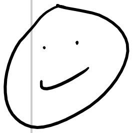


# Section 1: Modular Arithmetic

HW # 1-4 p. 13 at the end of the notes

In this section, we discuss the basics of rings and fields. As we will see, the most basic number systems that we are accustomed to working with are examples of rings and fields. First, we review some basic set notation and then the basics of modular arithmetic.

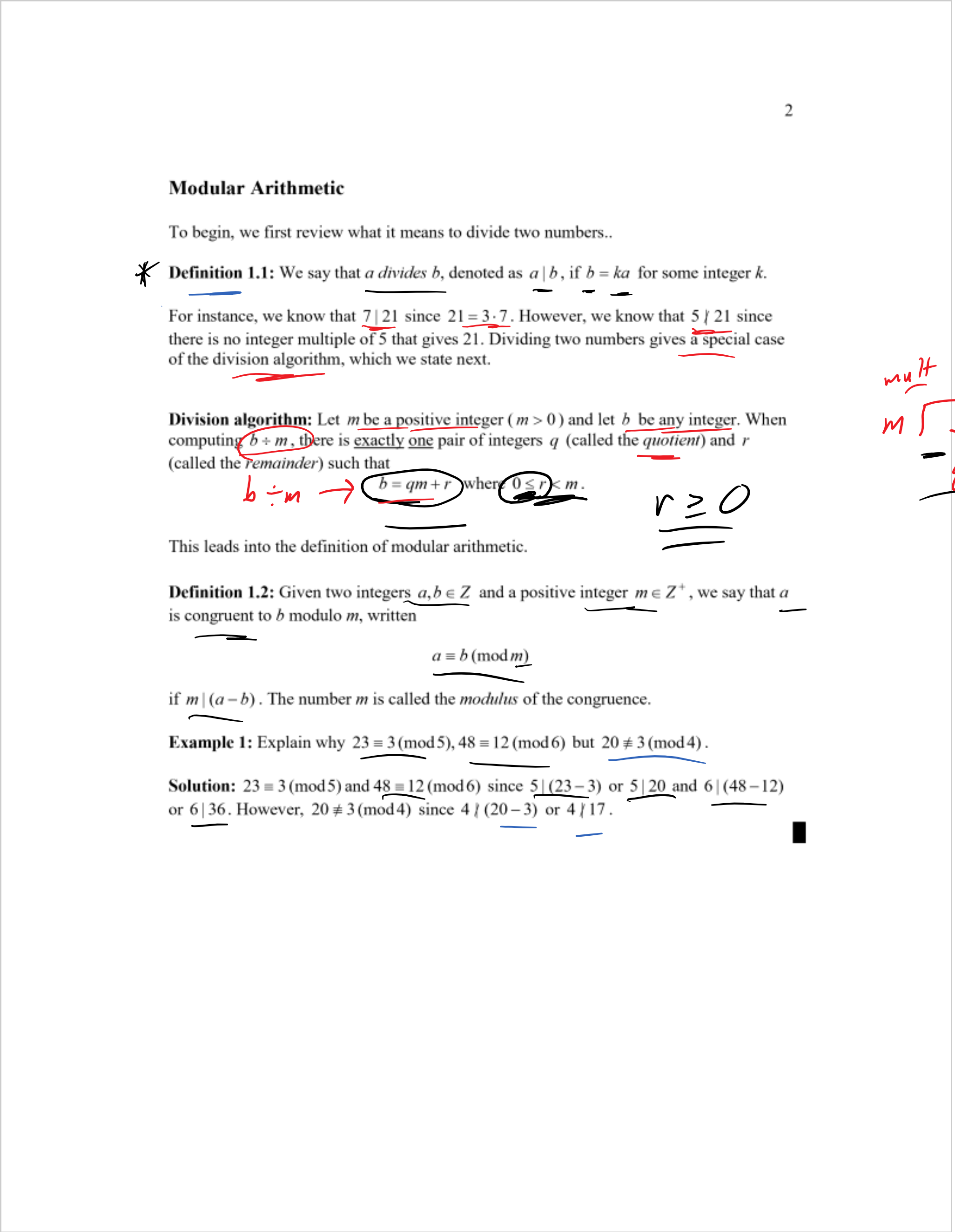
## Notation for Special Sets

Recall that a set is a collection of objects enclosed in braces. The objects in the sets are call *elements*. If $a$ is an element of a set, we write $a \in S$. For example, $2 \in \{1, 2, 3, 4\}$ but $5 \notin \{1, 2, 3, 4\}$. Sets can have both a finite and an infinite number of elements. The following represents special notations that are used for widely known infinite sets.

