Sam Grayson's Notebook (with LaTeX)

February 5, 2015

1.1 $ma = b$ for some m Definition of 'divides'
$na = c$ for some n 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 $ma = b$ for some m Definition of 'divides'
$na = c$ for some n 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 $a|b^n$*

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

1.6 $ka = b$ for some k 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'
$3n = k - b$ for some n 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	$n\|(a-b)$	Definition of 'mod'
	$kn = a-b$ for some k	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
	$a^2a \equiv b^2b \pmod{n}$	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

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

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

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

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

1.23

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

$n\|(a - b)$	Definition of modulo
$a - b = cn$ for some c	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 r
$b = dn + r$	Let r
$a - b = cn - dn = (c - d)n$	Algebra
$n\|(a - b)$	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)
$k|nb$ Theorem 1.3
$k|(a - nb)$ Theorem 1.2
$k|r$ Subsitution ■

1.33 Lemma: Let $a = nb + r$. $k|b$ and $k|r$ imply $k|a$.
$k|nb$ Therorem 1.3
$k|(nb + r)$ Theorem 1.1
$k|a$ Substitution ■

$(a, b) = k$	Let
$k\|a$	Definition of k (GCD)
$k\|b$	Definition of k (GCD)
$k\|r_1$	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
$m\|a$	Lemma
$m\|b$	Definition of GCD
$(b, r_1) > m \wedge m > k$	Definition of GCD
$(b, r_1) = k$	Contradiction

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

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
$c \mid a \wedge c \mid b$	Definition of GCD
$a = dc$ for some $d \wedge b = ec$ for some e	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
$c \mid a \wedge c \mid b$	Definition of GCD
$a = dc$ for some $d \wedge b = ec$ for some $e \wedge (d, e) = 1$	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

$bc = ka$ for some k	Definition of divides
$ax + by = 1$	1.38
$axc + byc = c = axc + kay = c = a(xc + ky) = c$	Algebra
$a \mid c$	Definition of divides ■

1.42

$n = ia$ for some $i \wedge n = jb$ for some j	Definition of divides
$ax + by = 1$	1.38
$axn + byn = n = axjb + byia = n = ab(xj + ui) = n$	Algebra
$ab \mid n$	Definitin of divides ■

1.43

$ax + ny = 1$ for some $x, y \wedge bw + nz = 1$ for some w, z	Theorem 1.38
$(ax + ny)(bw + nz) = 1 = abxw + n(axz + ybw + yzn)$	Algebra
$(ab, n) = 1$	Theorem 1.38 (converse)

■

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

1.45 See 1.44

1.46 $c = k(a, b)$ for some k

1.47 Given integers a, b, and c, there exist integers x and y that satisfy the equation if and only if $c = k(a, b)$ for some k

1.48 Show: $ax + by = c \to (a, b)|c$
$(a, b)|a \wedge (a, b)|b$ Definition of GCD
$(a, b)|ax \wedge (a, b)|by$ Theorem 1.3
$(a, b)|(ax + by)$ Theorem 1.1
$(a, b)|c$
Show: $(a, b)|c \leftarrow \exists x, y\{ax + by = c\}$
$au + bv = (a, b)$ Theorem 1.40
$c = k(a, b)$ Definition of divides
$kau + kbv = k(a, b) = c$ Algebra
Putting the two halves together
$ax + by = c \leftrightarrow (a, b)|c$ ∎

1.49 The linear diophantine equation can be represented as a line on a grid.
$ax + by = c$
$y = -\frac{a}{b}x + \frac{c}{b}$
The slope of this line is $-a/b$.
First we must simplify the fraction: $-\frac{a}{b} = -\frac{a/(a,b)}{b/(a,b)}$
Given one point, moving $\frac{b}{(a,b)}$ on the x-coordinate to the right moves $\frac{a}{(a,b)}$ down on the y-coordinate by the properties of slope.
$(y - \frac{a}{(a,b)}) = -\frac{a}{(a,b)}/\frac{b}{(a,b)}(x + \frac{b}{(a,b)}) + \frac{c}{b}$
$\frac{6}{(6,15)} = 2 \wedge \frac{15}{(6,15)} = 5$
$6 \cdot (-3 + 5) + 15 \cdot (5 - 2) = 12 = 6 \cdot 2 = 12$
$\forall c, d \in \mathbb{Z}\{6 \cdot (-3 + 5c) + 15 \cdot (5 - 2d) = 12\}$

1.50 $\forall a, b\{31 \cdot (30 - 21a) + 21 \cdot (40 + 31b) = 1770\}$

1.51 $ax_0 + by_0 = c$ Premise
$a(x_0 + \frac{b}{(a,b)}) + b(y_0 - \frac{a}{(a,b)}) = ax_0 + \frac{ab}{(a,b)} + by_0 - \frac{ab}{(a,b)}$ Distributive property
$ax_0 + \frac{ab}{(a,b)} + by_0 - \frac{ab}{(a,b)} = ax_0 + by_0$ Commutative property
$a(x_0 + \frac{b}{(a,b)}) + y(y_0 - \frac{a}{(a,b)}) = c$ Substitution ∎

