Sam Grayson: Test 1

February 13, 2015

All new numbers instantiated with 'for some' are assumed to be integers.

1. $\{a, b \in \mathbb{N} \wedge a|b \wedge b|a\} \to (a = b)$

$a = bc$ for some c	
$b = da$ for some d	Definition of divides
$a = cda$	Substitution
$cd = 1$	Identity property
$c = \pm 1 \wedge d = \pm 1$	Algebra
$a = \pm b$	Substitution
$a = b$	Eliminating extraneous solutions (noting $a, b \in \mathbb{N}$) $\blacksquare$

2. $\{a, b, c \in \mathbb{Z} \wedge c > 0 \wedge a \equiv b \pmod{c}\} \to (a, c) = (b, c)$

$c\|(b - a)$	Definition of modulo
$cn = b - a$	Definition of divides
$(a, c) = d$	Let
$(a, c)\|a \wedge (a, c)\|c$	Definition of GCD

$\blacksquare$

3. $\{a, b, d \in \mathbb{Z} \wedge (a \neq 0 \vee b \neq 0) \wedge d > 0 \wedge d|a \wedge d|b\} \to d|(a, b)$

$d\neg(a, b)$	Assume for contradiction
$(a, b)\|a \wedge (a, b)\|b$	Definition of GCD
$m(a, b) = a \wedge n(a, b) = b$ for some m, n	Definition of divides
$(m, n) = 1$	Test question 4
$d\|m(a, b) \wedge d\|n(a, b)$	Substitution
$(d, (a, b)) = 1$	Contradictive assumption
$d\|m \wedge d\|n$	Theorem 1.41
$(m, n) > d$	Definition of GCD
This contradicts $(m, n) = 1$	
$a\|(a, b)$	Contradiction $\blacksquare$

$\gcd(0, 0)$ is undefined. That is why we must specify that a and b are not both zero.

4. $d = (a, b) \to (\frac{a}{d}, \frac{b}{d}) = 1$

$d\|a \wedge d\|b$	Definition of GCD
$d\frac{a}{d} = a \wedge d\frac{b}{d} = b$ for some $\frac{a}{d}, \frac{b}{d}$	Definition of divides
$c = (\frac{a}{d}, \frac{b}{d}) \wedge$ for some c	Let
$c \neq 1$	Assume for contradiction
$c\|\frac{a}{d} \wedge c\|\frac{b}{d}$	Definition of GCD
$c\frac{a}{dc} = \frac{a}{d} \wedge c\frac{b}{dc} = \frac{b}{d}$ for some $\frac{a}{dc}, \frac{b}{dc}$	Definition of divides

$dc\frac{a}{dc} = a \wedge dc\frac{b}{dc} = b$ Substitution

$dc|a \wedge dc|b$

We don't know if dc is positive or negative

Therefore I try both

$-dc(-\frac{a}{dc}) = a \wedge -dc(-\frac{b}{dc}) = b$ Substitution

$-dc|a \wedge -dc|b$ Definition of divides

$dc > d \vee -dc > d$ Property of inequality

$(a, b) > dc \vee (a, b) > -dc$ Definition of GCD

Either way, I have found a common divisor (namely dc or $-dc$) greater than d. This contradicts the definition of GCD.

$c = 1$ Contradiction

$1 = (\frac{a}{d}, \frac{b}{d})$ Substitution ■

5. Let $a = 6$, $b = 2$, $c = 3$.
   - $a|(bc)$ since $6|6$
   - $a \not| b$ since $6 \not| 2$
   - $a \not| c$ since $6 \not| 3$

6. $\{a, b, c, n_1, n_2 \in \mathbb{Z} \wedge a \equiv b \pmod{n_1} \wedge a \equiv c \pmod{n_2}\} \rightarrow b \equiv c \pmod{(n_1, n_2)}$

7. (a) i. $2072 = 1813 \cdot 1 + 259$. Therefore $(2072, 1813) = (1813, 259)$
   ii. $1813 = 259 \cdot 7 + 0$. Therefore $(1813, 259) = (259, 0) = 259$
   iii. Therefore $(2072, 1813) = 259$

