Number Theory Notebook

Paul Schulze

January 22, 2021

1 Chapter 1

Divisibility and congruence

Theorem 1.1. *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Proof.

(1.1.1)	$\exists\, d_b \in \mathbb{Z} \ni b = a \cdot d_b$	because $a \mid b$
(1.1.2)	$\exists\, d_c \in \mathbb{Z} \ni c = a \cdot d_c$	because $a \mid c$
(1.1.3)	$b + c = a \cdot d_b + a \cdot d_c$	by (1.1.1) and (1.1.2)
(1.1.4)	$b + c = a \cdot (d_b + d_c)$	by distributive property
(1.1.5)	$d_b + d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
	$a \mid (b + c)$	by def'n of divides $\square$

Theorem 1.2. *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.*

Proof.

(1.2.1)	$\exists\, d_b \in \mathbb{Z} \ni b = a \cdot d_b$	because $a \mid b$
(1.2.2)	$\exists\, d_c \in \mathbb{Z} \ni c = a \cdot d_c$	because $a \mid c$
(1.2.3)	$b - c = a \cdot d_b - a \cdot d_c$	by (1.2.1) and (1.2.2)
(1.2.4)	$b - c = a \cdot (d_b - d_c)$	by distributive property
(1.2.5)	$d_b - d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
	$a \mid (b - c)$	by def'n of divides $\square$

Theorem 1.3. *Let a, b, and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid bc$.*

Proof.

(1.3.1)	$\exists\, d_b \in \mathbb{Z} \ni b = a \cdot d_b$	because $a \mid b$
(1.3.2)	$\exists\, d_c \in \mathbb{Z} \ni c = a \cdot d_c$	because $a \mid c$
(1.3.3)	$bc = (a \cdot d_b) \cdot (a \cdot d_c)$	by (1.3.1) and (1.3.2)
(1.3.4)	$bc = a \cdot (a \cdot d_b \cdot d_c)$	by associativity and commutativity
(1.3.5)	$a \cdot d_b \cdot d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
	$a \mid bc$	by def'n of divides $\square$

Question 1.4. *Can you weaken the hypothesis of the previous theorem and still prove the conclusion? Can you keep the same hypothesis, but replace the conclusion by the stronger conclusion that $a^2|bc$ and still prove the theorem?*

Yes. You can remove the $a|c$ condition to weaken the hypothesis, or with both $a|b$ and $a|c$ you can show $a^2|bc$.

Question 1.5. *Can you formulate your own conjecture along the lines of the above theorems and then prove it to make it your theorem?*

Yes.

Paul's Conjecture. *Let a, b, and c be integers. If $a|b$ and $a|c$, then $a^2|bc$.*

Proof. First, take lines (1.3.1) through (1.3.4) of the proof of Theorem 1.3. Then,

$d_b \cdot d_c \in \mathbb{Z}$	because $d_b \in \mathbb{Z}$ and $d_c \in \mathbb{Z}$
$a^2|bc$	by def'n of divides $\square$

Theorem 1.6. *Let a, b, and c be integers. If $a|b$, then $a|bc$.*

Proof.

(1.6.1)	$\exists d \in \mathbb{Z} \ni ad = b$	because $a|b$
(1.6.2)	$bc = adc$	by (1.6.1)
(1.6.3)	$dc \in \mathbb{Z}$	because $d \in \mathbb{Z}$ and $c \in \mathbb{Z}$
	$a|bc$	by def'n of divides $\square$

Exercise 1.7. *Answer each of the following questions, and prove that your answer is correct.*

1. *Is* $45 \equiv 9 \pmod 4$*?*
   Yes. $4 \cdot 9 = 36 = 45 - 9$.

2. *Is* $37 \equiv 2 \pmod 5$*?*
   Yes. $5 \cdot 7 = 35 = 37 - 2$.

3. *Is* $37 \equiv 3 \pmod 5$*?*
   No. $37 - 3 = 34$ which is not a multiple of 5.

4. *Is* $37 \equiv -3 \pmod 5$*?*
   Yes. $5 \cdot 8 = 40 = 37 - (-3)$.

