# 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 $\qquad\square$ |

**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 $\qquad\square$ |

**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 $\qquad\square$ |

**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 $a^2 \mid bc$ and still prove the theorem?*

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

**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,

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

**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 $\qquad \square$ |

**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) | $n\vert 0$ | By def'n of divides |
| (1.9.4) | $a - a = 0$ | |
| (1.9.5) | $n\vert(a - a)$ | By (1.9.3) and (1.9.4) |
| | $a \equiv a \pmod{n}$ | By def'n of modular congruence $\qquad\square$ |

**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) | $n\vert(b - a)$ | By (1.10.4), (1.10.5) |
| | $b \equiv a \pmod{n}$ | By def'n of modular congruence $\qquad\square$ |

**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) | $n\vert a - b$ | By $a \equiv b \pmod{n}$ |
| (1.11.2) | $n\vert b - c$ | 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) | $n\vert(a - c)$ | By def'n of divides |
| | $a \equiv c \pmod{n}$ | By def'n of modular congruence $\qquad\square$ |

**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) | $n\vert(a - b)$ | 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) | $n\vert(c - d)$ | 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) | $n\vert\left((a + c) - (b + d)\right)$ | By def'n of divides |
| | $a + c \equiv b + d \pmod{n}$ | By def'n of modular congruence $\qquad\square$ |

**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. $\square$

**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 $nk_1 k_2 + k_1 d + k_2 b \in \mathbb{Z}$ |
| | $ac \equiv bd \pmod{n}$ | $\square$ |

**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 |
| | $a^2 \equiv b^2 \pmod{n}$ | $\square$ |

**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) |
| | $a^3 \equiv b^3 \pmod{n}$ | $\square$ |

**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) |
| | $a^k \equiv b^k \pmod{n}$ | $\square$ |

**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. $\square$

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

 1.12
  $2 \equiv 12 \pmod{1}0$ and $5 \equiv 15 \pmod{1}0$ imply $7 \equiv 27 \pmod{1}0$.

 1.13
  $7 \equiv 27 \pmod{1}0$ and $12 \equiv 2 \pmod{1}0$ imply that $-5 \equiv 25 \pmod{1}0$.

 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*

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

*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 $a \equiv a \cdot 10^j \pmod{3}$. □

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 $n \equiv m \pmod{3}$. □

**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. □

**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 $3$. $\qquad\square$

**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 $n = a_k a_{k-1} \ldots a_1 a_0 = a_k a_{k-1} \ldots a_1 \cdot 10 + a_0$, and $2|10$ so $2 | \ldots \cdot 10$. Thus, $2 | \ldots \cdot 10 + a_0$ 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 there 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 $0 \leq r \leq n - 1$. $\qquad\square$

**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 $nq + r = nq' + r' \implies nq + r = nq + r' \implies r = r'$. $\qquad\square$

**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 $r_1 = r_2$. $\square$

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 $a \equiv b \pmod{n}$. $\square$

## 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 $n$.

**Exercise 1.31.** *Find the following greatest common divisors. Which pairs are relatively prime?*

1. $(36, 22)$
   2

2. $(45, -15)$
   15

3. $(-296, -88)$
   8

4. $(0, 256)$
   256

5. $(15, 28)$
   1 (relatively prime)

6. $(1, -2436)$
   1 (relatively prime)

**Theorem 1.32.** *Let $a$, $n$, $b$, $r$, and $k$ be integers. If $a = nb + r$ and $k|a$ and $k|b$, then $k|r$.*

*Proof.* Let $a = d_a k$ and $b = d_b k$, where $d_a$ and $d_b$ are the integers guaranteed by the facts that $k|a$ and $k|b$. Then, we have $d_a k = n d_b k + r$. Isolating $r$, we get $r = d_a k - n d_b k = k(d_a - n d_b)$. Since $n$, $d_a$, and $d_b$ are all integers, we know $d_a - n d_b$ is an integer. Thus, we've found $r$ is equal to $k$ times some integer, so $k|r$. $\square$

**Theorem 1.33.** *Let $a$, $b$, $n_1$, and $r_1$ be integers with $a$ and $b$ not both $0$. If $a = n_1 b + r_1$, then $(a, b) = (b, r_1)$.*

*Proof.* We will show that the common divisors of $a$ and $b$ are the same as the common divisors of $b$ and $r_1$, and thus conclude that the greatest element of $S$ is also the greatest element of $T$.

