Below is a collection of practice problems for midterm 2, many of which are borrowed from previous exams in similar courses. At students' request, I've provided a large collection of problems beyond a single practice exam. If you want to try a "model exam," you can use the first six problems for this purpose.

1. When the students in a classroom divide into groups of nine, there are four students left over. When the students break into groups of eleven, there is one student left over. Assuming that there are fewer than 100 students in the room, how many students must there be?

2. What is the remainder when 10^{100} is divided by 19?

3. (a) How many numbers between 1 and 1500 inclusive are relatively prime to 1500 (that is, share no common factors besides 1 with 1500)?
   (b) Find the sum of all positive divisors of 1500.
   (c) Find the remainder when 1493^{2002} is divided by 1500.

4. Prove that there are infinitely many prime numbers p such that $p \equiv 3 \pmod 4$.

   Since this is a fact that was proved in class, you should not simply cite the theorem from class, but rather give a proof. This is true for any other exam problems that ask you to prove a fact that was proved in class.

5. Let $n \geq 2$ be an integer such that $p = \frac{1}{2}(3^n - 1)$ is prime. Prove that n is also prime.

6. Suppose that p is a prime number, and a, b are integers such that $e_p(a) = 2$ and $e_p(b) = 3$. Prove that $e_p(ab) = 6$.

You can treat the first six problems as a "model exam." The remaining problems below are for additional practice.

7. Suppose that Bob's RSA public key is $(33, 13)$. Alice sends Bob the cipher text $c = 8$. What was Alice's plain text?
(Recall that if s is Alice's plain text, then she computes the cipher text c by computing the remainder when s^{13} is divided by 33.)

8. Suppose that a, e, f, and m are positive integers such that the following two congruences hold.

$$\begin{aligned} a^e &\equiv 1 \pmod{m} \\ a^f &\equiv 1 \pmod{m} \end{aligned}$$

Prove that

$$a^{\gcd(e,f)} \equiv 1 \pmod{m}.$$

9. Let $d(n)$ denote the number of divisors of n, including 1 and n. For example:

$$\begin{aligned} d(10) &= 4 \text{ (the divisors are } 1, 2, 5, 10) \\ d(17) &= 2 \text{ (the divisors are } 1, 17) \\ d(24) &= 8 \text{ (the divisors are } 1, 2, 3, 4, 6, 8, 12, 24) \end{aligned}$$

You may assume the following fact: if $\gcd(m, n) = 1$, then $d(mn) = d(m)d(n)$ (I encourage you to try to prove it, but you don't need to do it now).

(a) Find a formula for $d(p^k)$, where p is prime and $k \geq 1$.

(b) Compute $d(91000)$.

(c) Give a simple criterion to tell whether $d(n)$ is even or odd.

10. **Short answer questions.** You do not need to show any work. **Several questions have multiple possible answers; you only need to give one.**

(a) Compute the greatest common divisor of 77 and 91.

(b) Find a perfect number (that is, a positive number which is equal to twice the sum of all of its divisors, including 1 and itself).

(c) Find the smallest *positive* number of the form $15x + 39y$, where x and y are integers (positive or negative).

(d) Find a positive integer n such that $10^n \equiv 1 \pmod{113}$. (The number 113 is prime)

(e) Evaluate $\phi(130)$.

(f) Find a primitive root of 7.

11. Solve the congruence
$$x^{23} \equiv 5 \pmod{29}.$$
Your answer should be in the form $x \equiv a \pmod{m}$, where a is between 0 and $m-1$ inclusive.
(You may want to use the multiplication table on the last page.)
Hint. The answer will be congruent to 5^f for a well-chosen value of f.

12. Consider the rather large number $N = 2^{53^{69}}$ (Note that this is 2 raised to the power 53^{69}, not 2^{53} raised to the power 69.)
    (a) Find the remainder when N is divided by 4.
    (b) Find the remainder when N is divided by 25.
    (c) From parts (a) and (b), deduce the last two digits (units digit and tens digit) of N.