   (b) $2072 = 1813 \cdot 1 + 259$
   $1813 = 259 \cdot 7$
   $2072 = (259 \cdot 7) + 259$
   $2072 = 259 \cdot 8$
   $2072x + 1813y = 2048$
   $259 \cdot 8x + 259 \cdot 7y = 2048 = 11 \cdot 259$
   $259 \cdot (8x + 7y) = 259 \cdot 11$
   $259 \cdot 11 \cdot (8 + (-7)) = 259 \cdot 11$
   $259 \cdot (8 \cdot 11 + 7 \cdot (-11)) = 2849$
   $8 \cdot 259 \cdot 11 + 7 \cdot 259 \cdot (-11) = 2849$
   $2072 \cdot 11 + 1813 \cdot (-11) = 2849$
   $x = 11 \wedge y = -11$

   (c) $259 \cdot (8x + 7y) = 259 \cdot 11$
   $259 \cdot 11 \cdot (8 + (-7) + 0) = 259 \cdot 11$
   $259 \cdot 11 \cdot (8 \cdot 1 + 7 \cdot (-1) + 0) = 259 \cdot 11$
   $259 \cdot 11 \cdot (8 \cdot 1 + 7 \cdot (-1) + 8 \cdot 7 - 7 \cdot 8) = 259 \cdot 11$
   $259 \cdot 11 \cdot (8 \cdot (1 - 7) + 7 \cdot (-1 + 8)) = 259 \cdot 11$
   $259 \cdot 11 \cdot (8 \cdot (-6) + 7 \cdot 7) = 2849$
   $259 \cdot (8 \cdot (-66) + 7 \cdot 77) = 2849$

$8 \cdot 259 \cdot (-66) + 7 \cdot 259 \cdot 77 = 2849$
$2072 \cdot (-66) + 1813 \cdot 77 = 2849$
$x = -66 \wedge y = 77$

8. $\{a, b, c \in \mathbb{Z} \wedge (a \neq 0 \vee b \neq 0) \wedge c \neq 0\} \rightarrow (ca, cb) = |c|(a, b)$

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

$c \in \mathbb{Z} \backslash \{0\}$	Premise
Either $c > 0 \vee c = 0 \vee c < 0$	Trichotomy
$c \neq 0$	Premise
Temporarily assume $c > 0$	
$\lvert c\rvert = c$	Definition of absolute value
$\lvert c\rvert \in \mathbb{N}$	Definition of $\mathbb{N}$
$(ca, cb) = (\lvert c\rvert a, \lvert c\rvert b)$	Substitution
$(\lvert c\rvert a, \lvert c\rvert b) = \lvert c\rvert(a, b)$	Theorem 1.55
Temporarily assume $c < 0$	
$\lvert c\rvert = -c$	Definition of absolute value
$-c > 0$	Property of inequalities (multiplying by -1 flips direction)
$-c \in \mathbb{Z}$	Definition of $\mathbb{N}$
$(-ca, -cb) = -c(a, b)$	Theorem 1.55
$(\lvert c\rvert a, \lvert c\rvert b) = \lvert c\rvert(a, b)$	Substitution
All possibilities were tried	
$(\lvert c\rvert a, \lvert c\rvert b) = \lvert c\rvert(a, b)$	Constructive Dilemma ∎

9.

10. **Problem:** $\forall n \in \mathbb{N}\{6|(n^3 + 5n)\}$

Lemma: $6|(3n(n^2 + 1))$

Assume n is odd, such that $n = 2k+1$. $3n(n^2+1) = 3n(4k^2+2k+1+1) = 6n(2k^2+k+1)$. Therefore $3n(n^2 + 1)$ is divisible by 6.

Assume n is even, such that $n = 2k$. $3n(n^2 + 1) = 6k(n^2 + 1)$. Therefore $3n(n^2 + 1)$ is divisible by 6.

Therefore, for any integer n, $3n(n^2 + 1)$ is divisible by 6. □

Proof:

Let $n = 1$. $n^3 + 5n$ is divisible by 6, because $n^3 + 5n = 6$.

Assume $n^3 + 5n$ is divisible by 6.

$(n + 1)^3 + 5(n + 1) = (n^3 + 3n^2 + 3n + 1) + (5n + 5) = (n^3 + 5n) + (3n^2 + 3n + 6)$

Therefore $(n+1)^3+5(n+1)$ is the sum of things divisible by six (namely (n^3+5n), $3n(n^2+1)$, and 6).

Therefore, by the induction axiom, $n^3 + 5n$ is divisible by 6.