Math 202 Test and Solutions

A Little Number Theory

31 October, 2008

Ten questions, each worth the same amount. Complete ***five*** of your choice. I will only grade the first five I see. Make sure your name is on the top of each page you return.

Explain your reasoning for each problem whenever appropriate; that helps me give partial credit. Perform scratch work on scratch paper; keep your explanations clean.

Make final answers obvious by boxing or circling them. When a question asks you to construct a table or perform a computation, showing the table or writing out the computation's steps is a part of the question and is **not optional**.

And remember to read and answer the entire question. There is copious explanation before a few problems. The explanation repeats some relevant material from class.

Contents

1 Repeating Decimals

Another way to find the period of a decimal expansion is to consider powers of ten. To find the period of a fraction $\frac{1}{d}$, examine powers of ten modulo d. For example, consider $\frac{1}{3} = 0.\overline{3}$ and $\frac{1}{7} = 0.\overline{142857}$. The period of $0.\overline{3}$ is one, and the period of $0.\overline{142857}$ is six.

The following tables show the powers of ten modulo three and seven, respectively:

i	$10^i \equiv 10^i \pmod 3$
0	$1 \equiv 1 \pmod 3$
1	$10 \equiv 1 \pmod 3$
	$\vdots$

i	$10^i \equiv 10^i \pmod 7$
0	$1 \equiv 1 \pmod 7$
1	$10 \equiv 3 \pmod 7$
2	$100 \equiv 2 \pmod 7$
3	$1000 \equiv 6 \pmod 7$
4	$10000 \equiv 4 \pmod 7$
5	$100000 \equiv 5 \pmod 7$
6	$1000000 \equiv 1 \pmod 7$
	$\vdots$

In each table, a number eventually appears twice. The distance between those two appearances is equal to the decimal expansion's period. For 3 that difference is 1 (from 0 to 1), and for 7 the difference is 6 (from 0 to 6). Reasoning *inductively*, assume this is true. Note that the numbers in the table are *not* the same as the digits in the expansion.

- Construct similar tables to find the periods of $\frac{1}{27}$ and $\frac{1}{11}$. (You can check if you found the correct period by computing 1/27 and 1/11.)

  Solution: The tables for $\frac{1}{27}$ and $\frac{1}{11}$ are:

i	$10^i \equiv 10^i \pmod{27}$
0	$1 \equiv \mathbf{1} \pmod{27}$
1	$10 \equiv 10 \pmod{27}$
2	$100 \equiv 19 \pmod{27}$
3	$1000 \equiv \mathbf{1} \pmod{27}$
	$\vdots$

i	$10^i \equiv 10^i \pmod{11}$
0	$1 \equiv \mathbf{1} \pmod{11}$
1	$10 \equiv 10 \pmod{11}$
2	$100 \equiv \mathbf{1} \pmod{11}$
	$\vdots$

  The period of $\frac{1}{27}$ is **three**, and the period of $\frac{1}{11}$ is **two**. You can verify this with $1/27 = 0.\overline{037}$ and $1/11 = 0.\overline{09}$.

- Remembering that $\frac{1}{6} = 0.1\overline{6}$, construct a table showing that the period of $\frac{1}{6}$ is 1. What number repeats?

  Solution: A similar table for $\frac{1}{6} = 0.1\overline{6}$ is:

i	$10^i \equiv 10^i \pmod{6}$
0	$1 \equiv 1 \pmod{6}$
1	$10 \equiv \mathbf{4} \pmod{6}$
2	$100 \equiv \mathbf{4} \pmod{6}$
	$\vdots$

  Here, $10^i \equiv 4 \pmod{6}$ for $i > 0$. **The number 4 repeats, and the period is one.** Note that the repeating portion starts at $i = 1$ rather than $i = 0$, corresponding to the one non-repeating digit.

2 Positional Notation and Decimals

Write the following decimals as sums using positional notation:

- $123.47 = \boxed{\mathbf{1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 + 4 \cdot 10^{-1} + 7 \cdot 10^{-2}}}$
- $128.125 = \boxed{\mathbf{1 \cdot 10^2 + 2 \cdot 10^1 + 8 \cdot 10^0 + 1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 5 \cdot 10^{-3}}}$
- $13.2135 = \boxed{\mathbf{1 \cdot 10^1 + 3 \cdot 10^0 + 2 \cdot 10^{-1} + 1 \cdot 10^{-2} + 3 \cdot 10^{-3} + 6 \cdot 10^{-4}}}$
- $0.625 = \boxed{\mathbf{6 \cdot 10^{-1} + 2 \cdot 10^{-2} + 5 \cdot 10^{-3}}}$

Note: Small variations of the solutions throughout are fine.

