Sam Grayson's Notebook (with LaTeX)

January 24, 2015

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

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

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

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

1.5 *If $a \mid b$ then $a \mid b^n$*

$b = ka$	Definition of 'divides'
$b^n = (ka)^n = kk^{(n-1)}a^n$	Algebra
$k \mid b^n$	Definition of 'divides' $\blacksquare$

1.6	$ka = b$	Definition of 'divides'
	$ack = bc$	Algebra
	$a \mid bc$	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 $k \equiv b \pmod 3$

$3 \mid (k - b)$	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
	$n \mid (a - a)$	Definition of 'divides'
	$a \equiv 0 \pmod n$	Definition of 'mod' $\blacksquare$

1.10 $n|(a-b)$ Definition of 'mod'
$kn = a - b$ Definition of 'divides'
$-kn = b - a$ Algebra
$n|(b-a)$ Definition of 'divides'
$b \equiv a \pmod{n}$ ■

1.11 $n|(a-b)$ Definition of 'mod'
$n|(b-c)$ Definition of 'mod'
$n|(a-b+b-c)$ Theorem 1.1
$n|(a-c)$ Algebra
$a \equiv c \pmod{n}$ Definition of 'mod' ■

1.12 $n|(a-b)$ Definition of 'mod'
$n|(c-d)$ Definition of 'mod'
$n|(a+c-b-d))$ Theorem 1.1
$n|((a+c)-(b+d))$ 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 $n|(a-b)$ Definition of 'mod'
$n|(c-d)$ Definition of 'mod'
$n|(a-b)(c-d)$ 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
$a^2 a \equiv b^2 b \pmod{n}$ 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

$3\|a$	Premise (Base Case)
$3\|b$	Let b be an integer where… (Inductive Hypothesis)
$3\|9$	Arithmetic
$3\|(9b_k10^{k-1})$	Theorem 1.3
$3\|(b - 9b_k10^{k-1})$	Theorem 1.2
$3\|(b_{k-1} + b_k)b_{k-2} \dots b_0$	Algebra* (Inductive Step)
$3\|(a_k + a_{k-1} + a_{k-2} + \dots a_1 + a_0)$	Inductive axiom ■

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

$$\begin{aligned} b - b_k910^{k-1} &= \\ b - b_k(10-1)10^{k-1} &= \\ b + (-b_k10 \cdot 10^{k-1} + b_k110^{k-1}) &= \\ b + (-b_k10^k + b_k10^{k-1}) &= \end{aligned}$$

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

1.23

$3\|a$	Premise (Base Case)
$3\|(b_k + b_{k-1} + \dots + b_0)$	Assumption (Inductive Hypothesis)
$3\|9$	Arithmetic
$3\|(b_k9c)$ where c is k ones in a row	Theorem 1.3
$3\|(b_k + b_{k-1} + \dots + b_0 + b_k9c)$	Theorem 1.2
$3\|(b_k10^k + b_{k-1} + \dots + b_0)$	Algebra*
$3\|(a_k10^k + a_{k-1}10^{k-1} + \dots + a_010^0)$	Inductive Axiom
$3\|(a_ka_{k-1} \dots a_0)$	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 $n(q+1)$.

$A := \{k \mid k \in \mathbb{N} \ \wedge kn > m\}$	
$\exists a \ni (a \in A \wedge an > m \wedge \forall k \in A(a \leq k))$	Well-ordering Principle
$q := a - 1$	
$r := m - nq$	

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.

$r > n - 1$	Assume for contradiction
$r \geq n$	Property of inequalities (over $\mathbb{Z}$)
$\exists j \ni (r - n = j \wedge j \geq 0)$	Property of inequalities
$nq + r = m$	Algebra (from definition of r)
$nq + (n + j) = m$	Algebra (from definition of j)
$n(q+1) + j = m$	Algebra
$n(q+1) \leq m$	Property of inequalities
$n(q+1) > m$	Algebra (from definition of a)
$\therefore r \leq n - 1$	Contradiction

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.

$r < 0$	Assume for contradiction
$nq + r = m$	Algebra (from definition of r)
$nq > m$	Property of inequalities
$q \in A$	$q \in \mathbb{N} \wedge nq > m$ is the condition for A
$\forall k(k \in A \to q + 1 \leq k)$	Definition of a (smallest element in A)
$q + 1 \leq q$	Universal instantiation
$\therefore r \geq 0$	Contradiction

Proving q and r are integers:

They all came from sets that only contain integers.