Exercise 1.8. *For each of the following congruences, characterize all the integers m that satisfy that congruence.*

1. $m \equiv 0 \pmod 3$
   $m \in \{3z \mid z \in \mathbb{Z}\}$

2. $m \equiv 1 \pmod 3$
   $m \in \{3z + 1 \mid z \in \mathbb{Z}\}$

3. $m \equiv 2 \pmod 3$
   $m \in \{3z + 2 \mid z \in \mathbb{Z}\}$

4. $m \equiv 3 \pmod 3$
   $m \in \{3z \mid z \in \mathbb{Z}\}$

5. $m \equiv 4 \pmod 3$
   $m \in \{3z + 1 \mid z \in \mathbb{Z}\}$

Theorem 1.9. *Let a and n be integers with $n > 0$. Then $a \equiv a \pmod{n}$.*

Proof.

(1.9.1)	$0 \in \mathbb{Z}$	
(1.9.2)	$n \cdot 0 = 0$	
(1.9.3)	$n \mid 0$	By def'n of divides
(1.9.4)	$a - a = 0$	
(1.9.5)	$n \mid (a - a)$	By (1.9.3) and (1.9.4)
	$a \equiv a \pmod{n}$	By def'n of modular congruence $\square$

Theorem 1.10. *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*

Proof.

(1.10.1)	$a \equiv b \pmod{n}$	Given
(1.10.2)	$\exists d \in \mathbb{Z} \ni nd = a - b$	By def'n of modular congruence
(1.10.3)	$-1nd = -1 \cdot (a - b)$	By multiplicative property of equality
(1.10.4)	$n \cdot (-d) = b - a$	By various algebra
(1.10.5)	$-d \in \mathbb{Z}$	By multiplicative closure of $\mathbb{Z}$
(1.10.6)	$n \mid (b - a)$	By (1.10.4), (1.10.5)
	$b \equiv a \pmod{n}$	By def'n of modular congruence $\square$

Theorem 1.11. *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proof.

(1.11.1)	$n \mid a - b$	By $a \equiv b \pmod{n}$
(1.11.2)	$n \mid b - c$	By $b \equiv c \pmod{n}$
(1.11.3)	$\exists d_1 \in \mathbb{Z} \ni nd_1 = a - b$	By (1.11.1)
(1.11.4)	$\exists d_2 \in \mathbb{Z} \ni nd_2 = b - c$	By (1.11.2)
(1.11.5)	$nd_1 + nd_2 = (a - b) + (b - c)$	By additive property of equality
(1.11.6)	$n(d_1 + d_2) = a - c$	By various algebra
(1.11.7)	$d_1 + d_2 \in \mathbb{Z}$	By closure of integers under addition
(1.11.8)	$n \mid (a - c)$	By def'n of divides
	$a \equiv c \pmod{n}$	By def'n of modular congruence $\square$

Theorem 1.12. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.*

Proof.

(1.12.1)	$n \mid (a - b)$	By $a \equiv b \pmod{n}$
(1.12.2)	$\exists d_1 \in \mathbb{Z} \ni nd_1 = a - b$	By def'n divides
(1.12.3)	$n \mid (c - d)$	By $c \equiv d \pmod{n}$
(1.12.4)	$\exists d_2 \in \mathbb{Z} \ni nd_2 = c - d$	By def'n divides
(1.12.5)	$nd_1 + nd_2 = (a - b) + (c - d)$	By additive property of equality
(1.12.6)	$n \cdot (d_1 + d_2) = (a + c) - (b + d)$	By various algebra
(1.12.7)	$d_1 + d_2 \in \mathbb{Z}$	By additive closure of $\mathbb{Z}$
(1.12.8)	$n \mid ((a + c) - (b + d))$	By def'n of divides
	$a + c \equiv b + d \pmod{n}$	By def'n of modular congruence $\square$

Theorem 1.13. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.*

Proof. Notice $-c$ and $-d$ are integers, and $-c \equiv -d \pmod{n}$ (glossing over the proof of that for now). Then simply cite 1.12 and we're done. ☐

Theorem 1.14. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*

Proof.

