Prime Proofs

Karim El Shenawy

February 2021

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 3 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Theorems to Mark

3.9 Corollary

Let the natural number n be expressed in base 10 as

$$n = a_k a_{k-1} ... a_1 a_0.$$

Let $m = a_k + a_{k-1} + ... + a_1 + a_0$. *Then* $9 \mid n$ *if and only if* $9 \mid m$.

Proof. By contradiction, assume that $9 \nmid n$, where n is a natural number and can be expressed as $n = a_k a_{k-1} ... a_1 a_0$. Also suppose that $9 \mid m$ where m is a natural number and can be expressed as $m = a_k + a_{k-1} + ... + a_1 + a_0$. This also implies that that $n \equiv d \pmod 9$ where d is a natural number and $d \neq 0$. Moreover, we can express $n \equiv d \pmod 9$ as follows;

$\implies n \equiv d \pmod 9$

$\implies a_k a_{k-1} ... a_1 a_0 \equiv d \pmod 9$

Now lets express $a_k a_{k-1} ... a_1 a_0$ as multiple factors of 10:

$\implies (a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0) \equiv d \pmod 9$

Modular arithmetic respects distributively and thus by Modular Distributive Property we can distribute $\pmod 9$

$\implies (a_k \cdot 10^k \pmod 9 + a_{k-1} \cdot 10^{k-1} \pmod 9 + ... + a_1 \cdot 10^1 \pmod 9$

$+ a_0 \pmod 9) \equiv d \pmod 9$

By theorem 1.18, we can conclude that $10^k \pmod 9 \equiv 1^k \pmod 9 \equiv 1$.

$\implies (a_k + a_{k-1} + ... + a_1 + a_0) \equiv d \pmod 9$

Since, $m = a_k + a_{k-1} + ... + a_1 + a_0$, we can express the above equation interms of m;

$\implies m \equiv d \pmod 9$

Based off the theorm in, given that $9 \mid m$, thus $m \pmod 9 \equiv 0$. Therefore, d has to be zero., thus 9 must divide m so then $9 \mid n$. $\square$

3.14 Theorem

Given any integer a and any natural number n, there exists a unique integer t in the set $0, 1, 2, ..., n-1$ *such that* $a \equiv t \pmod n$.

Proof. Given an integer a and a natural number n. There exist integers t and q such that, by division algorithm, $a = nq + t$ where t is in the set $0, 1, 2, ..., n-1$. We can express $a = nq + t$ as follows;

$\implies a = nq + t$
$\implies a - t = nq$
$\implies n \mid a - t$
$\implies a \equiv t \pmod n$ By Definition of Congruence

By $a \equiv t \pmod n$, we can conclude that a is congruent to one or more elements from the set $0, 1, 2, ..., n-1$, since t is apart of that set. Thus a must be congruent to t modulo n where t is a unique integer in $0, 1, 2, ..., n-1$. $\square$

3.16 Theorem

Let n be a natural. Every complete residue system modulo n contains n elements.

Proof. Suppose there exist this set m where $m = \{0, 1, 2, 3, 4, ..., n-1\}$ where n is some natural number. Also let me be a complete residue system mod$n$ and suppose that the size of m is greater than n.
Now at least two elements from m must have the same remainder when divided by n, by Pigeonhole Principle. This contradicts he aforementioned statement that m is a complete residue system mod$n$. Therefore complete residue system modulo n must contains equal or less than the size of m. $\square$

3.19 Theorem

Let a, b, and n be integers with $n > 0$. *Show that* $ax \equiv b \pmod n$ *has a solution if and only if there exist integers x and y such that* $ax + ny = b$.

Proof. We'll need to prove 2 parts;

1. Let $a, b, n \in \mathbf{Z}$ with $n > 0$. By definition, $ax \equiv b \pmod n \implies n \mid ax - b$ and thus also $ax - b = np$ for some integer p. Moreover, by direct proof,

$$\begin{aligned} ax - b &= np \\ ax - np &= b \\ ax + n(-p) &= b \\ ax + ny &= b \end{aligned}$$

Since $p \in \mathbf{Z}$, let $y \in \mathbf{Z}$ such that $p = -y$

Thus $ax \equiv b \pmod{n}$ has a solution such that $ax + ny = b$ for some integer x and y.

2. Given that $ax + ny = b$ where $a, b, n, x, y \in \mathbf{Z}$ and $n > 0$. By direct proof, assume that x and y exist we can assimilate the following

$$\begin{aligned} ax + ny &= b \\ ax - b &= -ny \\ ax - b &= n(-y) \\ ax - b &= n(-y) \\ ax &\equiv b \pmod{n} \end{aligned}$$

Now by contradiction let's assume that x and y did not exist;

$$\begin{aligned} a + n &= b \\ a - b &= n \\ a &\equiv b \pmod{n} \end{aligned}$$

Which is not the solution. Thus x and y must exist.

□

3.20 Theorem

Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$.

Proof. We'll need to prove 2 parts;

1. Let a, b, and n be integers with $n > 0$. Given $ax \equiv b \pmod{n}$, then by definition,

$$\begin{aligned} &\implies ax \equiv b \pmod{n} \\ &\implies n \mid ax - b \\ &\implies ny = ax - b && \text{by definition where y is some integer.} \\ &\implies b = ax - ny \end{aligned}$$

Now say p = (a,n), then by Theorem 1.40, $p = as + nt, \exists s, t \in \mathbf{Z}$. Thus p must divide a and n, where $p \mid a \implies a = pg$. Similarly $p \mid n \implies n = ph$ where g and h are some integers.
Substituting a and n in $b = ax - ny$ results to $b = pgx - phy = p(gx - hy)$. Since $(gx - hy)$ will result to some integer, let that integer be z, $z = (gx - hy)$. Therefore $b = p(z)$ which implies that $p \mid b$ or rather $(a, n) \mid b$.

