MATH 13150: Freshman Seminar Practice Final Exam Answers

1. Compute $7^{1003} \pmod{33}$.

   $\phi(33) = 20, 7^{1000} \equiv 1 \pmod{33}$, so answer is $7^3 \equiv 13 \pmod{33}$

2. Suppose Alice wants to send a message to Bob using the RSA algorithm and $p = 11$, $q = 13$, and $k = 13$. If the secret number she wants to send Bob is "a=4", what is the encoded message she sends?

   $4^{13} \equiv 108 \pmod{143}$

3. Suppose Bob receives the encoded message "2" from Alice, and the messages was encoded using the RSA algorithm with $p = 11$, $q = 13$, and $k = 37$. What is the decoded message?

   $13 * 37 \equiv 1 \pmod{120}, so 2^{13*37} \equiv 2 \pmod{143}$. Answer is $2^{1/37} \equiv 2^{13} \equiv 41 \pmod{143}$

4. Suppose Alice has sent an encoded secret number to Bob using the RSA algorithm. Eve intercepts the encoded message "5" and knows that $n = 51$ and $k = 11$. What is the secret number?

   n=51 gives $\phi(n) = 32.11 * 3 \equiv 1 \pmod{32}$, so the secret number is $5^3 \equiv 23 \pmod{51}$

5. (a) How many seven digit phone numbers are there if a phone number cannot begin with 0?

   $9 \cdot 10^6$

   (b) How many seven digit phone numbers are there if a phone number cannot begin with 0, and no digits are repeated?

   $9 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4$

6. A class with 8 boys and 9 girls is choosing a three person team to play baseball against a team from another class. You can express your answer in terms of binomial numbers such as $\binom{5}{2}$; you do not need to convert binomial numbers into ordinary numbers.

   (a) How many possible three person teams have at least one girl?

   $\binom{17}{3} - \binom{8}{3}$

   (b) Suppose the team is to have a pitcher, a catcher, and a fielder. How many ways are there for the class to choose these three players, provided one of the players must be a girl?

   $\frac{17!}{14!} - \frac{8!}{5!}$

7. (a) Compute $\phi(495)$.
   240
   (b) How many numbers from 1 to 495 are relatively prime to 495?
   240
   (c) How many numbers from 1 to 495 are relatively prime to 165?
   The answer is still 240. Since $495 = 3^2 \cdot 5 \cdot 11$ and $165 = 3 \cdot 5 \cdot 11$ have the same prime factors, being relatively prime to 495 is the same as being relatively ptime to 165.
   (d) How many numbers from 1 to 495 are relatively prime to 495 and also to 101?
   The answer is 237. We consider the list of numbers from 1 to 495 that are relatively prime to 495. There are 240 numbers on that list. We have to decide how many of these 240 numbers are also relatively prime to 101. Since 101 is prime, the numbers from 1 to 495 that are not relatively prime to 101 are 101, 202, 303, and 404. Of these, 101, 202 and 404 are relatively prime to 495, but 303 is not. So we should omit $101, 202$ and 303 from the list, giving $240 - 3 = 237$ numbers.

8. Explain the answers to the following problems.
   (a) Does 5 divide $\binom{40}{20}$?
   Yes, because 5^5 divides the numberator and only 5^4 divides the denominator, so a factor of 5 remains.
   (b) Does 35 divide $\binom{40}{20}$?
   Yes. We already saw that 5 divides $\binom{40}{20}$. Also, 7 divides $\binom{40}{20}$ since 7^3 divides the numerator and only 7^2 divides the denominator, so 35 divides $\binom{40}{20}$.
   (c) Does 4 divide $\binom{1001}{998}$?
   Yes, because $\binom{1001}{998} = \dfrac{1001 \cdot 1000 \cdot 999}{3 \cdot 2 \cdot 1}$, and 2^3 divides the numerator but only 2^1 divides the denominator, so a factor of 2^2 remains.

9. Do the following computations **mod 44** (hint $\phi(44) = 20$)
   (a) Compute $5^{20} + 5^{40} + 5^{60} + 5^{80} + 5^{100} - 5^{120} \pmod{44}$
   $4 \pmod{44}$
   (b) Compute $43^{2445} \pmod{44}$.
   $43 \pmod{44}$

10. Let $a = 3^2 \cdot 5^3 \cdot 7^2 \cdot 11^5$ and let $b = 18360$.

    (a) Find the greatest common divisor $gcd(a, b)$ of a and b. Express your answer in terms of its prime factorization and say how many divisors $gcd(a, b)$ has.
    $3^2 \cdot 5$

    (b) What is the prime factorization of the least common multiple of a and b?
    $2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11^5 \cdot 17$

11. Does $\frac{1}{13} \pmod{152}$ exist. Explain why or why not, and if it exists, compute it and express the answer as a positive number.

