10.7 Linear Algebra for Cryptography

1 Codes can use finite fields as alphabets: letters in the message become numbers $0, 1, \ldots, p-1$.

2 The numbers are added and multiplied $(mod\ p)$. Divide by p, keep the remainder.

3 A Hill Cipher multiplies blocks of the message by a secret matrix $E\ (mod\ p)$.

4 To decode, multiply each block by the inverse matrix $D\ (mod\ p)$. Not a very secure cipher!

Cryptography is about encoding and decoding messages. Banks do this all the time with financial information. Amazingly, modern algorithms can involve extremely deep mathematics. "Elliptic curves" play a part in cryptography, as they did in the sensational proof by Andrew Wiles of Fermat's Last Theorem.

This section will not go that far! But it will be our first experience with *finite fields* and *finite vector spaces*. The field for $\mathbf{R}^n$ contains all real numbers. The field for "modular arithmetic" contains only p integers $0, 1, \ldots, p-1$. There were infinitely many vectors in $\mathbf{R}^n$—now there will only be p^n messages of length n in message space. The alphabet from A to Z is finite (as in $p = 26$).

The codes in this section will be easily breakable—they are much too simple for practical security. The power of computers demands more complex cryptography, because that power would quickly detect a small encoding matrix. But a matrix code (the Hill Cipher) will allow us to see linear algebra at work in a new way.

All our calculations in encoding and decoding will be "**mod p**". But the central concepts of linear independence and bases and inverse matrices and determinants survive this change. We will be doing "linear algebra with finite fields". Here is the meaning of *mod* p:

$\boldsymbol{27 \equiv 2\ (mod\ 5)}$	means that $\boldsymbol{27 - 2}$ **is divisible by** $\boldsymbol{5}$
$\boldsymbol{y \equiv x\ (mod\ p)}$	means that $\boldsymbol{y - x}$ **is divisible by** $\boldsymbol{p}$

Dividing y by 5 produces one of the five possible remainders $x = 0, 1, 2, 3, 4$. All the numbers $5, -5, 10, -10, \ldots$ with no remainder are congruent to zero $(mod\ 5)$. The numbers $y = 6, -4, 11, -9, \ldots$ are all congruent to $x = 1 (mod\ 5)$.

We use the word **congruent** for the symbol $\equiv$ and we call this "modular arithmetic". Every integer y produces one of the values $x = 0, 1, 2, \ldots, p-1$.

The theory is best if p is a prime number. With $p = 26$ letters from A to Z, we unfortunately don't start with a prime p. Cryptography can deal with this problem.

Modular Arithmetic

Linear algebra is based on linear combinations of vectors. Now our vectors $(x_1, \ldots, x_n)$ are strings of integers limited to $x = 0, 1, \ldots, p-1$. All calculations produce these integers when we work "$mod\ p$". This means: *Every integer y outside that range is divided by p and x is the remainder*:

$y = qp + x$	$y \equiv x\ (mod\ p)$	y **divided by** p **has remainder** x

Addition $mod\ 3$ $10 \equiv 1\ (mod\ 3)$ and $16 \equiv 1\ (mod\ 3)$ and $10 + 16 \equiv 1 + 1\ (mod\ 3)$

I could add $10 + 16$ and divide 26 by 3 to get the remainder 2.
Or I can just add remainders $1 + 1$ to reach the same answer 2.

Addition $mod\ 2$ $11 \equiv 1\ (mod\ 2)$ and $17 \equiv 1\ (mod\ 2)$ and $11 + 17 = 28 \equiv 0\ (mod\ 2)$

The remainders added to $1 + 1$ *but this is not* 2. The final step was $2 \equiv 0\ (mod\ 2)$.

Addition $mod\ p$ is completely reasonable. So is **multiplication $mod\ p$**. Here $p = 3$:

$10 \equiv 1\ (mod\ 3)$ times $16 \equiv 1\ (mod\ 3)$ gives 1 times $1 \equiv 1$ $\quad 160 \equiv 1\ (mod\ 3)$

$5 \equiv 2\ (mod\ 3)$ times $\ 8 \equiv 2\ (mod\ 3)$ gives 2 times $2 \equiv 1$ $\quad 40 \equiv 1\ (mod\ 3)$

Conclusion: We can safely add and multiply modulo p. So we can take linear combinations. This is the key operation in linear algebra. **But can we divide ?**

In the real number field, the inverse is $1/y$ (for any number except $y = 0$). This means: We found another real number z so that $yz = 1$. Invertibility is a requirement for a field. **Is inversion always possible $mod\ p$?** For every number $y = 1, \ldots, p-1$ can we find another number $z = 1, \ldots, p-1$ so that $yz \equiv 1\ mod\ p$?