2. Given integers p, a, b, n with $n > 0$. Let $p = (a, n)$. We know that $p \mid b$ where $b = pz = p(gx - hy)$ for some integer z that is equal to

$(gx - hy), \exists g, h, x, y \in \mathbf{Z}$. Then, by direct proof;

$$\begin{aligned} b &= p(gx - hy) \\ b &= pgx - phy \\ b &= ax - ny \qquad \text{Since (proven in 1.) } a = pg \text{ and } n = ph \\ ny &= ax - b \\ ax &\equiv b \pmod{n} \end{aligned}$$

Thus, $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$.

□

3.28 Theorem

Let a, b, m, and n be integers with $m > 0$, $n > 0$, and $(m, n) = 1$. Then the system

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

has a unique solution modulo mn.

Proof. Given the system above, we know from theorem 3.27 that the system has a solution if and only if $(n, m) \mid a - b$ and in this case $(n, m) \mid a - b \implies 1 \mid a - b$. However, to show that the solution x modulo mn unique, we need to satisfy that for the following given system, $x_0 = x_1$;

$$\begin{aligned} x_0 &\equiv a \pmod{n} \text{ and } x_0 \equiv b \pmod{m} \\ x_1 &\equiv a \pmod{n} \text{ and } x_1 \equiv b \pmod{m} \end{aligned}$$

By subtraction of each congruence $x_0 - x_1$, we get the following;

$$\begin{aligned} x_0 - x_1 \equiv a - a \equiv 0 \pmod{n} &\implies n \mid (x_0 - x_1) \\ x_0 - x_1 \equiv b - b \equiv 0 \pmod{m} &\implies m \mid (x_0 - x_1) \end{aligned}$$

Since $gcd(n, m) = 1$ and $x_0 - x_1$ is a multiple of both n and m, by theorem 1.42, we can express $mn \mid (x_0 - x_1)$. Thus, this implies that $x_0 - x_1 \equiv 0 \pmod{mn} \implies x_0 \equiv x_1 \pmod{mn}$ which satisfies the uniqueness if the solution x. □

Practice Theorems from A Modular World

3.1 Exercise

Show that 41 divides $2^{20} - 1$ by following these steps. Explain why each step is true.

1. $2^5 \equiv -9 \pmod{41}$. *This step is true because* $2^5 + 9 = 41$ *which if of course is divisible by 41.*

2. $(2^5)^4 \equiv (-9)^4 \pmod{41}$. *This is true because it follows the following theorem 1.18, let a, b, k and n be integers with* $n > 0$ *and* $k > 0$. *If* $a \equiv b \pmod{n}$

$$a^k \equiv b^k \pmod{n}$$

3. $2^{20} \equiv 81^2 \pmod{41} \equiv (-1)^2 \pmod{41}$. *This step is true because* $2^{20} = (2^5)^4$ *and* $(-9)^4 = 81^4$. *As well as, since* $81 - (2)41 = -1$ *and using theorem 1.18,* $81^2 \equiv (-1)^2 \pmod{41}$ *is also true.*

4. $2^{20} - 1 \equiv 0 \pmod{41}$. *True because* $2^{20} - 1 = (2^5)^4 - 1$ *which is divisble by 41.*

3.2 Question

In your head, can you find the natural number k, $0 \leq k \leq 11$, *such that* $k \equiv 37^{453} \pmod{12}$*?*

Proof. By Direct proof,

$\implies k \equiv 37^{453} \pmod{12}$

$\implies k \equiv 1^{453} \pmod{12}$

$\implies k \equiv 1 \pmod{12}$

Thus k = 1. □

3.3 Question

In your head or using paper and pencil, but no calculator, can you find the natural number k, $0 \leq k \leq 6$, *such that* $2^{50} \equiv k \pmod{12}$*?*

Proof. By Direct proof, we can disassemble 50 as a product of primes (Fundamental Theorem of Arithmetic);

$\implies 2^{50} \equiv k \pmod{7}$

$\implies 2^{48} \cdot 2^2 \equiv k \pmod{7}$

$\implies 2^{24 \cdot 2} \cdot 2^2 \equiv k \pmod{7}$

$\implies 2^{3 \cdot 2^4} \cdot 2^2 \equiv k \pmod{7}$①

Moreover, we know that $8 \equiv 1 \pmod 7$ and that $2^3 = 8$. This way we can reconstruct 2^{50} to find the value of k;

$\implies 8 \equiv 1 \pmod 7$

$\implies 2^3 \equiv 1 \pmod 7$

$\implies 2^{3 \cdot 2^4} \equiv 1^{2^4} \pmod 7$

$\implies 2^{3 \cdot 2^4} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod 7$

$\implies 2^{3 \cdot 2^4} \cdot 2^2 \equiv 4 \pmod 7$①

$\implies 2^{50} \equiv 4 \pmod 7$

Thus k = 4. □

3.4 Question

Using paper and pencil, but no calculator, can you find the natural number k, $0 \leq k \leq 11$, such that $39^{453} \equiv k \pmod{12}$?

