4 The Number of Invertible Matrices over a Residue Class Ring

We want as clearly as possible to get an idea how large the number

$$\nu_{ln} := \#GL_l(\mathbb{Z}/n\mathbb{Z})$$

of invertible $l \times l$ matrices over the residue class ring $\mathbb{Z}/n\mathbb{Z}$ is.

In the special case $l = 1$ the number ν_{1n} simply counts the invertible elements of $\mathbb{Z}/n\mathbb{Z}$ and is given as the value $\varphi(n)$ of the EULER φ-function.

In the general case we easily find a trivial *upper bound* for ν_{ln}:

$$\nu_{ln} \leq \#M_{ll}(\mathbb{Z}/n\mathbb{Z}) = n^{l^2}.$$

To find a *lower bound* we note that (over any ring R) matrices of the form

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ * & & 1 \end{pmatrix} \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_l \end{pmatrix} \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$$

are always invertible if $d_1, \ldots, d_l \in R^\times$. This gives an injective map

$$R^{\frac{l(l-1)}{2}} \times (R^\times)^l \times R^{\frac{l(l-1)}{2}} \longrightarrow GL_l(R).$$

(Proof of injectivity: **Exercise.**) This gives the bound

$$\nu_{ln} \geq n^{\frac{l(l-1)}{2}} \cdot \varphi(n)^l \cdot n^{\frac{l(l-1)}{2}} = n^{l^2-l} \cdot \varphi(n)^l.$$

Taken together this yields:

Proposition 2

$$n^{l^2-l} \cdot \varphi(n)^l \leq \nu_{ln} \leq n^{l^2}.$$

Remarks

1. The idea of writing matrices as $A = VDW$ as above—where D is a diagonal matrix, V, a lower triangular matrix with only 1's in the diagonal, and W, an upper triangular matrix likewise with only 1's in the diagonal—gives an easy way of constructing invertible matrices without resorting to trial and error and calculating determinants. This method gives "almost all" invertible matrices—in the theory of algebraic groups this is the "big BRUHAT cell". Matrices of this type can be easily inverted by the formula $A^{-1} = W^{-1}D^{-1}V^{-1}$.

2. Two lower bounds for the φ-function that we cite without proofs yield handy bounds for ν_{ln}. The first of these bounds is

$$\varphi(n) > \frac{6}{\pi^2} \cdot \frac{n}{\ln n} \quad \text{for } n \geq 7.$$

   This yields

$$\nu_{ln} > n^{l^2-l} \cdot \left(\frac{6}{\pi^2} \cdot \frac{n}{\ln n}\right)^l = \frac{6^l}{\pi^{2l}} \cdot \frac{n^{l^2}}{(\ln n)^l} \quad \text{for } n \geq 7.$$

3. The other bound is

$$\varphi(n) > \frac{n}{2 \cdot \ln \ln n} \quad \text{for almost all } n.$$

   This yields

$$\nu_{ln} > \frac{1}{(2 \cdot \ln \ln n)^l} \cdot n^{l^2}$$

   or

$$\frac{1}{(2 \cdot \ln \ln n)^l} \quad < \quad \frac{\nu_{ln}}{n^{l^2}} \quad < \quad 1$$

   for almost all n.

Conclusion "Very many" to "almost all" matrices in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ are invertible. But also note that asymptotically the quotient ν_{ln}/n^{l^2} is not bounded away from 0.

Example For $n = 26$ we give a coarser but very simple version of the lower bound from Proposition 2: From $\varphi(26) = 12$ we get

$$\nu_{l,26} \geq 26^{l^2-l}12^l > 16^{l^2-l}8^l = 2^{4l^2-l}.$$

This gives the bounds $\nu_{2,26} > 2^{14}$, $\nu_{3,26} > 2^{33}$, $\nu_{4,26} > 2^{60}$, $\nu_{5,26} > 2^{95}$. We conclude that the linear cipher is secure from exhaustion at least for block size 5.

Finally we derive an exact formula for ν_{ln}.

Lemma 2 *Let $n = p$ prime. Then*

$$\nu_{lp} = p^{l^2} \cdot \rho_{lp} \quad \textit{where} \quad \rho_{lp} = \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

In particular for fixed l the relative frequency of invertible matrices, ρ_{lp}, converges to 1 with increasing p.

Proof. We successively build an invertible matrix column by column and count the possibilities for each column. Since $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field the first column is an arbitrary vector $\neq 0$. This makes $p^l - 1$ choices.

