

CS556 Introduction to Cryptography - Prof. Ming-Deh Huang  
Scribe: Iftikhar A Burhanuddin, Caimu Tang  
{burhanud|caimut}@usc.edu  
Class #7 - September 17, 2002

**Announcements:**

Lecture notes for classes #5 and #6 are online.

**Topics for today:**

1. How big is  $GL_2(\mathbf{Z}/N\mathbf{Z})$ ?
2. Security of Matrix Ciphers

Claim: If  $\det(A) \in \mathbf{Z}/N\mathbf{Z}^*$  and for some  $k$ ,  $(\det A)^k = 1$ , then  $A^{k-1}$  is an inverse of  $A$ . Here's a counterexample take  $N = 12$  and  $A = \begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix}$   $\det(A) = 5 \pmod{12}$  and  $\det(A)^2 = 1 \pmod{12}$  but  $A^2 = \begin{pmatrix} 9 & 8 \\ 4 & 9 \end{pmatrix}$  and  $A.A^2 \neq I$

**1. How big is  $GL_2(\mathbf{Z}/N\mathbf{Z})$ ?**

One security metric is the size of the key space and we'll now recap what we've learnt so far.

- Caesar:  $E(x) = x + k$ , where  $k \in \mathbf{Z}/N\mathbf{Z}$ .  
#keys = #k =  $N$
- Linear:  $E(x) = ax + b$ , where  $a \in \mathbf{Z}/N\mathbf{Z}^*$  and  $b \in \mathbf{Z}/N\mathbf{Z}$ .  
#keys = # $(a, b) = \phi(N) * N$
- Digraph:  $E(x) = Ax + b$ , where  $A \in GL_2(\mathbf{Z}/N\mathbf{Z})$  and  $b \in \mathbf{Z}/N\mathbf{Z}^2$  and  $GL_2(\mathbf{Z}/N\mathbf{Z}^*) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \in \mathbf{Z}/N\mathbf{Z}^* \}$ .  
#keys = # $(A, b) = |GL_2(\mathbf{Z}/N\mathbf{Z})| * N^2$ . Clearly  $|GL_2(\mathbf{Z}/N\mathbf{Z})|$  is upper bounded by  $N^4$ , let's derive tighter bounds.

For  $A \in M_2(\mathbf{Z}/N\mathbf{Z})$ ,  $A^{-1}$  exists iff  $\det A \in \mathbf{Z}/N\mathbf{Z}^*$ . Let's first consider the case when  $N = p$  is prime and let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  where  $a, b, c, d \in \mathbf{Z}/p\mathbf{Z}$

**Lemma:**  $\det(A) \neq 0 \Leftrightarrow (a, b) \neq (0, 0)$  and  $(c, d) \neq \lambda(a, b)$  for all  $\lambda \in \mathbf{Z}/p\mathbf{Z}$ .

So  $\#(a, b) = p^2 - 1$  and  $\#(c, d)$  for each  $(a, b) = p^2 - p$ . Therefore  $\#A \in GL_2(\mathbf{Z}/p\mathbf{Z}) = (p^2 - 1)(p^2 - p)$ . And this forms the argument for the next lemma.

**Lemma:** For prime  $p$ ,  $|GL_2(\mathbf{Z}/p\mathbf{Z})| = (p^2 - 1)(p^2 - p)$ .

On the other hand suppose  $N$  is composite, for example, say  $N = 12 = 3 * 4$  and  $A = \begin{pmatrix} 7 & 2 \\ 4 & 11 \end{pmatrix}$ . Observe that  $A$  is not invertible and let's investigate what happens in the matrix  $A$  reduced modulo the factors of 12.

$A \bmod 4 = \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}$ , which is invertible and  $A \bmod 3 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ , which is not invertible. So do the residue matrices give us evidence on the non-invertibility of  $A$ ? Yes!

**Thm:** Suppose  $\gcd(n, m) = 1$  and let  $A \in M_2(\mathbf{Z}/nm\mathbf{Z})$ . Then  $A \in GL_2(\mathbf{Z}/nm\mathbf{Z}) \Leftrightarrow A \bmod n \in GL_2(\mathbf{Z}/n\mathbf{Z})$  and  $A \bmod m \in GL_2(\mathbf{Z}/m\mathbf{Z})$

**Proof:** The Chinese Remainder Theorem tells us that the following maps are bijections

$$\begin{array}{lcl} \mathbf{Z}/nm\mathbf{Z} & \rightarrow & \mathbf{Z}/m\mathbf{Z} \quad X \quad \mathbf{Z}/n\mathbf{Z} \quad \dots (i) \\ x & \mapsto & (x \bmod m \quad , \quad x \bmod n) \\ \mathbf{Z}/nm\mathbf{Z}^* & \rightarrow & \mathbf{Z}/m\mathbf{Z}^* \quad X \quad \mathbf{Z}/n\mathbf{Z}^* \quad \dots (ii) \end{array}$$