Proof. By direct proof, since $39 \equiv 3 \pmod{12}$, we can also say that

$\implies 39^{453} \equiv k \pmod{12}$

$\implies (13 \cdot 3)^{453} \equiv k \pmod{12}$

$\implies 13^{453} \cdot 3^{453} \equiv k \pmod{12}$

$\implies 1^{453} \cdot 3^{453} \equiv k \pmod{12}$

$\implies 3^{453} \equiv k \pmod{12}$

□

3.5 Exercise

Show that 39 divides $17^{48} - 5^{24}$?

Proof. By direct proof, we need to prove that $17^{48} - 5^{24} \equiv 0 \pmod{39}$ by calculating the congruent of $17^{48} = 17^{2^4 * 3}$ and $5^{24} = 5^{2^3 * 3}$ modulo 39 separately as follows,

$$\begin{aligned}
17^2 &\equiv 16 \pmod{39} \\
17^{2^2} &\equiv 16^2 \pmod{39} \\
17^{2^2} &\equiv 196 \pmod{39} \\
17^{2^2} &\equiv 1 \pmod{39} \\
17^{2^2 * 12} &\equiv 1 \pmod{39} \\
17^{2^4 * 3} &\equiv 1 \pmod{39}
\end{aligned}$$

And similarly,

$$\begin{aligned}
5^3 &\equiv 8 \pmod{39} \\
5^4 &\equiv 8 * 5 \pmod{39} \\
5^{2^2} &\equiv 49 \pmod{39} \\
5^{2^2} &\equiv 1 \pmod{39} \\
5^{2^2 * 6} &\equiv 1 \pmod{39} \\
5^{2^3 * 3} &\equiv 1 \pmod{39}
\end{aligned}$$

Thus $17^{48} - 5^{24} \equiv 0 \pmod{39} \implies 1 - 1 \pmod{39} \equiv 0 \pmod{39}$. □

3.6 Question (Describe technique)

Let a, n, and r be natural numbers. Describe how to find the number k ($0 \leq k \leq n-1$) such that $k \equiv a^r \pmod{n}$ subject to the restraint that you never multiply numbers larger than n and that you only have to do about $\log_2 r$ such multiplications.

Solution. Let a, n, r and k be natural numbers where k is $0 \leq k \leq n-1$, then we can proceed with the following;

$$\begin{aligned}
k_1 &\equiv a^2 \pmod{n} && 0 \leq k_1 \leq n-1 \\
k_1 \cdot a &\equiv a^3 \pmod{n} && \\
k_2 &\equiv a^3 \pmod{n} && \text{Where } k_2 = k_1 * a \text{ and } 0 \leq k_2 \leq n-1 \\
k_3 &\equiv a^4 \pmod{n} && \text{Where } k_3 = k_2 * a \text{ and } 0 \leq k_3 \leq n-1 \\
&... && \\
k_r * a &\equiv a^{r+2} \pmod{n} && \text{Where } k_r = k_{r-1} * a \text{ and } 0 \leq k_r \leq n-1 \\
k_{r-1} &\equiv a^r \pmod{n} &&
\end{aligned}$$

Thus, you never multiply numbers larger than n.

3.7 Question

Let $f(x) = 13x^{49} - 27x^{27} + x^{14} - 6$. Is it true that

$$f(98) \equiv f(-100) \pmod{99}?$$

Proof. By direct proof, we need to evaluate the each function:

$$\begin{aligned}
&f(98) \equiv (13(98)^{49} - 27(98)^{27} + (98)^{14} - 6) \pmod{99} \\
&f(98) \equiv (13(-1)^{49} - 27(-1)^{27} + (-1)^{14} - 6) \pmod{99} \quad 98 \equiv -1 \pmod{99} \\
&f(98) \equiv (13(-1) - 27(-1) + 1 - 6) \pmod{99} \\
&f(98) \equiv (-13 + 27 + 1 - 6) \pmod{99}
\end{aligned}$$

And similarly,

$$f(-100) \equiv (13(-100)^{49} - 27(-100)^{27} + (-100)^{14} - 6) \pmod{99}$$
$$f(-100) \equiv (13(-1)^{49} - 27(-1)^{27} + (-1)^{14} - 6) \pmod{99} \qquad -100 \equiv -1 \pmod{99}$$
$$f(-100) \equiv (13(-1) - 27(-1) + 1 - 6) \pmod{99}$$
$$f(-100) \equiv (-13 + 27 + 1 - 6) \pmod{99}$$

Therefore, $f(98) \equiv f(-100) \pmod{99} \equiv (-13 + 27 + 1 - 6) \pmod{99}$ (mod 99), making it true. □

3.8 Theorem

Suppose $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Let a, b, and m be integers with $m > 0$. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof. We can prove the theorem by direct proof. Let a and b be integers, now using the same $f(x)$ from the theorem, we get $f(a)$ and $f(b)$ as following;

$$f(a) = a_n a^n + a_{n-1} a^{n-1} + ... + a_0$$
$$f(b) = a_n b^n + a_{n-1} b^{n-1} + ... + a_0$$

Then we can express $f(a) \equiv f(b) \pmod{m}$ from the theorem as $f(a) - f(b) \equiv 0 \pmod{m}$ where m divides $f(a) - f(b)$. Lets attempt at finding the difference between each equation;

$$\implies f(a) - f(b)$$
$$\implies (a_n a^n + a_{n-1} a^{n-1} + ... + a_0) - (a_n b^n + a_{n-1} b^{n-1} + ... + a_0)$$
$$\implies a_n(a^n - b^n) + a_{n-1}(a^{n-1} - b^{n-1}) + ... + a_1(a - b)$$

