Solutions for the 2nd Practice Midterm

1. (a) **Use the Euclidean Algorithm to find the greatest common divisor of 44 and 17.**
   The Euclidean Algorithm yields:

$$\begin{aligned} 44 &= 2 \cdot 17 + 10 \\ 17 &= 1 \cdot 10 + 7 \\ 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1. \end{aligned}$$

   Therefore the greatest common divisor of 44 and 17 is $\boxed{1}$.

   (b) **Find whole numbers x and y so that $44x + 17y = 1$ with $x > 10$.**
   Since the g.c.d. of 44 and 17 is 1 we know that a solution to $44x + 17y = 1$ has to exist, and we can obtain it by running the Euclidean Algorithm backwards:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ 1 &= 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 2 \cdot 10 \\ 1 &= 3 \cdot (17 - 10) - 2 \cdot 10 = 3 \cdot 17 - 5 \cdot 10 \\ 1 &= 3 \cdot 17 - 5 \cdot (44 - 2 \cdot 17) = 13 \cdot 17 - 5 \cdot 44. \end{aligned}$$

   So $44x + 17y = 1$ with $x = -5$, $y = 13$. We need to find a different solution with $x > 10$. For this we add a "zero combination"

$$\begin{aligned} -5 \cdot 44 + 13 \cdot 17 &= 1 \\ 17 \cdot 44 - 44 \cdot 17 &= 0 \end{aligned}$$

   and get

$$12 \cdot 44 - 31 \cdot 17 = 1.$$

   Therefore $\boxed{x = 12,\ y = -31}$ is a possible solution with $x > 10$.

   (c) Find whole numbers x and y so that $44x + 17y = 1$ with $y > 10$.
   The first solution above already works: $\boxed{x = -5,\ y = 13}$.

2. **For each of the following four parts say whether there are whole numbers x and y satisfying the equation. If an equation has a solution, write down a possible choice of x and y.**

   (a) $69x + 123y = 2$.
   Both $69 = 3 \cdot 23$ and $123 = 3 \cdot 41$ are divisible by 3 (in fact 3 is the g.c.d. of 69 and 123). Therefore $69x + 123y = 2$ $\boxed{\text{does not have a solution}}$ because 2 is not divisible by 3.

(b) $47x + 21y = 2$.
Use the Euclidean Algorithm:

$$47 = 2 \cdot 21 + 5$$
$$21 = 4 \cdot 5 + 1.$$

The g.c.d. is 1, so the given equation has a solution. Running the Euclidean Algorithm backwards gives:

$$1 = 21 - 4 \cdot 5$$
$$1 = 21 - 4 \cdot (47 - 2 \cdot 21) = 9 \cdot 21 - 4 \cdot 47.$$

Finally, we multiply by two:

$$2 = 18 \cdot 21 - 8 \cdot 47.$$

Therefore $\boxed{x = -8,\ y = 18}$ is a possible solution.

(c) $47x - 21y = 6$.
From (b) we know that the g.c.d. of 47 and 21 is 1, so the equation has a solution. In fact we only need to multiply the last equation of the solution of (b) by 3 (and be careful in reading off x and y because the sign in the equation changed!):

$$6 = 54 \cdot 21 - 24 \cdot 47,$$

so $\boxed{x = -24,\ y = -54}$ work.

(d) $49x + 21y = 6$.
As 7 divides both $49 = 7^2$ and $21 = 3 \cdot 7$ but not 6, this linear combination problem has $\boxed{\text{no solution}}$ in whole numbers x, y.

3. (a) **Is the binomial coefficient $\binom{12}{4}$ divisible by 11?**
By the formula for the the binomial coefficients we have

$$\binom{12}{4} = \frac{12 \times 11 \times 10 \times 9}{2 \times 3 \times 4} = \frac{11 \times 10 \times 9}{2} = 3^2 \times 5 \times 11$$

In particular the binomial coefficient $\boxed{\text{is divisible}}$ by 11.

(b) **How many divisors does $\binom{12}{4}$ have?**
Any of its divisors is of the form $3^a 5^b 11^c$ where $a = 0, 1, 2$, $b = 0, 1$, $c = 0, 1$. This implies that the total number of divisors is $3 \times 2 \times 2 = \boxed{12}$.

