

Notebook Swag

Sam Grayson

April 19, 2015

3.11 **Theorem:** Let f be an n -degree polynomial such that $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ and $a_n > 0$. $\exists k \in \mathbb{N} (\forall x > k (f(x) > 0))$.

Proof: $x > |a_{n-1}|$ is sufficient for $x^n > a_{n-1} x^{n-1}$. That is because multiplying both sides of the condition by x^{n-1} (valid operation since $x^{n-1} > 0$, since $x > 0$) gives $x x^{n-1} > a_{n-1} x^{n-1}$, equivalently $x^n > a_{n-1} x^{n-1}$. That simply arises from the initial condition. After this point, the n th term dominates the $(n-1)$ th term.

If the first term dominates the zeroth term at some point k_1 , and the second term dominates the first term at some point k_2 , then at some point greater than k_1 and greater than k_2 , the third term dominates the second term and the second term dominates the first term ($|a_2 x^2| > |a_1 x| > |a_0|$). Therefore the third term dominates the first term ($|a_2 x^2| > |a_0|$).

Continuing in this way, there is some point k_n the n th term dominates the $(n-1)$ th term. The $(n-1)$ th term dominates the $(n-2)$ th term after k_{n-1} . Therefore for $x > k$ where $k = \max(k_n, k_{n-1}, \dots, k_1)$, the n th term dominates. $a_n > 0$ by the premise. Therefore $|a_n x^n| > |a_{n-1} x^{n-1}| > \cdots > |a_0|$. Therefore $n|a_n x^n| > |a_{n-1} x^{n-1}| + \cdots + |a_0|$. Since n is a positive constant multiplier, we can absorb it into a_n . If it dominates the first term, and the first term is positive, then whether or not the later terms are positive or negative the polynomial will be positive. Therefore, after the point k_n the first term dominates every other term by more than a factor of n . $\exists k \in \mathbb{N} (\forall x > k (f(x) > 0))$ ■

3.12 **Theorem:** Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. $\forall y \in \mathbb{N} (\exists k \in \mathbb{N} (x > k \rightarrow f(x) > y))$

Proof: S

3.14 **Theorem:** $\forall i \in \mathbb{Z} (\forall j \in \mathbb{N} (\exists! r \in \mathbb{N} (i \equiv r \pmod{j} \wedge 0 \leq r < j)))$

Proof:

Let $i \in \mathbb{N}$	(for universal generalization)
Let $j \in \mathbb{N}$	(for universal generalization)
If $i > 0$	
Conclude: $\exists! q, r \in \mathbb{N} (i = qj + r \wedge 0 \leq r < j)$	Division algorithm
Otherwise $i < 0$	
$\exists! p, r \in \mathbb{N} (-i = pj + t \wedge 0 \leq t < j)$	Division algorithm
$-i = pj + t \wedge 0 \leq t < j$	Existential generalization
$i = -pj - t$	Existential generalization
$i = -pj - j + j - t$	Algebra
$i = -(p+1)j + j - t$	Algebra
$0 \leq t < j$	Simplification

$-j < -t \leq 0$	Property of inequalities
$0 < j - t \leq j$	Property of inequalities
If $j - t < j$	
Let $q = -(p + 1)$ Let $r = j - t$	
$0 < r < j$	Property of inequalities
$0 \leq r < j$	Property of inequalities
Conclude: $\exists!q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	Existential generalization
Otherwise $j - t \geq j$	
$j - t \leq j \wedge j - t \geq j$	Conjunction
$j - t = j$	Property of inequalities
$t = 0$	Identity property
$i = pj$ Let $r = 0$	
Conclude: $\exists!q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	Existential generalization
$\exists!q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	Constructive dilemma
Conclude: $\exists!q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	Constructive dilemma
$\forall i \in \mathbb{N}(\forall j \in \mathbb{N}(\exists!r \in \mathbb{N}(i \equiv r \pmod{j} \wedge 0 \leq r < j)))$	Universal generalization (used twice) ■

- 3.15
1. $\{0, 1, 2, 3\}$
 2. $\{-4, -3, -2, -1\}$
 3. $\{0, 5, 10, 15\}$

Let $A \in \text{CRS}(n)$ stand for A is a possible Complete Residue System (CRS) for mod n .