Notation for Special Sets

1. $Z$ = the set of integers $\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$
2. $Q$ = the set of rational numbers (numbers that can be expressed as the quotient $\frac{m}{n}$ of two integers $m$ and $n$, where $n \neq 0$.
3. $\mathrm{R}$ = the set of real numbers.
4. $Z^+, Q^+$, and $\mathrm{R}^+$ represent the set of positive integers, positive rational numbers, and positive real numbers, respectively. For example, $Z^+ = \{1, 2, 3, 4, 5, 6, \ldots\}$.
5. $\mathrm{C}$ = the set of complex numbers, that is, numbers of the form $a + bi$, were $i$ is the imaginary unit given by $i = \sqrt{-1}$. Examples of the complex numbers include $2 + 3i$ and $4 - \frac{3}{2} i$.
6. $Z^*, Q^*$, $\mathrm{R}^*$, and $\mathrm{C}^*$ represent the set of non-zero integers, non-zero rational numbers, non-zero real numbers, and non-zero complex numbers, respectively. For example, $Z^* = \{\ldots, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, \ldots\}$.
7. $M_n(\mathrm{R})$ represent the set of $n \times n$ matrices with real entries. The matrices

$$\begin{bmatrix} 3 & -3 & 0 \\ 3 & -6 & 1 \\ -1 & 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & -1 \\ 2 & 3 \end{bmatrix} \text{ are examples.}$$



## Modular Arithmetic

To begin, we first review what it means to divide two numbers..

* **Definition 1.1:** We say that *a divides b*, denoted as $a \mid b$, if $b = ka$ for some integer *k*.

For instance, we know that $7 \mid 21$ since $21 = 3 \cdot 7$. However, we know that $5 \nmid 21$ since there is no integer multiple of 5 that gives 21. Dividing two numbers gives a special case of the division algorithm, which we state next.

**Division algorithm:** Let $m$ be a positive integer ($m > 0$) and let $b$ be any integer. When computing $b \div m$, there is exactly one pair of integers $q$ (called the *quotient*) and $r$ (called the *remainder*) such that

$$b \div m \rightarrow \boxed{b = qm + r} \text{ where } \boxed{0 \le r} < m.$$

$r \ge 0$

This leads into the definition of modular arithmetic.

**Definition 1.2:** Given two integers $a, b \in Z$ and a positive integer $m \in Z^+$, we say that $a$ is congruent to $b$ modulo $m$, written

$$a \equiv b \pmod{m}$$

if $m \mid (a - b)$. The number $m$ is called the *modulus* of the congruence.

**Example 1:** Explain why $23 \equiv 3 \pmod 5$, $48 \equiv 12 \pmod 6$ but $20 \not\equiv 3 \pmod 4$.

**Solution:** $23 \equiv 3 \pmod 5$ and $48 \equiv 12 \pmod 6$ since $5 \mid (23 - 3)$ or $5 \mid 20$ and $6 \mid (48 - 12)$ or $6 \mid 36$. However, $20 \not\equiv 3 \pmod 4$ since $4 \nmid (20 - 3)$ or $4 \nmid 17$. ∎

