Sam Grayson's Notebook (with $\LaTeX$)

January 14, 2015

1.1 $ma = b$ Definition of 'divides'
$na = c$ Definition of 'divides'
$na + ma = b + c$ Algebra
$(n + m)a = b + c$ Algebra
$a|(b + c)$ Definition of 'divides' $\blacksquare$

1.2 Let $d = -c$
$a|(b + d)$ Theorem 1.1
$a|(b - c)$ substitution $\blacksquare$

1.3 $ma = b$ Definition of 'divides'
$na = c$ Definition of 'divides'
$mana = bc$ Algebra
$a|bc$ Definition of 'divides' $\blacksquare$

1.4 $mana = bc$ see last proof
$a^2|bc$ Definition of 'divides' $\blacksquare$

1.5 *If $a|b$ then $a|b^n$*
$b = ka$ Definition of 'divides'
$b^n = (ka)^n = kk^{(n-1)}a^n$ Algebra
$k|b^n$ Definition of 'divides' $\blacksquare$

1.6 $ka = b$ Definition of 'divides'
$ack = bc$ Algebra
$a|bc$ Definition of 'divides' $\blacksquare$

1.7
1. $45 - 9 = 36 = 9 \cdot 4.$ True
2. $37 - 2 = 35 = 7 \cdot 5.$ True
3. $37 - 3 = 34.$ False
4. $37 - (-3) = 40 = 8 \cdot 5.$ True

1.8 let k be all the numbers
where $k \equiv b \pmod 3$
$3|(k - b)$ Definition of 'mod'
$3n = k - b$ Definition of 'divides'
$3n + k = n$ Algebra $\blacksquare$

1. $3n$
2. $3n + 1$
3. $3n + 2$
4. $3n$
5. $3n + 1$

1.9 $a - a = 0 = 0n$ Arithmetic
$n|(a - a)$ Definition of 'divides'
$a \equiv 0 \pmod n$ Definition of 'mod' $\blacksquare$

1.10	$n \mid (a-b)$	Definition of 'mod'
	$kn = a-b$	Definition of 'divides'
	$-kn = b-a$	Algebra
	$n \mid (b-a)$	Definition of 'divides'
	$b \equiv a \pmod{n}$ ■	
1.11	$n \mid (a-b)$	Definition of 'mod'
	$n \mid (b-c)$	Definition of 'mod'
	$n \mid (a-b+b-c)$	Theorem 1.1
	$n \mid (a-c)$	Algebra
	$a \equiv c \pmod{n}$	Definition of 'mod' ■
1.12	$n \mid (a-b)$	Definition of 'mod'
	$n \mid (c-d)$	Definition of 'mod'
	$n \mid (a+c-b-d))$	Theorem 1.1
	$n \mid ((a+c)-(b+d))$	Algebra
	$a+c \equiv b+d \pmod{n}$	definion 'mod' ■
1.13	let $e = -c$ and $f = -d$	
	$a+e \equiv b+f$	Theorem 1.12
	$a-c \equiv b-d$	substitution ■
1.14	$n \mid (a-b)$	Definition of 'mod'
	$n \mid (c-d)$	Definition of 'mod'
	$n \mid (a-b)(c-d)$	Theorem 1.3 ■
1.15	$a \equiv b \pmod{n}$	Premise
	$a^2 \equiv b^2 \pmod{n}$	Theorem 1.14 ■
1.16	$a \equiv b \pmod{n}$	Premise
	$a^2 \equiv b^2 \pmod{n}$	Theorem 1.15
	$a^2a \equiv b^2b \pmod{n}$	Theorem 1.14
	$a^3 \equiv b^3 \pmod{n}$	Algebra ■
1.17	$a \equiv b \pmod{n}$	Premise
	$a^{k-1} \equiv b^{k-1} \pmod{n}$	Premise
	$a^{k-1}a \equiv b^{k-1}b \pmod{n}$	Theorem 1.14
	$a^k \equiv b^k \pmod{n}$	Algebra ■
1.18	Base case:	
	$a \equiv b \pmod{n}$	Premise
	Inductive Hypothesis:	
	$a^{k-1} \equiv b^{k-1} \pmod{n}$	(assumption)
	Inductive step:	
	$a^{k-1}a \equiv b^{k-1}b \pmod{n}$	Theorem 1.14
	$a^k \equiv b^k \pmod{n}$	Algebra
	Conclusion:	
	$a^k \equiv b^k \pmod{n}$	inductively ■

