0.1 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[1], we may assume that S has a positive integer.

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

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

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 $a \in S$,
   $$r = a - mq \in S$$
   . 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 1. *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
$$\exists m \geq 0 \in \mathbb{Z} \text{ such that } S = m\mathbb{Z}.$$

[1] Without loss of generality

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

Theorem 2 (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

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

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 1 (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 3. *$a \neq 0$, $b \neq 0$.*

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

0.2 September 24th

Proof. Note that

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

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 $a = a_1 d$, $b = b_1 d$, 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 $x - x_0 = b_1 t$, and similarily $y_0 - y = a_1 t$. Hence

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

Example

$$710x + 68y = 6$$

[2] Recall

$$710 \cdot (-9) + 68 \cdot 94 = 2$$
$$710 \cdot (-9 \times 3) + 68 \cdot (94 \times 3) = 2 \times 3 = 6$$

[2] Maybe an eaxm problem?

Hence

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

Definition 2 (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 4. *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 2.

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

Recall

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

Theorem 5. *For $a > 0, b > 0 \in \mathbb{Z}$,*

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

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

Theorem 6. *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 $a_i \in \mathbb{Z}$, $0 \le a_i \le b-1$ 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 3 (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 3. 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 7 (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 8. *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 $j \mid (n+1)!$. Thus $j \mid ((n+1)!+j)$.

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

> **Definition 4 (Mersenne Primes).** *A **Mersenne prime** is a Mersenne number*[3] *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 $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$

0.3 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 $p = 1$. [4]

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 4. Using Mersenne numbers and some theorem of groups[5], we can show the infinitude of primes.

---

[4] Proof exists at Wikipedia
[5] Lagrange theorem

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

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

Definition 5 (Fermat Primes). *A **Fermat prime** is a Fermat number*[6] *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 9. *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 10. *A regular polygon of n sides can be constructed using an unmarked ruler and compass if and only if*

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

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

e. g.

$$3 = 2^{2^0} + 1 \qquad \text{: constructive}$$
$$5 = 2^{2^1} + 1 \qquad \text{: constructive}$$
$$7 \qquad \text{: not constructive}$$
$$17 = 2^{2^2} + 1 \qquad \text{: constructive}$$

Theorem 11.
$$(F_m, F_n) = 1$$
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

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

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

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

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 5. 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 12 (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 13. *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 14 (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*[7].

Proof. (Using WOP; see the book.)

1 Congrugences

1.1 October 1st

Definition 6. $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$

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

Theorem 15. *1. $a \equiv a$ (mod 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 $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_n x^n$, where $a_i, b_i \in \mathbb{Z}$. Suppose $a_i \equiv b_i$ (mod 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 16. $a, b, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $d = (c, m)$.

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

$$a \equiv r \pmod m$$

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

Proof. Use the division algorithm.

Definition 7. *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.[8]
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 18. *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

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

[8] The least nonnegative residues modulo m

then

$$ar_j \equiv ar_k.$$

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

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

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

Definition 8. *$a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $(a, m) = 1$.*

*A solution of $ax \equiv 1$ (mod 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 7. $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$. $(\mathbb{Z}_n^*, *)$ is a group.

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

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

1.2 October 8th

Definition 9 (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 10 (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 20 (Euler's Theorem). *If $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with $(a, m) = 1$ then*

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

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 $a^{\phi(m)} \equiv 1 \pmod m$.[9] □

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

$$a^{p-1} \equiv 1 \text{ (mod } p\text{)}.$$

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

Corollary 4. *Let p : prime. Then*

$$a^p \equiv a \ (mod\ p).$$

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

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

Hence x can be any integer.

Theorem 21 (Wilson's Theorem). *If p is a prime, then*

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

Was conjectured by Wilson; and proved by Lagrange.

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

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

($\Rightarrow$) Note that

$$a^2 \equiv 1 \text{ (mod } p)$$

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 $a \equiv -1$ (mod p). □

Proof (of theorem). If $p = 2$, then $(p-1)! = 1 \equiv -1$ (mod 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 $ab \equiv 1$ (mod 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 22. *If $n\in\mathbb{Z}^+$ and*

$$(n-1)! \equiv -1 \ (mod\ m),$$

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 8. 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 $p \equiv 1 \pmod{4}$.