$A \subset \mathbb{N} \subset \mathbb{Z}$	Stuff I learned
$a \in A$	Definition of a
$a \in \mathbb{Z}$	Property of sets
$q \in \mathbb{Z}$	Closure (Definition of q)
$r \in \mathbb{Z}$	Closure (definition of r)

1.27

$\exists q', r' \in \mathbb{Z}(m = q'n + r' \wedge r' \neq r \wedge q' \neq q \wedge 0 \leq r \leq q' - 1)$	Assume for contradiction
$r' < n$	Assumption (restriction on r')
$q'n + n > m$	Property of inequalities (because $q'n + r = m$)
$n(q' + 1) > m$	Algebra
$q' + 1 \in A$	Definition of A
$q' + 1 \neq q + 1$	Property of inequalities
$q' + 1 > q + 1$	Definition of a (smallest element in A)
$q' \geq q + 1$	Property of inequalities (over $\mathbb{Z}$)
$qn + r = m$	Definition of r
$qn + n > m$	Property of inequalities (replace r with something greater-than r)
$(q + 1)n > m$	Algebra
$q'n > m$	Property of inequalities (replace $q+1$ with something greater-than-or-equal to it)
$q'n + r' > m$	Property of inequalities (add a positive number to the bigger side and it is still bigger)
$\neg\exists q', r' \in \mathbb{Z}(m = q'n + r' \wedge r' \neq r \wedge q' \neq q \wedge 0 \leq r \leq q' - 1)$	Contradiction

1.28

$n \vert (a - b)$	Definition of modulo
$a - b = cn$	Definition of divides
$b = dn + e \wedge 0 \leq e \leq n - 1$	Division algorithm
$a - dn - e = cn$	Algebra
$a = (c + d)n + e \wedge 0 \leq e \leq n - 1$	Algebra
This satisfies the division algorithm	
$(c + d)n + e - b = cn$	Algebra
$b = dn + e \wedge 0 \leq e \leq n - 1$	Algebra
Therefore, same remainder (namely e)	■

$a = cn + r$	Let
$b = dn + r$	Let
$a - b = cn - dn = (c - d)n$	Algebra
$n \vert (a - b)$	Definition of divides

■

1.29 Yes. 1

1.30 No. There are a finite number of integer factors.

1.31
1. No
2. No
3. No
4. Yes
5. Yes
6. Yes

1.32

$a - nb = r$	Algebra (from premise)
$k \mid nb$	Theorem 1.3
$k \mid (a - nb)$	Theorem 1.2
$k \mid r$	Subsitution ■

1.33 Lemma: Let $a = nb + r$. $k|b$ and $k|r$ imply $k|a$.

$k \mid nb$	Therorem 1.3
$k \mid (nb + r)$	Theorem 1.1
$k \mid a$	Substitution ■

$(a, b) = k$	Let
$k \mid a$	Definition of k (GCD)
$k \mid b$	Definition of k (GCD)
$k \mid r_1$	Theorem 1.32
At this point, we know that k is a common divisor. Assume for the sake of contradiction that k is not the greatest common divisor.	
$(b, r_1) = m \wedge m > k$	Assume for contradiction
$m \mid a$	Lemma
$m \mid b$	Definition of GCD
$(b, r_1) > m \wedge m > k$	Definition of GCD
$(b, r_1) = k$	Contradiction

1.34
$$\begin{array}{ccccc} (51,15) & = & (51 - 3 \cdot 15, 15) & = & \\ (6,15) & = & (6, 15 - 2 \cdot 6) & = & \\ (6,3) & = & (6 - 2 \cdot 3, 3) & = & \\ (0,3) & & & = & 3 \end{array}$$

1.35 The Euclidean Algorithm:

1. Let a and b be arguments of GCD where (WLOG) $a > b > 0$.
2. Find q_0 and r_0 such that $a = b \cdot q_0 + r_0$
3. Observe $(a, b) = (b, r_1)$ by 1.33
4. Find q_1 and r_1 such that $b = r_0 \cdot q_1 + r_1$
5. Observe $(b, r_1) = (r_1, r_2)$ by 1.33
6. Starting wtih $i = 2$, until $r_i = 0$:
   A. Find q_i and r_i such that $r_{i-2} = r_{i-1} \cdot q_i + r_i$
   B. Observe $(r_{i-1}, r_i) = (r_i, r_{i+1})$ by 1.33
   C. Let $i := i + 1$
7. $r_i = 0$, therefore $(a, b) = (ri - 1, 0) = r_{i-1}$

