Answers to the Practice Questions for 2nd 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:

$$\begin{aligned} 47 &= 2 \cdot 21 + 5 \\ 21 &= 4 \cdot 5 + 1. \end{aligned}$$

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

$$\begin{aligned} 1 &= 21 - 4 \cdot 5 \\ 1 &= 21 - 4 \cdot (47 - 2 \cdot 21) = 9 \cdot 21 - 4 \cdot 47. \end{aligned}$$

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) **What is the largest prime number dividing the binomial coefficient $\binom{12}{4}$?**
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 $\boxed{11}$ is the largest prime dividing the binomial coefficient $\binom{12}{4}$. (Note: this can be immediately seen also from the second expression in the above equation, because 11 is the largest prime occurring in any of the factors and 11 occurs in the numerator but not in the denominator.)

(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 the divisors of $\binom{12}{4}$ are divisible by 3?**
The divisors of $\binom{12}{4}$ that are 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) **Compute** $\operatorname{lcm}(m, n)$**.**

   Using the prime factorization as in part (a), we find: $\operatorname{lcm}(m, n) = \boxed{2^2 \cdot 3^3 \cdot 5^5 \cdot 11}$.

   (c) **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 $18 - 9 = \boxed{9}$.

   (d) **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. As always, when working mod n, leave your answer in the range 0, 1, . . . , $n - 1$.**

   (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 $1/11 \equiv \boxed{4} \pmod{43}$.

6. (a) **Compute $21^{4600} \pmod{47}$.**

   Since 47 is prime and $21 \not\equiv 0 \pmod{47}$, we can apply Fermat's Theorem:

$$21^{4600} \equiv (21^{46})^{100} \equiv \boxed{1} \pmod{47}.$$

(b) **Compute** $21^{4601} \pmod{47}$**.**

$$21^{4601} = 21^{4600} \cdot 21 \equiv \boxed{21}$$

by part (a).

(c) **Compute** $21^{4599} \pmod{47}$**. (Hint: your work on 2(b) will help).**

Using part (a) (or part (b)):

$$21^{4599} \equiv 21^{4600} \cdot 21^{-1} \equiv 21^{-1} \equiv 1/21.$$

So we need to find the reciprocal of 21 (mod 47). This requires us to solve the combo problem

$$21x + 47y = 1,$$

where x will be the reciprocal we are looking for. Using the Euclidean Algorithm in the usual way, we arrive at the solution $x = 9$, $y = -4$. Thus $2^{4599} \equiv \boxed{9}$.

7. (a) **Compute** $87^{51} \pmod{47}$**.**

We can use Fermat's Theorem since 47 is a prime and $87 \not\equiv 0 \pmod{47}$. Thus:

$$87^{51} \equiv 87^5.$$

To compute this, use the doubling method:

$$\begin{aligned} 87^1 &\equiv -7 \\ 87^2 &\equiv 49 \equiv 2 \\ 87^4 &\equiv 4 \end{aligned}$$

and so the answer is $(-7) \cdot 4 \equiv -28 \equiv \boxed{19}$.

(b) **Compute** $94^{46} \pmod{47}$**.**

We *cannot* use Fermat's Theorem because $94 \equiv 0 \pmod{47}$. But it's much easier!

$$94^{46} \equiv 0^{46} \equiv \boxed{0} \pmod{47}.$$

8. (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 $5^9 \equiv 9^{18} \equiv \boxed{1} \bmod 19$.

9. (a) **Use the Euclidean Algorithm to find the reciprocal of $40 \bmod 93$. 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.

10. **The goal of this problem is to find reciprocals mod 23 for all the non-zero numbers mod 23. Record your answers in the table below.**

x	1	2	3	4	5	6	7	8	9	10	11
$1/x$	1										

x	12	13	14	15	16	17	18	19	20	21	22
$1/x$											

(a) **What is $\frac{1}{22}$ mod 23?**

Since $22 \equiv -1$ mod 23, the reciprocal $1/22$ is congruent modulo 23 to $1/(-1) = -1 \equiv \boxed{22}$.

(b) **Use the fact that $2^{11} \equiv 2048 \equiv 1$ mod 23 to find the reciprocals of 2, 4, 8, and 16.**

Since $2048 = 2 \times 1024 = 4 \times 512 = 8 \times 256 = 16 \times 128$ we see that $1/2 \equiv 1024 \equiv 12$ mod 23 (and hence $1/12 \equiv 2$), that 4 and $512 \equiv 6$ are each other's reciprocals, that 8 and $256 \equiv 3$ are each other's reciprocals, and that 16 and $128 \equiv 13$ are each other's reciprocals. (Of course, there are easier ways to notice most of these facts.)

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

$1/21 \equiv -1/2 \equiv -12 \equiv 11$ and conversely.
$1/20 \equiv -1/3 \equiv -8 \equiv 15$ and conversely.
$1/19 \equiv -1/4 \equiv -6 \equiv 17$ and conversely.
$1/7 \equiv -1/16 \equiv -13 \equiv 10$ and conversely.
Multiplying, $1/9 \equiv 1/3 \times 1/3 \equiv 64 \equiv 18$ and conversely.
Finally, $1/5 \equiv 14$ and conversely by process of elimination. We verify $5 \times 14 \equiv 70 \equiv 1$.

x	1	2	3	4	5	6	7	8	9	10	11
$1/x$	1	12	8	6	14	4	10	3	18	7	21

x	12	13	14	15	16	17	18	19	20	21	22
$1/x$	2	16	5	20	13	19	9	17	15	11	22

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

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

(a) **Find 3^{12} (mod 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

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

This is a special case of Wilson's theorem, which states that $(p-1)! \equiv -1 \pmod{p}$, or equivalently, that $(p-2)! \equiv 1 \pmod{p}$.

(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. **In analogy with the divisibility rule for 11, can you come up with a divisibility rule for 1001? (Hint: it will only be useful for really large numbers)**

Since 1001 is 1 different than a power of 10, if we expand out a number in terms of powers of 10, then we can reduce 10^3 to -1, 10^4 to -10, 10^5 to -100, 10^6 to 1, etc. So

$$a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 - a_3 \cdot -a_4 \cdot 10 - a_5 \cdot 10^2 + a_6 + a_7 \cdot 10 + a_8 \cdot 10^2 - a_9 - \cdots$$

In words, we break up our number into three digit chunks, and alternate adding and subtracting them. If the resulting number is divisible by 1001 (or 7, 11 or 13) then our initial number was divisible by 1001 (or 7, 11, 13 respectively).

For example, we can apply this process to 2506181496, yielding

$$\begin{aligned} 2506181496 &\equiv 496 - 181 + 506 - 2 \pmod{1001} \\ &\equiv 819 \pmod{1001} \end{aligned}$$

So 2506181496 is not divisible by 1001. We can now easily check divisibility by 7, 11 and 13:

$$\begin{aligned} 2506181496 &\equiv 819 \equiv 119 \equiv 0 \pmod{7} \\ 2506181496 &\equiv 819 \equiv 49 \equiv 5 \pmod{11} \\ 2506181496 &\equiv 819 \equiv 39 \equiv 0 \pmod{13} \end{aligned}$$

So 2506181496 is divisible by 7 and 13, but not 11.