

1. Compute  $7^{1003} \pmod{33}$  (if you got the answer by using the RSA project, then say that you did; otherwise, show some steps).

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

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?

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

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?

$$n=51 \text{ gives } \phi(n) = 32. 11 * 3 \equiv 1 \pmod{32}, \text{ so the secret number is } 5^3 \equiv 23 \pmod{51}$$

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

8. Explain the answers to the following problems.

- (a) Does 5 divide  $\binom{40}{20}$ ?

Yes, because  $5^5$  divides the numerator and only  $5^4$  divides the denominator.

- (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  $\binom{1001}{998} = \frac{1001 \cdot 1000 \cdot 999}{3 \cdot 2 \cdot 1}$ , and  $2^3$  divides the numerator but only  $2^1$  divides the denominator.

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 (mod 44)

- (b) Compute  $43^{2445} \pmod{44}$ .

43 (mod 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 (mod 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  $p = 31$ ,  $A = 11$ ,  $k = 3$  and  $l = 4$ . What is the password?  
 Since  $k \cdot l = 12$ , the answer is  $11^{12} \pmod{31}$ . But  $11^{12} \equiv 16 \pmod{31}$ , so the password is "16".
- (c) Alice and Bob create a password with  $p = 23$ ,  $A = 5$ ,  $k = 7$  and  $l = 5$ . What is the password?  
 Since  $k \cdot l = 7 \cdot 5 = 35$ , the password is  $5^{35} \equiv 21 \pmod{23}$ , so the password is "23".
- (d) Alice and Bob create a password with  $p = 211$ ,  $k = 34$ ,  $l = 17$ , and  $A = 3$ . What is the password?  
 Since  $k \cdot l = 34 \cdot 17 = 578$ , the password is  $3^{578} \equiv 182 \pmod{211}$ , so the password is "182". Use the modular arithmetic calculator for this one.
- (e) Alice and Bob create a password with  $p = 29$ ,  $k = 5$ ,  $l = 3$  and  $A = 2$ . What is the password?  
 Since  $5 \cdot 3 = 15$ , the password is  $2^{15} \pmod{29} \equiv 27 \pmod{29}$ , so the password is "27".
14. Extra Credit: Answer the following question to the best of your ability, or explain why you do not care. The question is encoded using a Caesar shift cipher.

OZG KZGMDV TW LZW FGLJW VSEW KLSJLAFY IMSJLWJTSUC FWPL QWSJ?

Have a great summer!