1.19 12. $6 \equiv 2 \pmod{4}$

$5 \equiv 1 \pmod{4}$

$6+5 \equiv 2+1 \pmod 4$

13. $6-5 \equiv 2-1 \pmod 4$

14. $6 \cdot 5 \equiv 2 \cdot 1$

15. $6^2 \equiv 2^2 \pmod 4$

16. $6^3 \equiv 2^3 \pmod 4$

17. $6^4 \equiv 2^4 \pmod 4$

18. $6^k \equiv 2^k \pmod 4$

1.20 No
Consider the case wehre $n=4$, $c=0$, $a=1$, and $b=2$.
$ac \equiv bc \pmod n$
$a \neq b$

1.21 See 1.22 and 1.23

1.22

$3 \mid a$	Premise (Base Case)
$3 \mid b$	Let b be an integer where... (Inductive Hypothesis)
$3 \mid 9$	Arithmetic
$3 \mid (9b_k 10^{k-1})$	Theorem 1.3
$3 \mid (b - 9b_k 10^{k-1})$	Theorem 1.2
$3 \mid (b_{k-1} + b_k)b_{k-2} \dots b_0$	Algebra* (Inductive Step)
$3 \mid (a_k + a_{k-1} + a_{k-2} + \dots a_1 + a_0)$	Inductive axiom ■

Here is the algebra I used in the step labeled 'Algebra*':

$$\begin{aligned} b - b_k 9 10^{k-1} &= \\ b - b_k(10-1)10^{k-1} &= \\ b + (-b_k 10 \cdot 10^{k-1} + b_k 1 10^{k-1}) &= \\ b + (-b_k 10^k + b_k 10^{k-1}) &= \end{aligned}$$

$$\begin{array}{cccccc} & b_k & b_{k-1} & b_{k-2} & \dots & b_0 \\ + & (-b_k) & b_k & 0 & \dots & 0 \quad = \\ \hline & & (b_k + b_{k-1}) & b_{k-2} & \dots & b_0 \end{array}$$

1.23

$3 \mid a$	Premise (Base Case)
$3 \mid (b_k + b_{k-1} + \dots + b_0)$	Assumption (Inductive Hypothesis)
$3 \mid 9$	Arithmetic
$3 \mid (b_k 9c)$ where c is k ones in a row	Theorem 1.3
$3 \mid (b_k + b_{k-1} + \dots + b_0 + b_k 9c)$	Theorem 1.2
$3 \mid (b_k 10^k + b_{k-1} + \dots + b_0)$	Algebra*
$3 \mid (a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_0 10^0)$	Inductive Axiom
$3 \mid (a_k a_{k-1} \dots a_0)$	Definition of digits ■

Here is the algebra I used in the step labeled 'Algebra*':

$$\begin{aligned}
b_k + b_{k-1} + \ldots + b_0 + b_k 9c &= \\
b_k + b_{k-1} + \ldots + b_0 + b_k d &= \quad \text{where d is a number with } k \text{ nines} \\
b_k + b_{k-1} + \ldots + b_0 + b_k(10^k - 1) &= \\
b_k + b_{k-1} + \ldots + b_0 + b_k 10^k - b_k &= \\
b_{k-1} + \ldots + b_0 + b_k 10^k &
\end{aligned}$$

1.24 $4|a$ if and only if $4|(a_1 + a_3 + \ldots)(a_0 + a_2 + a_4 + \ldots)$

1.25
1. $m = nq + r$ where $m = 25$, $n = 7$, $q = 3$, and $r = 4$
2. $m = 277$, $n = 4$, $q = 66$, and $r = 1$
3. $m = 33$, $n = 11$, $q = 3$, $r = 0$
4. $m = 33$, $n = 45$, $q = 0$, $r = 33$

1.26 Setup:
(Make a list of multiples of n that are greater than m and choose the smallest one to define $n(q + 1)$.)
$A := \{k | k \in \mathbb{N} \ \wedge kn \geq m + n\}$
$\exists a \ni (a \in A \wedge a \geq m + n \wedge \forall k \in A(a \leq k))$
$q := a - 1$
$r := m - nq$

Proving r satisfies upper bound
(If it didn't, then a wouldn't be an element of A, but we know that a is in A.) $r > n - 1$
$r \geq n$
$\exists j \ni (r - j = n \wedge j > 0)$
$nq + r = m$
$nq + (n + j) = m$
$n(q + 1) + j = m$
$n(q + 1) < m$
$n(q + 1) < m + n$
$n(q + 1) \geq m + n$
$\therefore r \leq n - 1$

Proving r satisfies lower bound
(If it didn't, then there would be another element smaller than a in A, but a is the least element in A.)
$nq + r = m$
$nq > m$

$\forall k(k \in A \rightarrow q + 1 \leq k)$
$\therefore r \geq 0$
■