Arithmetic mod 26

- Addition and multiplication are well-defined mod 26; what does this mean?
- Write $a \equiv b \bmod 26$ if 26 divides $a - b$; equivalently a and b have the same remainder when divided by 26.
- If $a \equiv a'$ and $b \equiv b' \bmod 26$ then $a + b \equiv a' + b' \bmod 26$ and $ab \equiv a'b' \bmod 26$; why?
- Once we know that addition and multiplication is well-defined then we know that they are commutative, associative operations on the integers mod 26, 0 acts as the additive identity, 1 acts as the multiplicative identity and they satisfy the distributive law:

$$a(b + c) \equiv ab + ac \bmod 26.$$

- That is, the integers modulo 26 are a ring.

Invertible elements mod 26

- But it is not a field: not every non-zero element has a multiplicative inverse.
- If $\gcd(a, 26) \neq 1$ then a does not have a multiplicative inverse.
- Inverses, if they exist, are unique.
- Claim: if $\gcd(a, 26) = 1$ then there is a b such that $ab \equiv 1$ mod 26.
- In fact, $\gcd(a, 26) = 1$ iff there are k, ℓ such that $ka + 26\ell = 1$.
- Aside: If a does have a multiplicative inverse then it equals a^r for some r.
- Next up: linear algebra mod 26!

Block ciphers

- Character replacement ciphers are subject to character frequency analysis.
- Block ciphers replace blocks of n characters with other blocks of n characters.
- Even for $n = 5$, since $26^5 \approx 12 \times 10^6$, you would be hard pressed to get a frequency analysis to work.
- The goal with a block cipher (as with any cipher) is to have some easy method of encrypting, in this case blocks of characters, which is somehow difficult to decrypt.
- Enter Hill and the idea of using matrix multiply mod 26.

Hill cipher

- Fix a matrix A which is $n \times n$ and contains entries mod 26.
- If you are given a vector u, an n-tuple, with entries mod 26, then you compute uA and this is the encryption of u. Everything is understood mod 26.
- For example, if $u = (2, 0, 19)$ (CAT) and A is the matrix

$$\begin{pmatrix} 5 & 1 & 3 \\ 1 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix}$$

then $uA = (3, 14, 6)$ (DOG).

Hill cipher, cont'd

- Remember that the encryption method has to be one-to-one. In this case, this means that that we should have $uA = vA$ for different u and v. Or said another way, we shouldn't have $(u - v)A = 0$ if $u - v \neq 0$.
- That is, you want A to be invertible. What does that mean here when we are working mod 26?
- A is invertible if there is some matrix B such that $AB = I$ mod 26.
- Fact: TFAE
  1. A is invertible.
  2. The only solution to $uA = 0$ is $u = 0$.
  3. $\det(A)$ is invertible mod 26.

Attacks on the Hill cipher

- Three types of attacks are going to work:
- If you have temporary access to the encryption machine.
- If you have temporary access to the decryption machine.
- If you have a sufficiently long cleartext/ciphertext pair.
- The goal in all cases is to figure out what A is.
- If you have access to either machine, feed it the standard basis.
- What to do in the third case is best seen on the blackboard.