APM 5347 TEST 0 CORRECTIONS

JASON MEDCOFF

1. You are given a ciphered text, known to have been encrypted with a Vigenre cipher. You notice that the sequence jhfp appears at position 51 and 100 in the text. What does that tell you about the length of the key used? Why?

Solution. The difference in positions is $100 - 51 = 49$, so we have a good chance that the key length divides 49. The divisors of 49 are 1, 7, and 49. It seems likely that the key length is 7, as a key of length one reduces to a monoalphabetic cipher, and a key length of 49 is probably too large to be practical.

2. Use the supplied Vigenre table to encrypt the sentence todayisabeautifulday using the key martin.

Solution. We begin by writing the plaintext and the repeated key as follows:

$$\begin{array}{ccccccccccccccccccccc} t & o & d & a & y & i & s & a & b & e & a & u & t & i & f & u & l & d & a & y \\ m & a & r & t & i & n & m & a & r & t & i & n & m & a & r & t & i & n & m & a \end{array}$$

Using a Vigenre table, we compute the ciphered letters column by column, obtaining the ciphertext "foutgveasxihfiwntqmy".

3. Establish a one-to-one correspondence between the divisors of a positive integer n which are less than $\sqrt{n}$ and those that are greater than $\sqrt{n}$.

Solution. Let L_n be the set of divisors of n less than $\sqrt{n}$, and let G_n be the set of divisors of n greater than $\sqrt{n}$. Define a function

$$f : L_n \mapsto G_n,\ f(\ell) = \frac{n}{\ell} \text{ for some } \ell \in L_n.$$

We can easily show f is invertible; define a new function

$$h : G_n \mapsto L_n,\ h(g) = \frac{n}{g} \text{ for some } g \in G_n.$$

Then

$$f(h(g)) = f(n/g) = \frac{n}{\frac{n}{g}} = g$$

and similarly $h(f(\ell)) = \ell$. Therefore, f is invertible, and thus a one-to-one correspondence between the divisors as described.

4. True or False: the product of four consecutive positive integers is divisible by 24. Why or why not?

Solution. Every set of four consecutive integers contains one pair of even numbers; one is congruent to 2 mod 4 and the other is congruent to 0 mod 4. The product of these two is divisible by 8. The set also contains at least one number divisible by 3. So we have factors of 3 and 8, giving way to a larger factor of $(8)(3) = 24$.

5. Prove that $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b \mid a$.

Solution. $\Longleftarrow$) Since b divides a, we can write $a = kb$ for some integer k. We know that $a\mathbb{Z} = \{az : z \in \mathbb{Z}\}$, and since $a = kb$, we can write this as $\{kbz : z \in \mathbb{Z}\}$. Since kz is an integer, we see that every az in $a\mathbb{Z}$ is in $b\mathbb{Z}$. Thus $a\mathbb{Z} \subseteq b\mathbb{Z}$.

$\Longrightarrow$) Since every az in $a\mathbb{Z}$ is also in $b\mathbb{Z} = \{bz : z \in \mathbb{Z}\}$, it must be that $az = bzk$ for some k. Divide by z and we have $a = bk$, so $b \mid a$.

6. Find the gcd of 489 and 177 and express it as a linear combination of the two integers (i.e. find x and y such that $\gcd(489, 177) = 489x + 177y$).

Solution. Apply the Euclidean Algorithm.

$$\begin{aligned}
489 &= 177(2) + 135\\
177 &= 135(1) + 42\\
135 &= 42(3) + 9\\
42 &= 9(4) + 6\\
9 &= 6(1) + 3\\
6 &= 3(2)
\end{aligned}$$

We see that the gcd is 3. Obtain x and y by going backwards; first write each equation in terms of the remainder.

$$\begin{aligned}
3 &= 9 + 6(-1)\\
6 &= 42 + 9(-4)\\
9 &= 135 + 42(-3)\\
42 &= 177 + 135(-1)\\
135 &= 489 + 177(-2)
\end{aligned}$$

Substitute each remainder into the previous equation, collecting terms along the way.

$$\begin{aligned}
42 &= 489(-1) + 177(3)\\
9 &= 489(4) + 177(-11)\\
6 &= 489(-17) + 177(47)\\
3 &= 489(21) + 177(-58).
\end{aligned}$$

7. Describe, in detail, either Fermat's or Pollard's rho method to factor an integer and then illustrate on 51469 by manually running the algorithm and finding a factor.

Solution. Pollard's rho algorithm relies on choosing a function from a subset of the integers to itself and finding a collision. We compute iterated functions until we find such a collision giving way to a nontrivial factor.

Take $n = 51469$. Choose $f(x) = x^2 + 1$. Let $a, b = 2, 2$ and $d = 1$. Compute $a = f(a) = 5$ and $b = f(f(a)) = 677$. Then the gcd of $a - b$ and n is $\gcd(-672, 51469) = 1$. Again, compute $a = f(a) = 26$ and $b = f(f(a)) = 458330$. Then $\gcd(458304, 51469) = 11$. So 11 is a factor of 51469.