The examples $3^{-1} \equiv 4\ (mod\ 11)$ and $2^{-1} \equiv 6\ (mod\ 11)$ and $5^{-1} \equiv 9\ (mod\ 11)$ all succeed. Can you solve $7z \equiv 1\ (mod\ 11)$? Inverting numbers will be the key to inverting matrices.

Let me show that inversion $mod\ p$ has a problem when p is not a prime number. The example $p = 26$ factors into 2 times 13. **Then $y = 2$ cannot have an inverse $z\ (mod\ 26)$.** The requirement $2z \equiv 1\ (mod\ 26)$ is impossible to satisfy because $2z$ and 26 are even.

Similarly 5 has no inverse z when p is 25. We can't solve $5z \equiv 1\ (mod\ 25)$. The number $5z - 1$ is never going to be a multiple of 5, so it can't be a multiple of 25.

Inversion of every y $(0 < y < p)$ will be possible if and only if p is prime.

Inversion needs $y, 2y, 3y, \ldots, py$ to have different remainders when divided by p.

If my and ny had the same remainder x then $(m - n)y$ would be divisible by p.

The prime number p would have to divide either $m - n$ or y. Both are impossible.

So $y, \ldots, py$ have different remainders: **One of those remainders must be $x = 1$.**

The Enigma Machine and the Hill Cipher

Lester Hill published his cipher (his system for encoding and decoding) in the American Mathematical Monthly (1929). The idea was simple, but in some way it started the transition of cryptography from linguistics to mathematics. Codes up to that time mainly mixed up alphabets and rearranged messages. The **Enigma code** used by the German Navy in World War II was a giant advance—using machines that look to us like primitive computers. The English set up Bletchley Park to break Enigma. They hired puzzle solvers and language majors. And by good luck they also happened to get Alan Turing.

I don't know if you have seen the movie about him: *The Imitation Game*. A lot of it is unrealistic (like *Good Will Hunting* and *A Beautiful Mind* at MIT). But the core idea of breaking the Enigma code was correct, using human weaknesses in the encoding and broadcasting. The German naval command openly sent out their coded orders—knowing that the codes were too complicated to break (if it hadn't been for those weaknesses). The codebreaking required English electronics to undo the German electronics. It also required genius.

Alan Turing was surely a genius—England's most exceptional mathematician. His life was ultimately tragic and he ended it in 1954. The biography by Andrew Hodges is excellent. Turing arrived at Bletchley Park the day after Poland was invaded. It is to Winston Churchill's credit that he gave fast and full support when his support was needed.

The Enigma Machine had gears and wheels. The Hill Cipher only needs a matrix. That is the code to be explained now, using linear algebra. You will see how decoding involved inverse matrices. All steps use modular arithmetic, multiplying and inverting $mod\ p$.

I will follow the neat exposition of Professor Spickler of Salisbury State University, which he made available on the Web: **facultyfp.salisbury.edu/despickler/personal/index.asp**

Modular Arithmetic with Matrices

Addition, subtraction, and multiplication are all we need for $A\boldsymbol{x}$ (matrix times vector). To multiply $mod\ p$ we can multiply the integers in A times the integers in $\boldsymbol{x}$ as usual—and then replace every entry of $A\boldsymbol{x}$ by its value $mod\ p$.

Key questions: When can we solve $A\boldsymbol{x} \equiv \boldsymbol{b}\ (mod\ p)$? Do we still have the four subspaces $\boldsymbol{C}(A), \boldsymbol{N}(A), \boldsymbol{C}(A^{\mathrm{T}}), \boldsymbol{N}(A^{\mathrm{T}})$? Are they still orthogonal in pairs? Is there still an inverse matrix $mod\ p$ whenever the determinant of A is nonzero $mod\ p$? I am happy to say that the last three answers are *yes* (but the inverse question requires p to be a prime number).

We can find $A^{-1}\ (mod\ p)$ by Gauss-Jordan elimination, reducing $[A\ \ I]$ to $[I\ \ A^{-1}]$ as in Section 2.5. Or we can use determinants and the cofactor matrix C in the formula $A^{-1} = (\det A)^{-1}\, C^{\mathrm{T}}$. I will work $mod\ 3$ with a 2 by 2 integer matrix A :

$$\left[\begin{array}{cc|cc} A & & I & \end{array}\right] = \left[\begin{array}{cc|cc} \mathbf{2} & \mathbf{0} & 1 & 0 \\ \mathbf{2} & \mathbf{1} & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{array}\right] \rightarrow \begin{array}{c}\text{multiply row 1} \\ \text{by } 2^{-1} \equiv 2\end{array} \rightarrow \left[\begin{array}{cc|cc} 1 & 0 & \mathbf{2} & \mathbf{0} \\ 0 & 1 & \mathbf{2} & \mathbf{1} \end{array}\right] = \left[\begin{array}{cc|cc} & I & & A^{-1} \end{array}\right]$$

