{\frac{23-1}{2}} \pmod{23} \\ &\equiv 5^{11} \pmod{23} \\ &\equiv \left(5^2\right)^5 \cdot 5 \pmod{23} \\ &\equiv 2^5 \cdot 5 \pmod{23} \\ &\equiv -1 \pmod{23}.\end{aligned}$$

Hence $\left(\frac{5}{23}\right) = -1$.

Theorem 40. *p : odd prime, $p \nmid a$, $p \nmid b$.*

1. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3. $\left(\frac{a^2}{p}\right) = 1$.

Proof. 1., 3. It's trivial.

2. By Euler criterion,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}, \qquad \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}},$$

and

$$\left(\frac{ab}{p}\right) \equiv ab^{\frac{p-1}{2}}.$$

Thus

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv ab^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right)$$

hence $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proposition. p : odd prime.

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \pmod 4\\ -1 & \text{if } p\equiv 3 \pmod 4\end{cases}$$

5.3 November 5th

(Just returned from Bangkok; due to jet lag, errors may occur for this day's lecture notes. Please read with care.)

Question. How can we calcaulate $\left(\frac{a}{p}\right)$?

Suppose that $a=\pm p_1^{e_1}p_2^{e_2}\times\cdots p_i^{e_i}$, where $p_1,p_2,p_3,\cdots,p_i$ are distinct primes. Since $p\nmid a$ and $p\neq p_i, \forall 1\leq i\leq k$. Thus

$$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{p_1}{p}\right)^{e_1}\times\cdots\times\left(\frac{p_i}{p}\right)^{e_i}.$$

Hence in order to calcaulate $\left(\frac{a}{p}\right)$, it suffice to be able to calculate $\left(\frac{q}{p}\right)$ where p and q are distinct primes.

Lemma 7 (Gauss's Lemma). *p : odd prime. $p\nmid a$.*

If s is the number of least positive residues mod p of the integers $a,2a,3a,\cdots,\frac{p-1}{2}a$ that are greater than $\frac{p}{2}$, then $\left(\frac{a}{p}\right)=(-1)^s$.

e. g. $\left(\frac{5}{11}\right)$

The least positive residues of

$$1\cdot 5 \quad 2\cdot 5 \quad 3\cdot 5 \quad 4\cdot 5 \quad 5\cdot 5$$

Note that $s=2$.

Proof. (Proof left for homework; due November 7th.)

Theorem 41. *p : odd prime.*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$
$$= \begin{cases} 1 & \textit{if } p \pm 1 \pmod 8 \\ -1 & \textit{if } p \pm 3 \pmod 8 \end{cases}$$

24

Proof. By Gauss's Lemma, $\left(\frac{2}{p}\right) = (-1)^s$ where s is the number of least positive residues mod p of the integers $1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \cdots, \frac{p-1}{2} \times 2$ that are greater than $\frac{p}{2}$.

Since all of these integers are less than p, we need only count these greater than $\frac{p}{2}$ to find. Note that the integers $2j$ where $1 \leq j \leq \frac{p-1}{2}$ are less than $\frac{p}{2}$ whem $j \leq \frac{p}{4}$.

Thus $\exists \left\lfloor \frac{p}{4} \right\rfloor$ integers in the set less that $\frac{p}{2}$. By Gauss's lemma,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor}.$$

To prove the theorem, it suffice to show that $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2$ for every odd integer p.

Note that it holds for a positive integer p if and only if it holds for $p+8$. It can be checked that it holds for $p \equiv \pm 1$, $p \equiv \pm 3 \pmod 8$. Hence we conclude that it holds for every odd integer p.

e. g.

$$\left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = 1\,(-1) = -1$$

Theorem 42 (The Law of Quadratic Reciprocity). *p, q : distinct odd primes.*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

or

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Proof. (See the book.)

Remark 17. Note that

$$\frac{p-1}{2} = \begin{cases} \text{even} & \text{if } p \equiv 1 \pmod 4 \\ \text{odd} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

thus

$$\frac{p-1}{2}\frac{q-1}{2} = \begin{cases} \text{even} & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4 \\ \text{odd} & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Since $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are ± 1,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Theorem 43. *$p, q = 2p+1$: p, q are odd primes.*

$M_p = 2^p - 1$: Mersenne number.