Let $A \in \text{CCRS}(n)$ stand for A is the Canonical Complete Residue System (CCRS) for mod n .

3.16 **Theorem:** $B \in \text{CRS}(n) \rightarrow |B| = n$

Proof:

Let $A \in \text{CCRS}(n)$	
Let $B \in \text{CRS}(n)$	For conditional
Let $f : A \rightarrow B$ where $a \mapsto b$ if $a \equiv b \pmod{n}$	
$\forall a \in A(\exists!b \in B(x \equiv b \pmod{n}))$	Definition of CRS
$\forall a \in \text{cod}(f)(\exists!b \in \text{dom}(f)(f(a) = b))$	Substitution
Thus f is a bijective map	
$ A = n$	By inspection
Thus $ A = B = n$	Bijection
$B \in \text{CRS}(n) \rightarrow B = n$	Conditional proof ■

3.17 **Theorem:** $\neg \exists a \in S(\exists b \in S(a \equiv b \pmod{n} \wedge a \neq b)) \rightarrow S \in \text{CRS}(n)$

Let $\text{rem}(x \pmod{n})$ (read “remainder of x modulo n”) denote the number in the Complete Canonical Residue System congruent to $x \pmod{n}$.

Lemma: $a = b \rightarrow a \equiv b \pmod{n}$ **Proof:**

$a - b = 0$ Algebra
 $0n = 0$ Zero-property of multiplication
 $n \mid (a - b)$ Definition of divides
 $a \equiv b \pmod{n}$ Definition of modulo ■

Proof:

Assume $\neg \exists a \in S(\exists b \in S(a \equiv b \pmod{n} \wedge a \neq b))$ (for conditional)
 Assume $\exists a \in S(\exists b \in S(\text{rem}(a \pmod{n}) = \text{rem}(b \pmod{n})))$ (for contradiction)
 $a \equiv \text{rem}(a \pmod{n})$ Definition of remainder
 $b \equiv \text{rem}(b \pmod{n})$ Definition of remainder
 $a \equiv \text{rem}(a \pmod{n}) \equiv b$ Lemma and transitivity
 $\exists a \in S(\exists b \in S(a \equiv b \pmod{n} \wedge a \neq b))$ Existential generalization
 $\neg \exists a \in S(\exists b \in S(\text{rem}(a \pmod{n}) = \text{rem}(b \pmod{n})))$ Contradiction
 ■

- 3.18 1. $x \equiv 1 \pmod{3}$
 2. $x \equiv 4 \pmod{5}$
 3. No solution.
 4. $x \equiv 14 + 71n \pmod{213}$ for $n \in \{0, 1, 2\}$

3.19 **Theorem:** $\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x, y \in \mathbb{Z}(ax - ny = b)$

Proof:

$\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x \in \mathbb{Z}(b \equiv ax \pmod{n})$ Theorem 1.10
 $\exists x \in \mathbb{Z}(b \equiv ax \pmod{n}) \leftrightarrow \exists x \in \mathbb{Z}(n \mid (b - ax))$ Definition of modulo
 $\exists x \in \mathbb{Z}(n \mid (b - ax)) \leftrightarrow \exists x, y \in \mathbb{Z}(ny = b - ax)$ Definition of divides
 $\exists x, y \in \mathbb{Z}(ny = b - ax) \leftrightarrow \exists x, y \in \mathbb{Z}(ax + ny = b)$ Algebra
 $\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x, y \in \mathbb{Z}(ax - ny = b)$ Transitivity ■

3.20 **Theorem:** $\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \gcd(a, n) \mid b$

Proof:

$\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x, y \in \mathbb{Z}(ax - ny = b)$ Theorem 3.19
 $\exists x, y \in \mathbb{Z}(ax - ny = b) \leftrightarrow \gcd(a, n) \mid b$ 1.48
 $\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \gcd(a, n) \mid b$ Transitivity ■