Now let's replace  $x$  by matrix  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and derive some interesting results.

$$\begin{array}{lcl} M_2(\mathbf{Z}/nm\mathbf{Z}) & \rightarrow & M_2(\mathbf{Z}/m\mathbf{Z}) \quad X \quad M_2(\mathbf{Z}/n\mathbf{Z}) \quad \dots (i') \\ A & \mapsto & (A \bmod m \quad , \quad A \bmod n) \\ GL_2(\mathbf{Z}/nm\mathbf{Z}) & \rightarrow & GL_2(\mathbf{Z}/m\mathbf{Z}) \quad X \quad GL_2(\mathbf{Z}/n\mathbf{Z}) \quad \dots (ii') \end{array}$$

Now CRT says that  $a$  is uniquely determined by  $a \bmod n$  and  $a \bmod m$  and so are  $b, c, d$  and so  $(i) \Rightarrow (i')$  is a bijection.

$$\begin{array}{lcl} A \in GL_2(\mathbf{Z}/nm\mathbf{Z}) & \Leftrightarrow & \det(A) \in \mathbf{Z}/nm\mathbf{Z}^* \\ \text{(by (ii))} & \Leftrightarrow & \det(A) \bmod n \in \mathbf{Z}/n\mathbf{Z}^* \text{ and } \det(A) \bmod m \in \mathbf{Z}/m\mathbf{Z}^* \\ & \Leftrightarrow & A \bmod n \in GL_2(\mathbf{Z}/n\mathbf{Z}) \text{ and } A \bmod m \in GL_2(\mathbf{Z}/m\mathbf{Z}) \end{array}$$

Therefore  $(ii')$  is also a bijection.  $\diamond$

A consequence of the above theorem is that

$$|GL_2(\mathbf{Z}/nm\mathbf{Z})| = |GL_2(\mathbf{Z}/n\mathbf{Z})| * |GL_2(\mathbf{Z}/m\mathbf{Z})|$$

and hence the number of invertible matrices over  $\mathbf{Z}/N\mathbf{Z}$  depends on the decomposition of  $N$ . If  $p, q$  are primes then

$$\begin{aligned} |GL_2(\mathbf{Z}/pq\mathbf{Z})| &= (p^2 - 1)(p^2 - p)(q^2 - 1)(q^2 - q) \\ \Rightarrow |GL_2(\mathbf{Z}/pq\mathbf{Z})|/N^4 &= (1 - \frac{1}{p^2})(1 - \frac{1}{p})(1 - \frac{1}{q^2})(1 - \frac{1}{q}) \end{aligned}$$

And when  $p$  and  $q$  are *big* the probability that a random matrix is invertible is very close to 1.

## 2. Security of Matrix Ciphers

If you recollect the Caesar scheme can be broken by getting hold of one plaintext and it's corresponding ciphertext. So how about the matrix scheme  $E : x \mapsto Ax + b$ ? We'll show that 3 such pairs are usually enough to crack the system. Consider  $y_i = Ax_i + b$ ,  $i = 1, 2, 3$ . Subtracting the first equation from the second and the third gives us  $y_2 - y_1 = A(x_2 - x_1)$  and  $y_3 - y_1 = A(x_3 - x_1)$ . If we let  $X := [x_2 - x_1, x_3 - x_1]$  and  $Y := [y_2 - y_1, y_3 - y_1]$  then the above equations are equivalent to  $AX = Y$ . If  $X$  happened to be invertible then we can solve for  $A (= X^{-1}Y)$ . In general *most* matrices are invertible and therefore 3 pairs of plaintext-ciphertext are *enough*, unless we were born under a bad sign!

We can generalize to the  $k$ -dimensional matrix case. Say  $A = (a_{ij})_{k \times k}$  and  $\Delta_{ij} := (-1)^{i+j} \det(A')$  where  $A'$  is a  $k - 1$  dimensional matrix obtained by removing row  $i$  and column  $j$  from  $A$ . Let  $\Delta := (\Delta_{ij})_{k \times k}$  and  $I_{k \times k}$  the  $k \times k$  identity matrix.

**Lemma:**  $A \cdot \Delta^T = \det(A) \cdot I_{k \times k}$ .

Using the above lemma we can extend the bijective maps  $(i')$  and  $(ii')$  to  $k \times k$  matrices.

**Question:** For  $k \in \mathbf{Z}_{>2}$ ,  $|GL_k(\mathbf{Z}/pq\mathbf{Z})| = ?$

*Remark:* The encryption schemes we've seen so far are *linear* and we can crack them using linear algebra tricks. Also decryption keys  $(A^{-1}, -Ab)$  can be derived from the encryption keys  $(A, b)$  and vice-versa. In the coming classes we'll look at asymmetric schemes where simple tricks generally bear no fruit.