Write the following **binary** numbers in positional notation (using powers of 2 rather than 10) and find their decimal equivalents:

- $10000000.001_2 = \boxed{\mathbf{1 \cdot 2^7 + 1 \cdot 2^{-3} = 128.125}}$
- $0.101_2 = \boxed{\mathbf{1 \cdot 2^{-1} + 1 \cdot 2^{-3} = 0.625}}$
- $1101.0101_2 = \boxed{\mathbf{1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^0 + 1 \cdot 2^{-2} + 1 \cdot 2^{-4} = 12.3125}}$

Perform the following operations digit-by-digit, showing your work in either tabular form or expanded form. Do not expand carries until the end. For example, consider adding $30.2 + 79.8 = 90.1$ in tabular form showing the carries:

$$\begin{array}{rrrr}
 & 1 & 0 & .3\\
+ & 7 & 9 & .8\\
\hline
 & 8 & 9 & 11\\
 & 8 & 9 & 1 \cdot 10^1 + 1\\
 & 8 & 9 + 1 & 1\\
 & 8 & 10 & 1\\
 & 8 & 1 \cdot 10^1 + 0 & 1\\
 & 8{+}1 & 0 & 1\\
 & 9 & 0 & 1\\
\hline
 & 9 & 0 & .1
\end{array}$$

The expanded form is similar, but each line is an explicit sum with powers of 10. Either form is acceptable.

The operations to perform:

- Base 10 (decimal): $628 + 113$
  Solution: Forms of $628 + 113 = 741$:

Tabular:

$$\begin{array}{crrr}
 & 6 & 2 & 8 \\
+ & 1 & 1 & 3 \\
\hline
 & 7 & 3 & 11 \\
 & 7 & 3 & 10^1+1 \\
 & 7 & 3{+}1 & 1 \\
 & 7 & 4 & 1 \\
\hline
 & 7 & 4 & 1
\end{array}$$

Expression:

$$\begin{aligned}
628+113 &= (6\cdot 10^2 + 2\cdot 10^1 + 8\cdot 10^0) \\
&\qquad + (1\cdot 10^2 + 1\cdot 10^1 + 3\cdot 10^0) \\
&= (6+1)\cdot 10^2 + (2+1)\cdot 10^1 + (8+3)\cdot 10^0 \\
&= 7\cdot 10^2 + 3\cdot 10^1 + 11\cdot 10^0 \\
&= 7\cdot 10^2 + 3\cdot 10^1 + (1\cdot 10^1 + 1)\cdot 10^0 \\
&= 7\cdot 10^2 + (3+1)\cdot 10^1 + 1\cdot 10^0 \\
&= 7\cdot 10^2 + 4\cdot 10^1 + 1\cdot 10^0 \\
&= 741
\end{aligned}$$

- Base 10 (decimal): $2.6+7.5$
  Solution: Forms of $2.6+7.5=10.1$:

Tabular:

$$\begin{array}{crrr}
 & & 2 & .6 \\
+ & & 7 & .5 \\
\hline
 & & 9 & 11 \\
 & & 9 & 10^1+1 \\
 & & 9{+}1 & 1 \\
 & & 10+0 & 1 \\
 & 1 & 0 & 1 \\
\hline
 & 1 & 0 & .1
\end{array}$$

Expression:

$$
\begin{aligned}
2.6 + 7.5 &= 2 \cdot 10^0 + 6 \cdot 10^{-1} + 7 \cdot 10^0 + 5 \cdot 10^{-1} \\
&= (2+7) \cdot 10^0 + (6+5) \cdot 10^{-1} \\
&= 9 \cdot 10^0 + 11 \cdot 10^{-1} \\
&= 9 \cdot 10^0 + (1 \cdot 10^1 + 1) \cdot 10^{-1} \\
&= 9 \cdot 10^0 + 1 \cdot 10^0 + 1 \cdot 10^{-1} \\
&= (9+1) \cdot 10^0 + 1 \cdot 10^{-1} \\
&= 10 \cdot 10^0 + 1 \cdot 10^{-1} \\
&= 1 \cdot 10^1 + 1 \cdot 10^{-1} \\
&= 10.1
\end{aligned}
$$

- Base 2 (binary): $1101_2 + 101_2 = 10010_2$.
  Solution: Entries in the tabular form all are binary.
  Forms of $1101_2 + 101_2 = 10010_2$:

Tabular:

$$
\begin{array}{lrrrrr}
 & & 1 & 1 & 0 & 1 \\
+ & & & 1 & 0 & 1 \\
\hline
 & & 1 & 10 & 0 & 10 \\
 & & 1{+}1 & 0 & 0{+}1 & 0 \\
 & & 10 & 0 & 0{+}1 & 0 \\
 & 1 & 0 & 0 & 1 & 0 \\
\hline
 & 1 & 0 & 0 & 1 & 0
\end{array}
$$