3.21 It has a solution.

$$\begin{aligned}
3.22 \quad & 213 - 8 \cdot 24 = 21 \\
& 24 - 1 \cdot 21 = 3 \\
& 24 - 1 \cdot (213 - 8 \cdot 24) = 3 \\
& 9 \cdot 24 - 213 = 3 \\
& 41 \cdot (9 \cdot 24 - 213) = 41 \cdot 3 = 123 \\
& 369 \cdot 24 - 41 \cdot 213 = 123 \\
& (369 + n \cdot 71) \cdot 24 - (41 + n \cdot 8) \cdot 213 = 123 \\
& 213 \mid ((369 + n \cdot 71) \cdot 24 - 213) \\
& x = 369 + n \cdot 71
\end{aligned}$$

3.23 **Algorithm:** Find all solutions of $ax = b \pmod{n}$ for $0 \leq x < n$

I wrote this algorithm in Python so that it would be more precise. I spent a lot of time making it accessible to non-programmers. Please spend as much time trying to understand it as I spent trying to make it understandable

First, there are four things you must understand about Python code:

- Lines that begin with a `#` are comments for the reader. They are ignored by the computer. They show up in gray.
- Single equals-sign means assignment of the right-hand value to the left-hand variable. `x = 2` says “Make x equal to 2.” Double equals-sign tests for equivalence. `x == 2` asks the question “Is x equal to 2?”. Ordered-pairs (called n-tuples) are allowed in any assignment or equality tests.
- Any statement that ends in a colon is a control-flow statement. It controls when the statements immediately following it are executed. Those statements are indented to show that they are dependent on the control-flow statement. For example, in the following code, lines 2 and 3 run only if x is 2 (from line 1) otherwise lines 5 and 6 run. Line 7 is not indented, so it is not controlled by the if-else from line 1. Line 9 runs once for every element in the set `[1, 2, 3, 4, 5]`, where each iteration a takes on one value from that list.

```

1  if x == 2:
2      a = 3
3      b = 5
4  else:
5      a = 6
6      b = 10
7  c = 4
8  for a in [1, 2, 3, 4, 5]:
9      n = n + a

```

- A function is defined by a line beginning with “def”, the name of the function, a temporary name given to the function parameters, and then a colon (this is a kind of control-flow statement). The function ends with a line that says ‘return’ and then a value. `def f(x):` and then a line that says `return 2 * x`. If later you see `f(10)`, it evaluates to 20.

```

1 def linear_diophantine(a, b, c):
2     # Returns (x_0, y_0), (r_x, r_y) where  $ax + by = c$ 
3     # when  $x = x_0 + nr_x$  and  $y = y_0 + nr_y$ 
4     g = gcd(a, b)
5     if c == g:
6         for x in count():
7             # Loop over this with  $x = \{0, 1, 2, 3 \dots\}$ 
8             if mod(a * x, g, b):
9                 # execute this block iff  $a \cdot x \equiv g \pmod{b}$ 
10                y = (g - a*x) / b
11                # at this point  $ax + by = g$ 
12                # therefore x and y are solutions
13                # theorem 1.53 states solutions for x are spaced  $b / g$  apart
14                # and solutions for y are spaced  $-a / g$  apart
15                return (x, y), (b / g, -a / g)
16    else:
17        # solve a simpler diophantine equation first
18        (u_0, v_0), (r_u, r_v) = linear_diophantine(a, b, g)
19        # at this point  $ua + vb = g$ 
20        # multiplying both sides by  $\frac{c}{g}$  gives
21        #  $u_0 \frac{c}{g} a + v_0 \frac{c}{g} b = g \frac{c}{g} = c$ 
22        (x_0, y_0) = (u_0 * c / g, v_0 * c / g)
23        # the spacing between solutions doesn't change
24        (r_x, r_y) = (r_u, r_v)
25        return (x_0, y_0), (r_x, r_y)
26
27 def linear_congruence(a, b, n):
28     # Returns  $x_0, n$  where  $ax \equiv b \pmod{n}$  when  $x \equiv x_0 \pmod{n}$ 
29     # this function relies on the linear_diophantine function,
30     # because why reinvent the wheel?
31     (x_0, y_0), (x_i, y_i) = linear_diophantine(a, -n, b)
32     return x_0, x_i

