Homework 3 for Modular Arithmetic

Math-270: Discrete Mathematics

January 10, 2018

Review Questions

1. If a is coprime to b, what is $\gcd(a, b)$?
2. If the $\gcd(k, N) = 1$ then what do we know about $k^{-1} \bmod N$?

Note: The next few problems work mod 26. Feel free to use the mod 26 Cayley table.

3. Using the affine cipher with encryption function $f(p) = 11p + 14 \bmod 26$, how would you encrypt "STATS"?
4. Using the affine cipher with decryption function $g(c) = 21c+8 \bmod 26$, how would you decrypt "BEQ?"
5. Using the affine cipher with encryption function $f(p) = 11p + 14 \bmod 26$, how would you decrypt "CMFR"? (Danger: I said encryption function, not decryption function!)
6. What is the decryption function associated with the affine encryption function $f(p) = 17p + 20 \bmod 26$?
7. What is the encryption function associated with the affine encryption function $g(c) = 21c + 8 \bmod 26$?
8. Under what conditions for x and y would $f(p) = xp + y \bmod N$ have unique decodability? (hard)

New Questions

9. When we say that $\phi(a) = b$, what does that really mean?
10. What is $\phi(187)$?
11. What is $\phi(35)$?
12. What is $\phi(19)$?
13. What is $\phi(101)$?
14. A reliable person tells you that $\phi(5491) = 4896$. How many integers z with $0 < z < 5491$ are non-invertible mod 5491? How many are invertible mod 5491?
15. A reliable person tells you that $\phi(125) = 100$. How many integers z with $0 < z < 125$ are non-invertible mod 125? How many are invertible mod 125?
16. What is $5393^{763} \bmod 55$? Hint: use the upstairs-downstairs principle.
17. What is $1849^{1066} \bmod 77$? Hint: use the upstairs-downstairs principle.
18. What is $1921^{1914} \bmod 101$? Hint: use the upstairs-downstairs principle.
19. What are the last two digits of 1929^{1963}? Hint: use the upstairs-downstairs principle, and the fact that $\phi(100) = 40$.

Review Answers

1. Definitely the $gcd(a, b) = 1$. That's because "a is coprime to b" is an abbreviation for "$\gcd(a, b) = 1$." Lastly, note that writing "a is relatively prime to b" is equivalent to both of these.

2. If the $\gcd(k, N) = 1$ then we know that k^{-1} exists mod N, but we don't know anything more.

3. "STATS" becomes (18, 19, 0, 19, 18) and encrypts to $(f(18), f(19), f(0), f(19), f(18)) = (4, 15, 14, 15, 4)$ and that becomes "EPOPE."

4. "BEQ" becomes (1, 4, 16) and encrypts to $(g(1), g(4), g(16)) = (3, 14, 6)$ and that becomes "DOG."

5. Carry out the following steps:

   (a) "CMFR" becomes (2, 12, 5, 17).

   (b) Solve $2 = 11p + 14$ mod 26 for p. The answer is $p = 6$.

   (c) Solve $12 = 11p + 14$ mod 26 for p. The answer is $p = 14$.

   (d) Solve $5 = 11p + 14$ mod 26 for p. The answer is $p = 11$.

   (e) Solve $17 = 11p + 14$ mod 26 for p. The answer is $p = 5$.

   (f) (6, 14, 11, 5) becomes "GOLF."

6. The goal is to find the inverse function for $f(p) = 17p + 20$ mod 26.

$$\begin{aligned}
f(p) &= 17p + 20 \\
c &= 17p + 20 \\
c - 20 &= 17p \\
23(c - 20) &= 23(17p) \\
23c - 460 &= (391)p \\
23c - 460 + 18(26) &= (390 + 1)p \\
23c - 460 + 468 &= (26(15) + 1)p \\
23c + 8 &= (1)p \\
23c + 8 &= g(c)
\end{aligned}$$

   Therefore, the decryption function is $g(c) = 23c + 8$.

7. The goal is to find the inverse function for $g(c) = 21c + 8$ mod 26.

$$\begin{aligned}
g(c) &= 21c + 8 \\
p &= 21c + 8 \\
p - 8 &= 21c \\
5(p - 8) &= 5(21c) \\
5p - 40 &= 105c \\
5p - 40 + 52 &= (104 + 1)c \\
5p + 12 &= (4(26) + 1)c \\
5p + 12 &= c \\
5p + 12 &= f(p)
\end{aligned}$$

   Therefore, the encryption function is $f(p) = 5p + 12$.

8. The x has to be invertible mod N, and that means that $\gcd(x, N)$=1. That answers the question.

   Now you might be curious what the decryption function is. Suppose that x and z are inverses mod N. Let's see what happens.

$$\begin{aligned} c &= f(p) \\ c &= xp + y \\ c - y &= xp \\ z(c-y) &= z(xp) \\ zc - zy &= (zx)p \\ zc - zy &= (1)p \\ zc - zy &= g(c) \end{aligned}$$

   As you can see, $g(c) = zc - zy$ will turn any ciphertext c into the associated plaintext p. Since we have a function, we now know that any plaintext can be decoded. That means the encryption function is surjective. Since the domain and range are the same finite set (the integers mod N), we know that $f(p)$ being surjective also implies that $f(p)$ is injective and therefore bijective. Since the encryption function is bijective, the cipher is uniquely decodable.

   We've now proven that if x is invertible mod N, then $f(p) = xp + y$ mod N is uniquely decodable. The converse is also true. If $f(p) = xp + y$ mod N is uniquely decodable then x is invertible. This proof is harder, but you can ask me about it during office hours.

9. When we say that $\phi(a) = b$, what we mean is that

   - There are b integers z such that $0 < z < a$ and z is relatively prime to a.
   - There are b integers z such that $0 < z < a$ and z is coprime to a.
   - There are b integers z such that $0 < z < a$ and z is invertible mod a.
   - Of course, it goes without saying that since each of these three sentences is saying the same thing, that they are each acceptable answers.

10. We must notice that $187 = 11(17)$. Then $\phi(187) = \phi(17 \times 11) = 16 \times 10 = 160$. Note, this is only possible because 11 and 17 are prime.

11. While 35 is not prime, it is the product of two primes, so $\phi(35) = \phi(7 \times 5) = 6 \times 4 = 24$.

12. Because 19 is prime, $\phi(19) = 18$.

13. Because 101 is prime, $\phi(101) = 100$.

14. Because $\phi(5491) = 4896$, of the 5490 numbers z such that $0 < z < 5491$, we have 4896 that are invertible mod 5491, and $5490 - 4896 = 594$ that are not invertible mod 5491.

15. Because $\phi(125) = 100$, of the 124 numbers z such that $0 < z < 125$, we have 100 that are invertible mod 125, and $124 - 100 = 24$ that are not invertible mod 125.

16. The answer is $5393^{763} \equiv 27$ mod 55.

17. The answer is $1849^{1066} \equiv 1$ mod 77.

18. The answer is $1921^{1914} \equiv 22$ mod 101.

19. Because $1929^{1963} \equiv 89$ mod 100, we know that the last two digits of 1929^{1963} in the ordinary integers will be 89.