(c) **How many of them are divisible by 3?**
The ones divisible by 3 must have the property that $a = 1$ or $a = 2$ so their total number is $2 \times 2 \times 2 = \boxed{8}$.

4. **Let $m = 1100$ and $n = 2^2 \times 3^3 \times 5^5$.**

(a) **Compute $\gcd(m, n)$.**
The first thing to notice is that $m = 11 \times 100 = 11 \times 2^2 \times 5^2$. This implies that the greatest common divisor of m and n is $\boxed{2^2 \times 5^2}$.

(b) **How many whole numbers divide m but not n?**

To find how many whole numbers divide m but not n, by the subtraction principle, we have to subtract from the number of the divisors of m the number of divisors which also divide n. A whole number divides both m and n if and only if it divides $\gcd(m, n)$. The number of divisors of m is $(1 + 1)(2 + 1)(2 + 1) = 18$ and the number of divisors of $\gcd(m, n) = 2^2 5^2$ is $(2 + 1)(2 + 1) = 9$. The final answer is $18 - 9 = \boxed{9}$.

(c) **How many whole numbers divide n but not m?**

Analogously, here we have to subtract the number of divisors of $\gcd(m, n)$ from the number of divisors of n. We get the final answer $(2 + 1)(3 + 1)(5 + 1) - 9 = \boxed{63}$.

5. **Do the following calculations.**

(a) $7 \cdot 9 \pmod{36}$.

This is straight-forward: $7 \cdot 9 \equiv 63 \equiv \boxed{27} \pmod{36}$.

(b) $8 - 21 \pmod{31}$.

Again, this is an easy computation: $8 - 21 \equiv -13 \equiv \boxed{18} \pmod{31}$.

(c) $68 \cdot 69 \cdot 71 \pmod{72}$.

If we note that $68 \equiv -4$, $69 \equiv -3$, and $71 \equiv -1$ (all of these are taken $\pmod{72}$), then we get

$$68 \cdot 69 \cdot 71 \equiv -4 \cdot -3 \cdot -1 \equiv -12 \equiv \boxed{60} \pmod{72}.$$

(d) $108! \pmod{83}$.

Note that 83 divides 108!. Therefore, $108! \equiv \boxed{0} \pmod{83}$.

(e) $60^{59} \pmod{61}$.

Observe that $60 \equiv -1 \pmod{61}$. Thus

$$60^{59} \equiv (-1)^{59} \equiv -1 \equiv \boxed{60} \pmod{61}$$

(f) $1/2 \pmod{17}$.

We see that $2 \cdot 9 \equiv 18 \equiv 1 \pmod{17}$. This means that $1/2 \equiv \boxed{9} \pmod{17}$.

(g) $1/11 \pmod{43}$.

We could use the Euclidean algorithm, but inspired by the last problem, we can see a short-cut. Note that $4 \cdot 11 \equiv 44 \equiv 1 \pmod{43}$. Thus $1/11 \equiv \boxed{4} \pmod{43}$.

(h) $1/2 \pmod{8}$.

It's obvious that 2 and 8 are not relatively prime, and thus that this fraction $\boxed{\text{does not exist}}$.

6. (a) **What is the last digit of 3^{10}?**

To find the last digit of a number is the same as computing this number mod10. We have

$$3^{10} \equiv 9^5 \equiv (-1)^5 \equiv -1 \equiv 9 \bmod 10$$

so the last digit is $\boxed{9}$.

(b) **Compute $2^{(3^{10})} \pmod{11}$. (Note that this is *not* the same as $(2^3)^{10} \pmod{11}$.)**

If we let $a = 3^{10}$, then we now have to compute $2^a \bmod 11$. But we know that $a \equiv 9 \bmod 10$ and by Fermat's theorem $2^a \equiv 2^9 \bmod 11$. Now $2^9 \equiv 8^3 \equiv (-3)^3 \equiv -27 \equiv \boxed{6} \bmod 11$.

(c) **Compute $3^{(2^{10})} \pmod{11}$.**
Notice that the last digit of 2^{10} is 4 and we have

$$3^{2^{10}} \equiv 3^4 \equiv 81 \equiv \boxed{4} \bmod 11.$$

7. (a) **Find an x between 0 and 19 such that $x^2 \equiv 5 \bmod 19$.**
By trying various possibilities we find that $9^2 = 81 \equiv \boxed{5} \bmod 19$.