```

This code relies on auxiliary functions. They are listed below.

```

1 # this is a function from the standard library
2 # count() -> {0, 1, 2, 3, ...}
3 from itertools import count
4
5 def cmod(a, n):
6     # Returns c such that  $a \equiv c \pmod{n}$  and  $0 \leq c < n$  WLOG  $n > 0$ 
7     # this c is the remainder in the division algorithm
8     # and c is in the canonical complete residue system
9     n = abs(n)
10    if a > 0:

```

```

11     while a >= n:
12         a = a - n
13     return a
14 else:
15     while a < 0:
16         a = a + n
17     return a
18
19 def divides(d, a):
20     # Returns true if  $d|a$ 
21     # (equivalent to if the remainder upon division is zero, return true)
22     return cmod(a, d) == 0
23
24 def mod(a, b, n):
25     # Returns true if  $a \equiv b \pmod{n}$ 
26     # (equivalent to  $n|(b-a)$ )
27     return divides(n, b - a)
28
29 def gcd(a1, b1):
30     # Returns the greatest common multiple
31     # WLOG  $a > b > 0$ 
32     a = max(abs(a1), abs(b1))
33     b = min(abs(a1), abs(b1))
34     r = cmod(a, b)
35     if r == 0:
36         return b
37     else:
38         return gcd(b, r)

```

Theorem: There are $\frac{n}{\gcd(a,n)}$ solutions to the linear congruence.

Proof:

$$0 \leq x_0 < \frac{n}{\gcd(a,n)}$$

$$0 + (\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} \leq x_0 + (\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} < \frac{n}{\gcd(a,n)} + (\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} \quad \text{Addition}$$

$$0 + (\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} \leq x_0 + (\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} < \frac{n}{\gcd(a,n)} + \gcd(a, n) \frac{n}{\gcd(a,n)} - \frac{n}{\gcd(a,n)} \quad \text{Distribution}$$

$$(\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} \leq x_0 + (\gcd(a, n) - 1) \frac{n}{\gcd(a,n)} < \gcd(a, n) \frac{n}{\gcd(a,n)} \quad \text{Identity}$$

For all $0 \leq m \leq \gcd(a, n) - 1$, there are solutions at $x_0 + m \frac{n}{\gcd(a,n)}$ in the CCRS

There are $\gcd(a, n)$ solutions ■

3.24 3.20, 3.23a, and 3.23b taken together prove this theorem. The big idea is that a linear congruence is a special kind of linear diophantine equation.

3.25 **Exercise:** Solve for x in

$$\begin{aligned}x &\equiv 3 \pmod{17} \\x &\equiv 10 \pmod{16} \\x &\equiv 0 \pmod{15}\end{aligned}$$

x satisfies $x \equiv 3 \pmod{17}$ when $x = 3 + j \cdot 17$
 $x = \{3, 20, 37, 54, 71, 88, 105, \textcolor{green}{122}, 139, 156, 173, 190, 207, 224, 241, 258, 275, 292, 309, 326, 343, 360, 377, \textcolor{green}{394}, \dots\}$

x satisfies $x \equiv 10 \pmod{16}$ and all previous equations when $x = 122 + j \cdot 272$
 $x = \{\textcolor{green}{122}, \textcolor{green}{394}, 666, 938, 1210, 1482, 1754, 2026, 2298, 2570, 2842, 3114, 3386, 3658, \textcolor{red}{3930}, 4202, 4474, 4746, 5018, 5290, 5562, 5834, 6106, 6378, 6650, 6922, 7194, 7466, 7738, \textcolor{red}{8010}, 8282, 8554, 8826, 9098, 9370, 9642, 9914, 10186, 10458, 10730, 11002, 11274, 11546, 11818, \textcolor{green}{12090}, \dots\}$

x satisfies $x \equiv 0 \pmod{15}$ and all previous equations when $x = 3930 + j \cdot 4080$
 $x = \{\textcolor{red}{3930}, \textcolor{red}{8010}, \textcolor{green}{12090}, \dots\}$

Notice that the next solution-set is all of the previous solutions that satisfy the next equation. The solution-set at each step is a subset of the solution-set above it. I have marked which numbers are ‘carried over’ from the previous solution-set to the next solution-set with color, underlines, and overlines.