Expression:

$$
\begin{aligned}
1101_2 + 101_2 &= (1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^0) + (1 \cdot 2^2 + 1 \cdot 2^0) \\
&= 1 \cdot 2^3 + (1+1) \cdot 2^2 + (1+1) \cdot 2^0 \\
&= 1 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2^0 \\
&= 1 \cdot 2^3 + 1 \cdot 2^3 + 1 \cdot 2^1 \\
&= (1+1) \cdot 2^3 + 1 \cdot 2^1 \\
&= 2 \cdot 2^3 + 1 \cdot 2^1 \\
&= 1 \cdot 2^4 + 1 \cdot 2^1 \\
&= 10010_2
\end{aligned}
$$

- Base 2 (binary): $1001_2 + 101_2$.

Solution: Entries in the tabular form all are binary.
Forms of $1001_2 + 101_2 = 1110_2$:

Tabular:

$$\begin{array}{lrrrr}
 & 1 & 0 & 0 & 1 \\
+ & & 1 & 0 & 1 \\
\hline
 & 1 & 1 & 0 & 10 \\
 & 1 & 1 & 0{+}1 & 0 \\
 & 1 & 1 & 1 & 0 \\
\hline
 & 1 & 1 & 1 & 0
\end{array}$$

Expression:

$$\begin{aligned}
1001_2 + 101_2 &= (1 \cdot 2^3 + 1 \cdot 2^0) + (1 \cdot 2^2 + 1 \cdot 2^0) \\
&= 1 \cdot 2^3 + 1 \cdot 2^2 + (1 + 1) \cdot 2^0 \\
&= 1 \cdot 2^3 + 1 \cdot 2^2 + 2 \cdot 2^0 \\
&= 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 \\
&= 1110_2
\end{aligned}$$

3 Modular Arithmetic

Remember the divisibility form or algorithm. Any integer b can be written in terms of another integer $a \neq 0$ as

$$b = q \cdot a + r \quad \text{where} \quad 0 \leq r < |a|.$$

Recall that $|a|$ is the absolute value of a. There are only $|a|$ possible *remainders* r. Each value defines a *congruence class modulo* a.

We denote that two numbers b and c are in the same congruence class modulo a by writing.

$$b \equiv c \pmod{a}.$$

Both b and c have the same remainder r, with $0 \leq r < |a|$, when divided by a.

Find two additional positive members of each congruence class, and illustrate each with a "clock-face" or "number circle" diagram showing how many trips around a circle it takes to reach your examples:

$$5 \pmod{7} \equiv \boxed{\mathbf{-2}} \pmod{7} \equiv \boxed{\mathbf{12}} \pmod{7}$$

$$-1 \pmod{3} \equiv \boxed{\mathbf{-4}} \pmod{3} \equiv \boxed{\mathbf{2}} \pmod{3}$$

Fill in the blanks with a value at least zero and less than the modulus, and illustrate these by hops around a number circle:

$$1 + 2 + 3 \equiv \boxed{\mathbf{0}} \pmod{3}$$

$$5 - 7 \equiv \boxed{\mathbf{7}} \pmod{9}$$

(Remember that the result must be non-negative.)

Fill in the blanks with a value at least zero and less than the modulus:

$$5 \cdot \boxed{\mathbf{6}} \equiv 1 \pmod{29}$$

$$1/5 \equiv \boxed{\mathbf{6}} \pmod{29}$$

(Hint for above: Consider the previous part.)

$$453 \cdot (3826 + 9471) \equiv \boxed{\mathbf{1 \cdot (0 + 1) \equiv 1 \cdot 1 = 1}} \pmod{2}$$

(Hint for above: Reduce the numbers *before* computing.)

$$87 \cdot 183635281 \equiv \boxed{\mathbf{0 \cdot 183635281 \equiv 0}} \pmod{87}$$

(Hint for above: You shouldn't need to calculate anything.)