(b) **What does Fermat's theorem say about powers of x?**
Fermat's theorem says that $x^{18} \equiv 1 \bmod 19$ for any x not divisible by 19.

(c) **Compute $5^9 \bmod 19$.**
Combining the two congruences from the last two parts, we find that $5^9 \equiv 9^{18} \equiv \boxed{1} \bmod 19$.

8. (a) **Use the Euclidean Algorithm to find the reciprocal of 40 mod 93. Check your work by verifying that your answer is in fact a solution of $40x \equiv 1 \bmod 93$.**
We find $\gcd(40, 93)$ as a linear combination ("combo") of 40 and 93:

$$\begin{aligned} 13 &= 93 - 2 \times 40 \\ 1 &= 40 - 3 \times 13 = 40 - 3 \times (93 - 2 \times 40) = 7 \times 40 - 3 \times 93, \end{aligned}$$

so $7 \times 40 \equiv 1 \bmod 93$ and the reciprocal of 40 is $\boxed{7}$. Check:

$$7 \times 40 = 280 = 1 + 3 \times 93 \equiv 1 \bmod 93.$$

(b) **Using your answer to the first part, find the reciprocals mod 93 of 4 and 89. (Hint: $4 + 89 = 93$.)**
Since $1/40$ is 7 mod 93 we have

$$1/4 = 10/40 = 10 \times (1/40) \equiv 10 \times 7 = 70 \bmod 93.$$

Thus the reciprocal of 4 is $\boxed{70}$ mod 93. Since $89 \equiv -4 \bmod 93$, it follows that the reciprocal of 89 is -70, that is, $\boxed{23}$ mod 93.

9. (a) **Which of the numbers 90, 91, 92, . . . , 100 has a reciprocal mod 100?**
The numbers with a reciprocal mod n are those that are relatively prime to n. Here $n = 100$, and a number is relatively prime to 100 if and only if it is neither even nor a multiple of 5. Of the numbers between 90 and 100, those that match this description are $\boxed{91, 93, 97, \text{and } 99}$.

(b) **Choose two of the numbers you found in the first part and compute their reciprocals mod 100.**
The easiest reciprocal is that of 99, because $99 \equiv -1 \bmod 100$ so the reciprocal of 99 is $1/-1 = -1 \equiv \boxed{99} \bmod 100$. Since $91 \equiv -9$ and $97 \equiv -3$, the reciprocals of 91 and 97 can both be obtained using the fact that

$$-1 \equiv 99 = 3 \times 33 = 9 \times 11 \bmod 100 :$$

the reciprocal of 97 is $1/97 \equiv (-99)/(-3)$, which is to say $\boxed{33}$, and likewise the reciprocal of 91 is $\boxed{11}$. If you chose 93, you had to work hard, probably using the Euclidean Algorithm as above; for the record, the reciprocal of 93 mod 100 is $\boxed{57}$.

10. **The goal of this problem is to find reciprocals mod 21 for all the numbers mod 21 that have such a reciprocal. Record your answers in the table below.**

x	0	1	2	3	4	5	6	7	8	9
$1/x$	NONE	1								

x	10	11	12	13	14	15	16	17	18	19	20
$1/x$											

(a) **Identify all the numbers x other than 0 that have no reciprocal mod 21, and enter NONE in the $1/x$ box of every such number.**

The numbers that have no reciprocal mod 21 are those that are not relatively prime to 21, that is, the numbers that have a common factor with 21 other than 1. These are the multiples of 3 or of 7. Having accounted for zero already, this leaves us with 3 and its multiples 6, 9, 12, 15, 18, and with 7 and its multiple 14.

(b) **What is $\frac{1}{20}$ mod 21?**

Since $20 \equiv -1 \bmod 21$, the reciprocal $1/20$ is congruent modulo 21 to $1/(-1) = -1 \equiv \boxed{20}$.

(c) **Use the fact that $2^6 \equiv 64 \equiv 1 \bmod 21$ to find the reciprocals of 2, 4, 8, and 16.**

Since $64 = 2 \times 32 = 4 \times 16 = 8 \times 8$ we see that $1/2 \equiv 32 \equiv 11 \bmod 21$, that 4 and 16 are each other's reciprocals, and that 8 is its own reciprocal.