Then one of the following holds.

1. $q \mid M_p$
2. $q \mid (M_p + 2)$

Moreover,

$$q \mid M_p \Leftrightarrow q \equiv 1 \text{ or } q \equiv -3 \pmod 8$$
$$q \mid (M_p + 2) \Leftrightarrow q \equiv -1 \text{ or } q \equiv 3 \pmod 8$$

Proof. By Fermat's, $2^{q-1} \equiv 0 \pmod q$, then

$$\begin{aligned} M_p(M_p + 2) &= (2^p - 1)(2^p + 1) \\ &= 2^{2p} - 1 = 2^{q-1} - 1 \\ &\equiv 0 \pmod q. \end{aligned}$$

Since q is prime, $q \mid M_p$ or $q \mid (M_p + 2)$.

Note that

$$\begin{aligned} q \mid M_p &\Leftrightarrow 2^p = 2^{\frac{q-1}{2}} \equiv 1 \pmod q \\ &\Leftrightarrow \left(\frac{2}{q}\right) = 1 \end{aligned}$$

and

$$\begin{aligned} 2 \mid (2^p - 2) &\Leftrightarrow 2^p = 2^{\frac{q-1}{2}} \equiv -1 \pmod q \\ &\Leftrightarrow \left(\frac{2}{q}\right) = -1 \end{aligned}$$

Hence it follows from the fact that

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = \begin{cases} 1 & q \equiv \pm 1 \pmod 8 \\ -1 & q \equiv \pm 3 \pmod 8 \end{cases}$$

Theorem 44 (Pelpin's Test). $F_m = 2^{2^m} + 1$ *is a prime if and only if* $3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$.

Proof. ($\Leftarrow$) Suppose that $3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$. Then $3^{F_m-1} \equiv 1 \pmod{F_m}$.

If p is a prime that $p \mid F_m$, then $3^{F_m-1} \equiv 1 \pmod{p}$. Note that $(3, p) = 1$. Then

$$\operatorname{ord}_p 3 \mid (F_m - 1) = 2^{2^m}$$

, and so $\operatorname{ord}_p 3$ must be a power of 2.

However, since $\operatorname{ord}_p 3 \nmid 2^{2^n-1} = \frac{F_m-1}{2}$. This is a contradiction.

5.4 November 7th

Therefore $\operatorname{ord}_p 3 = 2^{2^m} = F_m - 1$.

Note that $\operatorname{ord}_p 3 = F_m - 1 \le p - 1 \because 3^{p-1} \equiv 1 \pmod{p}$ by Fermat. Hence $p = F_m$. Therefore F_m is prime.

($\Rightarrow$) Suppose $F_m = 2^{2^m} + 1$ is prime. Note that

$$\begin{aligned}
\left(\frac{3}{F_m}\right) &= (-1)^{\frac{F_m-1}{2}\frac{3-1}{2}} \left(\frac{F_m}{3}\right) \\
&= \left(\frac{F_m}{3}\right) \\
&= \left(\frac{2}{3}\right) \qquad \because F_m \equiv 2 \pmod{3} \\
&= -1.
\end{aligned}$$

By Euler criterion, $\left(\frac{3}{F_m}\right) = 3^{\frac{F_m-1}{2}} \pmod{F_m}$. Hence we conclude that $3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}$.

Definition 18 (Jacobi symbol). *n: odd positive integer > 1, $(a,n)=1$. Then the **Jacobi symbol** $\left(\frac{a}{n}\right)$ is defined by*

$$\begin{aligned}\left(\frac{a}{n}\right) &= \left(\frac{a}{p_1^{t_1}p_2^{t_2}\times\cdots\times p_m^{t_m}}\right)\\ &= \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2}\times\cdots\times\left(\frac{a}{p_m}\right)^{t_m}\end{aligned}$$

where $n = p_1^{t_1}p_2^{t_2}\times\cdots\times p_m^{t_m}$ is a prime factorization of n.