Assume we have already chosen i columns. These must be linearly independent hence span a linear subspace of $\mathbb{F}_p^l$. This subspace consists of p^i elements. The $(i+1)$-th column then is an arbitrary vector outside of this subspace for which we have $p^l - p^i$ choices. Summing up this yields

$$\prod_{i=0}^{l-1}(p^l - p^i) = \prod_{i=0}^{l-1} p^l(1 - p^{i-l}) = p^{l^2} \prod_{j=1}^{l} \left(1 - \frac{1}{p^j}\right)$$

choices. $\diamond$

Lemma 3 *Let $n = p^e$ with p prime and $e \geq 1$.*

(i) *Let $A \in M_{ll}(\mathbb{Z})$. Then $A \bmod n$ is invertible in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ if and only if $A \bmod p$ is invertible in $M_{ll}(\mathbb{F}_p)$.*

(ii) *The number of invertible matrices in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$ is*

$$\nu_{ln} = n^{l^2} \cdot \rho_{lp}.$$

(iii) *The relative frequency of invertible matrices in $M_{ll}(\mathbb{Z}/p^e\mathbb{Z})$ is ρ_{lp}, independent of the exponent e.*

Proof. (i) Since $\gcd(p, \operatorname{Det} A) = 1 \Longleftrightarrow \gcd(n, \operatorname{Det} A) = 1$, both statements are equivalent with $p \nmid \operatorname{Det} A$.

(ii) Without restriction we may assume that A has all its entries in $[0 \ldots n-1]$. Then we write $A = pQ + R$ where all entries of R are in $[0 \ldots p-1]$ and all entries of Q are in $[0 \ldots p^{e-1} - 1]$. The matrix $A \bmod n$ is invertible if and only if $R \bmod p$ is invertible. For R we have ν_{lp} choices by Lemma 2, and for Q we have $p^{(e-1)l^2}$ choices. Taken together this proves the claim.

(iii) is a direct consequence of (ii). $\diamond$

Lemma 4 *For m and n coprime $\nu_{l,mn} = \nu_{lm}\nu_{ln}$.*

Proof. The Chinese Remainder Theorem gives a ring isomorphism

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

and extends to an isomorphism of the (non-commutative) rings

$$M_{ll}(\mathbb{Z}/mn\mathbb{Z}) \longrightarrow M_{ll}(\mathbb{Z}/m\mathbb{Z}) \times M_{ll}(\mathbb{Z}/n\mathbb{Z}).$$

The assertion follows from the equality of the numbers of invertible elements. $\diamond$

Induction immediately yields:

Theorem 2 *For $n \in \mathbb{N}$*

$$\nu_{ln} = n^{l^2} \cdot \prod_{\substack{p \text{ prime} \\ p|n}} \rho_{lp}.$$

In particular the relative frequency of invertible matrices $\rho_{ln} = \nu_{ln}/n^{l^2}$ is independent from the exponents of the prime factors of n. The explicit formula is

$$\rho_{ln} = \prod_{\substack{p \text{ prime} \\ p|n}} \rho_{lp} = \prod_{\substack{p \text{ prime} \\ p|n}} \prod_{i=1}^{l} \left(1 - \frac{1}{p^i}\right).$$

Example For $n = 26$ the explicit formula is

$$\nu_{l,26} = 26^{l^2} \cdot \prod_{i=1}^{l} \left(1 - \frac{1}{2^i}\right) \left(1 - \frac{1}{13^i}\right)$$

This evaluates as $\nu_{1,26} = 12$, $\nu_{2,26} = 157,248$, $\nu_{3,26} = 1,634,038,189,056 \approx 1.5 \cdot 2^{40}$. Comparing this value of $\nu_{3,26}$ with the lower bound 2^{33} from above shows how coarse this bound is. For $l = 4$ we even get $\nu_{4,26} \approx 1.3 \cdot 2^{73}$, almost secure from exhaustion.

Exercise Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$ the increasing sequence of the primes. Let $n_r = p_1 \cdots p_r$ for $r \geq 1$. Show that for fixed l

$$\lim_{r \to \infty} \rho_{ln_r} = 0.$$

This means that the relative frequency of invertible matrices is decreasing for this sequence of moduli. *Hint*: Let ζ be the Riemann ζ-function. Which values has ζ at the natural numbers $i \geq 1$?