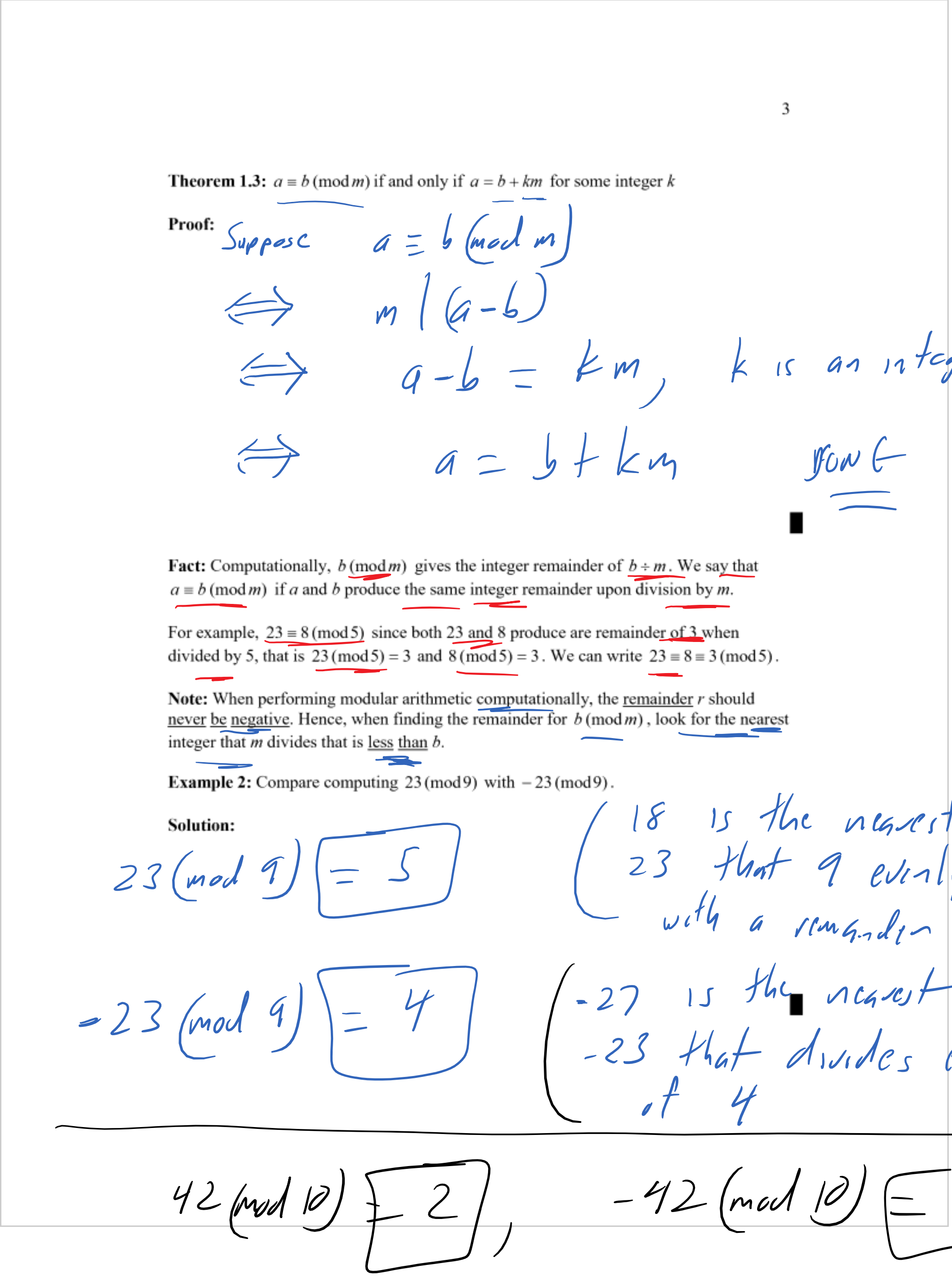
mult

$$\begin{array}{r|l} & q \\ \hline m & b \\ & -qm \\ \hline & r \end{array}$$

$b = qm + r$

$r = b - qm$

$r < m$



**Theorem 1.3:** $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some integer $k$

**Proof:** Suppose $a \equiv b \pmod{m}$

$\Longleftrightarrow \quad m \mid (a-b)$

$\Longleftrightarrow \quad a - b = km$, k is an integer (Definition of Divisibility)

$\Longleftrightarrow \quad a = b + km$ DONE

∎

**Fact:** Computationally, $b \pmod{m}$ gives the integer remainder of $b \div m$. We say that $a \equiv b \pmod{m}$ if $a$ and $b$ produce the same integer remainder upon division by $m$.

For example, $23 \equiv 8 \pmod{5}$ since both 23 and 8 produce are remainder of 3 when divided by 5, that is $23 \pmod{5} = 3$ and $8 \pmod{5} = 3$. We can write $23 \equiv 8 \equiv 3 \pmod{5}$.

**Note:** When performing modular arithmetic computationally, the remainder $r$ should never be negative. Hence, when finding the remainder for $b \pmod{m}$, look for the nearest integer that $m$ divides that is less than $b$.

**Example 2:** Compare computing $23 \pmod{9}$ with $-23 \pmod{9}$.

**Solution:**

$23 \pmod{9} \boxed{= 5}$

(18 is the nearest integer less than 23 that 9 evenly divides ($9 \cdot 2 = 18$) with a remainder of 5)