Let $S$ be the set of common divisors of $a$ and $b$, and let $T$ be the set of common divisors of $b$ and $r_1$. We will show $S = T$ by double inclusion.

First, let's show $S \subset T$. Take an arbitrary $s \in S$. Since $s|a$ and $s|b$, we conclude $\exists d_a, d_b \in \mathbb{Z} \ni a = sd_a, b = sd_b$. We can then rearrange $a = n_1 b + r_1$ to read $r_1 = a - n_1 b$, and then plug in our previous two equations to get $r_1 = sd_a - n_1 sd_b \implies r_1 = s(d_a - n_1 d_b)$. Since $d_a$, $d_b$, and $n_1$ are all integers, we know $d_a - n_1 d_b$ is an integer, thus implying that $s|r_1$. Since we know $s|b$ since $s \in S$, we conclude $s \in T$. Thus, any arbitrary $s \in S$ is an element of $T$, so $S \subset T$.

Showing that $T \subset S$ proceeds in much the same way. Take $t \in T$, conclude since $t|b$ and $t|r_1$ we find $\exists d_b d_r \in \mathbb{Z} \ni b = td_b, r_1 = td_r$, and then plug those in to $a = n_1 b + r_1$ to get $a = n_1 td_b + td_r \implies a = t(n_1 d_b + d_r)$. Since $n_1$, $d_b$, and $d_r$ are integers, we find $t|a$, and since $t|b$ because $t \in T$, we thus conclude $t \in S$. Thus any arbitrary $t \in T$ is an element of $S$, so $T \subset S$.

Thus, by double inclusion, $S = T$. This implies that the greates element of $S$, i.e. $(a, b)$, is equal to the greatest element of $T$, i.e. $(b, r_1)$. $\qquad\square$

**Exercise 1.34.** *Use the preceding theorem to show that if $a = 51$ and $b = 15$, then $(51, 15) = (6, 3) = 3$.*

*Proof.* Since $51 = 3 \cdot 15 + 6$, we find $(51, 15)$, we cite 1.33 to see $(51, 15) = (15, 6)$. Then, since $15 = 2 \cdot 6 + 3$, we again cite 1.33 to find $(15, 6) = (6, 3)$. We see that $(6, 3) = 3$ by inspection. Then, since equality is transitive, we conclude $(51, 15) = (6, 3) = 3$. $\qquad\square$

**Exercise 1.35.** *Using the previous theorem and the Division Algorithm successively, devise a procedure for finding the greatest common divisor of two integers.*

Well you kind of gave the game away when you said to use 1.33 and the divsion algorithm successively huh. If you're trying to find $(a, b)$, you simply invoke the division algorithm to get $a = nb + r$ (assuming WLOG that $a \geq b$), and then rewrite $(a, b)$ as $(b, r)$. Then, you use the divion algorithm to get $b = nr + r'$, simplifying to $(r, r')$, etc. etc., until at some point you have $(x, 0)$, which by inspection is equal to $x$.

You will always reach $(x, 0)$ because the divison algorithm produces a remainder $r$ that is strictly less than the smaller input $b$, so (informally) the smaller of the two numbers you're working with always gets smaller while never going negative.

**Exercise 1.36.** *Use the Euclidean Algorithm to find the following.*

1. $(96, 112)$
   $112 = 1 \cdot 96 + 16$, simplifying the problem to $(96, 16)$. Then $96 = 5 \cdot 16 + 0$, so we get $(16, 0) = 16$

2. $(162, 31)$
   $162 = 5 \cdot 31 + 7 \implies (31, 7) \implies 31 = 4 \cdot 7 + 3 \implies (7, 3) \implies 7 = 2 \cdot 3 + 1 \implies (3, 1) = 1$.

3. $(0, 256)$
   Since everything divides $0$, this is trivially $256$.