(d) **Fill in the rest of the table.**

Since 11 is the reciprocal of 2, we know that 2 is the reciprocal of 11. Thus also gives us that the reciprocals of $-2, -4, -8, -11, -16$ (a.k.a. $19, 17, 13, 10, 5 \bmod 21$) are respectively $-11, -16, -8, -2, -4$ (a.k.a. $10, 5, 13, 19, 17 \bmod 21$). The complete table is therefore

x	0	1	2	3	4	5	6	7	8	9
$1/x$	NONE	1	11	NONE	16	17	NONE	NONE	8	NONE

x	10	11	12	13	14	15	16	17	18	19	20
$1/x$	19	2	NONE	13	NONE	NONE	4	5	NONE	10	20

11. **Please make the requested computations modulo 11 putting your answers in the range**

$$\{0, 1, 2, \ldots, 10\}.$$

(a) **Find $3^{12} \pmod{11}$.**

Since 11 is prime, Fermat's theorem tells us that $3^{10} \equiv 1 \pmod{11}$. Thus

$$3^{12} \equiv 3^{10} \cdot 3^2 \equiv \boxed{9} \pmod{11}.$$

(b) **Find $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \pmod{11}$.**

Note that

$$\begin{aligned} 2 \cdot 6 &\equiv 12 \equiv 1 \pmod{11}, \\ 3 \cdot 4 &\equiv 12 \equiv 1 \pmod{11}, \\ 7 \cdot 8 &\equiv 56 \equiv 1 \pmod{11}, \\ 5 \cdot 9 &\equiv 45 \equiv 1 \pmod{11}. \end{aligned}$$

Thus, by grouping all of these numbers into pairs, we see that

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv \boxed{1} \pmod{11}.$$

(c) **Does a solution to the equation**

$$5^{10}y \equiv 6^{61} \pmod{11}$$

exist? If it does, please find it.

Fermat's theorem tells us that $5^{10} \equiv 1 \pmod{11}$. Thus the equation simplifies to $y \equiv 6^{61} \pmod{11}$. Again using Fermat's theorem, we see that

$$6^{61} \equiv \left(6^{10}\right)^6 \cdot 6 \equiv 6 \pmod{11}.$$

So we can further simplify our equation to $y \equiv 6 \pmod{11}$. This clearly has exactly one solution, namely $\boxed{y = 6}$.

12. **Prof. Mazur goes to the supermarket and buys several dozen eggs. He uses them to make several batches of his famous crème brûlée. Each batch requires 7 eggs. When he's done cooking, he notices that he has 4 eggs left over. If he knows he bought less than 10 dozen eggs, how many dozen did he buy?**

Let x be the number of dozens of eggs he bought. Then the problem tells us that $12x \equiv 4 \pmod{7}$. We can simplify this by noting that $12 \equiv 5 \pmod{7}$. So we want to solve $5x \equiv 4 \pmod{7}$. One could use the Euclidean algorithm, but in this case it's not too hard to guess an answer since 7 is a small modulus. We see that $5 \cdot 5 \equiv 25 \equiv 4 \pmod{6}$. Thus $x \equiv 5 \pmod{7}$ (note that we know there is a unique solution since 5 and 7 are relatively prime, and thus division by 4 is well-defined in arithmetic $\pmod{7}$). Of course, Prof. Mazur bought some whole number of eggs, that is, a number in normal arithmetic, not a number in arithmetic $\pmod{7}$. Right now, all we know is that this number has remainder 5 when divided by 7. However, of all the numbers with that property, 5 is the only one which is positive and less than 10 (since we know he bought less than 10 dozen, and obviously one can't buy a negative number of eggs). Thus, Prof. Mazur must have bought $\boxed{5}$ dozen eggs.