By pure chance $A^{-1} \equiv A$! Multiplying A times A mod 3 does give the identity matrix:

$$A^2 = AA^{-1} = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 6 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (mod\ 3).$$

The determinant of A is 2, and the cofactor formula from Section 5.3 also gives $A^{-1} \equiv A$:

$$\begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}^{-1} = 2^{-1} \begin{bmatrix} 1 & -0 \\ -2 & 2 \end{bmatrix} \equiv 2 \begin{bmatrix} 1 & -0 \\ -2 & 2 \end{bmatrix} \equiv \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix} (mod\ 3).$$

Theorem. A^{-1} exists $mod\ p$ if and only if $(\det A)^{-1}$ exists $mod\ p$.
The requirement is: $\det A$ and p have no common factors.

Encryption with the Hill Cipher

The original cipher used the letters A to Z with $p = 26$. Hill chose an n by n encryption matrix E so that $\det E$ is not divisible by 2 or 13. Then the number $\det E$ has an inverse mod 26 and so does the matrix E. The inverse matrix $E^{-1} \equiv D\,(mod\ 26)$ will be the decryption matrix that decodes the message.

Now convert each letter of the message into a number from 0 to 25. The obvious choice from $A = 0$ to $Z = 25$ is acceptable because the matrix will make this cipher stronger.

> Ignore spaces and divide the message into blocks $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$ of size n. Then multiply each message block $(mod\ p)$ by the encryption matrix E. The coded message is $E\boldsymbol{v}_1, E\boldsymbol{v}_2, \ldots$ and you know what the decoder will do.

Spikler's example has $D = E^{-1} =$ $\det E = 583 \equiv 11\ (mod\ 26)$

$$\begin{bmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{bmatrix} (mod\ 26).$$

Of course a codebreaker will not know E or D. And the block size n is generally unknown too. For the matrices Hill had in mind n would not be very large and a computer could quickly discover E and D.

I am not sure if Hill's Cipher could become seriously difficulty to break by choosing very large matrices and a large prime number p. And by encoding the coded message a second time, using a different block size n_2 and large matrix E_2 and large prime p_2.

Finite Fields and Finite Vector Spaces

In algebra, a field **F** is a set of scalars that can be added and multiplied and inverted (except 0 can't be inverted). Familiar examples are the real numbers **R** and the complex numbers **C** and the rational numbers **Q** (containing every ratio p/q of integers). From a field you build vectors $\boldsymbol{v} = (f_1, f_2, \ldots, f_n)$. From linear combinations of vectors you build vector spaces. *So linear algebra begins with a field* **F**.

I taught for ten years from a textbook that started with fields. On the way to $\mathbf{R}^n$, we lost a lot of students. That was a signal—the emphasis was misplaced if we wanted the

course to be useful. I believe the right way is to understand $\mathbf{R}^n$ and its subspaces first, as you do. Then you can look at other fields and vector spaces with a natural question in mind: *What is new when the field is not* $\mathbf{R}$?

These pages are asking that question for **finite fields**. The possibilities become more limited but also highly interesting. The starting point (and not quite the ending point) is the finite field $\mathbf{F}_p$. It contains only the numbers $0, 1, \ldots, p-1$ and p is a prime number. I will focus first on the field $\mathbf{F}_2$ with only 2 members "**0**" and "**1**". You could think of **0** and **1** as "even" and "odd" because the rules to add and multiply are obeyed by the even numbers and odd numbers: even + odd = *odd* and even × odd = *even*.

Addition table

	0	1
0	0	1
1	1	0

Multiplication table

	0	1
0	0	0
1	0	1

This is addition and multiplication "mod 2".

From this field $\mathbf{F}_2$ we can build vectors like $\boldsymbol{v} = (0, 0, 1)$ and $\boldsymbol{w} = (1, 0, 1)$. There are three components with two choices each: a total of $2^3 = 8$ different vectors in the vector space $(\mathbf{F}_2)^3$. You know the requirements on a subspace and the possibilities it opens up:

a) The zero-dimensional subspace containing only $\mathbf{0} = (0, 0, 0)$.

b) One-dimensional subspaces containing $\mathbf{0}$ and a vector like $\boldsymbol{v}$. Notice $\boldsymbol{v} + \boldsymbol{v} = \mathbf{0}$!

c) Two-dimensional subspaces with a basis like $\boldsymbol{v}$ and $\boldsymbol{w}$ and 4 vectors $\mathbf{0}, \boldsymbol{v}, \boldsymbol{w}, \boldsymbol{v} + \boldsymbol{w}$.

d) The full three-dimensional subspace $(\mathbf{F}_2)^3$ with 8 vectors.