4. $(-288, -166)$
   $-166 = 1 \cdot -288 + 122 \implies (-288, 122) \implies -288 = -3 \cdot 122 + 78 \implies (122, 78) \implies 122 = 1 \cdot 78 + 44 \implies (78, 44) \implies 78 = 1 \cdot 44 + 34 \implies (44, 34) \implies 44 = 1 \cdot 34 + 10 \implies (34, 10) = 2$ by inspection.

5. $(1, -2436)$
   Since the only integers that divide $1$ are $-1$, $0$, and $1$, we trivially find $1$.

**Exercise 1.37.** *Find integers $x$ and $y$ such that $162x + 31y = 1$.*

By division algorithm, $162 = 5 \cdot 31 + 7 \implies 7 = 1 \cdot 162 + (-5) \cdot 31$.

By division algorithm, $31 = 4 \cdot 7 + 3 \implies 3 = 1 \cdot 31 + (-4) \cdot 7 = 1 \cdot 31 + (-4) \cdot (1 \cdot 162 + (-5) \cdot 31) = (-4) \cdot 162 + 21 \cdot 31$.

By division algorithm, $7 = 2 \cdot 3 + 1 \implies 1 = 1 \cdot 7 + (-2) \cdot 3 = 1 \cdot (1 \cdot 162 + (-5) \cdot 31) + (-2) \cdot ((-4) \cdot 162 + 21 \cdot 31) = 9 \cdot 162 + (-47) \cdot 31$.

Thus, we've found our solution $x = 9$ and $y = -47$.

**Theorem 1.38.** *Let $a$ and $b$ be integers. If $(a, b) = 1$, then there exist integers $x$ and $y$ such that $ax + by = 1$.*

*Proof.* If either $a$ or $b$ is negative, replace it with $-a$ or $-b$ for the rest of this proof. At then end, you can replace either $x$ or $y$ with $-x$ or $-y$ to get an answer; for instance, if $a = -3$, we can replace $a = 3$, do the proof to obtain $x_0$ and $y_0$ such that $3x_0 + by_0 = 1$ and then realize that $(-3)(-x_0) + by_0 = 1$, which since $-x_0$ is still an integer still suffices. Now we will only be worrying about non-negative $a$ and $b$s.

We will demonstrate an algorithm to find $x$ and $y$. WLOG, assume $a \geq b$. Invoke the division algorithm to get $a = n_1 b + r_1$. Then invoke it agian to get $b = n_2 r_1 + r_2$. Then invoke it agian to get $r_1 = n_3 r_2 + r_3$. Etc. etc. etc.

We will show that the series "remainder" generated by this algorithm eventually has to hit 0: in other words, $\exists i \in \mathbb{N} \ni r_i = 0$. To do this, we must notice that for any index $j$, since $r_j$ is generated by calling the division algorithm on $r_{j-2}$ and $r_{j-1}$, we find that $r_j \leq r_{j-1} - 1$. Notice, then, that we can apply this to $r_{j-1}$ to obtain $r_{j-1} \leq r_{j-2} - 1$, and then plug that in to our previous inequality to get $r_j \leq r_{j-1} - 1 \leq r_{j-2} - 2$.

By inspection (i.e. I'm lazy and don't want to formalize this), we notice we can continually apply this. We will apply this to $r_b$, and notice that $r_b \leq r_{b-1} - 1 \leq r_{b-2} - 2 \leq \cdots \leq r_1 - (b-1) \leq b - b$. Since $b - b = 0$, we find $r_b \leq 0$, but since $r_b$ is a remainder from the division algorithm we know $r_b \geq 0$, so we conclude $r_b = 0$.

Notice we have *not* proven that $r_b$ is the *first* 0, only that the remainders must *eventually* reach 0 at *some* point.

Now, keep invoking the division algorithm until the "remainder" generated by the algorithm is 0: we will label that step $k + 1$, so that we find $r_{k-1} = n_{k+1} r_k + 0$. We will show that $r_k$ is 1.

By invoking 1.33 repeatedly, we find that $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = (r_k, r_{k+1})$. Since $r_{k+1} = 0$, we conclude $(a, b) = (r_k, 0)$. Since 0 divides everything, $(r_k, 0) = r_k$, so $(a, b) = r_k$, and since $a$ and $b$ are relatively prime we conclude $1 = r_k$.