Remark 18. 1. If n is odd prime, then the Jacobi symbol is same as Legendre symbol.
2. When n is composite, $\left(\frac{a}{n}\right)$ does not tell us where $x^2 \equiv a \pmod{n}$ has a solution.

e. g. $a = 2, n = 15$

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$$

but $x^2 \equiv 2 \pmod{15}$ has no solutions.

Theorem 45. *1.* $a \equiv b \pmod{m} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
4. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$
5. $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$ *if* $(n,m)=1$

Proof. (Easy; see the book.)

Example 11. $\left(\frac{713}{1009}\right)? \Rightarrow 713 = 23\cdot 31$, 1009 is prime.

1.

$$\begin{aligned}
\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) \\
&= \left(\frac{20}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) \\
&= \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) \\
&= \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) \\
&= \left(\frac{2}{3}\right) = -1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) \\
&= \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) \\
&= \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) \\
&= \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) \\
&= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) \\
&= -\left(\frac{4}{3}\right) = -1
\end{aligned}$$

$$\begin{aligned}
\left(\frac{713}{1009}\right) &= \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right) \\
&= (-1)(-1) = 1.
\end{aligned}$$

2.

$$\begin{aligned}
\left(\frac{713}{1009}\right) = \left(\frac{1009}{713}\right) &= \left(\frac{296}{713}\right) \\
&= \left(\frac{2^3}{713}\right)\left(\frac{37}{713}\right) = \left(\frac{2}{713}\right)\left(\frac{37}{713}\right) \\
&= \left(\frac{37}{713}\right) = \left(\frac{713}{37}\right) = \left(\frac{10}{37}\right) \\
&= \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{37}{5}\right) \\
&= -\left(\frac{2}{5}\right) = 1
\end{aligned}$$

6 Continued Fractions

6.1 November 7th

Using the Euclidean algorithm, we can express rational numbers as continued fractions.

Definition 19 (Finite Continued Fraction). *A* ***finite continued fraction*** *is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} = [a_0; a_1, a_2, \cdots, a_n]$$

where $a_0, a_1, \cdots, a_n$ are real numbers whom of which $a_1, a_2, \cdots, a_n$ are positive.

A finite continued fraction is simple if $a_0, a_1, \cdots, a_n \in \mathbb{Z}$.

Theorem 46. *Every finite simple continued fraction represents a rational number. Conversely, every rational number can be expressed as a finite simple continued fraction.*

Remark 19. $\frac{62}{23} = [2, 1, 2, 3, 2] = [2, 1, 2, 3, 1, 1]$

Definition 20. *A continued fraction* $[a_0; a_1, \cdots, a_k]$ *where k is a nonnegative integer less than n is called the k-**th convergerent** of a continued fraction* $[a_0; a_1, \cdots, a_n]$.

The k-th convergent is denoted by C_k.

Theorem 47. *Let* $a_0, a_1, \cdots, a_n$ *be real numbers with* $a_1, a_2, \cdots, a_n > 0$. *Define the sequence* $\{p_i\}$ *and* $\{q_i\}$ *recursively as*

$$\begin{cases} p_0 := a_0 & q_0 := 1 \\ p_1 := a_1 a_0 & q_1 := a_1 \\ p_k := a_k p_{k-1} + p_{k-2} & q_k := a_k q_{k-1} + q_{k-2} \qquad \text{for } k = 2, 3, \cdots, n \end{cases}$$

then $C_k = \frac{p_k}{q_k}$.

6.2 November 12th

Proof.

$$\begin{aligned} k = 0 \qquad & C_0 = [a_0] = \frac{a_0}{1} = \frac{a_0}{q_0} \\ k = 1 \qquad & C_1 = [a_0;, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1} \\ k = 2 \qquad & C_2 = [a_0;, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_0 (a_1 a_2 + 1) + a_2}{a_1 a_2 + 1} = \frac{p_2}{q_2} \end{aligned}$$

Assume that the results hold for a positive integer $2 \le k \le n$. Note that

$$\begin{aligned} C_{k+1} &= [a_0; a_1, a_2, \cdots, a_k] \\ &= \left[a_0; a_1, a_2, \cdots, a_k + \frac{1}{a_{k+1}}\right] \\ &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \vdots \leftarrow \text{(see the text.)} \\ &= \frac{p_{k+1}}{q_{k+1}} \end{aligned}$$

Theorem 48. $k \in \mathbb{Z}^+$. $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$.