1.36

1. 16
2. 1
3. 256
4. 2
5. 1

1.37 $x = 9$, $y = -47$

1.38 The Linear Diophantine Algorithm:

1. Complete the EA
2. Recall the result: $r_i = 0$ and $r_{i-1} = 1$
3. Recall the second-to-last step: $r_{i-3} = r_{i-2} \cdot q_{i-} + r_i$
4. Let Equation A represent: $r_{j-2} - r_{j-1} \cdot q_j = 1$
5. Starting with $i := i - 1$, until $i = 0$:
   A. Justification: $r_{i-2} = r_{i-1} \cdot q_i + r_i$
      $r_{i-2} - r_{i-1} \cdot q_i = r_i$
      r_i is a linear combination of r_{i-1} and r_{i-2}
   B. Substitute r_i for $r_{i-2} - r_{i-1} \cdot q_i$ in Equation A
   C. $i := i - 1$
6. Observe that the left hand side is a linear combination of r_0 and r_1
7. Observere that the right hand side of Equation A is 1
8. Substitute $r_1 = b - r_0 \cdot q_0$, and substitue $r_0 = a - b \cdot q_0$
9. Now a linear combination of a and b sums to 1

1.39

$(a, b) = c$	Let
$c \vert a \wedge c \vert b$	Definition of GCD
$a = dc \wedge b = ec$	Definition of divides
$ax + by = 1$	Premise
$dcx + ecy = (dx + ey)c = 1$	Algebra
$c = 1$	Multiplication over integers ■

1.40

$(a, b) = c$	Let
$c \vert a \wedge c \vert b$	Definition of GCD
$a = dc \wedge b = ec \wedge (d, e) = 1$	Definition of divides
$\exists x, y \ni (dx + ey = 1)$	Theorem 1.38
$ax + by = dcx + ecy = (dx + ey)c = 1c = c$	Algebra
$ax + by = (a, b)$	Substitution ■

1.41

$a = a_0 a_1 \ldots a_n \wedge b = b_0 b_1 \ldots b_{n'} \wedge c = c_0 c_1 \ldots c_{n''}$	Fundamental Theorem of 'rithmetic
$A = \{a_0, a_1, \ldots a_n\} \wedge B = \{b_0, b_1, \ldots b_{n'}\} \wedge C = \{c_0, c_1, \ldots c_{n''}\}$	Let
$A \cap B = \emptyset$	Coprime common factors lemma
$A \subset (B \cup C)$	Divisibility-subset lemma
$\forall a_i \in A\{a \in (B \cup C)\}$	Definition of subset
$\forall a_i \in A\{a \in B \vee a \in C\}$	Definition of union
$\forall a_i \in A\{a \notin B\}$	Null intersection
$\forall a_i \in A\{a \in C\}$	Disjunctive syllogism
$A \subset C$	Definition of subset
$a \vert c$	Subset divides superset lemma ■

1.42	$A = \{\text{factors of a}\}, B = \{\text{factors of b}\}, N = \{\text{factors of n}\}$	Fundamental theorem of 'rithmetic
	$A \subset N \land B \subset N$	Divisibility-subset lemma
	$\forall a \in A\{a \in N\} \land \forall b \in B\{a \in N\}$	Definition of Subset
	$A \cap B = \emptyset$	Coprime common factors lemma
	$\forall a \in A\{a \notin B\} \land \forall b \in B\{b \notin A\}$	Null intersection
	$\forall a \in A\{a \notin B \land a \in N\} \land \forall b \in B\{b \notin A \land b \in N\}$	Conjunction Introduction
	$\forall c \in (A \cup B)\{c \in N\}$	Definition of union (without duplicates)
	$(A \cup B) \subset N$	Definition of subset
	$ab \vert n$	Divisibility-subset lemma ■

1.43	$A = \{\text{factors of a}\}, B = \{\text{factors of b}\}, N = \{\text{factors of n}\}$	Fundamental theorem of 'rithmetic
	$A \cap N = \emptyset \land B \cap N = \emptyset$	Coprime common factors lemma
	$\forall a \in A\{a \notin N\} \land \forall b \in B\{b \notin N\}$	Null intersection
	$\neg(\exists a \in A\{a \in N\} \lor \exists b \in Bb \in N)$	DeMorgan's
	$\neg\exists c \in (A \cup B)\{c \in N\}$	Definition of union
	$\forall c \in (A \cup B)\{c \notin N\}$	Quantificaional Negation
	$(A \cup B) \not\subset N$	Definition of subset
	$(ab, n) = 1$	Coprime common factors lemma ■

1.44	$(n, c) = 1$	Missing hypothesis
	$n \vert (ac - bc) = n \vert c(a - b)$	Definition of mod
	$n \vert (a - b)$	1.41
	$a \equiv b \pmod{n}$	Definition of mod ■