$-23 \pmod{9} \boxed{= 4}$

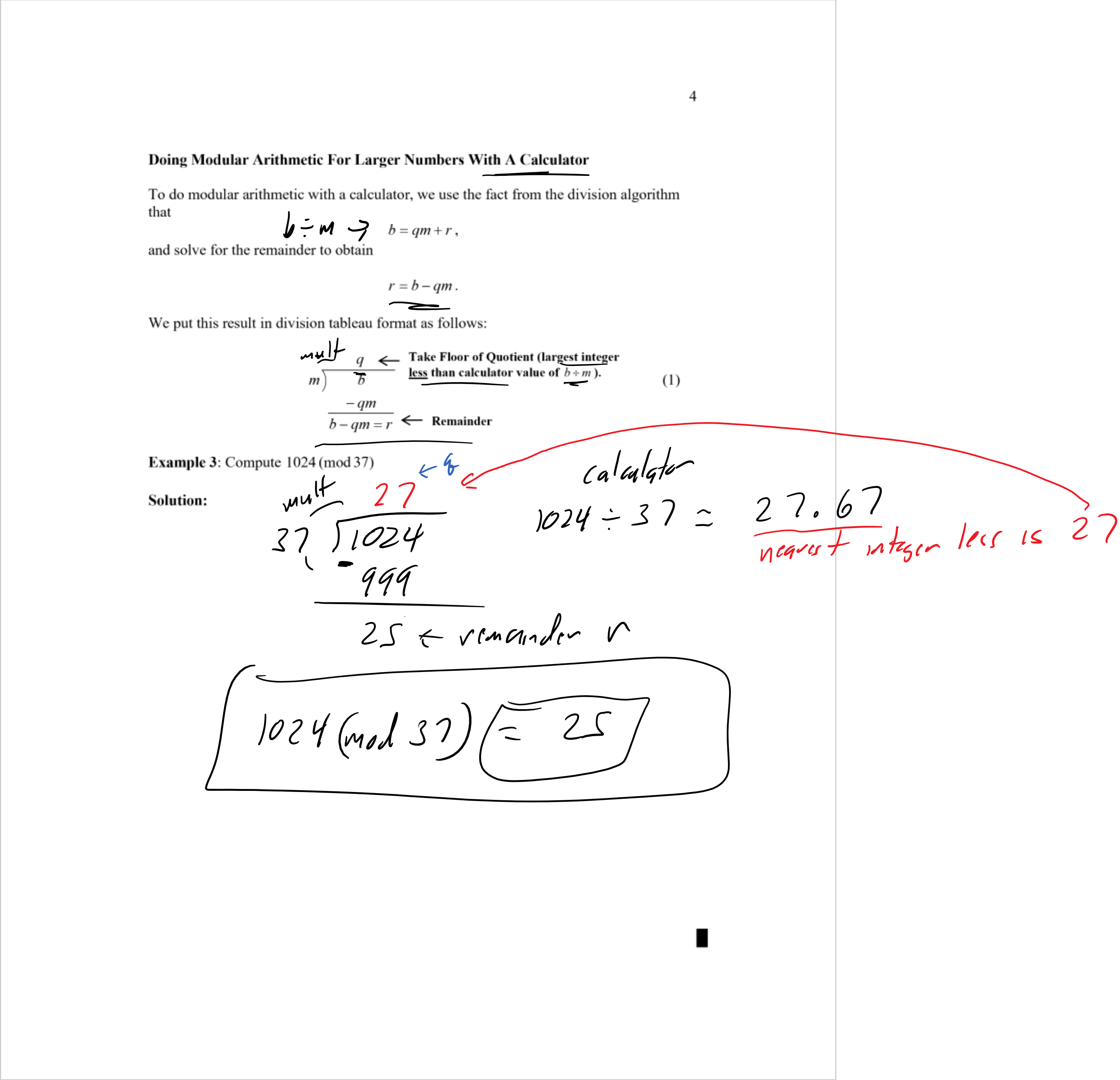
(-27 is the nearest integer less than -23 that divides evenly with a remainder of 4)

---

$42 \pmod{10} \boxed{= 2}$, $\quad -42 \pmod{10} \boxed{= 8}$

# Page 4

Tuesday, August 18, 2020 5:50 PM



**Doing Modular Arithmetic For Larger Numbers With A Calculator**

To do modular arithmetic with a calculator, we use the fact from the division algorithm that

$$b \div m \rightarrow \quad b = qm + r\,,$$

and solve for the remainder to obtain

$$r = b - qm\,.$$

We put this result in division tableau format as follows:

$$\begin{array}{rl} \text{mult} & q \\ m\,\big) & b \\ & -qm \\ \hline & b - qm = r \end{array}$$

← **Take Floor of Quotient (largest integer less than calculator value of $b \div m$).** (1)

← **Remainder**

**Example 3**: Compute 1024 (mod 37)

**Solution:**

$$\begin{array}{rl} \text{mult} & 27 \leftarrow q \\ 37\,\big) & 1024 \\ & -999 \\ \hline & 25 \leftarrow \text{remainder } r \end{array}$$

calculator

$1024 \div 37 \simeq 27.67$

nearest integer less is 27

$$\boxed{1024 \pmod{37} \equiv 25}$$

**Example 4:** Compute $500234 \pmod{10301}$

**Solution:** Using a calculator, we obtain $\dfrac{500234}{10301} \approx 48.6$. The largest integer less than 48.6 is 48. Hence, we assign $q = floor(48.6) = 48$. If we let $b = 500234$ and $m = 10301$ in (2), then

$$\begin{array}{r|l} & \underline{\;\;48\;\;\;\;\;} \\ 10301 & 500234 \quad . \\ & \underline{-494448} \\ & 5786 \end{array}$$

The remainder of the division is $r = 5786$. Hence, $500234 \pmod{10301} = 5786$. ■

**Example 5:** Compute $-3071 \pmod{107}$

**Solution:** Using a calculator, we obtain $\dfrac{-3071}{107} \approx -28.7$. The largest integer less than $-28.7$ is $-29$. Hence, we assign $q = floor(-28.7) = -29$. If we let $b = -3071$ and $m = 107$ in (2), then

mult

$$\begin{array}{r|r} & \underline{-29} \\ 107 & -3071 \\ & \oplus \\ & \underline{--3103} \\ & 32 \end{array}$$