Proof.

$$\begin{aligned} k &= 1 \qquad & p_1 q_0 - p_0 q_1 &= (a_0 a_1 + 1) - a_0 a_1 = 1 \\ k &= 2 \qquad & p_2 q_1 - p_1 q_2 &= (a_2 p_1 + a_0) a_1 - p_1 (a_2 a_1 + 1) = -1 \end{aligned}$$

Use induction for $k \ge 3$. (See the text)

Corollary 7. *p_k, q_k are relatively prime.*

Proof. Let $d_k = (p_k, q_k)$. By theorem,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Thus $d_k \mid (-1)^{k-1}$, hence $d_k = 1$.

Corollary 8.

$$\begin{aligned} C_k - C_{k-1} &= \frac{(-1)^{k-1}}{q_k q_{k-1}} \qquad & \textit{for } 1 \le k \le n \\ C_k - C_{k-2} &= \frac{a_k (-1)^k}{q_k q_{k-2}} \qquad & \textit{for } 2 \le k \le n \end{aligned}$$

Proof. By theorem,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Then

$$\begin{aligned}
C_k - C_{k-1} &= \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \\
&= \frac{p_k q_{k-1} - q_k p_{k-1}}{q_k q_{k-1}} \\
&= \frac{(-1)^{k-1}}{q_k q_{k-1}} \\
C_k - C_{k-2} &= \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} \\
&= \frac{p_k q_{k-2} - q_k p_{k-2}}{q_k q_{k-2}} \\
&= \frac{(a_k p_{k-1} + p_{k-2})\, q_{k-2} - (a_k q_{k-1} + q_{k-2})\, p_{k-2}}{q_k q_{k-2}} \\
&= \frac{a_k (-1)^{k-2}}{q_k q_{k-2}} \\
&= \frac{a_k (-1)^{k}}{q_k q_{k-2}}
\end{aligned}$$

Theorem 49. *Let C_k be the kth convergent of finite simple continued fraction $[a_0; a_1, a_2, \cdots, a_n]$. Then*

$$C_1 > C_3 > C_5 > \cdots$$

$$C_2 < C_4 < C_6 < \cdots$$

and

$$C_{2j+1} > C_{2k} \quad \text{for } j = 0, 1, 2, \cdots \quad k = 0, 1, 2, \cdots$$

i. e.

$$C_0 < C_2 < C_4 < \cdots < C_5 < C_3 < C_1.$$

Proof. By corollary,

$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}}.$$

Thus

$$\begin{cases} C_k - C_{k-2} < 0 & \text{if } k \text{ is odd} \\ C_k - C_{k-2} > 0 & \text{if } k \text{ is even} \end{cases}$$

and so

$$C_1 > C_3 > C_5 > \cdots$$

$$C_2 < C_4 < C_6 < \cdots.$$

Note that

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m}q_{2m-1}} < 0,$$

and so $C_{2m} < C_{2m-1}$. Therefore

$$C_{2j+1} > C_{2j+2k+1} > C_{2j+2k+2} > C_{2k}$$

for $j = 0, 1, 2, \cdots, k = 0, 1, 2, \cdots$.

Remark 20. Consider $79x \equiv 3 \pmod{103} \Leftrightarrow 79x + 103y = 3$. Note that

$$\frac{79}{103} = [0; 1, 3, 3, 2, 3].$$

It can be seen that $p_5q_4 - p_4q_5 = 79 \cdot 30 - (-23) \cdot 104 = 1$. Thus

$$79x + 103y = 3 \Leftarrow \begin{cases} x = 90 \\ y = -69 \end{cases}$$

Suppose that we have an infinite sequence of $a_0, a_1, a_2, \cdots$ such that $a_0, a_1, \cdots > 0$. We define **infinite continued fractions** as limits of finite continued fractions.

