

MATH 470 Homework 2

1. Find all primes p for which the matrix $\begin{bmatrix} 1 & 3 \\ 5 & 7 \end{bmatrix}$ is invertible (mod p).

This matrix has determinant $\det A = 7 - 15 = -8$. To invert this mod p we require that $\gcd(\det A, p) = 1$. Obviously, $\gcd(-8, p) = 2$ if $p = 2$ so the matrix isn't invertible (mod 2). For any prime $p > 2$, $\gcd(8, p) = 1$ and so the matrix is invertible mod every odd prime.

2. Alice and Bob agree to use a Hill cipher with the 3×3 encryption matrix $M = \begin{bmatrix} 1 & 3 & 4 \\ 2 & 8 & 7 \\ 9 & 6 & 5 \end{bmatrix}$.
What should they use for the decryption matrix assuming they will use the normal 26 letter alphabet without spaces?

The answer is simply M^{-1} and we compute this to be $M^{-1} = \begin{bmatrix} 16 & 19 & 23 \\ 5 & 1 & 5 \\ 12 & 1 & 10 \end{bmatrix}$.

3. Eve intercepts messages from Alice that are intended for her two friends Bob and Ann:

ZJMXBZVZTHNGTTHXRQXZYTFVIXTTYUKQFHU

ZJMMRLFLNHNGTTHXRQXZYTFVIXTTYUKQFHU

Eve knows that Alice is using a Hill cipher and probably one with a small matrix. Alice also has a tendency to start every message with the salutation "dear xxx".....

It certainly seems that a very similar message was sent - perhaps differing only in (part of) the initial part. Can you read the message and recover Alice's key?

Can the block size be 2? If so, then "de" gets mapped to "ZJ" in both messages (correct), but "ar" gets mapped to "MX" in one and to "MM" in the other. If we believe that the message starts with "dear" then this is impossible - the matrix cannot take the same plaintext and provide two different codetexts. How about blocksize= 4? Then "dear" gets mapped to "ZJMX" in one message but to "ZJMM" in the other - again impossible. We clearly don't have enough information to do much if the blocksize was 5 or greater since we would have to recover at least 25 elements - and there isn't enough information to come close to this. This leaves a blocksize of $N = 3$ to try. In this case "dea" goes to "ZJM" in both messages, but now the next threesome is different in each codetext as we expect since the plaintext is "ran" in one and "rbo" in the other. We should also expect the next three letters in the cipher text to be different since the 7th letter in the plaintexts differ - one is "n", the other "b". From then on we are into the message and as we see the cipher texts are indeed the same. We should believe that $N = 3$.

What do we have? "dea" = $[3 \ 4 \ 0]$ goes into "ZJM" = $[25 \ 9 \ 12]$; "ran" = $[17 \ 0 \ 13]$ goes into "MRL" = $[12 \ 17 \ 11]$; and "rbo" = $[17 \ 1 \ 14]$ goes into "XBZ" = $[23 \ 1 \ 25]$. If M is the key matrix then we have $PM = C$ where P is the plaintext matrix and C the codetext.

$$\text{Here } P = \begin{bmatrix} 3 & 4 & 0 \\ 17 & 0 & 13 \\ 17 & 1 & 14 \end{bmatrix} \quad C = \begin{bmatrix} 25 & 9 & 12 \\ 12 & 17 & 11 \\ 23 & 1 & 25 \end{bmatrix}.$$

We can invert P since $\det P = 107$ and $\gcd(107, 26) = 1$. In fact,

$$P^{-1} = \begin{bmatrix} 13 & 10 & 0 \\ 23 & 12 & 13 \\ 3 & 13 & 14 \end{bmatrix} \text{ so } M := P^{-1}C = \begin{bmatrix} 3 & 1 & 6 \\ 4 & 8 & 5 \\ 7 & 2 & 9 \end{bmatrix}. \text{ Hence } M^{-1} = \begin{bmatrix} 10 & 3 & 9 \\ 25 & 11 & 9 \\ 4 & 1 & 20 \end{bmatrix}.$$

Using this, we decrypt to get the message. *dearbobtodoornottodothatisthequestion*

Note here that a message that starts with a known greeting is very dangerous for certain types of cipher - especially when the strong suspicion is that the addressee's name follows. Just think of a letter that went out to dozens of individuals starting with "dear professor xxxxxxxx" and ending with "yours sincerely yyyyyyyy". Quite a large blocksize Hill cipher could be cracked immediately with this information.

4. You were given information that a small amount of known plaintext was encrypted by a linear feedback shift register cipher. Subtracting, you find the first several bits of the key

1 0 1 0 0 1 1 1 0 1 0 0 1 1 1

Use this to try and determine the coefficients of the recursion sequence $x_{n+m} = \sum_{k=0}^{m-1} c_k x_{n+k}$ - where x_k, c_k are integers (mod 2) and hence break the cipher completely.