13. (a) Let p be an *odd* prime (i.e. a prime besides 2), and k be a positive integer. Prove that if $a^2 \equiv 1 \pmod{p^k}$, then either $a \equiv 1 \pmod{p^k}$ or $a \equiv -1 \pmod{p^k}$.
    (b) Find all integers a between 1 and 63 inclusive such that $a^2 \equiv 1 \pmod{64}$.

14. The number 2 is a primitive root modulo 29 (you may assume this without proof). If it is useful, you may use the modulo 29 multiplication table provided at the back of the packet.
    (a) Prove $e_{29}(4) = 14$.
    (b) State, with proof, a specific number $a \in \{1, \cdots, 28\}$ with order 7 modulo 29.
    (c) Give an example of another primitve root modulo 29. You do not need to prove that your answer is correct; just state the number and how you obtained it.

Multiplication table modulo 29:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	1	3	5	7	9	11	13	15	17	19	21	23	25	27
3	0	3	6	9	12	15	18	21	24	27	1	4	7	10	13	16	19	22	25	28	2	5	8	11	14	17	20	23	26
4	0	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	1	5	9	13	17	21	25
5	0	5	10	15	20	25	1	6	11	16	21	26	2	7	12	17	22	27	3	8	13	18	23	28	4	9	14	19	24
6	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23
7	0	7	14	21	28	6	13	20	27	5	12	19	26	4	11	18	25	3	10	17	24	2	9	16	23	1	8	15	22
8	0	8	16	24	3	11	19	27	6	14	22	1	9	17	25	4	12	20	28	7	15	23	2	10	18	26	5	13	21
9	0	9	18	27	7	16	25	5	14	23	3	12	21	1	10	19	28	8	17	26	6	15	24	4	13	22	2	11	20
10	0	10	20	1	11	21	2	12	22	3	13	23	4	14	24	5	15	25	6	16	26	7	17	27	8	18	28	9	19
11	0	11	22	4	15	26	8	19	1	12	23	5	16	27	9	20	2	13	24	6	17	28	10	21	3	14	25	7	18
12	0	12	24	7	19	2	14	26	9	21	4	16	28	11	23	6	18	1	13	25	8	20	3	15	27	10	22	5	17
13	0	13	26	10	23	7	20	4	17	1	14	27	11	24	8	21	5	18	2	15	28	12	25	9	22	6	19	3	16
14	0	14	28	13	27	12	26	11	25	10	24	9	23	8	22	7	21	6	20	5	19	4	18	3	17	2	16	1	15
15	0	15	1	16	2	17	3	18	4	19	5	20	6	21	7	22	8	23	9	24	10	25	11	26	12	27	13	28	14
16	0	16	3	19	6	22	9	25	12	28	15	2	18	5	21	8	24	11	27	14	1	17	4	20	7	23	10	26	13
17	0	17	5	22	10	27	15	3	20	8	25	13	1	18	6	23	11	28	16	4	21	9	26	14	2	19	7	24	12
18	0	18	7	25	14	3	21	10	28	17	6	24	13	2	20	9	27	16	5	23	12	1	19	8	26	15	4	22	11
19	0	19	9	28	18	8	27	17	7	26	16	6	25	15	5	24	14	4	23	13	3	22	12	2	21	11	1	20	10
20	0	20	11	2	22	13	4	24	15	6	26	17	8	28	19	10	1	21	12	3	23	14	5	25	16	7	27	18	9
21	0	21	13	5	26	18	10	2	23	15	7	28	20	12	4	25	17	9	1	22	14	6	27	19	11	3	24	16	8
22	0	22	15	8	1	23	16	9	2	24	17	10	3	25	18	11	4	26	19	12	5	27	20	13	6	28	21	14	7
23	0	23	17	11	5	28	22	16	10	4	27	21	15	9	3	26	20	14	8	2	25	19	13	7	1	24	18	12	6
24	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5
25	0	25	21	17	13	9	5	1	26	22	18	14	10	6	2	27	23	19	15	11	7	3	28	24	20	16	12	8	4
26	0	26	23	20	17	14	11	8	5	2	28	25	22	19	16	13	10	7	4	1	27	24	21	18	15	12	9	6	3
27	0	27	25	23	21	19	17	15	13	11	9	7	5	3	1	28	26	24	22	20	18	16	14	12	10	8	6	4	2
28	0	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1