Given that $(a^n - b^n)$ is divisible by $(a - b)$, since $(a^n - b^n) = (a - b)(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1} + b)$. We can observe that $(a - b)$ divides each element in $a_n(a^n - b^n) + a_{n-1}(a^{n-1} - b^{n-1}) + ... + a_1(a - b)$, thus allowing us to express it as follows;

$$\implies a_n((a - b) \cdot k_1) + a_{n-1}((a - b) \cdot k_n) + ... + a_1(a - b)$$

Where all $k_1, ..., k_n$ are some integers

$$\implies (a - b)(a_n k_1 + a_{n-1} k_n + ... + a_1)$$
$$\implies (a - b)(a_n k_1 + a_{n-1} k_n + ... + a_1)$$
$$\implies (a - b)t$$

Since $(a_n k_1 + a_{n-1} k_n + ... + a_1)$ will result to some integer, we can then say that t is that integer.

$$\implies f(a) - f(b) = (a - b)t$$

Given that $a \equiv b \pmod{m}$, we then know that $a - b \equiv 0 \pmod{m}$. Hence, m must divide $a - b$ or it can be expressed $(a - b) = ms$ for some integer s.

Therefore, we can express $f(a) - f(b)$ as;

$$f(a) - f(b) = (a - b)t$$
$$f(a) - f(b) = mst \qquad \text{for some integers s and t}$$

Thus, since $f(a) - f(b) = mst$, we can then say that m does divide $f(a) - f(b)$. □

3.9 Corollary

Let the natural number n be expressed in base 10 as

$$n = a_k a_{k-1} ... a_1 a_0.$$

Let $m = a_k + a_{k-1} + ... + a_1 + a_0$. *Then* $9 \mid n$ *if and only if* $9 \mid m$.

Proof. By contradiction, assume that $9 \nmid n$, where n is a natural number, we know that $n \equiv d \pmod 9$ where d is a natural number and $d \neq 0$. By direct proof, we can express $n \equiv d \pmod 9$ as follows;

$\implies n \equiv d \pmod 9$

$\implies a_k a_{k-1} ... a_1 a_0 \equiv d \pmod 9$

$a_k a_{k-1} ... a_1 a_0$ can be expressed as multiple factors of 10

$\implies (a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0) \equiv d \pmod 9$

By Modular Distributive Property,

$\implies (a_k \cdot 10^k \pmod 9 + a_{k-1} \cdot 10^{k-1} \pmod 9 + ... + a_1 \cdot 10^1 \pmod 9 + a_0 \pmod 9) \equiv d \pmod 9$

Given that $10^k \pmod 9 \equiv 1^k \equiv 1$, by theorem 1.18

$\implies (a_k + a_{k-1} + ... + a_1 + a_0) \equiv d \pmod 9$

Since, $m = a_k + a_{k-1} + ... + a_1 + a_0$,

$\implies m \equiv d \pmod 9$

Given that $9 \mid m$, thus $m \pmod 9 \equiv 0$. Therefore, d has to be zero., thus 9 must divide m so then $9 \mid n$. □

3.9 - Exercise

(a) 36 distinct times.

(b) By using corollary 3.9, we know that for each 6 digit number is divisible by 37, then the total of adding each digit must also be divisible by 37.

3.10 Corollary

Let the natural number n be expressed in base 10 as

$$n = a_k a_{k-1} ... a_1 a_0.$$

Let $m = a_k + a_{k-1} + ... + a_1 + a_0$. *Then* $3 \mid n$ *if and only if* $3 \mid m$.

Proof. By contradiction, assume that $3 \nmid n$, where n is a natural number, we know that $n \equiv d \pmod 3$ where d is a natural number and $d \neq 0$. By direct proof, we can express $n \equiv d \pmod 3$ as follows;

$\implies n \equiv d \pmod 3$

$\implies a_k a_{k-1} ... a_1 a_0 \equiv d \pmod 3$

$a_k a_{k-1} ... a_1 a_0$ can be expressed as multiple factors of 10

$\implies (a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0) \equiv d \pmod 3$

By Modular Distributive Property,

$\implies (a_k \cdot 10^k \pmod 3 + a_{k-1} \cdot 10^{k-1} \pmod 3 + ... + a_1 \cdot 10^1 \pmod 3 + a_0 \pmod 3)) \equiv d \pmod 3$

Given that $10^k \pmod 3 \equiv 1^k \equiv 1$, by theorem 1.18

$\implies (a_k + a_{k-1} + ... + a_1 + a_0) \equiv d \pmod 3$

Since, $m = a_k + a_{k-1} + ... + a_1 + a_0$,

$\implies m \equiv d \pmod 3$

Given that $3 \mid m$, thus $m \pmod 3 \equiv 0$. Therefore, d has to be zero. Therefore, thus 3 must divide m so then $3 \mid n$. □

3.11 Theorem

Suppose $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ *is a polynomial of degree* $n > 0$ *and suppose* $a_n > 0$. *Then there is an integer k such that if* $x > k$, *then* $f(x) > 0$.

Proof. Given $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ is a polynomial of degree $n > 0$ and suppose $a_n > 0$. Let $f(x) > 0$, we'll need to prove that $m > 0$, $\exists k \in \mathbf{Z}$ such that $x > k \implies f(x) > m > 0$.
By induction, **Base case (n = 1):**

$\implies f(x) = a_1 x + a_0$

$\implies f(x) > m$ With $f(x) > m$, we can then say

$\implies a_1 x + a_0 > m$

$\implies x > \dfrac{m - a_0}{a_1}$

assume that $f(x) = m > 0$, then

$\implies a_1 x + a_0 > m - a_0 + a_0 > m = 0$

Pick $k = [\dfrac{m - a_0}{a_1}$then, $x > k$ (Ceiling Function)]

$\implies f(x) > m > 0$

Theorem holds for n = 1.
Inductive Hypothesis: Assume n = n + 1, then Theorem still holds.