Theorem 50. *Let $a_0, a_1, \cdots$ be an infinite sequence of integers with $a_0, a_1, \cdots > 0$, and let $C_k := [a_0; a_1, a_2, \cdots, a_k]$. Then $\lim_{k\to\infty} C_k = \alpha$ exists.*

Proof. Recall

$$C_0 < C_2 < C_4 < \cdots < C_5 < C_3 < C_1.$$

By Monotone Convergence Theorem,

$$\lim_{n\to\infty} C_{2n+1} = \alpha_1 \qquad \lim_{n\to\infty} C_{2n} = \alpha_2$$

for some $\alpha_1, \alpha_2 \in \mathbb{R}$. Note that

$$C_{2n+1} - C_{2n} = \frac{(-1)^{2n}}{q_{2k+1}q_{2k}} = \frac{1}{q_{2k+1}q_{2k}}$$

and $q_k > k \; \forall k \in \mathbb{Z}^+$. Therefore

$$\begin{aligned} 0 &= \lim_{n\to\infty} (C_{2n+1} - C_{2n}) \\ &= \lim_{n\to\infty} C_{2n+1} - \lim_{n\to\infty} C_{2n} \\ &= \alpha_1 - \alpha_2, \end{aligned}$$

and so $\alpha_1 = \alpha_2$.

Definition 21. *In the theorem above,* α *is called the value of an* ***infinite simple continued fraction*** $[a_0; a_1, a_2, \cdots]$.

Theorem 51. *Let* $a_0, a_1, \cdots$ *be integers with* $a_1, a_2, \cdots > 0$. *Then* $[a_0; a_1, a_2, \cdots]$ *is irrational.*

Proof. Let $\alpha = [a_0; a_1, a_2, \cdots]$ and $C_k = \frac{p_k}{q_k} = [a_0; a_1, a_2, \cdots, a_k]$. For $n \in \mathbb{Z}^+$,

$$C_{2n} < \alpha < C_{2n+1}$$

and so

$$0 < \alpha - C_{2n} < C_{2n+1} - C_{2n}.$$

Note that

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}},$$

thus

$$0 < \alpha - C_{2n} = \alpha - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n}q_{2n+1}}.$$

Assume that α is rational, so that $\alpha = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b > 0$. Note that

$$aq_{2n} - bp_{2n} \in \mathbb{Z} \text{ for all } n \in \mathbb{N}.$$

Since $q_{2n+1} > 2n+1$ for $n \geq 2$, $\exists n_0 \in \mathbb{Z}^+$ such that

$$q_{2n_0+1} > b \text{ so that } \frac{b}{q_{2n_0}+1} < 1.$$

But this makes a contradiction because

$$0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}} < 1.$$

6.3 November 14th

Theorem 52. *Let $\alpha = \alpha_0$ be an irrational number and define the sequence $a_0, a_1, \cdots$ recursively by*

$$\begin{aligned} a_k &:= \lfloor \alpha_k \rfloor \\ \alpha_{k+1} &= \frac{1}{\alpha_k - a_k} \qquad\qquad \text{for } k = 0, 1, \cdots \end{aligned}$$

then $\alpha = [a_0; a_1, a_2, \cdots]$.

Proof. Clearly $a_k \in \mathbb{Z}\ \forall k$. Note that $\alpha_0 = \alpha$ is irrational if α_k is irrational, then α_{k+1} is irrational. Thus α_k is irrational for every k.

Thus

$$\alpha_k \neq a_k \text{ and } a_k < \alpha_k < a_k + 1 \qquad \forall k,$$

and so $0 < \alpha_k - a_k < 1$, hence

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} < 1$$

and

$$a_{k+1} = \lfloor \alpha_{k+1} \rfloor \geq 1 \qquad \text{for } k = 0, 1, 2, \cdots.$$

Therefore $a_1, a_2, \cdots$ are positive integers. Note that

$$\alpha_k = a_k + \frac{1}{\alpha_k + 1} \qquad \text{for } k = 0, 1, 2, \cdots,$$

and so

$$\begin{aligned}\alpha = \alpha_0 &= a_0 + \frac{1}{\alpha_1} \\ &= a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} \\ &= \vdots\end{aligned}$$