Thus, $-3071 \pmod{107} = 32$ ■

## Generalization of Modular Arithmetic

**Fact:** The common remainder of two numbers have when they are divided can be used to define a *congruence* class. The remainder $r$ will be the smallest positive integer in the congruence class. Suppose $r$ is the remainder of $x$ divided by $m$, that is

$$x \equiv r \pmod{m}.$$

Theorem 1 says that then

$$x = r + km \text{, where } k \text{ is an integer.}$$

Page 6

Tuesday, August 18, 2020 5:50 PM

$-3 \equiv 25 \equiv 11 \equiv 32 \equiv 4 \pmod 7$

**Example 6:** Find all elements of the congruence class $x \equiv 4 \pmod 7$.

**Solution:** $x = 4 + 7k$, $k$ is an integer

$k = 1 \rightarrow x = 4 + 7(1) = 11$

$k = 2 \rightarrow x = 4 + 7(2) = 18$

$k = -1 \rightarrow x = 4 + 7(-1) = -3$

$\bar{4} = \{\dots, -17, -10, -3, \overset{+7}{4}, \overset{+7}{11}, \overset{+7}{18}, \overset{+7}{25}, 32, \dots\}$

set of integers having a remainder of 4 when divided by 7.

■

**Example 7** Find congruence class $\bar{2}$ modulo 7.

**Solution:**

$$\bar{2} = \{\dots, -19, -12, -5, \overset{+7}{2}, \overset{+7}{9}, 16, 23, 30, \dots\}$$

■

**Note:** For $x \equiv b \pmod 7$, the set of distinct congruence classes are $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$, $\bar{5}$, and $\bar{6}$. This partitions the integers $Z$ into disjoint subsets.

**Fact:** Given $x \equiv b \pmod m$, $Z$ can be partitioned into distinct congruence classes of the form

$$\left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots \overline{m-1}\right\}$$

**Definition 3:** We define the set of integers modulo $m$, denoted by $Z_m$, as the set

$$Z_m = \{0, 1, 2, 3, \dots m-1\}$$

For example, $Z_6 = \{0, 1, 2, 3, 4, 5\}$ and $Z_{50} = \{0, 1, 2, 3, \dots 49\}$. Informally, $Z_m$ represents all for the possible integer remainders in modulo $m$ arithmetic. This set will be important when we study later concepts.

## The Greatest Common Divisor of Two Numbers

The greatest common divisor of two numbers, denoted as gcd(*a*,*b*), is the largest number that divides *a* and *b* evenly with no remainder. For example, gcd(10, 20). = 10 and gcd(72, 108) = 36. Find the greatest common division of two numbers becomes more difficult is the numbers become larger. However, there is a well known method known as the Euclidean algorithm that will allows us to find the greatest common divisor of larger numbers which we state next.

### The Euclidean Algorithm

The Euclidean Algorithm makes repeated use of the division algorithm to find the greatest common divisor of two positive integers. If we are given two positive integers *a* and *b* where $a \geq b$, then if $b \mid a$, then $\gcd(a,b) = b$, If $b \nmid a$, then we compute

$$
\begin{array}{rl}
a \div b \rightarrow & a = q_1 b + r_1 \\
b \div r_1 \rightarrow & b = q_2 r_1 + r_2 \\
r_1 \div r_2 \rightarrow & r_1 = q_3 r_2 + r_3 \\
 & r_2 = q_4 r_3 + r_4 \\
 & \vdots \\
 & r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \\
 & r_{n-2} = q_n r_{n-1} + \boxed{r_n} \leftarrow \gcd(a,b) \\
 & r_{n-1} = q_{n+1} r_n + 0
\end{array}
$$

Never Shifted Quotients!

The last nonzero remainder, $r_n$, is the greatest common divisor of *a* and *b*, that is, $\gcd(a,b) = r_n$.

**Note:** In general, we can write each equation of the Euclidean Algorithm Table as

$$r_{i-1} = q_{i+1}\, r_i + r_{i+1}$$

Here, we can assign $r_{-1} = a$ and $r_0 = b$.

Euclidean Alg

Never Shift Quotients!

**Example 8:** Find the greatest common divisor of $a = 2299$ and $b = 627$.

**Solution:** $a > b$, start with $a \div b$

$$2299 = \overset{q}{\underline{3}} \cdot 627 + \overset{r}{\underline{418}}$$

$$627 = \underline{1} \cdot 418 + \underline{209} \leftarrow \text{GCD last non-zero remainder}$$

$$418 = \underline{2} \cdot 209 + \underline{0}$$

$$\boxed{\gcd(2299, 627) = 209}$$

■

$2299 \div 627 \approx 3.\underline{67}$

$$\begin{array}{r} 3 \leftarrow q \\ 627 \overline{)\,2299} \\ -1881 \\ \hline 418 \leftarrow r \end{array}$$

$$\begin{array}{r} 1 \leftarrow q \\ 418 \overline{)\,627} \\ -418 \\ \hline 209 \leftarrow r \end{array}$$