What are the possible bases for $(\mathbf{F}_2)^3$? The standard basis contains $(1, 0, 0)$ and $(0, 1, 0)$ and $(0, 0, 1)$. Those vectors are linearly independent and they span $(\mathbf{F}_2)^3$. Their eight combinations with coefficients 0 and 1 fill all of $(\mathbf{F}_2)^3$.

What about matrices that multiply those vectors? The matrices will be 1 by 3, or 2 by 3, or 3 by 3. When they are 3 by 3 we can ask if they are invertible. Their determinants can only be 0 (singular matrix) or 1 (invertible matrix). Let me leave you the pleasure of deciding whether these matrices are invertible. *And how would you find the inverse* ?

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \qquad C = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Out of 2^9 possible matrices over $\mathbf{F}_2$, I will guess that most are singular.

To conclude this discussion of $\mathbf{F}_2$, I mention a field with $2^2 = 4$ members. It will not come from multiplication $(mod\ 4)$, because 4 is not prime. The multiplication 2 times 2 will give 0 (and 2 has no inverse): *not a field*. But we can start with the numbers 0 and 1 in $\mathbf{F}_2$ and invent two more numbers a and $1 + a$—provided they follow these two rules: $(\boldsymbol{a} + \boldsymbol{a} = \mathbf{0})$ and $(\boldsymbol{a} \times \boldsymbol{a} = \mathbf{1} + \boldsymbol{a})$. Then a and $1 + a$ are inverses. Not obvious !

Add	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

Multiply	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	$1+a$	1
$1+a$	0	$1+a$	1	a

Beyond $p = 2$, we have the fields $\mathbf{F}_p$ for all prime numbers p. They use addition and multiplication $mod\ p$. They are alphabets for codes. They provide the components for vectors $\boldsymbol{v} = (f_1, \ldots, f_n)$ in the space $(\mathbf{F}_p)^n$. They provide the entries for matrices that multiply those vectors. These fields $\mathbf{F}_p$ are the most frequently used finite fields.

The only other finite fields have p^k members. The example above of $0, 1, a, 1 + a$ had $2^2 = 4$ members. We will leave it there and get back safely to $\mathbf{R}$.

Problem Set 10.7

1 If you multiply n whole numbers (even or odd) when is the answer odd? Translate into multiplication $(mod\ 2)$: If you multiply 0's and 1's when is the answer 1 ?

2 If you add n whole numbers (even or odd) when is the sum of the numbers odd? Translate into adding 0's and 1's $(mod\ 2)$. When do they add to 1 ?

3 (a) If $y_1 \equiv x_1$ and $y_2 \equiv x_2$, why is $y_1 + y_2 \equiv x_1 + x_2$? All are $mod\ p$.
Suggestion: $y_1 = p\,q_1 + x_1$ and $y_2 = p\,q_2 + x_2$. Now add $y_1 + y_2$.

(b) Can you be sure that $x_1 + x_2$ is smaller than p ? *No*. Give an example where there is a smaller x with $(y_1 + y_2) = x\,(mod\ p)$.

4 $p = 39$ is not prime. Find a number a that has no inverse $z\ (mod\ 39)$. This means that $az \equiv 1\ (mod\ 39)$ has no solution. Then find a 2 by 2 matrix A that has no inverse matrix $Z\ (mod\ 39)$. This means that $AZ \equiv I\ (mod\ 39)$ has no solution.

5 Show that $y \equiv x\,(mod\ p)$ *leads to* $-y \equiv -x\,(mod\ p)$.

6 Find a matrix that has independent columns in $\mathbf{R}^2$ but dependent columns $(mod\ 5)$.

7 What are all the 2 by 2 matrices of 0's and 1's that are invertible $(mod\ 2)$?

8 Is the row space of A still orthogonal to the nullspace in modular arithmetic $(mod\ 11)$? Are bases for those subspaces still bases $(mod\ 11)$?

9 (Hill's Cipher) Separate the message THISWHOLEBOOKISINCODE into blocks of 3 letters. Replace each letter by a number from 1 to 26 (normal order). Multiply each block by the 3 by 3 matrix L with 1's on and below the diagonal. What is the coded message (in numbers) and how would you decode it?

10 Suppose you know the original message (the plaintext). Suppose you also see the coded message. How would you start to discover the matrix in Hill's Cipher ? For a very long message do you expect success ?