(1.14.1)	$n \mid (a-b)$	By $a \equiv b \pmod{n}$
(1.14.2)	$\exists k_1 \in \mathbb{Z} \ni a - b = nk_1$	
(1.14.3)	$a = nk_1 + b$	
(1.14.4)	$n \mid (c-d)$	By $c \equiv d \pmod{n}$
(1.14.5)	$\exists k_2 \in \mathbb{Z} \ni c - d = nk_2$	
(1.14.6)	$c = nk_2 + d$	
(1.14.7)	$ac = (nk_1 + b)(nk_2 + d)$	By (1.14.3) and (1.14.6)
(1.14.8)	$ac = n^2 k_1 k_2 + nk_1 d + nk_2 b + bd$	
(1.14.9)	$ac - bd = n \cdot (nk_1 k_2 + k_1 d + k_2 b)$	
(1.14.10)	$n \mid (ac - bd)$	Since $nk_1 k_2 + k_1 d + k_2 b \in \mathbb{Z}$
	$ac \equiv bd \pmod{n}$	

☐

Exercise 1.15. *Let a, b, and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.*

Proof.

(1.15.1)	$a \equiv b \pmod{n}$	Given
(1.15.2)	$a \cdot a \equiv b \cdot b \pmod{n}$	1.14
	$a^2 \equiv b^2 \pmod{n}$	

☐

Exercise 1.16. *Let a, b, and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.*

Proof.

(1.16.1)	$a \equiv b \pmod{n}$	Given
(1.16.2)	$a^2 \equiv b^2 \pmod{n}$	1.15
(1.16.3)	$a \cdot a^2 \equiv b \cdot b^2 \pmod{n}$	By 1.14 on (1.16.1) and (1.16.2)
	$a^3 \equiv b^3 \pmod{n}$	

☐

Exercise 1.17. *Let a, b, k, and n be integers with $n > 0$ and $k > 1$. Show that if $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.*

Proof.

(1.17.1)	$a \equiv b \pmod{n}$	Given
(1.17.2)	$a^{k-1} \equiv b^{k-1} \pmod{n}$	1.15
(1.17.3)	$a \cdot a^{k-1} \equiv b \cdot b^{k-1} \pmod{n}$	By 1.14 on (1.17.1) and (1.17.2)
	$a^k \equiv b^k \pmod{n}$	

☐

Theorem 1.18. *Let a, b, k, and n be integers with $n > 0$ and $k > 0$. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$*

Proof. Our base case is 1.9. Our induction hypothesis is "a, b, k, and n are integers with $n > 0$ and $k > 1$ such that $\forall j \ni 0 < j < k$, we find $a^j \equiv b^j \pmod{n}$. Notice our induction hypothesis fulfills the criteria for 1.17, and in fact 1.17 covers our induction step. ☐

Exercise 1.19. *Illustrate each of Theorems 1.12 - 1.18 with an example using actual numbers*

1.12
$2 \equiv 12 \pmod 10$ and $5 \equiv 15 \pmod 10$ imply $7 \equiv 27 \pmod 10$.

1.13
$7 \equiv 27 \pmod 10$ and $12 \equiv 2 \pmod 10$ imply that $-5 \equiv 25 \pmod 10$.

1.14
$2 \equiv 7 \pmod 5$ and $3 \equiv 8 \pmod 5$ imply that $6 \equiv 56 \pmod 5$.

1.15
$2 \equiv 7 \pmod 5$ implies that $4 \equiv 49 \pmod 5$.

1.16
$1 \equiv 3 \pmod 2$ implies that $1 \equiv 27 \pmod 2$.

1.17
$1 \equiv 3 \pmod 2$ and $1 \equiv 27 \pmod 2$ imply that $1 \equiv 81 \pmod 2$.

1.18
$1 \equiv 3 \pmod 2$ implies that $1 \equiv 81 \pmod 2$.

Question 1.20. *Let a, b, c, and n be integers for which $ac \equiv bc \pmod n$. Can we conclude that $a \equiv b \pmod n$? If you answer "yes", try to give a proof. If you answer "no", try to give a counterexample.*

No. Notice $1 \cdot 0 \equiv 2 \cdot 0 \pmod 5$ and yet $1 \not\equiv 2 \pmod 5$.

Theorem 1.21. *Let a natural number n be expressed in base 10 as*

$$n = a_k a_{k-1} \dots a_1 a_0$$

If $m = a_k + a_{k-1} + \cdots + a_1 + a_0$ then $n \equiv m \pmod 3$.