**Example 9:** Find the greatest common divisor of $a = 54321$ and $b = 9875$.

**Solution:** Noting that $54321 > 9875$ and applying the Euclidean algorithm gives

$$\begin{aligned} 54321 &= \overset{q}{5} \cdot 9875 + \overset{r}{4946} \\ 9875 &= 1 \cdot 4946 + 4929 \\ 4946 &= 1 \cdot 4929 + 17 \\ 4929 &= 289 \cdot 17 + 16 \\ 17 &= 1 \cdot 16 + \boxed{1} \leftarrow \gcd(54321, 9875) \\ 16 &= 1 \cdot 16 + 0 \end{aligned}$$

Since the last non-zero remainder is 1, gcd(54321, 9875)= 1.

■

$$\begin{array}{r} 5 \\ 9875 \overline{)\,54321} \\ -49375 \\ \hline 4946 \leftarrow r \end{array}$$

$a = 9875$, $b = 54321$

$$9875 = \underline{0} \cdot 54321 + \underline{9875}$$

$$54321 = \underline{\quad} \cdot 9875 + \underline{\quad}$$

$$\begin{array}{r} 0 \\ 54321 \overline{)\,9875} \\ 0 \\ \hline 9875 \end{array}$$

**Theorem 1.4:** For any two positive integers *a* and *b*, there are integers *u* and *v* where

$$au + bv = \gcd(a,b)$$

**Fact:** When executing the Euclidean algorithm equations,

$$\begin{aligned}
a &= q_1 b + r_1\\
b &= q_2 r_1 + r_2\\
r_1 &= q_3 r_2 + r_3\\
r_2 &= q_4 r_3 + r_4\\
&\vdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}\\
r_{n-2} &= q_n r_{n-1} + r_n\\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

We can create a table to determine the $\gcd(a,b) = r_n$, $u$, and $v$ as follows:

| **Row** | **Q** | **R** | **U** | **V** |
|---|---|---|---|---|
| $-1$ | $--$ | $a$ | $u_{-1} = 1$ | $v_{-1} = 0$ |
| $0$ | $--$ | $b$ | $u_0 = 0$ | $v_0 = 1$ |
| $1$ | $q_1$ | $r_1$ | $u_1$ | $v_1$ |
| $2$ | $q_2$ | $r_2$ | $u_2$ | $v_2$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $i$ | $q_i$ | $r_i$ | $u_i$ | $v_i$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $n$ | $q_n$ | $r_n$ | $u_n$ | $v_n$ |

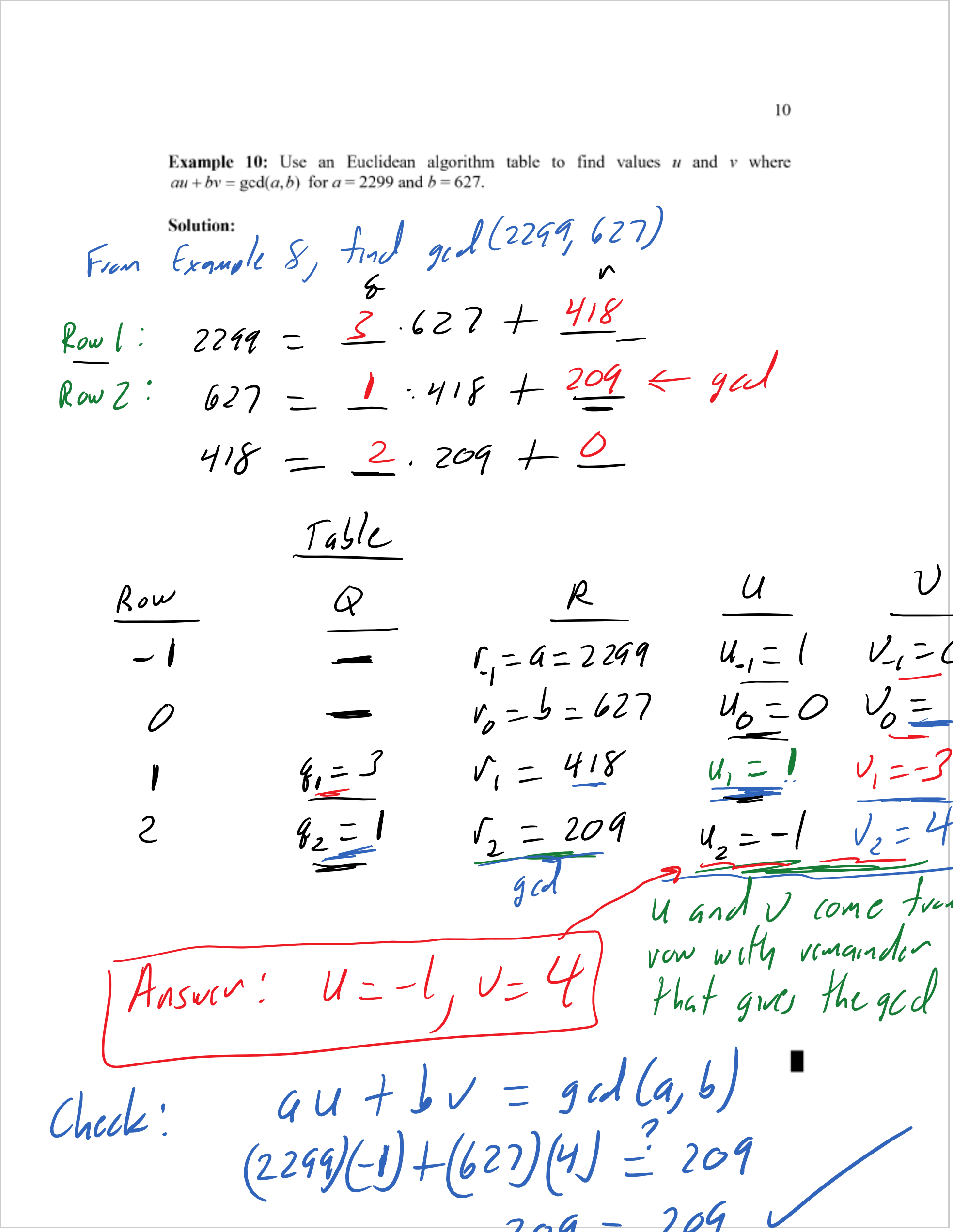
→ identity matrix $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