This is similar to the Hill cipher in terms of method of attack. We first try a recursion scheme of length 2: $x_{n+2} = c_0 x_n + c_1 x_{n+1}$. This gives $1 = x_3 = 1 \cdot c_0 + 0 \cdot c_1 = c_0$ and $0 = x_4 = 0 \cdot c_0 + 1 \cdot c_1 = c_1$. Thus $c_0 = 1$ and $c_1 = 0$ so that $x_{n+2} = x_n$. This would give a sequence where every other term is the same, and this does not fit here (and would be a bad choice anyway since it would be easily recognisable).

If we try length 3 then we have the scheme: $x_{n+3} = c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2}$. This gives $x_4 = 1 \cdot c_0 + 0 \cdot c_1 + 1 \cdot c_2 = 0$, $x_5 = 0 \cdot c_0 + 1 \cdot c_1 + 0 \cdot c_2 = 0$, $x_6 = 1 \cdot c_0 + 0 \cdot c_1 + 0 \cdot c_2 = 1$. Hence $c_0 = 1$, $c_1 = 0$ and $c_2 = 1$ and so we would have $x_{n+3} = x_n + x_{n+2}$. We check this out and see it does indeed generate our sequence.

If the length is four, $x_{n+4} = c_0 x_n + c_1 x_{n+1} + c_2 x_{n+2} + c_3 x_{n+3}$. Using $x_5 - x_8$ gives $c_0 + c_2 = 0$, $c_1 = 1$, $c_0 + c_3 = 1$, $c_2 + c_3 = 1$. This is **not** uniquely solvable, having two possible solutions: $c_0 = 0$, $c_1 = 1$, $c_2 = 0$, $c_3 = 1$ and $c_0 = 1$, $c_1 = 1$, $c_2 = 1$, $c_3 = 0$. Either of these generate our given sequence. Note this is exactly the behaviour we expect in light of the theorem on page 48. The shortest recursion sequence is the one of length 3; $x_{n+3} = x_n + x_{n+2}$ and all longer sequences generate a matrix with zero determinant (mod 2),

5. Find the gcd of 5678 and 1785. (Do this one by hand and show all steps).

$$\begin{aligned} 5678 &= 3 \cdot 1785 + 323 \\ 1785 &= 5 \cdot 323 + 170 \\ 323 &= 1 \cdot 170 + 153 \\ 170 &= 1 \cdot 153 + 17 \\ 153 &= 9 \cdot 17 + 0 \end{aligned}$$

Thus the gcd = 17. We have $q_1 = 3$, $q_2 = 5$, $q_3 = q_4 = 1$ and so from $x_n = -q_{n-1} x_{n-1} + x_{n-2}$ with $x_0 = 1$, $x_1 = 0$ we obtain $x_2 = 1$, $x_3 = -5$, $x_4 = 6$, $x_5 = -11$, For the y_j sequence, $y_0 = 0$,

$y_1 = 1$ and so $y_2 = -3, y_3 = 16, y_4 = -19, y_5 = 35$, Hence $(-11)5678 + (35)1785 = 17$.

6. Find the gcd of 123456789 and 987654321 (your program should do all the work, but print out each step).

This was a tease - no computer necessary here - a much easier problem than either of the others:

$$987654321 = 8 \cdot 123456789 + 9$$

$$123456789 = 13717421 \cdot 9 + 0$$

Thus the gcd = 9 .

Here $x_0 = 1, x_1 = 0, x_2 = 1; y_0 = 0, y_1 = 1, y_2 = -q_1 = -8$; Thus $987654321(1) + 123456789(-8) = 9$. (You weren't asked for this, but since it was so easy to do)

7. Calculate $d := \mathbf{gcd}(3579, 1357)$. Use the Extended Euclidean algorithm to find integers x and y such that $3579x + 1357y = d$. Show *all* the intermediate steps of the calculation.

		$x_0 = 1$	$y_0 = 0$
		$x_1 = 0$	$y_1 = 1$
$3579 = 2 \cdot 1357 + 865$	$q_1 = 2$	$x_2 = 1$	$y_2 = -2$
$1357 = 1 \cdot 865 + 492$	$q_2 = 1$	$x_3 = -1$	$y_3 = 3$
$865 = 1 \cdot 492 + 373$	$q_3 = 1$	$x_4 = 2$	$y_4 = -5$
$492 = 1 \cdot 373 + 119$	$q_4 = 1$	$x_5 = -3$	$y_5 = 8$
$373 = 1 \cdot 119 + 16$	$q_5 = 1$	$x_6 = 11$	$y_6 = -29$
$119 = 7 \cdot 16 + 7$	$q_6 = 7$	$x_7 = -80$	$y_7 = 211$
$16 = 2 \cdot 7 + 2$	$q_7 = 2$	$x_8 = 171$	$y_8 = -451$
$7 = 3 \cdot 2 + 1$	$q_8 = 3$	$x_9 = -593$	$y_9 = 1564$
$2 = 1 \cdot 1 + 0$			

Thus the gcd = 1, and $(-593)3579 + (1564)1357 = 1$.