We want to show that

$$\lim_{k\to\infty} [a_0; a_1, a_2, \cdots] = \alpha.$$

Note that, by theorem 12.9,

$$\begin{aligned}\alpha &= [a_0; a_1, a_2, \cdots, a_k, \alpha_{k+1}] \\ &= \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}},\end{aligned}$$

hence

$$\begin{aligned}|\alpha - C_k| &= \left| \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \right| \\ &= \left| \frac{-(p_k q_{k-1} - p_{k-1} q_k)}{(\alpha_{k+1} q_k + q_{k-1})\, q_k} \right| \\ &= \left| \frac{(-1)^k}{(\alpha_{k+1} q_k + q_{k-1})\, q_k} \right| \\ &< \left| \frac{(-1)^k}{q_{k+1} q_k} \right|\end{aligned}$$

Thus

$$|\alpha - C_k| < \frac{1}{q_{k+1} q_k} < \frac{1}{(k+1)\,k} \to 0 \text{ as } k \to \infty,$$

hence

$$\lim_{k\to\infty} C_k = \alpha = [a_0; a_1, a_2, \cdots].$$

Theorem 53 (Uniqueness of Infinite Continued Fraction). *If the two infinite simple continued fractions $[a_0; a_1, a_2, \cdots]$ and $[b_0; b_1, b_2, \cdots]$ represent two same irrational number, then $a_k = b_k$ for $k = 0, 1, 2, \cdots$.*

Proof. Let $\alpha = [a_0; a_1, a_2, \cdots]$. Since $C_0 = a_0$ and $C_1 = a_0 + \frac{1}{a_1}$, it follows that

$$C_0 = a_0 < \alpha < a_0 + \frac{1}{a_1} = C_1,$$

thus $a_0 = \lfloor \alpha \rfloor$.

Note that

$$[a_0; a_1, a_2, \cdots] = a_0 + \frac{1}{[a_1, a_2, \cdots]}.$$

Suppose that $[a_0; a_1, a_2, \cdots] = [b_0; b_1, b_2, \cdots]$. Then $b_0 = \lfloor \alpha \rfloor = a_0$ and

$$a_0 + \frac{1}{[a_1; a_2, \cdots]} = b_0 + \frac{1}{[b_1; b_2, \cdots]},$$

thus

$$\frac{1}{[a_1; a_2, \cdots]} = \frac{1}{[b_1; b_2, \cdots]}.$$

Continuing this process by induction gives $a_k = b_k$ for $k = 0, 1, \cdots$.

e. g.

$$\begin{aligned} \sqrt{3} &= [1; 1, 2, 1, 2, \cdots] \\ &= \left[1; \overline{1, 2}\right] \end{aligned}$$

(calculation left for homework.)

Theorem 54. *If α is an irrational number, then there are infinitely many rational number $\frac{p}{q}$ such that*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Proof. Let $\frac{p_k}{q_k}$ be the k-th convergent of an infinite simple continued fraction of α. Then we know that

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k q_{k+1}} < \frac{1}{q_k^2}.$$

Remark 21. Is is known that the convergent of an infinite simple continued fraction of α are the best approximation to α in the sense that $\frac{p_k}{q_k}$ is closest to α than any other rational numbers with a denominator less that q_k.

Definition 22 (Periodic Continued Fraction). *An infinite simple continued fraction* $[a_0; a_1, a_2, \cdots]$ *is* ***periodic*** *if* $\exists N, k \in \mathbb{Z}^+$ *such that* $a_n = a_{n+k}$ *for all* $n \geq N$.[25]

Definition 23 (Quadratic Irrational). $\alpha \in \mathbb{R}$ *is said to be* ***quadratic irrational*** *if* α *is irrational and* α *is a root of* $Ax^2 + Bx + C = 0$, *where* $A, B, C \in \mathbb{Z}$ *and* $A \neq 0$.

e. g. $\sqrt{3}$ is a quadratic irrational, while $\sqrt[3]{3}$ is not.

Lemma 8. α *is quadratic irrational if and only if* $\exists a, b, c \in \mathbb{Z}$ *with* $b > 0$, $c \neq 0$ *such that* b *is not a perfect square and*

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Proof. ($\Rightarrow$) By the assumption,

$$A\alpha^2 + B\alpha + C = 0 \quad \text{where} \quad A, B, C \in \mathbb{Z} \text{ and } A \neq 0.$$

Then

$$\alpha = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

Since α is irrational, $B^2 - 4AC > 0$, and $B^2 - 4AC$ is not a perfect square. Put $(a, b, c) = \left(-B, B^2 - 4AC, 2A\right)$, or $(a, b, c) = \left(B, B^2 - 4AC, -2A\right)$. Then

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

($\Leftarrow$) It is trivial.