<u>**Notes**</u>

1. The quotients under **Q** and remainders under **R** are computed using the basic Euclidean algorithm process. The table is complete when $r_{n+1} = 0$. The last non-zero remainder $r_n$ is the greatest common divisor of *a* and *b*, that is, $\gcd(a,b) = r_n$.
2. The $u_i$'s under **U** and $v_i$'s under **V** are found using the formulas
$$\begin{aligned}u_{i+1} &= u_{i-1} - q_{i+1}\,u_i\\ v_{i+1} &= v_{i-1} - q_{i+1}\,v_i\end{aligned}$$
3. For row *i*, we have $au_i + bv_i = r_i$. The values *u* and *v* where $au + bv = \gcd(a,b)$ are found in the last row where $au_n + bv_n = r_n = \gcd(a,b)$. That is, $u = u_n$ and $v = v_n$.

Page 10

Tuesday, August 18, 2020 5:50 PM



**Example 10:** Use an Euclidean algorithm table to find values $u$ and $v$ where $au + bv = \gcd(a,b)$ for $a = 2299$ and $b = 627$.

**Solution:**

From Example 8, find gcd(2299, 627)

Row 1: $2299 = \underset{}{\overset{q}{\underline{3}}} \cdot 627 + \overset{r}{\underline{418}}$

Row 2: $627 = \underline{1} \cdot 418 + \underline{209}$ ← gcd

$418 = \underline{2} \cdot 209 + \underline{0}$

Table

| Row | Q | R | U | V |
|---|---|---|---|---|
| $-1$ | — | $r_{-1} = a = 2299$ | $u_{-1} = 1$ | $v_{-1} = 0$ |
| $0$ | — | $r_0 = b = 627$ | $u_0 = 0$ | $v_0 = 1$ |
| $1$ | $q_1 = 3$ | $r_1 = 418$ | $u_1 = 1$ | $v_1 = -3$ |
| $2$ | $q_2 = 1$ | $r_2 = 209$<br>gcd | $u_2 = -1$ | $v_2 = 4$ |

u and v come from row with remainder that gives the gcd

$$\boxed{\text{Answer: } u = -1,\ v = 4}$$

Check: $au + bv = \gcd(a,b)$

$(2299)(-1) + (627)(4) \overset{?}{=} 209$

$209 = 209$ ✓

$u$'s: $u_{i+1} = u_{i-1} - q_{i+1} u_i$

$u_1 = u_{-1} - q_1 \cdot u_0$

$u_1 = 1 - 3 \cdot 0$

$u_1 = 1 - 0 = 1$

$u_2 = u_0 - q_2 u_1$

$u_2 = 0 - 1 \cdot 1$

$u_2 = 0 - 1 = -1$

$v$'s $v_{i+1} = v_{i-1} - q_{i+1} v_i$

$v_1 = v_{-1} - q_1 v_0$

$v_1 = 0 - 3 \cdot 1 = -3$

$v_2 = v_0 - q_2 v_1$

$v_2 = 1 - 1 \cdot (-3)$

$v_2 = 1 + 3 = 4$

**Example 11:** Use an Euclidean algorithm table to find values $u$ and $v$ where $au + bv = \gcd(a,b)$ for $a = 54321$ and $b = 9875$.