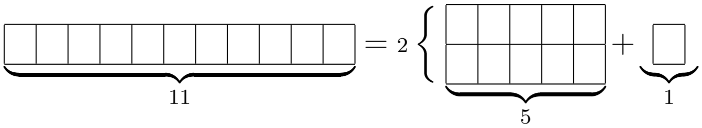
4 Divisibility

The division form or division algorithm expresses one integer b in terms of another $a \neq 0$,

$$b = q \cdot a + r \quad \text{where} \quad 0 \leq r < |a|.$$

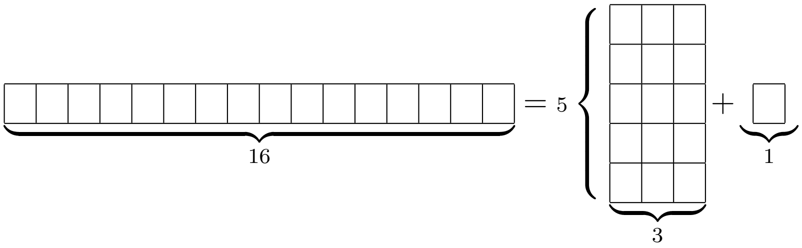
The quantity q is the *quotient* and r is the *remainder*. We say that a divides b, or $a \mid b$ if $r = 0$ in this form.

We can illustrate the division form with boxes. For example, we can draw $11 = 2 \cdot 5 + 1$ as

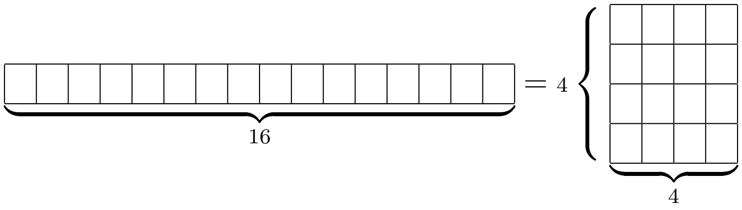


Complete the following division forms, answer, illustrate each with a block diagram:

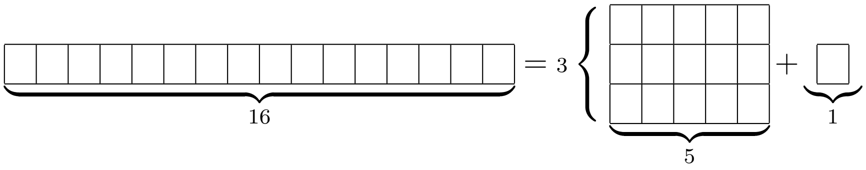
- $16 = \boxed{\mathbf{5}} \cdot 3 + \boxed{\mathbf{1}}$. Does $3 \mid 16$? $\boxed{\textbf{No.}}$



- $16 = \boxed{\mathbf{4}} \cdot 4 + \boxed{\mathbf{0}}$. Does $4 \mid 16$? $\boxed{\textbf{Yes.}}$



- $16 = \boxed{\mathbf{3}} \cdot 5 + \boxed{\mathbf{1}}$. Does $5 \mid 16$? $\boxed{\textbf{No.}}$



We can use modular arithmetic (arithmetic with remainders) and positional notation ($123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$) to assist with some easier divisibility rules.

Because $10 \equiv 1 \pmod{3}$, we can expand $123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 \equiv 1 \cdot 1^2 + 2 \cdot 1^1 + 3 \cdot 1^0 \equiv 1 + 2 + 3 \equiv 1 + 2 + 0 \equiv 0 \pmod{3}$, so $3 \mid 123$.

- Using a similar method, does 9 divide 38462203639098?

  Solution: Because $10 \equiv 1 \pmod{9}$, $9 \mid 38462203639098$ if the sum of 38462203639098's digits is equivalent to zero modulo 9. $3+8+4+6+2+2+3+6+3+9+9+8 = 63 \equiv 0 \pmod{9}$, so $\mathbf{9 \mid 38462203639098}$.

- Does 9 divide $3846220364\underline{4}90\underline{89}$? (The underlined digits are different.)

  Solution: Rather than adding all the digits again, we can look at the difference in the individual digits. The last two are just transposed, so their sum is the same. The change in the other digit is 1, so we know that the sum of the digits will change by one and $\mathbf{9 \nmid 38462203649089}$.

- State an easy rule in English for divisibility by 9.

  Solution: One easy rule is that the sum of the digits must be divisible by 9. Another is that the sum must be equivalent to zero modulo 9, which implies you can wrap the sum around 9 as you go.

- What is $10^k \pmod{5}$ for $k = 1$ and for integers $k > 1$? So what is a divisibility rule for 5?

  Solution: Because $10 = 2 \cdot 5$, $10^k = (2 \cdot 5)^k = 2^k \cdot 5^k$. Thus $5^k \mid 10^k$, and $5 \mid 10^k$ for all integer $k > 1$. Using the expansion of a number by positional notation, **five divides a number if five divides its last digit**, or, equivalently, if its last digit is five or zero.

5 Rational Arithmetic

The method for adding fractions can be derived as follows:

$$
\begin{aligned}
\frac{a}{b}+\frac{c}{d} &= \frac{a}{b}\cdot 1+\frac{c}{d}\cdot 1 && \textbf{mult. identity, \#2}\\
&= \frac{a}{b}\cdot\frac{d}{d}+\frac{c}{d}\cdot\frac{b}{b} && \frac{\mathbf{d}}{\mathbf{d}}=\mathbf{1},\ \#7\\
&= \frac{ad}{bd}+\frac{cb}{db} && \textbf{mult. of fractions, \#6}\\
&= \frac{ad}{bd}+\frac{cb}{\mathbf{bd}} && \textbf{comm. of mult., \#4}\\
&= \frac{ad+cb}{bd}. && \textbf{add frac. of equal denom., \#8}
\end{aligned}
$$

(The bold is to emphasize what changed in one line above.)

Justify each line in the derivation by labeling it with one of the following arithmetic properties or rules:

1. additive identity
2. multiplicative identity
3. commutativity of addition
4. commutativity of multiplication
5. distributivity of multiplication over addition
6. multiplying fractions
7. $1=\frac{d}{d}$ for any non-zero d
8. adding fractions of equal denominators

Compute and reduce to lowest terms by removing common factors from the numerator and denominator:

$$
\begin{aligned}
\frac{1}{2}+\frac{1}{3} &= \boxed{\mathbf{\frac{5}{6}}} & \qquad \frac{3}{8}\cdot 4 &= \boxed{\mathbf{\frac{3}{2}}}\\
\frac{1}{2}-\frac{1}{3} &= \boxed{\mathbf{\frac{1}{6}}} & \qquad \frac{3}{8}\cdot\frac{4}{7} &= \boxed{\mathbf{\frac{3}{14}}}\\
\frac{5}{6}-\frac{1}{3} &= \boxed{\mathbf{\frac{1}{2}}} & \qquad \frac{3}{8}\Big/\frac{4}{7}=\frac{3}{8}\div\frac{4}{7} &= \boxed{\mathbf{\frac{21}{32}}}
\end{aligned}
$$

6 Distributive Property of Rational Arithmetic

Complete the proof that rational multiplication distributes over rational addition. That is, prove that

$$\frac{x}{y} \cdot \left(\frac{a}{b} + \frac{c}{d}\right) = \frac{xa}{yb} + \frac{xc}{yd}.$$

A skeleton[1] for the derivation, using bold to highlight a change that might be missed:

$$\begin{aligned}
\frac{x}{y} \cdot \left(\frac{a}{b} + \frac{c}{d}\right) &= \frac{x}{y} \cdot \boxed{\frac{\mathbf{ad + cb}}{\mathbf{bd}}} && \textbf{add frac., \#6} \\
&= \frac{x \cdot (ad + cb)}{ybd} && \textbf{mul. frac., \#4} \\
&= \frac{xad + xcb}{ybd} && \textbf{int. distrib., \#3} \\
&= \frac{xad + \mathbf{cx}b}{ybd} && \textbf{int. mul. comm., \#2} \\
&= \boxed{\frac{\mathbf{xad}}{\mathbf{ybd}}} + \frac{cxb}{ybd} && \textbf{add frac., \#6} \\
&= \frac{xad}{ybd} + \frac{cxb}{y\mathbf{db}} && \textbf{int. mul. comm., \#2} \\
&= \frac{xa}{yb} \cdot \frac{d}{d} + \frac{cx}{yd} \cdot \frac{b}{b} && \textbf{mul. frac., \#4} \\
&= \frac{xa}{yb} \cdot \boxed{\mathbf{1}} + \frac{cx}{yd} \cdot \boxed{\mathbf{1}} && \mathbf{1} = \frac{\mathbf{d}}{\mathbf{d}}, \#5 \\
&= \frac{xa}{yb} + \frac{cx}{yd}. && \textbf{mul. ident., \#1}
\end{aligned}$$

Fill in the blanks in the column after "=" with the appropriate symbolic expression. Fill in the blanks to the right with the property or rule that justifies the step:

[1] Boo.

1. multiplicative identity
2. commutativity of *integer* multiplication
3. distributivity of *integer* multiplication over addition
4. multiplying fractions
5. $1 = \frac{d}{d}$ for any non-zero d
6. adding fractions

7 Prime factorization, the GCD, and the LCM

Factor the following numbers into products of primes raised to powers:

$$72 = 2^3 \cdot 3^2$$

$$1188 = \boxed{\mathbf{2^2 \cdot 3^3 \cdot 11^1}}$$

$$1170 = \boxed{\mathbf{2^1 \cdot 3^2 \cdot 5^1 \cdot 13}}$$

$$429 = \boxed{\mathbf{3^1 \cdot 11^1 \cdot 13^1}}$$

$$188 = \boxed{\mathbf{2^2 \cdot 47^1}}$$

$$1001 = \boxed{\mathbf{7^1 \cdot 11^1 \cdot 13^1}}$$

Recall that the greatest common divisor of a and b, written (a, b), is the largest integer that divides both a and b. The least common multiple, $\mathrm{lcm}(a, b)$, is the least *positive* integer divisible by a and b.

Using the factorizations above, provide the following results in factored and numerical forms:

$$(72, 30) = 2 \cdot 3 \qquad = 8$$

$$(1188, 188) = \boxed{\mathbf{2^2}} \qquad = \boxed{\mathbf{4}}$$

$$(1188, 188, 1001) = \boxed{\mathbf{1}} \qquad = \boxed{\mathbf{1}}$$

$$(1188, 188, 1170) = \boxed{\mathbf{2^1}} \qquad = \boxed{\mathbf{2}}$$

$$(1188, 1170) = \boxed{\mathbf{2^1 \cdot 3^2}} \qquad = \boxed{\mathbf{18}}$$

$$(188, 1170) = \boxed{\mathbf{2^1}} \qquad = \boxed{\mathbf{2}}$$

$$(1188, 1001) = \boxed{\mathbf{11^1}} \qquad = \boxed{\mathbf{11}}$$

$$(429, 1001) = \boxed{\mathbf{11^1 \cdot 13^1}} \qquad = \boxed{\mathbf{143}}$$

$$\mathrm{lcm}(1188, 429) = \boxed{\mathbf{2^2 \cdot 3^3 \cdot 11^1 \cdot 13^1}} \qquad = \boxed{\mathbf{15444}}$$

$$\mathrm{lcm}(429, 1001) = \boxed{\mathbf{3^1 \cdot 7^1 \cdot 11^1 \cdot 13^1}} \qquad = \boxed{\mathbf{3003}}$$

$$\mathrm{lcm}(1170, 1001) = \boxed{\mathbf{2^1 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^1 \cdot 13^1}} = \boxed{\mathbf{90090}}$$

8 Euclidean GCD algorithm

The Euclidean GCD algorithm applied to positive integers a and b uses the division form,

$$b = q \cdot a + r \quad \text{where} \quad 0 \leq r < a,$$

to reduce the problem of computing (b, a) to computing (a, r). Because r is a decreasing, non-negative integer, it eventually becomes zero and the algorithm terminates with the non-zero number being the greatest common divisor.

For example, consider computing $(12, 8)$. We express $12 = 1 \cdot 8 + 4$ to see that $(12, 8) = (8, 4)$. Now $8 = 2 \cdot 4 + 0$, so $(12, 8) = (8, 4) = (4, 0) = 4$.

Use the Euclidean algorithm to compute the following, remembering to show your work:

- $(1188, 188) = \boxed{(\mathbf{188}, \mathbf{60}) = (\mathbf{60}, \mathbf{28}) = (\mathbf{28}, \mathbf{4}) = \mathbf{4}}$

  The steps of the algorithm are as follows:

$$\begin{aligned} 1188 &= 6 \cdot 188 + 60 &\qquad (\mathbf{1188}, \mathbf{188}) &= (\mathbf{188}, \mathbf{60}) \\ 188 &= 3 \cdot 60 + 28 &\qquad (\mathbf{188}, \mathbf{60}) &= (\mathbf{60}, \mathbf{28}) \\ 60 &= 2 \cdot 28 + 4 &\qquad (\mathbf{60}, \mathbf{28}) &= (\mathbf{28}, \mathbf{4}) \\ 28 &= 7 \cdot 4 + 0 &\qquad (\mathbf{28}, \mathbf{4}) &= \mathbf{4} \end{aligned}$$

- $(1188, 1170) = \boxed{(\mathbf{1170}, \mathbf{18}) = \mathbf{18}}$

  The steps of the algorithm are as follows:

$$\begin{aligned} 1188 &= 1 \cdot 1170 + 18 &\qquad (\mathbf{1188}, \mathbf{1170}) &= (\mathbf{1170}, \mathbf{18}) \\ 1170 &= 65 \cdot 18 + 0 &\qquad (\mathbf{1170}, \mathbf{18}) &= \mathbf{18} \end{aligned}$$

- $(188, 1170) = \boxed{(\mathbf{1170}, \mathbf{188}) = (\mathbf{188}, \mathbf{42}) = (\mathbf{42}, \mathbf{20}) = (\mathbf{20}, \mathbf{2}) = \mathbf{2}}$

  The steps of the algorithm are as follows:

$$\begin{aligned} 1170 &= 6 \cdot 188 + 42 &\qquad (\mathbf{1170}, \mathbf{188}) &= (\mathbf{188}, \mathbf{42}) \\ 188 &= 4 \cdot 42 + 20 &\qquad (\mathbf{188}, \mathbf{42}) &= (\mathbf{42}, \mathbf{20}) \\ 42 &= 2 \cdot 20 + 2 &\qquad (\mathbf{42}, \mathbf{20}) &= (\mathbf{20}, \mathbf{2}) \\ 20 &= 10 \cdot 2 + 0 &\qquad (\mathbf{20}, \mathbf{2}) &= \mathbf{2} \end{aligned}$$

- $(1188, 1001) = \boxed{(\mathbf{1001}, \mathbf{187}) = (\mathbf{187}, \mathbf{66}) = (\mathbf{66}, \mathbf{55}) = (\mathbf{55}, \mathbf{11}) = \mathbf{11}}$

  The steps of the algorithm are as follows:

$$\begin{aligned}
1188 &= 1 \cdot 1001 + 187 & \qquad (\mathbf{1188}, \mathbf{1001}) &= (\mathbf{1001}, \mathbf{187}) \\
1001 &= 5 \cdot 187 + 66 & \qquad (\mathbf{1001}, \mathbf{187}) &= (\mathbf{187}, \mathbf{66}) \\
187 &= 2 \cdot 66 + 55 & \qquad (\mathbf{187}, \mathbf{66}) &= (\mathbf{66}, \mathbf{55}) \\
66 &= 1 \cdot 55 + 11 & \qquad (\mathbf{66}, \mathbf{55}) &= (\mathbf{55}, \mathbf{11}) \\
55 &= 5 \cdot 11 + 0 & \qquad (\mathbf{55}, \mathbf{11}) &= \mathbf{11}
\end{aligned}$$

- $(429, 1001) = \boxed{(\mathbf{1001}, \mathbf{429}) = (\mathbf{429}, \mathbf{143}) = \mathbf{143}}$

  The steps of the algorithm are as follows:

$$\begin{aligned}
1001 &= 2 \cdot 429 + 143 & \qquad (\mathbf{1001}, \mathbf{429}) &= (\mathbf{429}, \mathbf{143}) \\
429 &= 3 \cdot 143 + 0 & \qquad (\mathbf{429}, \mathbf{143}) &= \mathbf{143}
\end{aligned}$$

Remember that $(a, b) = (b, a)$, so you always can place the larger number on the left.

9 Irrationals That Act Like Rationals

The rational numbers $\mathbb{Q}$ (a.k.a. fractions) are *closed* over addition, subtraction, multiplication, and division (excepting division by zero). The irrationals $\mathbb{R} \setminus \mathbb{Q}$ are *not closed* over the same operations, as seen in the homework.

However, the *quadratic rationals* defined as

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,|\, a \in \mathbb{Q}, b \in \mathbb{Q}\}$$

are closed for a given d!

Show that the quadratic rationals $\mathbb{Q}(\sqrt{2})$, or numbers of the form $a + b\sqrt{2}$, are closed over addition and division.

- To show these numbers are closed under addition, first try an example. Fill in the blanks below with numbers:

  $$(2 + 10\sqrt{2}) + (3 + 20\sqrt{2}) = \boxed{\mathbf{5}} + \boxed{\mathbf{30}}\sqrt{2}.$$

  Now try it symbolically. Fill in the blanks with the correct symbolic expression:

  $$(a + b\sqrt{2}) + (c + d\sqrt{2}) = \boxed{\mathbf{(a+c)}} + \boxed{\mathbf{(b+d)}}\sqrt{2}.$$

- To show these numbers are closed under division, again start with an example. Compute x and y, then fill in the blanks with rational numbers. Hint: y is an integer.

  $$\frac{3 + 2\sqrt{2}}{2 + 1\sqrt{2}} = \frac{3 + 2\sqrt{2}}{2 + 1\sqrt{2}} \cdot \frac{2 - 1\sqrt{2}}{2 - 1\sqrt{2}}$$
  $$= \frac{x}{y} = \boxed{\frac{\mathbf{2} + \sqrt{\mathbf{2}}}{\mathbf{2}}} = \boxed{\mathbf{1}} + \boxed{\frac{\mathbf{1}}{\mathbf{2}}}\sqrt{2}.$$

  Now try it symbolically. Compute the expressions for x and y, then fill in the blanks with rational expressions. Again, y has no

$\sqrt{2}$ in it.

$$
\begin{aligned}
\frac{a+b\sqrt{2}}{c+d\sqrt{2}} &= \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \cdot \frac{c-d\sqrt{2}}{c-d\sqrt{2}} \\
&= \frac{x}{y} = \boxed{\mathbf{\frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}}} \\
&= \boxed{\mathbf{\frac{ac-2bd}{c^2-2d^2}}} + \boxed{\mathbf{\frac{bc-ad}{c^2-2d^2}}}\sqrt{2}.
\end{aligned}
$$

(Note: Showing that multiplication is closed is about the same as addition above, but it's not included in this question. And closure over division here is an actual use *for removing irrationals from denominators.)*

10 Linear Diophantine Equations

Everyone's favorite topic, or at least one of mine, is solving $ax + by = c$ over integers a, b, and c for **integer** solutions x and y. We can use the Euclidean GCD algorithm for finding an initial solution if one exists.

For an example, we solve $27x + 33y = 9$. First we compute $(27, 33)$. The steps of the Euclidean algorithm provide

$$\begin{aligned} 33 &= 27 \cdot 1 + 6, \\ 27 &= 6 \cdot 4 + 3, \text{ and} \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

So $(27, 33) = 3$. Because $3 \mid 9$, there are infinitely many solutions to $27x+33y = 9$. If $(27, 33)$ did not divide the right-hand side, there would be no solutions.

Next we find solutions to $27v + 33w = 3$. Then $x = 3v$ and $y = 3w$ will solve our original equation. First we re-write the equations above that do not have a zero remainder:

$$\begin{aligned} 3 &= 27 \cdot 1 + 6 \cdot (-4), \text{ and} \\ 6 &= 33 \cdot 1 + 27 \cdot (-1). \end{aligned}$$

Now we start with the first equation and substitute later equations into it until we have $3 = 27v + 33w$ for some integers v and w:

$$\begin{aligned} 3 &= 27 \cdot 1 + 6 \cdot (-4) \\ &= 27 \cdot 1 + (33 \cdot 1 + 27 \cdot (-1)) \cdot (-4) \\ &= 27 \cdot 1 + 33 \cdot (-4) + 27 \cdot 4 \\ &= 27 \cdot 5 + 33 \cdot (-4). \end{aligned}$$

Thus we have a solution $v = 5$ and $w = -4$. Multiplying by 3, $x = 15$ and $y = -12$ solves our original equation, $27 \cdot 15 + 33 \cdot (-15) = 9$.

Solve the following linear Diophantine equations for **integer** solutions x and y, or show that no solution exists:

- $64x + 336y = 32$: $\boxed{\mathbf{x = -10}, \mathbf{y = 2}}$

The Euclidean algorithm for the GCD terminates almost immediately with

$$\begin{aligned} 336 &= 64 \cdot 5 + 16, \text{ and} \\ 64 &= 16 \cdot 4 + 0. \end{aligned}$$

So $(336, 64) = 16 \mid 32$, and the equations have infinitely many solutions. Working backwards from the first line,

$$16 = 336 \cdot 1 + 64 \cdot (-5).$$

Doubling throughout,

$$32 = 336 \cdot 2 + 64 \cdot (-10),$$

so $\mathbf{x = -10}$ and $\mathbf{y = 2}$ solves this equation.

- $11x + 121y = 21$: $\boxed{\textbf{No solutions.}}$

  Here, $121 = 11^2$, so $(121, 11) = 11$. Because $11 \nmid 21$, there are no solutions.

- $13x + 11y = 7$: $\boxed{\mathbf{x = -35,\ y = 42}}$

  Running through the Euclidean algorithm,

$$\begin{aligned} 13 &= 11 \cdot 1 + 2, \\ 11 &= 2 \cdot 5 + 1, \text{ and} \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

  So $(13, 11) = 1 \mid 7$ and this equation has infinitely many solutions. From the first two lines of the algorithm,

$$\begin{aligned} 2 &= 13 \cdot 1 + 11 \cdot (-1), \text{ and} \\ 1 &= 11 \cdot 1 + 2 \cdot (-5). \end{aligned}$$

  Substituting up the chain,

$$\begin{aligned} 1 &= 11 \cdot 1 + 2 \cdot (-5) \\ &= 11 \cdot 1 + (13 \cdot 1 + 11 \cdot (-1)) \cdot (-5) \\ &= 11 \cdot 1 + 13 \cdot (-5) + 11 \cdot 5 \\ &= 11 \cdot 6 + 13 \cdot (-5). \end{aligned}$$

  So $13 \cdot (-5) + 11 \cdot 6 = 1$. Multiplying by seven, $13 \cdot (-35) + 11 \cdot 42 = 7$, so $\mathbf{x = -35}$, $\mathbf{y = 42}$ solves the original equation.