Inductive Step:

$\implies f(x) = a_{n+1}x^{n+1} + a_n x^n + ... + a1x + a_0$

$\implies f(x) = x(a_n x^n + a_n x^{n-1} + ... + a1) + a_0$

$\implies f(x) = x(g(n)) + a_0$

Where $g(n) = a_n x^n + a_n x^{n-1} + ... + a1$.

$g(n)$ degree is 1 and leading coefficient of g(n) is greater than 0.

Now there must be a k such that $g(n) > m - a_0, \forall x > k > 1$. $a_0 + xg(n) > a_0 + m - a_0 > m > 0, \forall x > k$. Therefore, the theorem still holds. □

3.12 Theorem

Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ is a polynomial of degree $n > 0$ and suppose $a_n > 0$. Then for any number M there is an integer k (which depends on M) such that if $x > k$, then $f(x) > M$.

Proof. Given $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ is a polynomial of degree $n > 0$ and suppose $a_n > 0$. Let $x = k + h$ where k is an integer such that if $x > k$ and h is positive.
$f(k+h) = a_n(k+h)^n + a_{n-1}(k+h)^{n-1} + ... + a_1(k+h) + a_0$ $f(k+h) = a_n k^n + a_{n-1}k^{n-1} + ... + a_1 k + a_0 +$ Some positive values with h. Let them be H. $f(k+h) = f(k) + H$. Thus, $f(k+h) = f(x) > f(k), \forall k$. □

3.13 Theorem

Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ is a polynomial of degree $n > 0$ with integer coefficients. Then $f(x)$ is a composite number for infinitely many integers x.

Proof. By fundamental theorem of arithmetic, f(x) can be expressed in the form of product of primes and depending on n, there can be an infinitely number of x integers. □

3.14 Theorem

Given any integer a and any natural number n, there exists a unique integer t in the set $0, 1, 2, ..., n-1$ such that $a \equiv t \pmod{n}$.

Proof. Given an integer a and a natural number n. There exist integers t and q such that, by division algorithm, $a = nq + t$ where t is in the set $0, 1, 2, ..., n-1$. We can express $a = nq + t$ as follows;

$\implies a = nq + t$

$\implies a - t = nq$

$\implies n \mid a - t$

$\implies a \equiv t \pmod{n}$ By Definition of Congruence

By $a \equiv t \pmod{n}$, this implies that a is congruent 1 or more elements from the set $0, 1, 2, ..., n-1$, since t is apart of that set. Thus a must be congruent to t modulo n. □

3.15 Exercise

Find three complete residue systems modulo 4: the canonical complete residue system, one containing negative numbers, and one containing no two consecutive numbers.

- $\{5, 6, 7, 8\} \Longrightarrow \{1, 2, 3, 0\}$
- $\{13, 14, 15, 16\} \Longrightarrow \{-1, 2, 3, 0\}$
- $\{23, 24, 25, 26\} \Longrightarrow \{3, 0, 1, 2\}$

3.16 Theorem

Let n be a natural. Every complete residue system modulo n contains n elements.

Proof. Suppose there exist this set m where $m = \{0, 1, 2, 3, 4, ..., n-1\}$ where n is some natural number. Also let me be a complete residue system mod$n$ and suppose that the size of m is greater than n.
Now at least two elements from m must have the same remainder when divided by n, by Pigeonhole Principle. This contradicts he aforementioned statement that m is a complete residue system mod$n$. Therefore complete residue system modulo n must contains equal or less than the size of m. □

3.17 Theorem

Let n be a natural number: Any set, $\{a_1, a_2, ..., a_n\}$, of n integers for which no two are congruent modulo n is a complete residue system modulo n.

Proof. Suppose that for set $A = \{a_1, a_2, ..., a_n\}$ where n is natural number and there are **no** two congruent modulo n in this set. Now, let B be another residue set with $n-1$ residues, $B = \{b_1, b_2, ..., b_{n-1}\}$.
We can conclude that a_1 is not congruent modulo n for any a_i, where i is $1 \leq i \leq n-1$. Similarity for $a_2, ..a_n$.
Thus, a_n is also not congruent to any a_i modulo n. By division algorithm, a_n can be expressed as $a_n = n(q) + b_n$, for some integer q and r. However, $a_n = n(q) + r$ implies that $a_n \equiv r \pmod{n}$. This is impossible since B has less elements than A therefore $a_n \equiv a_i \pmod{n}$ which contradicts our conclusions above. Therefore, the set a has to have no two elements that are congruent modulo n is a complete residue system modulo n. □

3.18 Exercise

Find all solutions in the appropriate canonical complete residue system modulo n that satisfy the following linear congruence:

1. $26x \equiv 14 \pmod 3$

   $\implies 2(13)x \equiv 2(7) \pmod 3$
   $\implies 13x \equiv 7 \pmod 3$
   $\implies 13(4) \equiv 7 \pmod 3$
   $\implies x = 4 + 3, 4 + 2(3)...$

2. $2x \equiv 3 \pmod 5$

   $\implies 2x \equiv 3 \pmod 5$
   $\implies 2(4) \equiv 3 \pmod 5$ $\implies x = 4 + 5, 4 + 2(5)...$

3. $4x \equiv 7 \pmod 8$

   $\implies 4x \equiv 7 \pmod 8$
   $\implies$ No possible solutions.