13. **Florian is running laps on a small track. In fact, it takes him exactly 17 seconds to run a lap. After running for a while, he has run a whole number of laps and he notices that the second hand on his watch has advanced 6 seconds. If he knows he ran less than 70 laps, how many laps did he run?**

Let x be the number of laps Florian ran. Then we have that $17x \equiv 6 \pmod{60}$. Since division by 17 is allowed $\pmod{60}$ (because 17 and 60 are relatively prime), we have that $x \equiv 6/17 \pmod{60}$. The Euclidean algorithm gives

$$\begin{aligned} 60 &= 3 \cdot 17 + 9 \\ 17 &= 9 + 8 \\ 9 &= 8 + 1. \end{aligned}$$

Running it backwards, we get

$$\begin{aligned} 1 &= 9 - 8 \\ 1 &= 9 - (17 - 9) = -17 + 2 \cdot 9 \\ 1 &= -17 + 2(60 - 3 \cdot 17) = 2 \cdot 60 - 7 \cdot 17. \end{aligned}$$

We conclude that $1/17 \equiv -7 \equiv 53 \pmod{60}$. Thus

$$x \equiv 6/17 \equiv 6 \cdot (-7) \equiv -42 \equiv 18 \pmod{60}.$$

As in the last problem, we want to know the number of laps Florian ran as a whole number, not just its congruence class $\pmod{60}$. However, 18 is the only number congruent to 18 $\pmod{60}$ which is positive and less than 70. Thus we conclude that Florian ran $\boxed{18}$ laps.

14. (a) **What is the 3rd root of** 9 (mod 29)**?**

(b) **What is the 37th root of** 6 (mod 41)**?**

(c) **Find all square roots of** 2 (mod 7)**.**

In the first two cases, k and $p-1$ are relatively prime, so we can solve the equation

$$kx + (p-1)y = 1,$$

but in the last case, ($k = 2,\ p-1 = 6$) we cannot solve this equation. This tells us that we need to deal with the first two cases differently from the last case.

(a) When $k = 3$ and $p - 1 = 28$, the equation

$$kx + (p-1)y = 1$$

has as solution $x = -9,\ \ y = 1$: that is,

$$3 \cdot (-9) + 28 \cdot (+1) = 1.$$

It also has as another solution $x = 19,\ \ y = -2$. SO we have that our 3rd root of 9 (mod 29) can be written as, for example,

$$9^{-9} \pmod{29}$$

or

$$9^{19} \pmod{29}.$$

If you are explicitly asked to put the answer in the range $\{0, 1, 2, \ldots, 28\}$ you could, for example, do the standard "successive squaring technique" to figure out what 9^{19} is mod 29. But you could also deal with 9^{-9} (mod 29) in the following way: use the "successive squaring technique" to figure out 9^9 mod 29, which is 6 and then 9^9 is just 1/6 mod 29. Writing $1 \equiv 30$ mod 29 we see that $1/6 \equiv 30/6 \equiv \boxed{5}$ mod 29. To check our answer, we need only raise 5 to the 3rd power and check that it is congruent to 9 mod 29, which it is: $5^3 = 125 = 9 + 4 \cdot 29$.

(b) $k = 37$, $a = 6$, and $p = 41$ When $k = 37$ and $p - 1 = 40$ the equation

$$kx + (p-1)y = 1$$

has as solution $x = 13,\ \ y = -12$: that is,

$$37 \cdot (13) + 40 \cdot (-12) = 1,$$

so the 37th root of 6 (mod 41) is given by

$$6^{13} \pmod{41}.$$

Again if you are explicitly asked to put the answer in the range $\{0, 1, 2, \ldots, 40\}$ you can use the standard "successive squaring technique," but if in the process of working it through ($6^2 \equiv -5,\ 6^4 \equiv 25$, these all being congruences modulo 41) you notice that $6^6 \equiv 6^2 \cdot 6^4 \equiv -125 \equiv -2$ mod 41, you are pretty much home, because then $6^{12} \equiv 4$ and so $6^{13} \equiv \boxed{24}$ mod 41. To check, you must raise 24 to the 37th power, but don't despair of this check (if you want to do it) because it is the same as raising it to the -3rd power (since $24^{40} \equiv 1$) . That is, we must check that $24^{-3} \equiv 6$, or:

$$24^3 \cdot 6 \equiv 1 \text{ mod } 41,$$

which you can do easily if you want to ...

(c) Here the simple thing to do is to square all the numbers mod 7 and see what you get, the full tally being $0, 1, 2, 4$ modulo 7. Any number congruent to one of these modulo 7 has a "square root mod 7" and any number *not* congruent to one of these mod 7 does not have a "square root mod 7." In particular, 2 does have a square root, and in fact, it has–as any decent number that has square roots modulo 7 (other than zero) will have–precisely two of them modulo 7. The two square roots of two modulo 7 are $\boxed{3 \text{ and } 4}$ (modulo 7).