First, a Lemma that will help us later.

Lemma 1.21.1. *Let a be an integer and j a natural number. Then $a \equiv a \cdot 10^j \pmod 3$.*

Proof. Notice that $1 \equiv 10 \pmod 3$. Then, by 1.18, we find $1^j \equiv 10^j \pmod 3$ and thus that $1 \equiv 10^j \pmod 3$. Then, since $a \equiv a \pmod 3$ (by 1.9), we invoke 1.14 to find $a \cdot 1 \equiv a \cdot 10^j \pmod 3$, implying that $a \equiv a \cdot 10^j \pmod 3$. $\square$

Now we begin our proof of the theorem in full.

Proof. Notice that n can be written as $a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$, or more easily as

$$n = \sum_{i=0}^{k} a_i \cdot 10^i$$

Now notice that

$$m = \sum_{i=0}^{k} a_i$$

By 1.21.1, we notice that $\forall i \; a_i \equiv a_i \cdot 10^i \pmod 3$. Thus, n and m are sums of terms that are congruent modulo 3. By repeatedly invoking 1.12, we eventually find that the two strings of congruent sums are themselves are congruent, i.e. that $n \equiv m \pmod 3$. $\square$

Theorem 1.22. *If a natural number is divisible by 3, then, when expressed in base 10, the sum of its digits is divisible by 3.*

Proof. Let the natural number be n, and the sum of its digits m. We're given by the theorem $n \equiv 0 \pmod 3$, and by 1.21 we know $n \equiv m \pmod 3$, so we can cite 1.11 and conclude $m \equiv 0 \pmod 3$, i.e. m is divisible by 3. $\square$

Theorem 1.23. *If the sum of the digits of a natural number expressed in base* 10 *is divisible by* 3*, then the number is divisible by* 3 *as well.*

Proof. Let the natural number be n, and the sum of its digits m. We're given by the theorem $m \equiv 0 \pmod 3$, and by 1.21 we know $n \equiv m \pmod 3$, so we can cite 1.11 and conclude $n \equiv 0 \pmod 3$, i.e. n is divisible by 3. $\square$

Exercise 1.24. *Devise and prove other divisibility criteria similar to the preceding one.*

A number is divisible by 2 if and only if its last digit is divisible by 2, because any (base 10) number $n = a_k a_{k-1} \dots a_1 a_0 = a_k a_{k-1} \dots a_1 \cdot 10 + a_0$, and $2|10$ so $2| \dots \cdot 10$. Thus, $2| \dots \cdot 10 + a_0$ iff $2|a_0$.

Similar proofs can be done for 5 and the last digit, 4 and the last 2 digits, 8 and the last 3 digits, 16 and the last 4 digits, 32 and the last 5 digits, etc.

The Division Algorithm

Exercise 1.25. *Illustrate the division algorithm for:*

1. $m = 25$, $n = 7$.
   $25 = 7 \cdot 3 + 4$.

2. $m = 277$, $n = 4$.
   $277 = 4 \cdot 69 + 1$.

3. $m = 33$, $n = 11$.
   $33 = 11 \cdot 3 + 0$.

4. $m = 33$, $n = 45$.
   $33 = 44 \cdot 0 + 33$.

Theorem 1.26. *Prove the existence part of the Division Algorithm. In other words, given natural numbers n and m, show their exist integers q and r such that $m = nq + r$ and $0 \leq r \leq n - 1$.*

Proof. Let $S = \{x \in \mathbb{Z} \mid nx > m\}$. By the Well-Ordering Axiom, S has a smallest element: call it s. Let $q = s - 1$. This definition gives us two important properties:

1. $nq \leq m$, for if $nq > m$ then $q \in S$ with $q < s$, which is impossible since s is the smallest element of S.

2. $m < n(q+1) = nq + n$, for $q + 1 = s$ and $sx > m$ because $s \in S$.

Now, we define $r = m - nq$, so that by definition $m = nq + r$. Since $nq \leq m$, we know $r \geq 0$. Since $m < nq + n$, and yet $m = nq + r$, implying $nq + r < nq + n \implies r < n \implies r \leq n - 1$.

