Notebook Swag

Sam Grayson

April 15, 2015

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

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 $xx^{n-1} > a_{n-1}x^{n-1}$, equivalently $x^n > a_{n-1}x^{n-1}$. That simply arises from the initial condition. After this point, the nth 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 $(|a_2x^2| > |a_1x| > |a_0|)$. Therefore the third term dominates the first term $(|a_2x^2 > a_0)$.

Continuing in this way, there is some point k_n the nth 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 $k = \max(k_n, k_{n-1}, \ldots, k_1)$, the nth term dominates. Since the polynomial is monic, $a_n > 0$. Therefore $|a_nx^n| > |a_{n-1}x^{n-1}| > \cdots > |a_0|$. Therefore $n|a_nx^n| > |a_{n-1}x^{n-1}| + \cdots + |a_0|$.

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 mod 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.

3.22
$213 - 8 \cdot 24 = 21$
$24 - 1 \cdot 21 = 3$
$24 - 1 \cdot (213 - 8 \cdot 24) = 3$
$9 \cdot 24 - 213 = 3$
$41 \cdot (9 \cdot 24 - 213) = 41 \cdot 3 = 123$
$369 \cdot 24 - 41 \cdot 213 = 123$
$(369 + n \cdot 71) \cdot 24 - (41 + n \cdot 8) \cdot 213 = 123$
$213 \mid ((369 + n \cdot 71) \cdot 24 - 213)$
$x = 369 + n \cdot 71$

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

Steps:

1. WLOG $a < n$, otherwise reduce a.
2. Let $r_1 := q_0 n - a$ with $0 \le r_1 < n$ by the Division algorithm.
3. Let $r_2 := q_1 a - r_1$ with $0 \le r_1 < a$ by the Division algorithm.
4. Starting with $i = 2$, repeating until $r_{i+2} = 0$
   A. Let $r_{i+1} := r_{i-1} - q_i r_i$ with $0 \le r_{i+1} < r_i$ by the Division algorithm.
   B. Let $i := i + 1$
5. $r_{i+1} = \gcd(n, a)$ by the argument in 2.35
6. Observe that $\gcd(n, a) = r_{i+1} = r_{i-1} - q_i r_i$ (from assignment of r_{i+1})
7. Starting with $j = i - 1$, until $j = 1$
   A. Replace r_{j+1} with $rj - 1 - q_j r_j$ (from the assignment of r_{i+1})
   B. Let $j := j - 1$
   C. Observe that r_j is a linear combination of r_{j-1} and r_j
8. Subsitute r_1 with $q_0 n - b$ and r_2 with $q_1 a - r_1$
9. Since $\gcd(n, a) = r_{i+1}$, and r_{i+1} is written as a linear combination of r_i and r_{i-1}, and r_1 and r_2 are written as a linear combinatino of a and b, $gcd(n, a)$ is written as a linear combination of a and b after substitution. Let that combination be $ax + ny = b$
10. Therefore $\frac{\gcd(n,a)}{b} ax + \frac{\gcd(n,a)}{b} ny = \frac{\gcd(n,a)}{b} b = b$ by algebra with additional solutions are found at $(\frac{\gcd(n,a)}{b} x + m\frac{n}{\gcd(n,a)})a + (\frac{\gcd(n,a)}{b} y - m\frac{a}{\gcd n,a})n = b$ by Theorem 1.51.
11. Therefore solution is found at $x = \frac{\gcd(n,a)}{b} a + m\frac{n}{\gcd(n,a)}$ ■

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

Proof:

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

$0 + (\gcd(a, n) - 1)\frac{n}{\gcd(a,n)} \le x_0 + (\gcd(a, n) - 1)\frac{n}{\gcd(a,n)} < \frac{n}{\gcd(a,n)} + (\gcd(a, n) - 1)\frac{n}{\gcd(a,n)}$ Additio

$0 + (\gcd(a, n) - 1)\frac{n}{\gcd(a,n)} \le x_0 + (\gcd(a, n) - 1)\frac{n}{\gcd(a,n)} < \frac{n}{\gcd(a,n)} + \gcd(a, n)\frac{n}{\gcd(a,n)} - \frac{n}{\gcd(a,n)}$ Distribu

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

For all $0 \le m \le \gcd(a, n) - 1$, 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 $x \equiv a \pmod{m}$, 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 $xm - dn = a - b$. By Theorem 1.48, this has solutions if and only if $\gcd(m, n) \mid (a - b)$.

3.26 Repeat the previous proof up to $cm - dn = a - b$. This has one solution every

3.27 Solve for x in

$x \equiv 3 \pmod{17}$
$x \equiv 10 \pmod{16}$
$x \equiv 0 \pmod{15}$

$x = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, , \dots\}$

x satisfies $1x \equiv 3 \pmod{17}$ and all previous equations when $x = 3 + j \cdot 17$
$x = \{3, 20, 37, 54, 71, 88, 105, 122, 139, 156, 173, 190, 207, 224, 241, 258, 275, 292, 309, 326, 343, 360, 377, 394, , \dots\}$

x satisfies $1x \equiv 10 \pmod{16}$ and all previous equations when $x = 122 + j \cdot 272$
$x = \{122, 394, 666, 938, 1210, 1482, 1754, 2026, 2298, 2570, 2842, 3114, 3386, 3658, 3930, 4202, 4474, 4746, 5018, 5290, 5562, 5834, 6106, 6378, 6650, 6922, 7194, 7466, 7738, 8010, 8282, 8554, 8826, 9098, 9370, 9642, 9914, 10186, 10458, 10730, 11002, 11274, 11546, 11818, 12090, , \dots\}$

x satisfies $1x \equiv 0 \pmod{15}$ and all previous equations when $x = 3930 + j \cdot 4080$

3.28 Solve for x in

$x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{4}$
$x \equiv 4 \pmod{5}$
$x \equiv 5 \pmod{6}$
$x \equiv 0 \pmod{7}$

$x = \{0, 1, 2, 3, 4, 5, , \dots\}$

x satisfies $1x \equiv 1 \pmod{2}$ and all previous equations when $x = 1 + j \cdot 2$
$x = \{1, 3, 5, 7, 9, 11, 13, 15, 17, , \dots\}$

x satisfies $1x \equiv 2 \pmod{3}$ and all previous equations when $x = 5 + j \cdot 6$
$x = \{5, 11, 17, 23, 29, 35, , \dots\}$

x satisfies $1x \equiv 3 \pmod{4}$ and all previous equations when $x = 11 + j \cdot 12$
$x = \{11, 23, 35, 47, 59, 71, 83, 95, 107, 119, 131, 143, 155, 167, 179, , \dots\}$

x satisfies $1x \equiv 4 \pmod{5}$ and all previous equations when $x = 59 + j \cdot 60$
$x = \{59, 119, 179, , \dots\}$

x satisfies $1x \equiv 5 \pmod{6}$ and all previous equations when $x = 59 + j \cdot 60$

4.1	2^0	(mod 7)	1
	2^1	(mod 7)	2
	2^2	(mod 7)	4
	2^3	(mod 7)	1
	2^4	(mod 7)	2
	2^5	(mod 7)	4
	2^6	(mod 7)	1