6.4 November 19th

Lemma 9. *α : quadratic irrational. $r, s, t, u \in \mathbb{Z}$, then $\frac{r\alpha+s}{t\alpha+u}$ is rational or quadratic irrational.*

Proof. By previous lemma,

$$\alpha = \frac{a+\sqrt{b}}{c} \text{ where } \cdots$$

then

$$\begin{aligned}\frac{r\alpha+s}{t\alpha+u} &= \frac{r\left(\frac{a+\sqrt{b}}{c}\right)+s}{t\left(\frac{a+\sqrt{b}}{c}\right)+u} \\ &= \frac{ar+cs+r\sqrt{b}}{at+cu+t\sqrt{b}} \\ &= \frac{(\qquad)+(\qquad)\sqrt{b}}{(at+cu)^2-t^2b} \text{ (see the book for detailed calculation.)}\end{aligned}$$

Theorem 55. *An infinite simple continued fraction of α is periodic if and only if α is quadratic irrational.*

e. g. $x = \left[3; \overline{1, 2}\right]$

$\Rightarrow y = \left[\overline{1; 2}\right] \Rightarrow y = [1; 2, y] = 1 + \frac{1}{2+\frac{1}{y}}$

Proof. ($\Rightarrow$, by Euler in 1737) Let

$$\alpha = [a_0; a_1, a_2, \cdots, a_{N-1}, \overline{a_N, a_{N+1}, \cdots, a_{N+k}}]$$

and

$$\beta = [\overline{a_N; a_{N+1}, \cdots, a_{N+k}}].$$

Then

$$\beta = [a_N; a_{N+1}, \cdots, a_{N+k}, \beta].$$

By Theorem 12.9.,

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}} \tag{1}$$

where $\frac{p_k}{q_k}$, $\frac{p_{k+1}}{q_{k+1}}$ are convergents of β. Clearly[26], β is irrational.

By (1),

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_k = 0,$$

thus β is a quadratic irrational.

Note that

$$\alpha = [a_0; a_1, a_2, \cdots, a_{N-1}, \beta].$$

By theorem,

$$\alpha = \frac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}}$$

where $\frac{p_{N-1}}{q_{N-1}}$, $\frac{p_{k+N-2}}{q_{k+N-2}}$ are convergents of α. Hence α is quadratic irrational, and it represents an infinite simple continued fraction.

($\Leftarrow$, by Lagrange in 1770)

Lemma 10. *If α is a quadratic irrational, then α can be written as*

$$\alpha = \frac{P + \sqrt{d}}{Q}$$

where $P, Q \in \mathbb{Z}$, $Q \neq 0$, $d > 0$, d is not perfect square, and $Q \mid \left(d - P^2\right)$.

Proof (of Lemma). By Lemma,

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Put $P := a|c|$, $Q := c|c|$, $d = bc^2$. Then $P, Q, d \in \mathbb{Z}$, $d > 0$, and d is not perfect square since b is also not.

[26] β is represented as an infinite simple continued fraction.

Note that

$$\begin{aligned} d - p^2 &= bc^2 - a^2c^2 \\ &= \left(b - a^2\right)c^2 \\ &= \pm\left(b - a^2\right)Q, \end{aligned}$$

thus $Q \mid \left(d - p^2\right)$.

Theorem 56. *α : quadratic irrational. By Lemma,*

$$\alpha_0 = \alpha = \frac{P_0 + \sqrt{d}}{Q_0}.$$

Define $\alpha_k := \frac{a_k + \sqrt{d}}{Q_k}$, $a_k := \lfloor \alpha_k \rfloor$, $P_{k+1} := a_k Q_k - P_k$, $Q_{k+1} := \frac{a - P_{k+1}^2}{Q_k}$ for $k = 0, 1, 2, \cdots$. Then

$$\alpha = [a_0; a_1, a_2, \cdots].$$

Proof. Claim $P_k, Q_k \in \mathbb{Z}$ with $Q_k \neq 0$ and $Q_k \mid \left(d - p_k^2\right)$.