    $117 \pmod{152}$

12. Does $\sqrt[5]{13} \pmod{37}$ exist? If so, find it. If not, explain why not.

    $22 \pmod{37}$

13. These are some password generation problems. I've included a number of them, because there was no homework on these kinds of problems.

    (a) Alice and Bob want to create a password for their next RSA exchange. If Alice picks the prime to be 19 and $A = 2$, and Alice picks $k = 12$ and Bob picks $l = 5$, what is the password?
    $2^{12 \cdot 5} \pmod{19} \equiv 2^{60} \pmod{19} \equiv 7 \pmod{19}$,
    so the answer is 7.

    (b) Alice and Bob create a password with $p = 31$ and $A = 11$. If Alice chooses $k = 3$ and Bob tells her that $C = A^l \equiv 5 \pmod{31}$, what is the password?
    The answer is $5^3 \equiv 1 \pmod{31}$.

    (c) Alice and Bob create a password with $p = 19$ and $A = 2$. Suppose Alice chooses $k = 6$, and Bob tells her that $C = B^l \equiv 14 \pmod{19}$. If Bob tells Alice that the password is 10, should she believe that it is really Bob?
    The answer is no. The password is $14^6 \equiv 7 \pmod{19}$.

14. Suppose a cricket chirps for the first time at 1:00:13 AM (thirteen seconds after 1 AM), and every thirteen seconds after that.

    (a) What is the seconds reading on your digital clock the 19th time the cricket chirps?
    The answer is $13 \cdot 19 \equiv 7 \pmod{60}$.

    (b) Find a value of k so that the kth time the cricket chirps, the seconds reading on your digital clock is 6.
    The answer is $k = 42$. To find this, observe that the kth time the cricket chirps, the seconds reading is $13k \pmod{60}$. This will read 6 when $13 \cdot k \equiv 6 \pmod{60}$, or when $k = \frac{6}{13} \pmod{60}$. To compute this, show $\frac{1}{13} \equiv 37 \pmod{60}$, so $\frac{6}{13} \equiv 6 \cdot 37 \equiv 42 \pmod{60}$.

15. (a) Compute $7^{32} \pmod{120}$.

    The answer is 1. Indeed, $\phi(120) = 32$, so $7^{32} \equiv 1 \pmod{120}$ using Euler's theorem.

    (b) Compute $7^{704} \pmod{120}$.

    The answer is again 1, since 704 is a multiple of 32.

    (c) Compute $7^{391} \pmod{120}$.

    The answer is 103. To find this, note that 32 divides 391 12 times with remainder 7. From this it follows that $7^{391} \equiv 7^7 \equiv 103 \pmod{120}$.

    (d) Compute $120^{64} \pmod{120}$.

    The answer is $0^{64} \equiv 0 \pmod{120}$, since $120 \equiv 0 \pmod{120}$.

    (e) Compute $30^{35} \pmod{120}$.

    The answer is 0, but the problem is tricky. To answer it, note that $30 = 2 \cdot 3 \cdot 5$, and $120 = 2^3 \cdot 3 \cdot 5$. Thus, $30^3 = 2^3 \cdot 3^3 \cdot 5^3$ is a multiple of 120, so $30^3 \equiv 0 \pmod{120}$. Hence, $30^{35} \equiv 30^3 \cdot 30^{32} \equiv 0 \cdot 30^{32} \equiv 0 \pmod{120}$.

16. (a) Compute $5^{36} \pmod{37}$.

    The answer is 1 by Fermat's theorem.

    (b) Compute $5^{327} \pmod{37}$.

    $327 \equiv 3 \pmod{36}$, so $5^{327} \equiv 5^3 \equiv 14 \pmod{37}$.

    (c) Compute $74^{36} \pmod{37}$.

    $0^{36} \equiv 0 \pmod{37}$.

17. Compute $\sqrt[5]{3} \pmod{17}$.

    Since $5 \cdot 13 \equiv 1 \pmod{16}$, the answer is $3^{13} \equiv 12 \pmod{17}$.