4. $24x \equiv 123 \pmod{213}$

   $\implies 24x \equiv 123 \pmod{213}$
   $\implies 8(3)x \equiv 41(3) \pmod{\dfrac{213}{(3, 213)} = 71}$
   $\implies 8x \equiv 41 \pmod{71}$
   $\implies 8x \cdot 9 \equiv 41 \cdot 9 \pmod{71}$ Since $8 * 9 \equiv \pmod{71}$
   $\implies x \equiv 396 \equiv 14 \pmod{71}$
   $\implies x = 14, 14 + 71, 14 + 2(71)...$

3.19 Theorem

Let a, b, and n be integers with $n > 0$. Show that $ax \equiv b \pmod n$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.

Proof. We'll need to prove 2 parts;

1. Let $a, b, n \in \mathbf{Z}$ with $n > 0$. By definition, $ax \equiv b \pmod n \implies n \mid ax - b$ and thus also $ax - b = np$ for some integer p. Moreover, by direct proof,

$$\begin{aligned} ax - b &= np \\ ax - np &= b \\ ax + n(-p) &= b \\ ax + ny &= b \end{aligned}$$

   Since $p \in \mathbf{Z}$, let $y \in \mathbf{Z}$ such that $p = -y$

Thus $ax \equiv b \pmod{n}$ has a solution such that $ax + ny = b$ for some integer x and y.

2. Given that $ax + ny = b$ where $a, b, n, x, y \in \mathbf{Z}$ and $n > 0$. By direct proof, assume that x and y exist we can assimilate the following

$$\begin{aligned} ax + ny &= b \\ ax - b &= -ny \\ ax - b &= n(-y) \\ ax - b &= n(-y) \\ ax &\equiv b \pmod{n} \end{aligned}$$

Now by contradiction let's assume that x and y did not exist;

$$\begin{aligned} a + n &= b \\ a - b &= n \\ a &\equiv b \pmod{n} \end{aligned}$$

Which is not the solution. Thus x and y must exist.

□

3.20 Theorem

Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$.

Proof. We'll need to prove 2 parts;

1. Let a, b, and n be integers with $n > 0$. Given $ax \equiv b \pmod{n}$, then by definition,

$$\begin{aligned} &\implies ax \equiv b \pmod{n} \\ &\implies n \mid ax - b \\ &\implies ny = ax - b && \text{by definition where y is some integer.} \\ &\implies b = ax - ny \end{aligned}$$

Now say p = (a,n), then by Theorem 1.40, $p = as + nt, \exists s, t \in \mathbf{Z}$. Thus p must divide a and n, where $p \mid a \implies a = pg$ and similarly $p \mid n \implies n = ph$ where g and h are some integers. Substituting a and n in $b = ax - ny$ results to $b = pgx - phy = p(gx - hy)$. Since $(gx - hy)$ will result to some integer, let that integer be z, $z = (gx - hy)$. Therefore $b = p(z)$ which implies that $p \mid b$ or rather $(a, n) \mid b$.

2. Given integers p, a, b, n with $n > 0$. Let $p = (a, n)$. We know that $p \mid b$ where $b = pz = p(gx - hy)$ for some integer z that is equal to $(gx - hy), \exists g, h, x, y \in \mathbf{Z}$. Then, by direct proof;

$$\begin{aligned} b &= p(gx - hy) \\ b &= pgx - phy \\ b &= ax - ny \qquad \text{Since (proven in 1.) } a = pg \text{ and } n = ph \\ ny &= ax - b \\ ax &\equiv b \pmod{n} \end{aligned}$$

Thus, $ax \equiv b \pmod{n}$ has a solution if and only if $(a, n) \mid b$.

□

3.21 Question

What does the proceeding theorem tell us about the congruence (4) in Exercise 3.18 above?

That $24x \equiv 123 \pmod{213}$ has a solution if and only if $(24, 213) \mid 123$.

3.22 Exercise

Use the Euclidean Algorithm to find a member x of the canonical complete residue system modulo 213 that satisfies $24x \equiv 123 \pmod{213}$. *Find all members x of the canonical complete residue system modulo 213 that satisfy* $24x \equiv 123 \pmod{213}$.

Done in question 3.18.

3.23 Question

Let a, b, and n be integers with $n > 0$. How many solutions are there to the linear congruence $ax \equiv b \pmod{n}$ in the canonical complete residue system modulo n? Can you describe a technique to find them?

There are infinite number. We can find them by simplifying the modulo with the fundamental rule of arithmetic as well as finding the new modulo $\frac{n}{((gcd(a,b)),n)}$. This way we are able to find the smallest possible x. Then any other x would be $x_0 + \frac{n}{((gcd(a,b)),n)} \times [1, ...]$.

3.24 Theorem

Let a, b, and n be integers with $n > 0$. Then

1. *The congruence $ax \equiv b \pmod{n}$ is solvable in integers if and only if $(a, n) \mid b$;*

2. *If x_0 is solution to the congruence $ax \equiv b \pmod{n}$, then all solutions are given by*

$$x_0 + (\tfrac{n}{(a,n)} \cdot m) \pmod{n}$$

for $m = 0, 1, 2, ..., (a, n) - 1$; *and*

3. *If* $ax \equiv b \pmod{n}$ *has a solution, then there are exactly (a,n) solution in the canonical complete residue modulo n.*

Proof. By theorem, 2.20 and 1.53. □

3.25 Exercise

A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained, In the ensuing brawl over who should get the extra coins, on pirates was killed. The coins were redistributed, but this time an equal division left 10 coins. Again they fought about who should get the remaining coins and another pirates was killed. Now fortunately, the coins could be divided evenly among the surviving 15 pirates. What was the fewest number of coins that could have been in the sack?