Note that the induction base is true. Now suppose that $P_k, Q_k \in \mathbb{Z}$ with $Q_k \neq 0$ and $Q_k \mid (d - P_k)^2$. Then

$$\begin{aligned} P_{k+1} &= a_k Q_k - P_k \in \mathbb{Z} \\ Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k} \\ &= \frac{d - (a_k Q_k - P_k)^2}{Q_k} \\ &= \frac{d - P_k^2}{Q_k} + 2a_k P_k - a_k^2 Q_k. \end{aligned}$$

By the induction hypothesis, $Q_{k+1} \in \mathbb{Z}$ and $Q_{k+1} \mid \left(d - P_{k+1}^2\right)$.

Claim $\alpha = [a_0; a_1, a_2, \cdots]$

Suffices to show that

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} \text{ for } k = 0, 1, 2, \cdots.$$

Note that

$$\begin{aligned}
\alpha_k - a_k &= \frac{p_k + \sqrt{d}}{Q_k} - a_k \\
&= \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} \\
&= \frac{\sqrt{d} - P_{k+1}}{Q_k} \\
&= \frac{\left(\sqrt{d} - P_{k+1}\right)\left(\sqrt{d} + P_{k+1}\right)}{Q_k\left(\sqrt{d} - P_{k+1}\right)} \\
&= \frac{d - P_{k+1}^2)}{Q_k\left(\sqrt{d} - P_{k+1}\right)} \\
&= \frac{Q_k + 1}{\sqrt{d} + P_{k+1}} \\
&= \frac{1}{\alpha_{k+1}}.
\end{aligned}$$

We return to our original proof ($\Leftarrow$).

By the previous theorem, $@a = [a_0; a_1, a_2, \cdots]$ where $a_k = \left\lfloor \frac{P_k + \sqrt{d}}{Q_k} \right\rfloor$. Note that

$$\alpha = [a_0; a_1, a_2, \cdots, a_{k-1}, \alpha_k],$$

thus $\alpha = \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}$ by theorem.

Definition 24. $\alpha = \frac{a+\sqrt{b}}{c}$*; Define* $\alpha' := \frac{a-\sqrt{b}}{c}$.

By taking conjugates,

$$\alpha' = \frac{p_{k-1}\alpha_k' + p_{k-2}}{q_{k-1}\alpha_k' + q_{k-2}}.$$

Then

$$\alpha_k' = -\frac{q_{k-2}}{q_{k-1}}\left(\frac{\alpha' - \frac{p_{k-2}}{q_{k-2}}}{\alpha' - \frac{p_{k-1}}{q_{k-1}}}\right).$$

Note that $\frac{p_{k-2}}{q_{k-2}} \to \alpha$, $\frac{p_{k-1}}{q_{k-1}} \to \alpha$ as $k \to \infty$. And so, $\frac{\alpha' - \frac{p_{k-2}}{q_{k-2}}}{\alpha' - \frac{p_{k-1}}{q_{k-1}}} \to 1$.

Thus $\exists N$ such thst $\alpha_k' < 0$ for $k \geq N$.

Since $\alpha_k > 0$ for $k \geq 1 (\because a_k := \lfloor \alpha_k \rfloor > 0)$, it follows that

$$\begin{aligned} \alpha_k - \alpha_k' &= \frac{P_k + \sqrt{d}}{Q_k} - \frac{P_k - \sqrt{d}}{Q_k} \\ &= \frac{2\sqrt{k}}{Q_k} > 0 \text{ for } k \geq N. \end{aligned}$$

Thus $Q_k > 0$ for $k \geq N$.

Since $Q_k Q_{k+1} = d - P_{k+1}^2$, it follows that for $k \geq N$, $Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 < d$.

Also for $k \geq N$,

$$P_{k+1}^2 < d = \left(P_{k+1}^2 + Q_k Q_{k+1}\right)$$

and so $-\sqrt{d} < P_{k+1} < \sqrt{d}$.