Notebook Swag

Sam Grayson

April 8, 2015

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

Proof:

Let $i \in \mathbb{N}$	(for universal generalization)
Let $j \in \mathbb{N}$	(for universal generalization)
If $i > 0$	
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \land 0 \le r < j)$	Division algorithm
Otherwise $i < 0$	
$\exists! p, r \in \mathbb{N}(-i = pj + t \land 0 \le t < j)$	Division algorithm
$-i = pj + t \land 0 \le t < j$	Existential generalization
$i = -pj - t$	Existential generalization
$i = -pj - j + j - t$	Algebra
$i = -(p+1)j + j - t$	Algebra
$0 \le t < j$	Simplification
$-j < -t \le 0$	Property of inequalities
$0 < j - t \le j$	Property of inequalities
If $j - t < j$	
Let $q = -(p+1)$ Let $r = j - t$	
$0 < r < j$	Property of inequalities
$0 \le r < j$	Property of inequalities
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \land 0 \le r < j)$	Existential generalization
Otherwise $j - t \ge j$	
$j - t \le j \land j - t \ge j$	Conjunction
$j - t = j$	Property of inequalities
$t = 0$	Identity property
$i = pj$ Let $r = 0$	
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \land 0 \le r < j)$	Existential generalization
$\exists! q, r \in \mathbb{N}(i = qj + r \land 0 \le r < j)$	Constructive dilemma
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \land 0 \le r < j)$	Constructive dilemma
$\forall i \in \mathbb{N}(\forall j \in \mathbb{N}(\exists! r \in \mathbb{N}(i \equiv r \pmod{j} \land 0 \le r < j)))$	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:** $B \in \text{CRS}(n) \to |B| = n$

Proof:

Let $A \in \text{CCRS}(n)$	
Let $B \in \text{CRS}(n)$	For conditional
Let $f : A \to B$ 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	
$\lvert A\rvert = n$	By inspection
Thus $\lvert A\rvert = \lvert B\rvert = n$	Bijection
$B \in \text{CRS}(n) \to \lvert B\rvert = n$	Conditional proof ∎

3.17 **Theorem:** f

3.18
1. $x \equiv 1 \pmod{3}$
2. $x \equiv 4 \pmod{5}$
3. No solution.
4. $x \equiv 156 \pmod{213}$

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 $0 \leq x < n$

Steps:

1. WLOG $a < n$, otherwise reduce a.
2. Let $r_1 := q_0 n - a$ with $0 \leq r_1 < n$ by the Division algorithm.
3. Let $r_2 := q_1 a - r_1$ with $0 \leq r_1 < a$ 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 $0 \leq r_{i+1} < r_i$ 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 $x = \frac{\gcd(n,a)}{b} a + m \frac{n}{\gcd(n,a)}$ ■

Proof:

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

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

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

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