- $x \equiv 3 \pmod{17}$, let $r_1 = 3$.
- $x \equiv 10 \pmod{16}$, let $r_2 = 10$.
- $x \equiv 0 \pmod{15}$, let $r_3 = 0$.

Let k be the product of each total number of pirates

$p = 15 \cdot 16 \cdot 17 = 4080$

let $p_1, p_2 and p_3$ be the quotient of p by each instance number of pirates.

Then we express each congruence from above using each quotient for some integer x_1, x_2 and x_3.

$p_1 = 4080 \div 17 = 240$

$\implies 240x \equiv 1 \pmod{17} \implies 240x_1 - 1 \equiv 0 \pmod{17}$

$p_2 = 4080 \div 16 = 255$

$\implies 255x \equiv 1 \pmod{16} \implies 255x_2 - 1 \equiv 0 \pmod{16}$

$p_3 = 4080 \div 15 = 272$

$\implies 272x \equiv 1 \pmod{15} \implies 272x_3 - 1 \equiv 0 \pmod{15}$

For each congruence, we can attempt to find x_1, x_2 and x_3 using the definition $a \mid b \implies a \cdot bc, \exists a, b, c \in \mathbf{Z}$.

For p_1:

$17 \mid 240x_1 - 1$
$\implies 17y_1 = 240x_1 - 1$, for some integer y_1
$\implies 240x_1 - 17y_1 = 1$
Note that gcd(240, 17) is 1. Thus by Theorem 1.39, $240a + 17b = 1$ for some integer a and b.
$\implies 240a + 17b = 1$
$\implies 240(-8) + 17(113) = 1$
$\implies a = -8$
$\implies x_1 \equiv -8 \equiv 9 \pmod{17}$

For p_2:

$16 \mid 255x_2 - 1$
$\implies 16y_2 = 255x_2 - 1$, for some integer y_2
$\implies 255x_2 - 16y_2 = 1$
Note that gcd(255, 16) is 1. Thus by Theorem 1.39, $255a + 16b = 1$ for some integer a and b.
$\implies 255a + 16b = 1$
$\implies 255(-1) + 16(16) = 1$
$\implies a = -1$
$\implies x_2 \equiv -1 \equiv 15 \pmod{16}$

For p_2:

$15 \mid 272x_3 - 1$
$\implies 15y_3 = 272x_3 - 1$, for some integer y_3
$\implies 272x_3 - 15y_3 = 1$
Note that gcd(272, 15) is 1. Thus by Theorem 1.39, $272a + 15b = 1$ for some integer a and b.
$\implies 272a + 15b = 1$
$\implies 272(-7) + 15(127) = 1$
$\implies a = -7$
$\implies x_3 \equiv -7 \equiv 8 \pmod{15}$

$n = (x_1 \times r_1 \times p_1) + (x_2 \times r_2 \times p_2) + (x_3 \times r_3 \times p_3)$
$n = (9 \times 3 \times 240) + (15 \times 10 \times 255) + (8 \times 0 \times 272) = 44730$
$n \pmod{p} \equiv 44730 \pmod{4080} \equiv 3930.$

Thus, $x = 3930$.

3.26 Exercise (Brathmagupta, 7th century A.D.)

When eggs in a basket are removed two, three, four, five, or six at a time, there remain, respectively, one, two, three, four, or five eggs. When they are taken out seven a a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

Let the smallest number of eggs be x. Based off the context, we can make a few assumptions about x;

- $7 \mid x$
- $x \pmod 2 \equiv 1$, thus an odd number.
- $x \pmod 3 \equiv 2$.
- $x \pmod 4 \equiv 3$.
- $x \pmod 5 \equiv 4$, thus the last digit of x must be 9 since 9 is odd.
- $x \pmod 6 \equiv 5$.

We can try to list all multiples of 7 that are odd and end with a 9. And then see if all assumptions apply;

- ~~49~~ since $49 \pmod 3 \equiv 1$
- 119 is the correct least number of eggs.
- ~~189~~ since $189 \pmod 3 \equiv 0$
- ~~259~~ since $259 \pmod 3 \equiv 1$
- ~~329~~ since $329 \pmod 4 \equiv 1$

Thus $x = 119$.

3.27 Theorem

Let a, b, m, and n be integers with $m > 0$ and $n > 0$. Then the system

$$x \equiv a \pmod n$$
$$x \equiv b \pmod m$$

has a solution if and only if $(n, m) \mid a - b$.

Proof. We can prove this theorem from 2 side Given the system above with x as it's solution. We can also identify that $x \equiv a \pmod n \implies x - a \equiv 0 \pmod n$ implies that $n \mid x - a$. Similarly for $x \equiv b \pmod m$ where $x - b$ is a multiple of m.

Moreover, by definition, $x - a$ and $x - b$ must also both multiples of gcd(n, m) where $gcd(n, m) \mid x - a$ and $gcd(n, m) \mid x - b$. That also implies also that

$(x-b)-(x-a)$ is also a multiple of gcd(n, m), by Theorem 1.2. By subtraction, we can get $a-b$ from $(x-b)-(x-a) = x-b-x+a = a-b$. Thus, $gcd(n,m) \mid a-b$.