Now, we take all of our equations and rewrite them to solve for the remainder. For example, $a = n_1 b + r_1$ becomes $r_1 = a + (-n_1)b$, and $b = n_2 r_1 + r_2$ becomes $r_2 = b + (-n_2)r_1$.

This gives us a bunch of equations of the form $r_j = \delta_j r_{j-2} + \gamma_j r_{j-1}$. This incldues one for $r_k$, namely $r_k = \delta_k r_{k-2} + \gamma_k r_{k-1}$. We can then substitute in lower indices of $r$ for $r_{k-2}$ and $r_{k-1}$, using the generic equation, to get something like $r_k = \delta_k(\delta_{k-2} r_{k-4} + \gamma_{k-2} r_{k-3}) + \gamma_k(\delta_{k-1} r_{k-3} + \gamma_{k-1} r_{k-2})$.

That looks horrifying, but the important bit is that we notice if we simplify it we get $r_k = A r_{k-4} + B r_{k-3} + C r_{k-2}$ with $A, B, C \in \mathbb{Z}$. That is, *by replacing all $r_j$'s with their respective equations, we have reduced the highest index on an $r$ in the right hand side by* 1. Previously, the highest index was $k - 1$, but now it's $k - 2$, because we had an equation to represent $r_{k-1}$ in terms of $r_{k-3}$ and $r_{k-4}$.

Notice, though, that not all $r$'s satisfy this property: namely, $r_1$ and $r_2$ simplify down to $a$ and $b$, which then don't have equations of their own. So, we apply the equations for $r_k$ through $r_1$ in "reverse" order, pairing down the maximum index of $k$ each time, until we're left with only $r_1$'s and $r_2$'s on the left hand side and can apply those equations to get a linear expression in $a$ and $b$ on the right hand side.

We've been talking a lot about the right hand side, but remember, the left hand side is $r_k$, and we've shown $r_k = 1$, so we've just found a linear expression in $a$ and $b$ that is equal to 1. In other words, $1 = ax + by$ for some $x, y \in \mathbb{Z}$. □

**Theorem 1.39.** *Let $a$ and $b$ be integers. If there exist integers $x$ and $y$ with $ax + by = 1$, then $(a, b) = 1$.*

*Proof.* Readers of the last proof will be glad to hear this one is much simpler.

By definition, $(a, b)|a$ and $(a, b)|b$. Then, $(a, b)|ax$ and $(a, b)|by$ by 1.6. Then, $(a, b)|ax + by$ by 1.1. Then, since $ax + by = 1$, we find $(a, b)|1$. We know $1|a$ and $1|b$, so $(a, b) \geq 1$. The only number $\geq 1$ that divides 1 is 1, so since $(a, b) \geq 1$ and $(a, b)|1$ we conclude $(a, b) = 1$. □

**Theorem 1.40.** *For any integers $a$ and $b$ not both 0, there are integers $x$ and $y$ such that $ax + by = (a, b)$.*

*Proof.* Let $c = a/(a, b)$ and $d = b/(a, b)$. Notice that since $(c, d)|c$ and $a = c \cdot (a, b)$ we find $((c, d) \cdot (a, b))|a$, and similarly since $(c, d)|d$ and $b = d \cdot (a, b)$ we find $((c, d) \cdot (a, b))|b$.

Since $c$ and $d$ are integers not both 0, $(c, d)$ must be a positive integer. Since $(c, d) \cdot (a, b)$ is a common factor of $a$ and $b$, and $(a, b)$ is the *greatest* common factor of $a$ and $b$, we find $(c, d) \cdot (a, b) \leq (a, b) \implies (c, d) = 1$.

Thus, we invoke 1.38 to find integers $x$ and $y$ such that $cx + dy = 1$. Then, we multiply both sides by $(a, b)$ to find that $(a, b) \cdot cx + (a, b) \cdot dy = (a, b)$. Since $a = (a, b) \cdot c$ and $b = (a, b) \cdot d$ we conclude $ax + by = (a, b)$. □