

Sam Grayson's Notebook (with L^AT_EX)

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' ■
- 1.2 Let $d = -c$
 $a|(b + d)$ Theorem 1.1
 $a|(b - c)$ substitution ■
- 1.3 $ma = b$ Definition of 'divides'
 $na = c$ Definition of 'divides'
 $mana = bc$ Algebra
 $a|bc$ Definition of 'divides' ■
- 1.4 $mana = bc$ see last proof
 $a^2|bc$ Definition of 'divides' ■
- 1.5 If $a|b$ then $a|b^n$
 $b = ka$ Definition of 'divides'
 $b^n = (ka)^n = k k^{(n-1)} a^n$ Algebra
 $k|b^n$ Definition of 'divides' ■
- 1.6 $ka = b$ Definition of 'divides'
 $ack = bc$ Algebra
 $a|bc$ Definition of 'divides' ■
- 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 ■
 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' ■

- 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
 $a+c \equiv b+d \pmod{n}$ definition '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. $6 \equiv 2 \pmod{4}$
 $5 \equiv 1 \pmod{4}$

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

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

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

$$15. \quad 6^2 \equiv 2^2 \pmod{4}$$

$$16. \quad 6^3 \equiv 2^3 \pmod{4}$$

$$17. \quad 6^4 \equiv 2^4 \pmod{4}$$

$$18. \quad 6^k \equiv 2^k \pmod{4}$$

1.20 No

Consider the case where $n = 4$, $c = 0$, $a = 1$, 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 |
| | $3 (9b_k 10^{k-1})$ | Theorem 1.3 |
| | $3 (b - 9b_k 10^{k-1})$ | 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*':

$$\begin{array}{rcccccc}
 & & & & & b - b_k 9 10^{k-1} & = \\
 & & & & & b - b_k (10 - 1) 10^{k-1} & = \\
 & & & & & b + (-b_k 10 \cdot 10^{k-1} + b_k 1 10^{k-1}) & = \\
 & & & & & b + (-b_k 10^k + b_k 10^{k-1}) & = \\
 + & \begin{array}{cccccc} & b_k & & b_{k-1} & & b_{k-2} & \dots & b_0 \\ (-b_k) & & b_k & & 0 & \dots & 0 & \end{array} & = \\
 \hline
 & (b_k + b_{k-1}) & & b_{k-2} & \dots & b_0 & &
 \end{array}$$

| | | |
|------|--|-----------------------------------|
| 1.23 | $3 a$ | Premise (Base Case) |
| | $3 (b_k + b_{k-1} + \dots + b_0)$ | Assumption (Inductive Hypothesis) |
| | $3 9$ | Arithmetic |
| | $3 (b_k 9c)$ where c is k ones in a row | Theorem 1.3 |
| | $3 (b_k + b_{k-1} + \dots + b_0 + b_k 9c)$ | Theorem 1.2 |
| | $3 (b_k 10^k + b_{k-1} + \dots + b_0)$ | Algebra* |
| | $3 (a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_0 10^0)$ | Inductive Axiom |
| | $3 (a_k a_{k-1} \dots a_0)$ | Definition of digits ■ |

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

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

$$1.24 \quad 4|a \text{ if and only if } 4|(a_1 + a_3 + \dots)(a_0 + a_2 + a_4 + \dots)$$

$$1.25 \quad 1. \ m = nq + r \text{ where } m = 25, \ n = 7, \ q = 3, \text{ and } r = 4$$

$$2. \ m = 277, \ n = 4, \ q = 66, \text{ and } r = 1$$

$$3. \ m = 33, \ n = 11, \ q = 3, \ r = 0$$

$$4. \ m = 33, \ n = 45, \ q = 0, \ r = 33$$

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

$$r \geq n$$

Inequality over integers

$$\exists j \ni (r - n = j \wedge j \geq 0)$$

Property of inequalities

$$nq + r = m$$

Algebra (from definition of r)

$$nq + (n + j) = m$$

Algebra

$$n(q + 1) + j = m$$

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)

$$q \leq q + 1$$

Universal instantiation

$$\therefore r \geq 0$$

Contradiction

Proving q and r are integers:

(They all came from sets that are only integers.) $A \subset$

Stuff I learned

$$\mathbb{N} \subset \mathbb{Z}$$

$$a \in A$$

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)