3.26 **Exercise:** Solve for x in

$$\begin{aligned}x &\equiv 1 \pmod{2} \\x &\equiv 2 \pmod{3} \\x &\equiv 3 \pmod{4} \\x &\equiv 4 \pmod{5} \\x &\equiv 5 \pmod{6} \\x &\equiv 0 \pmod{7}\end{aligned}$$

x satisfies $x \equiv 1 \pmod{2}$ when $x = 1 + j \cdot 2$
 $x = \{1, 3, \textcolor{green}{5}, 7, 9, \textcolor{green}{11}, 13, 15, \textcolor{green}{17}, 19, 21, \textcolor{green}{23}, \dots\}$

x satisfies $x \equiv 2 \pmod{3}$ and all previous equations when $x = 5 + j \cdot 6$
 $x = \{\textcolor{green}{5}, \underline{\textcolor{green}{11}}, \textcolor{green}{17}, \underline{\textcolor{green}{23}}, 29, 35, 41, \underline{\textcolor{green}{47}}, \dots\}$

x satisfies $x \equiv 3 \pmod{4}$ and all previous equations when $x = 11 + j \cdot 12$
 $x = \{\underline{\textcolor{green}{11}}, \underline{\textcolor{green}{23}}, \underline{\textcolor{green}{35}}, \underline{\textcolor{green}{47}}, \textcolor{red}{59}, 71, 83, 95, 107, \textcolor{red}{119}, 131, 143, 155, 167, \textcolor{red}{179}, \dots\}$

x satisfies $x \equiv 4 \pmod{5}$ and all previous equations when $x = 59 + j \cdot 60$
 $x = \{\textcolor{red}{59}, \textcolor{red}{119}, \textcolor{red}{179}, \dots\}$

x satisfies $x \equiv 5 \pmod{6}$ and all previous equations when $x = 59 + j \cdot 60$
 $x = \{\textcolor{red}{59}, \overline{\textcolor{red}{119}}, \textcolor{red}{179}, \dots\}$

This equation was redundant, since $x \equiv 1 \pmod{2}$ and $x \equiv 2 \pmod{3}$. This says that x is an odd number one less than a multiple of three. 5 is the only odd number one less than a multiple of three in the complete canonical residue system of 6, therefore this equation is equivalent to the two previous ones.

x satisfies $x \equiv 0 \pmod{7}$ and all previous equations when $x = 119 + j \cdot 420$
 $x = \{119, 539, 959, 1379, 1799, 2219, \dots\}$

3.27 Theorem: Let $a, b, m, n \in \mathbb{Z}$ where $m > 0$ and $n > 0$. The system $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ has solutions for x if and only if $\gcd(n, m) \mid (a - b)$

Proof: $x \equiv a \pmod{m}$, or equivalently $m \mid (x - a)$, or equivalently, $cm = x - a$, and by the same logic $dn = x - b$. Adding the system of equations together, $cm - dn = x - a - (x - b)$, or equivalently $cm - dn = a - b$. By Theorem 1.48, this has solutions if and only if $\gcd(m, n) \mid (a - b)$.

3.28 Theorem: Let $a, b, m, n \in \mathbb{Z}$ where $m > 0$, $n > 0$, and $\gcd(m, n) = 1$

Proof: Repeat the previous proof up to $cm - dn = a - b$. c has solutions every $\frac{n}{\gcd(m, n)} = n$ and d has solutions every $\frac{m}{\gcd(m, n)} = m$. $a + cm = x$ and $b + dn = x$. $x = a + m(c_0 + in) = a + mc_0 + inm$ and $x = b + n(d_0 + im) = b + nd_0 + inm$. Solving for x in terms of c and solving for x in terms of d both indicate solutions every nm . Therefore they are equivalent to the same thing \pmod{mn} .

$$\begin{array}{ll}
 4.1 & 2^0 \pmod{7} \quad 1 \\
 & 2^1 \pmod{7} \quad 2 \\
 & 2^2 \pmod{7} \quad 4 \\
 & 2^3 \pmod{7} \quad 1 \\
 & 2^4 \pmod{7} \quad 2 \\
 & 2^5 \pmod{7} \quad 4 \\
 & 2^6 \pmod{7} \quad 1
 \end{array}$$

4.2 Theorem: