MAT 308: Exam 2 **Name:** *Caleb M^{c}Whorter — Solutions*
Fall – 2022
11/18/2022
'∞' Minutes

Write your name on the appropriate line on the exam cover sheet. This exam contains 18 pages (including this cover page) and 10 questions. Check that you have every page of the exam. Answer the questions in the spaces provided on the question sheets. Be sure to answer every part of each question and show all your work. If you run out of room for an answer, continue on the back of the page — being sure to indicate the problem number.

Question	Points	Score
1	10	
2	10	
3	10	
4	10	
5	10	
6	10	
7	10	
8	10	
9	10	
10	10	
Total:	100	

1. (10 points) Consider the 'rule' $f : \mathbb{R} \to \mathbb{R}^2$ given by $t \mapsto (3\cos t, 3\sin t)$.
   (a) Is $f(t)$ a function? Explain.
   (b) Consider $\operatorname{im} f \subseteq \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$. If $(x, y) \in \operatorname{im} f$, show that $x^2 + y^2 = 9$.
   (c) Considered as a subset of $\mathbb{R}^2$, geometrically describe $\operatorname{im} f$.
   (d) Can $\operatorname{im} f$ be given by the image of a function of x? What about a function of y? Explain.

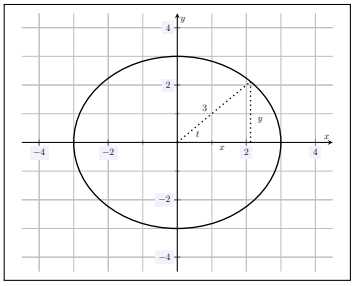
Solution.

(a) Yes, $f(t)$ is a function. For each input $t \in \mathbb{R}$, we have one output—namely, $f(t) = (3\cos t, 3\sin t) \in \mathbb{R}^2$. While $\cos t$ and $\sin t$ may be 2π-periodic, 2π translations of t would be different inputs. For example, $f(0)$ and $f(2\pi)$ have the same value as $f(0) = (3\cos 0, 3\sin 0) = (3, 0)$ and $f(2\pi) = (3\cos 2\pi, 3\sin 2\pi) = (3, 0)$ but $f(0)$ and $f(2\pi)$ are still well defined because the inputs are different.

(b) Suppose $\mathbf{v} \in \operatorname{im} f \subseteq \mathbb{R}^2$. As $\mathbf{v} \in \mathbb{R}^2$, we know $\mathbf{v} = (x, y)$ for some $x, y \in \mathbb{R}^2$. But because $\mathbf{v} \in \operatorname{im} f$, we know that $\mathbf{v} = (3\cos t, 3\sin t)$ for some $t \in \mathbb{R}$. But then using the fact that $\cos^2\theta + \sin^2\theta = 1$ for all $\theta \in \mathbb{R}$, we have...

$$\begin{aligned} x^2 + y^2 &= (3\cos t)^2 + (3\sin t)^2 \\ &= 9\cos^2 t + 9\sin^2 t \\ &= 9(\cos^2 t + \sin^2 t) \\ &= 9 \cdot 1 \\ &= 9 \end{aligned}$$

(c) Observe that elements of $\operatorname{im} f$ satisfy the relation $x^2 + y^2 = 9$. Geometrically, as a subset of the plane, $x^2 + y^2 = 9$ is a circle of radius 3 centered at the origin. This shows that $\operatorname{im} f$ must be a subset of this circle. The converse is true as well (though it is less immediate). Therefore, $\operatorname{im} f$ is the circle of radius 3 centered at the origin.



[Note: To see the converse, draw a ray at the angle $t \in \mathbb{R}$, measured from the positive x-axis counterclockwise, and let (x, y) be the point of intersection of this ray with the circle. Clearly, $x^2 + y^2 = 9$. But using trigonometry, we see that $\cos t = \frac{x}{3}$ and $\sin t = \frac{y}{3}$. This implies $x = 3\cos t$ and $y = 3\sin t$. Because each such point on the circle can be obtained this way, we can see that every point on the circle has the form $(3\cos t, 3\sin t)$ for some $t \in \mathbb{R}$.]

(d) Using (c), we can see that $\operatorname{im} f$ *is a circle with radius 3 centered at the origin. But then clearly* $\operatorname{im} f$ *cannot be a function of* x *because the circle fails the vertical line test; that is, there are different* x*-values corresponding to the same* y*-value (as shown below). Furthermore, the circle fails the horizontal line test, so that the circle cannot be a function of* y*; that is, there are different* y*-values corresponding to the same* x*-value.*

Alternatively, we can find distinct x*-values associated to the same* y*-value to show that* $f(t)$ *is not a function of its* x*-coordinate. Observe that* $f\left(\frac{\pi}{2}\right) = (0, 3)$ *and* $f\left(-\frac{\pi}{2}\right) = (0, -3)$*. But then* $0 \sim 3$ *and* $0 \sim -3$ *so that* $f(t)$ *cannot be a function of its* x*-coordinate. Observe also that* $f(0) = (3, 0)$ *and* $f(\pi) = (-3, 0)$*. But then* $0 \sim 3$ *and* $0 \sim -3$ *so that* $f(t)$ *cannot be a function of its* y*-coordinate.*

Putting (a)–(d) together, we observe that the circle with radius 3 centered at the origin is neither a function of x *or* y*, but it is a function of something—namely,* t *(its angles).*

2. (10 points) Define functions $f, g : \mathbb{R} \to \mathbb{R}$ by $f(x) = |x + 5|$ and $g(x) = 7 - 3x$.

   (a) Find an element in $\operatorname{im} f$ and also find an element in $\operatorname{im} g$.

   (b) Is $-5 \in \operatorname{im} f$? If not, explain why, and if so, find its preimage.

   (c) Is $12 \in \operatorname{im} g$? If not, explain why, and if so, find its preimage.

   (d) Compute $f\big([-6, 6)\big)$ and $g\big((-6, 6]\big)$.

   (e) Compute $f^{-1}\big([-1, 1]\big)$ and $g^{-1}\big([-1, 1]\big)$.

Solution.

(a) Given any $x \in \mathbb{R}$, we know that $f(x)$ and $g(x)$ are elements in the image of f and g, respectively. For instance, choosing $x = 0$, we have...

$$f(0) = |0 + 5| = |5| = 5$$

$$g(0) = 7 - 3(0) = 7 - 0 = 7$$

Therefore, we have $5 \in \operatorname{im} f$ and $7 \in \operatorname{im} g$. Of course, we need not have chosen $x = 0$, chosen x to be an integer, nor chosen the same x-value for both. For instance, we also have...

$$f\left(-\frac{11}{2}\right) = \left|-\frac{11}{2} + 5\right| = \left|-\frac{1}{2}\right| = \frac{1}{2}$$

$$g(\pi) = 7 - 3\pi$$

This shows that $\frac{1}{2} \in \operatorname{im} f$ and $7 - 3\pi \in \operatorname{im} g$.

(b) If $-5 \in \operatorname{im} f$, then there is $x \in \mathbb{R}$ such that $f(x) = -5$. But then $|x + 5| = -5$. Because $|x + 5| \geq 0$ for all $x \in \mathbb{R}$, there is no such x. Therefore, $-5 \notin \operatorname{im} f$.

(c) If $12 \in \operatorname{im} g$, then there is $x \in \mathbb{R}$ such that $g(x) = 12$. But then...

$$\begin{aligned} g(x) &= 12 \\ 7 - 3x &= 12 \\ -3x &= 5 \\ x &= -\frac{5}{3} \end{aligned}$$

Of course, this only shows that if $g(x) = 12$, then $x = -\frac{5}{3}$. We need show that $g(-5/3) = 12$. This is routine: $g\left(-\frac{5}{3}\right) = 7 - 3 \cdot -\frac{5}{3} = 7 + 5 = 12$. Therefore, $12 \in \operatorname{im} g$.

(d) Observe that if $x+5 \geq 0$, i.e. $x \geq -5$, then $f(x) = |x+5| = x+5$. If $x+5 < 0$, i.e. $x < -5$, then $f(x) = |x+5| = -(x+5) = -x-5$. But then using the fact that if $f(x)$ is a function and A, B are sets that $f(A \cup B) = f(A) \cup f(B)$, we have...

$$f\big([-6,6)\big) = f\big([-6,-5] \cup [-5,6)\big) = f\big([-6,-5]\big) \cup f\big([-5,6)\big) = [0,1] \cup [0,11) = [0,11)$$

Observe that $g(x)$ is linear because it is of the form $y = mx+b$ with $y = g(x)$, $x = x$, $m = -3$, and $b = 7$. Because $g(x)$ is continuous, it must take intervals to intervals, i.e. the image of an interval is an interval. Because $m = -3 < 0$, the function is decreasing. Putting these facts together, we know that $g([a,b]) = [g(b), g(a)]$, $g\big((a,b)\big) = \big(g(b), g(a)\big)$, etc. But then we have...

$$g\big((-6,6]\big) = (g(6), g(-6)] = (-11, 25]$$

(e) Observe that if $x+5 \geq 0$, i.e. $x \geq -5$, then $f(x) = |x+5| = x+5$. But then if $f(x) = c$ and $x \geq -5$, we have $c = f(x) = |x+5| = x+5$ so that $x = c-5$. Clearly, this then holds if $x = c-5 \geq -5$, i.e. $c \geq 0$. Now if $x+5 < 0$, i.e. $x < -5$, then $f(x) = |x+5| = -(x+5)$. But then if $f(x) = c$ and $x < -5$, we have $c = f(x) = |x+5| = -(x+5)$. But then we have $x = -c-5$. Clearly, this then holds if $x = -c-5 < -5$, i.e. $-c < 0$, which of course implies $c > 0$. Putting these two facts together, if $f(x) = |x+5| = c \geq 0$, then either $x = c-5$ or $x = -c-5$. We can check: if $x = c-5$, then $f(x) = |(c-5)+5| = |c| = c$, and if $x = -c-5$, then $f(x) = |(-c-5)+5| = |-c| = c$. But this then shows that if $c \geq 0$, then $f^{-1}(c) = \{-c-5, c-5\}$. Clearly, $f(x) = |x+5| \geq 0$ so that if $c < 0$, then $f(x) \neq c$ for all $x \in \mathbb{R}$, i.e. $f^{-1}(c) = \varnothing$. Using these facts and the fact that f^{-1} is the preimage of a function f and A, B are sets, then $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, we have...

$$f^{-1}\big([-1,1]\big) = f^{-1}\big([-1,0)\big) \cup f^{-1}\big([0,1]\big) = \varnothing \cup \big([-6,-5] \cup [-5,-4]\big) = [-6,-4]$$

Observe that if $g^{-1}(c) = x$, then $g(x) = c$. But then $7-3x = c$, which implies that $-3x = c-7$ so that $x = \frac{c-7}{-3} = \frac{7-c}{3}$. By the work in (d), because $g(x)$ is a decreasing linear function, the preimage of an interval must be an interval and $g^{-1}\big((a,b)\big) = \big(g^{-1}(b), g^{-1}(a)\big)$, $g^{-1}\big([a,b]\big) = \big[g^{-1}(b), g^{-1}(a)\big]$, etc. But then we have...

$$g^{-1}\big([-1,1]\big) = \big[g^{-1}(1), g^{-1}(-1)\big] = \left[\frac{7-1}{3}, \frac{7-(-1)}{3}\right] = \left[2, \frac{8}{3}\right]$$

3. (10 points) Define the function $f : \mathbb{R} \to \mathbb{R}$ via $x \mapsto x^2 + 5$.

   (a) Is $f(x)$ an injective function? If it is injective, explain why; if it is not injective, give a counterexample.

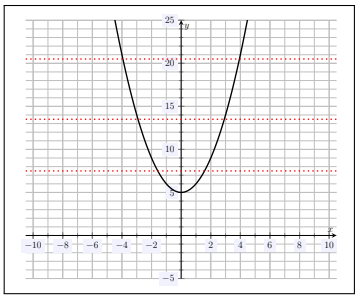
   (b) Is $f(x)$ a surjective function? If it is surjective, explain why; if it is not surjective, give a counterexample.

   (c) Is $f(x)$ a bijective function? Explain.

   (d) Does $f(x)$ have an inverse function? Explain.

Solution.

(a) The function $f(x)$ is not injective. If $f(x)$ is not injective, then there exist x, y with $x \neq y$ but $f(x) = f(y)$. Observe that if $x = -1$ and $y = 1$, we have $f(-1) = (-1)^2 + 5 = 1 + 5 = 6$ and $f(1) = 1^2 + 5 = 1 + 5 = 6$. But then $f(-1) = f(1)$ but $-1 \neq 1$. Therefore, $f(x)$ is not injective. In fact, if $c \in \mathbb{R}$ and $c \neq 0$, then $f(-c) = f(c)$ but $c \neq -c$: $f(-c) = (-c)^2 + 5 = c^2 + 5$ and $f(c) = c^2 + 5$ but we cannot have $c = -c$ because then $2c = 0$ so that $c = 0$, which is impossible if $c \neq 0$. Alternatively, we can see that $f(x)$ is not injective because it fails the horizontal line test: not every horizontal line intersects the function at most once



(b) The function $f(x)$ is not surjective. If $f(x)$ is not surjective, then there is $c \in \mathbb{R}$ such that $f(x) \neq c$ for all $x \in \mathbb{R}$. Let $c = 4$. If there were $x \in \mathbb{R}$ such that $f(x) = 4$, then we have...

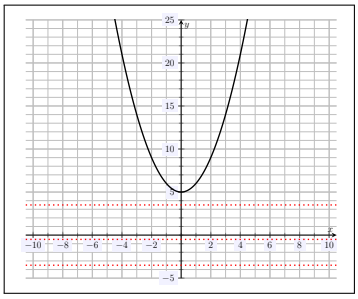
$$\begin{aligned} f(x) &= 4 \\ x^2 + 5 &= 4 \\ x^2 &= -1 \end{aligned}$$

But if $x \in \mathbb{R}$, then $x^2 \geq 0$. Therefore, there is no $x \in \mathbb{R}$ such that $x^2 = -1$. Therefore, $f(x)$ is not surjective. In fact, let $c < 5$. If there were $x \in \mathbb{R}$ such that $f(x) = c$, then we have...

$$\begin{aligned} f(x) &= c \\ x^2 + 5 &= c \\ x^2 &= c - 5 \end{aligned}$$

But because $c < 5$, we know that $c - 5 < 0$. But because $x^2 \geq 0$, if $x \in \mathbb{R}$, then clearly $x^2 \neq c - 5 < 0$. But then there is no such $x \in \mathbb{R}$ with $f(x) = c$ if $c < 5$.

Alternatively, we can see that $f(x)$ is not surjective because not every horizontal line intersects the function at least once.



(c) The function $f(x)$ is not bijective. By definition, a function is bijective if and only if it is injective and surjective. By (a), we know that $f(x)$ is not injective. Furthermore, by (b), we know $f(x)$ is not surjective. Therefore, $f(x)$ is not bijective.

(d) The function $f(x)$ does not have an inverse. A function $f : A \to B$ has an inverse function $f^{-1} : B \to A$ if and only if it is a bijection. By (c), we know that $f(x)$ is not a bijection. Therefore, $f(x)$ does not have an inverse function.

4. (10 points) A *fixed point* for a function $f : \mathbb{R} \to \mathbb{R}$ is $x_0 \in \mathbb{R}$ such that $f(x_0) = x_0$.

   (a) Show that -5 is a fixed point for $f(x) = 3x + 10$.

   (b) Show that 4 is not a fixed point for $g(x) = \dfrac{x+4}{2-x}$.

   (c) Find the fixed points for $h(x) = 2x^2 + 6x - 3$.

   (d) Use the quadratic formula to show that $j(x) = x^2 - 3x + 5$ has no fixed points in $\mathbb{R}$ but does have fixed points in $\mathbb{C}$.

Solution.

(a) If -5 is a fixed point for $f(x)$, then $f(-5) = -5$. We check this:

$$f(-5) = 3(-5) + 10 = -15 + 10 = -5$$

(b) If 4 is not a fixed point for $g(x)$, then $g(4) \neq 4$. We check this:

$$g(4) = \frac{4+4}{2-4} = \frac{8}{-2} = -4$$

(c) If x is a fixed point for $h(x)$, then $h(x) = x$. But then we have...

$$\begin{aligned} h(x) &= x \\ 2x^2 + 6x - 3 &= x \\ 2x^2 + 5x - 3 &= 0 \\ (2x-1)(x+3) &= 0 \end{aligned}$$

But then either $2x - 1 = 0$, which implies $x = \frac{1}{2}$, or $x + 3 = 0$, which implies $x = -3$. Of course, this only shows that if x is a fixed point, then $x = \frac{1}{2}$ or $x = -3$. This does not necessarily imply that $h\left(\frac{1}{2}\right) = \frac{1}{2}$ or $h(-3) = -3$. We need check this:

$$h\left(\frac{1}{2}\right) = 2\left(\frac{1}{2}\right)^2 + 6 \cdot \frac{1}{2} - 3 = \frac{1}{2} + 3 - 3 = \frac{1}{2}$$

$$h(-3) = 2(-3)^2 + 6(-3) - 3 = 18 - 18 - 3 = -3$$

Therefore, $x = -3$ and $x = \frac{1}{2}$ are fixed points for $h(x)$.

(d) If x is a fixed point for $j(x)$, then $j(x) = x$. But then we have...

$$j(x) = x$$

$$x^2 - 3x + 5 = x$$

$$x^2 - 4x + 5 = 0$$

$$x = \frac{-(-4) \pm \sqrt{(-4)^2 - 4(1)5}}{2(1)}$$

$$x = \frac{4 \pm \sqrt{16 - 20}}{2}$$

$$x = \frac{4 \pm 2i}{2}$$

$$x = 2 \pm i$$

Therefore, there can be no fixed points over $\mathbb{R}$ as the only possibilities are $x = 2 \pm i$. But then there are possible fixed points over $\mathbb{C}$. Indeed, we can check that $2 + i$ and $2 - i$ are fixed points:

$$j(2 + i) = (2 + i)^2 - 3(2 + i) + 5 = (3 + 4i) + (-6 - 3i) + 5 = 2 + i$$
$$j(2 - i) = (2 - i)^2 - 3(2 - i) + 5 = (3 - 4i) + (-6 + 3i) + 5 = 2 - i$$

Therefore, $2 + i$ and $2 - i$ are fixed points for $j(x)$.

5. (10 points) Showing all your work, compute the following:

   (a) $\displaystyle\sum_{k=-2}^{3}(5-k)$

   (b) $\displaystyle\prod_{k=1}^{5}(2k-3)$

   (c) $\displaystyle\sum_{k=0}^{1000}(k-7)$

   (d) $\displaystyle\sum_{k=0}^{1000}\left(\sqrt{k+5}-\sqrt{k}\right)$

   (e) $\displaystyle\prod_{k=1}^{1000}\left(1+\frac{1}{k}\right)$

Solution.

(a)

$$\sum_{k=-2}^{3}(5-k)=7+6+5+4+3+2=27$$

(b)

$$\prod_{k=1}^{5}(2k-3)=-1\cdot 1\cdot 3\cdot 5\cdot 7=-105$$

(c)

$$\sum_{k=0}^{1000}(k-7)=\sum_{k=0}^{1000}k+\sum_{k=0}^{1000}(-7)=\sum_{k=0}^{1000}k-7\sum_{k=0}^{1000}1=\frac{1000(1001)}{2}-7(1000-0+1)=500500-7007=493493$$

(d)

$$\begin{aligned}\sum_{k=0}^{1000}\left(\sqrt{k+5}-\sqrt{k}\right)&=(\cancel{\sqrt{5}}-\sqrt{0})+(\cancel{\sqrt{6}}-\sqrt{1})+(\cancel{\sqrt{7}}-\sqrt{2})+(\cancel{\sqrt{8}}-\sqrt{3})+(\cancel{\sqrt{9}}-\sqrt{4})+\\&\quad(\cancel{\sqrt{10}}-\cancel{\sqrt{5}})+(\cancel{\sqrt{11}}-\cancel{\sqrt{6}})+(\cancel{\sqrt{12}}-\cancel{\sqrt{7}})+\cdots+\\&\quad(\cancel{\sqrt{998}}-\cancel{\sqrt{993}})+(\cancel{\sqrt{999}}-\cancel{\sqrt{994}})+(\cancel{\sqrt{1000}}-\sqrt{995})+(\sqrt{1001}-\cancel{\sqrt{996}})+\\&\quad(\sqrt{1002}-\cancel{\sqrt{997}})+(\sqrt{1003}-\cancel{\sqrt{998}})+(\sqrt{1004}-\cancel{\sqrt{999}})+(\sqrt{1005}-\cancel{\sqrt{1000}})\\&=\sqrt{1005}+\sqrt{1004}+\sqrt{1003}+\sqrt{1002}+\sqrt{1001}-\sqrt{1}-\sqrt{2}-\sqrt{3}-\sqrt{4}\end{aligned}$$

(e)

$$\prod_{k=1}^{1000}\left(1+\frac{1}{k}\right)=\prod_{k=1}^{1000}\left(\frac{k+1}{k}\right)=\frac{\cancel{2}}{1}\cdot\frac{\cancel{3}}{\cancel{2}}\cdot\frac{\cancel{4}}{\cancel{3}}\cdot\frac{\cancel{5}}{\cancel{4}}\cdot\cdots\cdot\frac{\cancel{998}}{\cancel{997}}\cdot\frac{\cancel{999}}{\cancel{998}}\cdot\frac{\cancel{1000}}{\cancel{999}}\cdot\frac{1001}{\cancel{1000}}=1001$$

6. (10 points) Being sure to show all your work and fully justify your logic complete the following:

   (a) Using the definition of odd/even, show that -237 is odd but not even.

   (b) Express $1854/17$ using the division algorithm.

   (c) Find the prime factorization of 2040.

   (d) Compute $\gcd(2^{173} \cdot 3^{187} \cdot 5^{685} \cdot 11^{203},\ 2^{578} \cdot 3^{281} \cdot 7^{323} \cdot 13^{360})$ and find the next largest divisor of the two given numbers.

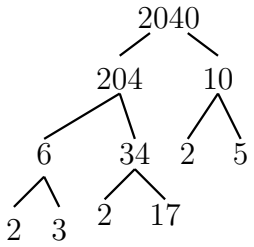
   (e) Compute $\operatorname{lcm}(2^{173} \cdot 3^{187} \cdot 5^{685} \cdot 11^{203},\ 2^{578} \cdot 3^{281} \cdot 7^{323} \cdot 13^{360})$ and find the next smallest multiple of the two given numbers.

Solution.

(a) If -237 is odd, then there exists a $k \in \mathbb{Z}$ such that $-237 = 2k + 1$. Observe that $-237 = 2(-119)+1$ so that -237 is odd. If -237 were even, there would exist $k \in \mathbb{Z}$ such that $-237 = 2k$. But this would imply that $k = \frac{-237}{2} \notin \mathbb{Z}$. Therefore, -237 is not even.

(b) Let $b = 1854$ and $a = 17$. We find $q, r \in \mathbb{Z}$ such that $b = qa + r$, where $0 \leq r < a$. Because $a > 0$, we have $q = \left\lfloor \frac{b}{a} \right\rfloor = \left\lfloor \frac{1854}{17} \right\rfloor = 109$. But then $r = b - qa = 1854 - 109(17) = 1854 - 1853 = 1$. Therefore, we have $1854 = 109(17) + 1$.

(c) Observe that...



Therefore, the prime factorization of 2040 is $2040 = 2^3 \cdot 3 \cdot 5 \cdot 17$.

(d) We know that if $a = \prod_i p_i^{a_i}$ and $b = \prod_i p_i^{b_i}$, where the p_i are prime and $a_i, b_i \geq 0$, then $\gcd(a, b) = \gcd\left(\prod_i p_i^{a_i}, \prod_i p_i^{b_i}\right) = \prod_i p^{\min(a_i, b_i)}$. But then we have...

$$\gcd(2^{173} \cdot 3^{187} \cdot 5^{685} \cdot 11^{203},\ 2^{578} \cdot 3^{281} \cdot 7^{323} \cdot 13^{360}) = 2^{173} \cdot 3^{187}$$

Any divisors of two positive integers a, b divides the $\gcd(a, b)$. But then if $\gcd(a, b) = \prod_i p_i^{g_i}$, where the p_i are prime and $g_i \geq 0$, any divisor of a, b must be of the form $\prod_i p_i^{d_i}$, where $0 \leq d_i \leq g_i$. Assuming $\gcd(a, b) > 1$, the next greatest divisor must have the same prime factorization as $\gcd(a, b)$ with one less power of the smallest prime divisor of $\gcd(a, b)$ with nonnegative power. Applying this in the case above, the next largest divisor is $2^{172} \cdot 3^{187}$.

(e) We know that if $a = \prod_i p_i^{a_i}$ *and* $b = \prod_i p_i^{b_i}$*, where the* p_i *are prime and* $a_i, b_i \geq 0$*, then* $\operatorname{lcm}(a,b) = \operatorname{lcm}\left(\prod_i p_i^{a_i}, \prod_i p_i^{b_i}\right) = \prod_i p^{\max(a_i,b_i)}$*. But then we have...*

$$\operatorname{lcm}(2^{173} \cdot 3^{187} \cdot 5^{685} \cdot 11^{203},\ 2^{578} \cdot 3^{281} \cdot 7^{323} \cdot 13^{360}) = 2^{578} \cdot 3^{281} \cdot 5^{686} \cdot 7^{323} \cdot 11^{203} \cdot 13^{360}$$

Any multiple of two positive integers a, b *must be a multiple of* $\operatorname{lcm}(a,b)$*. But then if* $\operatorname{lcm}(a,b) = \prod_i p_i^{\ell_i}$*, where the* p_i *are prime and* $\ell_i \geq 0$*, any divisor of* a, b *must be of the form* $\prod_i p_i^{d_i}$*, where* $g_i \leq \ell_i$*. But then the next smallest multiple must have the same prime factorization as* $\operatorname{lcm}(a,b)$ *with one additional power of the smallest possible prime—namely, 2. Applying this in the case above, the next smallest multiple is* $2^{579} \cdot 3^{281} \cdot 5^{686} \cdot 7^{323} \cdot 11^{203} \cdot 13^{360}$.

7. (10 points) Showing all your work, compute the following:

   (a) $(2468 \cdot 3579 + 97531)$ mod 2

   (b) $(10 - 18)^{100}$ mod 3

   (c) $(3^{11} + 3^{10})$ mod 4

   (d) $(16 \cdot -7)$ mod 5

   (e) $(-17 \cdot 13 + 145)$ mod 6

Solution.

(a)

$$(2468 \cdot 3579 + 97531) \equiv 0 \cdot 1 + 1 \equiv 0 + 1 \equiv 1 \textit{ mod } 2$$

(b)

$$(10 - 18)^{100} \equiv (-8)^{100} \equiv 1^{100} \equiv 1 \textit{ mod } 3$$

(c)

$$(3^{11} + 3^{10}) \equiv 3^{10}(3 + 1) \equiv 3^{10} \cdot 4 \equiv 3^{10} \cdot 0 \equiv 0 \textit{ mod } 4$$

(d)

$$16 \cdot -7 \equiv 1 \cdot 3 \equiv 3 \textit{ mod } 5$$

(e)

$$-17 \cdot 13 + 145 \textit{ mod } 1 \cdot 1 + 1 \equiv 1 + 1 \equiv 2 \textit{ mod } 6$$

8. (10 points) Being sure to show all your work and fully explaining your logic, complete the following:

   (a) What is the remainder when 2022^{2024} is divided by 2023?

   (b) What are the last three digits of 2022^{50}?

   (c) Show that working modulo two that $(x+y)^2 = x^2 + y^2$.

Solution.

(a) The remainder when 2022^{2024} *is divided by* 2023 *is* 2022^{2024} *mod* 2023*. We have...*

$$2022^{2024} \equiv (-1)^{2024} \equiv 1 \text{ mod } 2023$$

Therefore, the remainder when 2022^{2024} *is divided by* 2023 *is 1.*

(b) The last three digits of 2022^{50} *is the remainder when* 2022^{50} *is divided by 1000. But this is precisely* 2022^{50} *mod* 1000*. Observe...*

$$\begin{aligned}
2022^1 &\equiv 22 \text{ mod } 1000 \\
2022^2 \equiv (2022^1)^2 &\equiv 22^2 \equiv 484 \text{ mod } 1000 \\
2022^4 \equiv (2022^2)^2 &\equiv 484^2 \equiv 234256 \equiv 256 \text{ mod } 1000 \\
2022^8 \equiv (2022^4)^2 &\equiv 256^2 \equiv 65536 \equiv 536 \text{ mod } 1000 \\
2022^{16} \equiv (2022^8)^2 &\equiv 536^2 \equiv 287296 \equiv 296 \text{ mod } 1000 \\
2022^{32} \equiv (2022^{16})^2 &\equiv 296^2 \equiv 87616 \equiv 616 \text{ mod } 1000
\end{aligned}$$

Observe that $50 = 32 + 16 + 2$*. But then...*

$$2022^{50} \equiv 2022^{32+16+2} \equiv 2022^{32} \cdot 2022^{16} \cdot 2022^2 \equiv 616 \cdot 296 \cdot 484 \equiv 182336 \cdot 484 \equiv 336 \cdot 484 \equiv 162624 \equiv 624 \text{ mod } 1000$$

(c) Observe that working modulo 2, we have...

$$(x+y)^2 = (x+y)(x+y) = x^2+xy+yx+y^2 = x^2+xy+xy+y^2 = x^2+2xy+y^2 \equiv x^2+y^2 \text{ mod } 2$$

9. (10 points) Let $a = 1561$ and $b = 8525$.

   (a) Use the Euclidean algorithm to find $\gcd(a, b)$.

   (b) Explain why a^{-1} exists mod b.

   (c) Continuing your work in (a), use the extended Euclidean algorithm to compute a^{-1} mod 8525.

   (d) Prove that your answer in (c) is correct.

Solution.

(a) Repeatedly applying the division algorithm with $b = 8525$ and $a = 1561$ and using the fact that $a > 0$, we have...

$$8525 = 5(1561) + 720; \quad q = \left\lfloor \frac{8525}{1561} \right\rfloor = 5, \quad r = 8525 - 5(1561) = 8525 - 7805 = 720$$

$$1561 = 2(720) + 121; \quad q = \left\lfloor \frac{1561}{720} \right\rfloor = 2, \quad r = 1561 - 2(720) = 1561 - 1440 = 121$$

$$720 = 5(121) + 115; \quad q = \left\lfloor \frac{720}{151} \right\rfloor = 5, \quad r = 720 - 5(121) = 720 - 605 = 115$$

$$121 = 1(115) + 6; \quad q = \left\lfloor \frac{121}{115} \right\rfloor = 1, \quad r = 121 - 1(115) = 121 - 115 = 6$$

$$115 = 19(6) + 1; \quad q = \left\lfloor \frac{115}{6} \right\rfloor = 19, \quad r = 115 - 19(6) = 115 - 114 = 1$$

$$6 = 6(1) + 0; \quad q = \left\lfloor \frac{6}{1} \right\rfloor = 6, \quad r = 6 - 6(1) = 6 - 6 = 0$$

Therefore, $\gcd(1561, 8525) = 1$.

(b) We know that a^{-1} exists modulo N if and only if $\gcd(a, N) = 1$. Using (a), we know $\gcd(1561, 8525) = 1$. Therefore, 1561^{-1} exists modulo 8525.

(c) Using the extended algorithm, we can write $1561x + 8525y = \gcd(1561, 8525) = 1$ for some x, y. But taking this equation modulo 8525, we have $1561x \equiv 1$ mod 8525. But then $1561^{-1} \equiv x$ mod 8525.

(d) First, solving for the remainders, we have...

$$\begin{aligned} 1 &= 115 - 19(6) \\ 6 &= 121 - 1(115) \\ 115 &= 720 - 5(121) \\ 121 &= 1561 - 2(720) \\ 720 &= 8525 - 5(1561) \end{aligned}$$

But then using the extended Euclidean algorithm, we have...

$$\begin{aligned}
1 &= 115 - 19(6) \\
&= 115 - 19\big(121 - 1(115)\big) = 115 - 19 \cdot 121 + 19 \cdot 115 = 20 \cdot 115 - 19 \cdot 121 \\
&= 20\big(720 - 5(121)\big) - 19 \cdot 121 = 20 \cdot 720 - 100 \cdot 121 - 19 \cdot 121 = 20 \cdot 720 - 119 \cdot 121 \\
&= 20 \cdot 720 - 119\big(1561 - 2(720)\big) = 20 \cdot 720 - 119 \cdot 1561 + 238 \cdot 720 = 258 \cdot 720 - 119 \cdot 1561 \\
&= 258\big(8525 - 5(1561)\big) - 119 \cdot 1561 = 258 \cdot 8525 - 1290 \cdot 1561 - 119 \cdot 1561 \\
&= -1409 \cdot 1561 + 258 \cdot 8525
\end{aligned}$$

Taking this equation modulo 8525, we have $-1409 \cdot 1561 \equiv 1$ *mod* 8525*. But then* $-1409 \equiv 7116$ *mod* 8525 *is the inverse of 1561 modulo* 8525*, i.e.* $1561^{-1} \equiv 7116$ *mod* 8525*.*

(e) The inverse of an element a *mod* N *is an element* b *mod* N *such that* $ab \equiv 1$ *mod* N*. The inverse, when it exists, is unique. Therefore, we only need check that* $1561 \cdot 7116 \equiv 1$ *mod* 8525*. This is routine:*

$$1561 \cdot 7116 \equiv 11108076 \equiv 1303(8525) + 1 \equiv 1 \text{ mod } 8525$$

10. (10 points) Solve the following system of congruences and show that your solution is correct:

$$\begin{cases} x + 1 \equiv 2 \bmod 3 \\ x \equiv 0 \bmod 5 \\ 3x + 4 \equiv 2 \bmod 7 \\ 1 - x \equiv 4 \bmod 11 \end{cases}$$

Solution. *First, we put each congruence into the form* $x \equiv a_i \mod m_i$.

$$\begin{array}{llll} x + 1 \equiv 2 \textit{ mod } 3 & x \equiv 0 \textit{ mod } 5 & 3x + 4 \equiv 2 \textit{ mod } 7 & 1 - x \equiv 4 \textit{ mod } 11 \\ x \equiv 1 \textit{ mod } 3 & x \equiv 0 \textit{ mod } 5 & 3x \equiv -2 \textit{ mod } 7 & 1 \equiv x + 4 \textit{ mod } 11 \\ & & 3x \equiv 5 \textit{ mod } 7 & x \equiv -3 \textit{ mod } 11 \\ & & 3^{-1} \cdot 3x \equiv 3^{-1} \cdot 5 \textit{ mod } 7 & x \equiv 8 \textit{ mod } 11 \\ & & x \equiv 5 \cdot 5 \textit{ mod } 7 & \\ & & x \equiv 25 \textit{ mod } 7 & \\ & & x \equiv 4 \textit{ mod } 7 & \end{array}$$

Therefore, this system of congruences is equivalent to the following system of congruences:

$$\begin{cases} x \equiv 1 \textit{ mod } 3 \\ x \equiv 0 \textit{ mod } 5 \\ x \equiv 4 \textit{ mod } 7 \\ x \equiv 8 \textit{ mod } 11 \end{cases}$$

Because $\gcd(3, 5, 7, 11) = 1$*, the Chinese Remainder Theorem states that there is a solution, which is unique modulo* $M := 3 \cdot 5 \cdot 7 \cdot 11 = 1155$*. The solution(s) have the same residue class as* $x = \sum a_i N_i M_i$*, where* $M_i = M/m_i$ *and* $N_i = M_i^{-1}$ *mod* m_i*. From the work above, we have...*

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 0 \\ a_3 &= 4 \\ a_4 &= 8 \end{aligned}$$

Furthermore, we have...

$$\begin{aligned} M_1 &= \frac{M}{m_1} = \frac{1155}{3} = 5 \cdot 7 \cdot 11 = 385 \\ M_2 &= \frac{M}{m_2} = \frac{1155}{5} = 3 \cdot 7 \cdot 11 = 231 \\ M_3 &= \frac{M}{m_3} = \frac{1155}{7} = 3 \cdot 5 \cdot 11 = 165 \\ M_4 &= \frac{M}{m_4} = \frac{1155}{11} = 3 \cdot 5 \cdot 7 = 105 \end{aligned}$$

Now we need compute $N_i = M_i^{-1} \mod m_i$*. First, we reduce each* M_i *modulo* m_i*:*

$$M_1 = 385 \equiv 1 \textit{ mod } 3$$
$$M_2 = 231 \equiv 1 \textit{ mod } 5$$
$$M_3 = 165 \equiv 4 \textit{ mod } 7$$
$$M_4 = 105 \equiv 6 \textit{ mod } 11$$

Clearly, $N_1 = M_1^{-1}$ *mod* $3 = 1^{-1}$ *mod* $3 = 1$ *mod* 3*. Similarly, we know* $N_2 = M_2^{-1}$ *mod* $5 = 1^{-1}$ *mod* $5 = 1$ *mod* 5*. To compute* $N_3 = M_3^{-1}$ *mod* $7 = 4^{-1}$ *mod* 7*. But because* $4 \cdot 2 = 8 \equiv 1$ *mod* 7*, we know that* $N_3 = 4^{-1} \equiv 2$ *mod* 7*. Finally, we need to compute* $N_4 = M_4^{-1}$ *mod* $11 = 6^{-1}$ *mod* 11*. But because* $6 \cdot 2 = 12 \equiv 1$ *mod* 11*, we know that* $N_4 = 6^{-1} \equiv 2$ *mod* 11*. Therefore, we have...*

$$N_1 = 1$$
$$N_2 = 1$$
$$N_3 = 2$$
$$N_4 = 2$$

But then the unique solution modulo $M = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$ *is...*

$$\sum a_i N_i M_i = 1(1)385 + 0(1)231 + 4(2)165 + 8(2)105 = 385 + 0 + 1320 + 1680 = 3385 \equiv 1075 \textit{ mod } 1155$$

Therefore, the unique solution modulo 1155 is 1075 and the integer solutions are those integers n *such that* $n \equiv 1075$ *mod* 1155*, e.g.* -1235*,* -80*,* 1075*,* 2230*,* 3385*, etc.*