Thus, we have found q, r such that $m = nq + r$ and $0 \leq r \leq n - 1$. $\square$

Theorem 1.27. *Prove the uniqueness part of the Division Algorithm. In other words, given natual numbers n and m, if there are 4 integers q, q', r, and r', such that $m = nq + r = nq' + r'$ with $0 \leq r, r' \leq n - 1$ then $q = q'$ and $r = r'$.*

Proof. Notice that $nq + r = nq' + r'$ implies that $nq - nq' = r' - r \implies n(q - q') = r' - r$.

Since $0 \leq r, r' \leq n - 1$, we conclude that $-n + 1 \leq r' - r \leq n - 1$. By our previous equality, then, $-n + 1 \leq n(q - q') \leq n - 1 \implies -n < n(q - q') < n$. Since n is a natural number, we can divide by n to get $-1 < q - q' < 1$. Since q and q' are integers, $q - q'$ must also be an integer. The only integer between -1 and 1 is 0, so we conclude $q - q' = 0 \implies q = q'$.

Once we have $q = q'$, we see that $nq + r = nq' + r' \implies nq + r = nq + r' \implies r = r'$. $\square$

Theorem 1.28. *Let a, b, and n be integers with $n > 0$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. Equivalently, $a \equiv b \pmod{n}$ if and only if when $a = nq_1 + r_1$ $(0 \leq r_1 \leq n-1)$ and $b = nq_2 + r_2$ $(0 \leq r_2 \leq n-1)$ then $r_1 = r_2$.*

First, we will show that $a \equiv b \pmod{n} \implies r_1 = r_2$.

Proof. Notice by the definition of modular congruence that $a \equiv b \pmod{n}$ implies that $n|(b-a)$, or $\exists d \in \mathbb{Z} \ni nd = b - a$. Using $a = nq_1 + r_1$ and $b = nq_2 + r_2$ we get $nd = nq_1 + r_1 - nq_2 - r_2 = n(q_1 - q_2) + r_1 - r_2$. Then we get $nd - n(q_1 - q_2) = r_1 - r_2$ or $n(d - q_1 + q_2) = r_1 - r_2$.

Since $0 \leq r_1, r_2 \leq n - 1$ we find that $-n + 1 \leq r_1 - r_2 \leq n - 1 \implies -n < r_1 - r_2 < n$. Using our previous equation with $r_1 - r_2$ we get that $-n < n(d - q_1 + q_2) < n$, and dividing by n (which we can do because $n > 0$) we get $-1 < d - q_1 + q_2 < 1$. Since d, q_1, and q_2 are all integers, $d - q_1 + q_2$ is also an integer, and the only integer between -1 and 1 is 0 so we find $d - q_1 + q_2 = 0$.

Plugging this back in to $n(d - q_1 + q_2) = r_1 - r_2$, we find $n \cdot 0 = r_1 - r_2$, which implies $0 = r_1 - r_2$, or $r_1 = r_2$. □

Second, we will show that $r_1 = r_2 \implies a \equiv b \pmod{n}$.

Proof. Notice $a - b = nq_1 + r_1 - (nq_2 + r_2)$. With some simple rearranging, we obtain $a - b = n(q_1 - q_2) + r_1 - r_2$. Since we know $r_1 = r_2$, we know $r_1 - r_2 = 0$, and plugging this in we obtain $a - b = n(q_1 - q_2)$.

Since q_1 and q_2 are integers, $q_1 - q_2$ is also an integer. Thus, n times some integer is $a - b$: in other words, $n|(a - b)$.

Then, by the definition of modular congruence, we obtain $a \equiv b \pmod{n}$. □

Greatest common divisors and linear Diophantine equations

Question 1.29. *Do every two integers have at least one common divisor?*

Yes. For any two integers a and b, $1 \cdot a = a$ and $1 \cdot b = b$ so $1|a$ and $1|b$, making 1 a common divsor of a and b.

Question 1.30. *Can two integers have infinitely many common divisors?*

No, if the two integers are distinct. Any nonzero integer n can only have finitely many divisors, as any integer d such that $d < -|n|$ or $d > |n|$ cannot be a divisor (since $1d$ and $-1d$ have a greater absolute value than n, and $0d = 0 \neq n$). In other words, only the numbers f such that $-n \leq f \leq n$ are "eligibile" to be divisors of n, so there can only be finitely many divisors of n.