Furthermore, assuming the same system above, we can also prove this moving backwards and constructing the system's congruence given that $gcd(n,m) \mid a-b$. Firstly, we want to construct the solution $x \equiv a \pmod{n}$. By definition, $x = a + hn, \exists h \in \mathbf{Z}$. Hence, based off the second congruence, we need to find the integer h such that $a + hn \equiv b \pmod{m}$ which can also be expressed as $hn \equiv b - a \pmod{m}$.

Now, suppose that $t = gcd(n,m)$ thus $t \mid a-b$. Then by definition, $t \times s = a - b, \exists s \in \mathbf{Z}$ and $-s = \frac{b-a}{t}$. By theorem 1.40, we know that there exists the solution to $nx + my = t, \exists x, y \in \mathbf{Z}$. By definition of congruences, this can also be expressed as $nx \equiv t \pmod{m}$. By direct proof;

$$
\begin{aligned}
& nx \equiv t \pmod{m} && \\
& nx(-s) \equiv t(-s) \pmod{m} && \text{Multiplying } -s \text{ in both sides} \\
& n(-xs) \equiv b - a \pmod{m} && -s = \frac{b-a}{t} \\
& nh \equiv b - a \pmod{m} && \text{Since x, s and h} \in \mathbf{Z}\text{, we can say that } h = -xs
\end{aligned}
$$

Thus, $x = a + hn = a + n(-xs)$ which satisfies the system. □

3.28 Theorem

Let a, b, m, and n be integers with $m > 0$, $n > 0$, and $(m,n) = 1$. Then the system

$$
\begin{aligned}
x &\equiv a \pmod{n} \\
x &\equiv b \pmod{m}
\end{aligned}
$$

has a unique solution modulo mn.

Proof. Given the system above, we know from theorem 3.27 that the system has a solution if and only if $(n,m) \mid a-b$ and in this case $(n,m) \mid a-b \implies 1 \mid a-b$. However, to show that the solution x modulo mn unique, we need to satisfy that for the following given system, $x_0 = x_1$;

$$
\begin{aligned}
x_0 &\equiv a \pmod{n} \text{ and } x_0 \equiv b \pmod{m} \\
x_1 &\equiv a \pmod{n} \text{ and } x_1 \equiv b \pmod{m}
\end{aligned}
$$

By subtraction of each congruence $x_0 - x_1$, we get the following;

$$
\begin{aligned}
x_0 - x_1 \equiv a - a \equiv 0 \pmod{n} &\implies n \mid (x_0 - x_1) \\
x_0 - x_1 \equiv b - b \equiv 0 \pmod{m} &\implies m \mid (x_0 - x_1)
\end{aligned}
$$

Since $gcd(n,m) = 1$ and $x_0 - x_1$ is a multiple of both n and m, by theorem 1.42, we can express $mn \mid (x_0 - x_1)$. Thus, this implies that $x_0 - x_1 \equiv 0 \pmod{mn} \implies x_0 \equiv x_1 \pmod{mn}$ which satisfies the uniqueness if the solution x. □

3.29 Theorem (Chinese Remainder Theorem)

Suppose $n_1, n_2, ..., n_L$ are positive integers that are pairwise relatively prime, that is, $(n_i, n_j) = 1$ for $i \neq j, 1 \leq i, \jmath \leq L$. Then the system of L congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

has a unique solution modulo the product $n_1 n_2 n_3 ... n_L$.

Proof. Given the system above. Suppose that the solution x can be deconstructed as:

$$x = A_1 x_1 + A_2 x_2 + ... + A_L x_L$$

Since $n_1, n_2, ..., n_L$ are pairwise relatively prime. We know that no integers in $\{n_1, n_2, ..., n_L\}$ have any primes in the same set. Therefore, for example $\frac{n_1 n_2 ... n_L}{n_1} = n_2 ... n_L$. And the same goes for all integers. We can now replace all $A_1, A_2, .., A_L$ with the product of the corresponding $n_1, n_2, ..., n_L$;

$$\begin{aligned} \frac{n_1 n_2 ... n_L}{n_1} x_1 &\equiv a_1 \pmod{n_1} \\ \frac{n_1 n_2 ... n_L}{n_2} x_2 &\equiv a_2 \pmod{n_2} \\ &\cdots \\ \frac{n_1 n_2 ... n_L}{n_L} x_L &\equiv a_L \pmod{n_L} \end{aligned}$$

By Theorem 3.20, the solution for all x_L exists if and only if $(A_L, n_L) \mid a_L$. Thus we are able to find all possible solutions for $x_1, x_2, ..., x_L$ and also by replacing it back into the system we can then find the unique solution x.

Moreover, by contradiction, lets now assume that x' is found as a solution with x. Using the same proof as in theorem 3.28, we'll need to prove that $n_1 n_2 ... n_L \mid x - x'$. Since we know that $n_1, n_2, ..., n_L$ are pairwise relatively prime. We can conclude that $n_1 n_2 ... n_L \mid x - x'$ is valid. Thus, by definition, making $x \equiv x' \pmod{n_1 n_2 ... n_L}$ which satisfies the uniqueness if the solution. □

3.30 Blank Paper Exercise

- Modulo to the power
- Polynominal Modulo
- Canoical complete residue systems

- Linear Congrueneces
- Chinese Remainder Theorem
- Proof 3.24 and 3.29 were extremely difficult. Required a lot of research and readings.