1.52 See 1.51 and 1.53

1.53

$ax + by = c$	
$(a,b)\|a \wedge (a,b)\|b$	Definition of GCD
$(a,b)\|c$	Theorem 1.40
$p(a,b) = c \wedge m(a,b) = a \wedge n(a,b) = b$	Definition of divides
$m = \frac{a}{(a,b)} \wedge n = \frac{b}{(a,b)}$	Algebra*
$(m,n) = 1$	Lemma
$mx + ny = p$	Algebra
$m(x+h) + n(y-k) = p$ for some $h, k \in \mathbb{Z}$	Let
$mx + mh + ny - nk = mx + ny$	Distributive
$mh = nk$	Algebra
$m\|mh \wedge m\|nk$	Definition of divides
$m\|k$	Theorem 1.41 (recall $(m,n) = 1$)
$k = mj$ for some $j \in \mathbb{Z}$	Definition of divides*
$mh = nmj$	Substitution
$h = nj$	Algebra*
$k = \frac{aj}{(a,b)} \wedge h = \frac{jb}{(a,b)}$	Substitution (steps with asterisks in them) ∎

1.54 $(24, 9) = 3$

$24 \cdot 1 + 9 \cdot 1 = 33$

$\forall x, y \in \mathbb{Z}\{24 \cdot (1 + 3n) + 9 \cdot (1 - 8m) = 33\}$

1.55 First without Diophantine equations:

Show that $k \cdot \gcd(a,b)$ is a common divisor	
$\gcd(a,b)\|a \wedge \gcd(a,b)\|b$	Definition of GCD
$m \cdot \gcd(a,b) = a$ for some m	
$n \cdot \gcd(a,b) = b$ for some n	Definition of divides
$km \cdot \gcd(a,b) = ka \wedge kn \cdot \gcd(a,b) = b$	Algebra
$k \cdot \gcd(a,b)\|a \wedge k \cdot \gcd(a,b)\|b$	Definition of divides
Show that $k \cdot \gcd(a,b)$ is the **greatest** common divisor by contradiction	
$h > k \cdot \gcd(a,b) \wedge h\|ka \wedge h\|kb$	Assume (for contradiction)
$h = k \cdot \gcd(a,b) \cdot j$ for some j	**Unjustified Step**
$(k \cdot \gcd(a,b) \cdot j)\|ka \wedge (k \cdot \gcd(a,b) \cdot j)\|kb$	Substitution
$mjk \cdot \gcd(a,b) = ka$ for some m	
$njk \cdot \gcd(a,b) = kb$ for some n	Definition of divides
$mj \cdot \gcd(a,b) = a \wedge nj \cdot \gcd(a,b) = b$	Algebra
$j \cdot \gcd(a,b)\|a \wedge j \cdot \gcd(a,b)\|b$	Definition of divides (contradicts GCD)
$\neg\exists h\{h > k \cdot \gcd(a,b) \wedge h\|ka \wedge h\|kb\}$	Contradiction ∎

The book doesn't give a very good definition of GCD. Let $\gcd(a,b) = c$ if and only if $a = mc$ for some $m \in \mathbb{Z}$ and, $b = nc$ for some $n \in \mathbb{Z}$, and (crucially) $\gcd(m,n) = 1$

$\gcd(a, b) = c$	Let
$a = cj \wedge b = ci$ for some $j, i \in \mathbb{Z}$	Revised definition of GCD
$\gcd(i, j) = 1$	Revised definition of GCD
$ka = kcj \wedge kb = kci$	Substitution
$\gcd(ka, kb) = kc$	Reivsed definition of GCD (referencing previous two steps)
$\gcd(ka, kb) = kc = k \cdot \gcd(a, b)$	Substitution ∎

1.56 Here is my definifion of LCM. Let $a = \gcd(a, b) \cdot h$ for some $h \in \mathbb{Z}$ and $b = \gcd(a, b) \cdot k$ for some $k \in \mathbb{Z}$. I define the LCM such that $\operatorname{lcm}(a, b) = hk \cdot \gcd(a, b)$

1.57

$a = h \cdot \gcd(a, b)$ for some $h \in \mathbb{Z}$	
$b = k \cdot \gcd(a, b)$ for some $k \in \mathbb{Z}$	Let
$\operatorname{lcm}(a, b) = hk \cdot \gcd(a, b)$	Definition of LCM
$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = hk \cdot \gcd(a, b) \cdot \gcd(a, b) = ab$	Substitution ∎

1.58

$\operatorname{lcm}(a, b) = ab$	Premise
$\operatorname{lcm}(a, b) = ab \cdot \gcd(a, b)$	Previous theorem
$ab \cdot \gcd(a, b) = ab$	Substitution
$\gcd(a, b) = 1$	Identity property ∎