**Solution:** From Example 9, we ran the Euclidean Algorithm to find that $\gcd(54321,\ 9875) = 1$ using the following process:

$$
\begin{aligned}
&\textbf{Row 1:} & 54321 &= \overset{q}{5} \cdot 9875 + \overset{r}{4946} \\
&\textbf{Row 2:} & 9875 &= 1 \cdot 4946 + 4929 \\
&\textbf{Row 3:} & 4946 &= 1 \cdot 4929 + 17 \\
&\textbf{Row 4:} & 4929 &= 289 \cdot 17 + 16 \\
&\textbf{Row 5:} & 17 &= 1 \cdot 16 + 1 \leftarrow \text{gcd} \\
& & 16 &= 16 \cdot 1 + 0
\end{aligned}
$$

$q_1 = 5, \quad r_1 = 4946$

$q_2 = 1, \quad r_2 = 4929$

Hence, the $\gcd(54321, 9875) = 1$. Setting $u_{-1} = 1, v_{-1} = 0$ and $u_0 = 0$ and $v_0 = 1$ and using the equations

$$u_{i+1} = u_{i-1} - q_{i+1}\, u_i, \quad v_{i+1} = v_{i-1} - q_{i+1}\, v_i$$

gives the following calculation for each row.

**Row 1:** $q_1 = 5, r_1 = 4946$, $u_1 = u_{-1} - q_1 u_0 = 1 - 5 \cdot 0 = 1 - 0 = 1$, $v_1 = v_{-1} - q_1 v_0 = 0 - 5 \cdot 1 = 0 - 5 = -5$.

**Row 2:** $q_2 = 1, r_2 = 4929$, $u_2 = u_0 - q_2 u_1 = 0 - 1 \cdot 1 = 0 - 1 = -1$, $v_2 = v_0 - q_2 v_1 = 1 - 1 \cdot (-5) = 1 + 5 = 6$.

**Row 3:** $q_3 = 1, r_3 = 17$, $u_3 = u_1 - q_3 u_2 = 1 - 1 \cdot (-1) = 1 + 1 = 2$, $v_3 = v_1 - q_3 v_2 = -5 - 1 \cdot 6 = -5 - 6 = -11$.

**Row 4:** $q_4 = 289, r_4 = 16$, $u_4 = u_2 - q_4 u_3 = -1 - 289 \cdot 2 = -1 - 579 = -579$,
$v_4 = v_2 - q_4 v_3 = 6 - 289 \cdot (-11) = 6 + 3179 = 3185$.

**Row 5:** $q_5 = 1, r_5 = 1$, $u_5 = u_3 - q_5 u_4 = 2 - 1 \cdot (-579) = 2 + 579 = 581$,
$v_5 = v_3 - q_5 v_4 = -11 - 1 \cdot 3185 = -11 - 3185 = -3196$.

The previous results give the following Euclidean Algorithm Table:

| **Row** | **Q** | **R** | **U** | **V** |
|---|---|---|---|---|
| $-1$ | $--$ | $a = 54321$ | $u_{-1} = 1$ | $v_{-1} = 0$ |
| $0$ | $--$ | $b = 9875$ | $u_0 = 0$ | $v_0 = 1$ |
| $1$ | $5$ | $4946$ | $1$ | $-5$ |
| $2$ | $1$ | $4929$ | $-1$ | $6$ |
| $3$ | $1$ | $17$ | $2$ | $-11$ |
| $4$ | $289$ | $16$ | $-579$ | $3185$ |
| $5$ | $1$ | $1$ | $581$ | $-3196$ |

gcd

**continued on next page**

From the last row, we see that $u = u_5 = \underline{581}$ and $v = v_5 = \underline{-3196}$. This answer can be verified by checking

$$au + bv = (54321)(581) + (9875)(-3196) = 31560501 - 31560500 = 1 = \gcd(a,b) .$$

■

## Exercises

1. For the following, used the division algorithm to compute $b \div m$. State the quotient $q$ and remainder $r$ for the division. Use the result to compute $b \pmod{m}$.
   a. $b = 30$, $m = 7$.
   b. $b = -30$, $m = 7$.
   c. $b = 100$, $m = 26$.
   d. $b = -100$, $m = 26$.
   e. $b = 2047$, $m = 137$.
   f. $b = 123129$, $m = 10371$.
   g. $b = -319212$, $m = 31233$.

2. Use the Euclidean Algorithm to find the greatest common divisor of the following numbers.
   a. 72 and 300.
   b. 629 and 357
   c. 52598 and 2541
   d. 3854682 and 1095939
   e. 101 and 127.

3. For each exercise for Exercise 2, assign $a$ and $b$ and generate an Euclidean algorithm table to find integers $u$ and $v$ where $au + bv = \gcd(a, b)$. 3b

4. Find the set of elements that make up the following congruence classes.
   a. The elements of the congruence class $x \equiv 3 \pmod{7}$.
   b. The elements of the congruence class $x \equiv 7 \pmod{11}$.
   c. The elements of the congruence class $x \equiv 2 \pmod{26}$.