MA 437

LESSON 17

LATTICES, An Example

LATTICES

We will look at how lattices are used in cryptography. Before we define lattices, we look at a lead in example

Congruential Cryptosystem

This small example is not large enough to be secure. Nevertheless, it is a good example

Alice picks a positive integer, q and two positive integers f and g such that

$$f < \sqrt{q/2}, \quad \sqrt{q/4} < g < \sqrt{q/2}, \quad \gcd(f, gq) = 1$$

The last condition guarantees that f has an inverse mod g and mod q.

Alice computes $h = f^{-1} g \bmod q$. The choices of f and g guarantee that they are small compared to q, but h may be

large. h and q are made public.

Bob has message m to send. where $m < \sqrt{q/4}$. He picks r, $0 < r < \sqrt{q/2}$ and computes cipher text e

$$e = rh + m \mod q$$

where $0 < e < q$

e is sent to Alice.

Alice decrypts as follows: She finds

$$a \equiv fe \mod q$$

and

$$b \equiv f^{-1} a \mod q$$

She knows f has an inverse mod q.

Claim $b = m$

Verification

$$a = fe = f(rh+m) \equiv$$
$$frh + fm = frf^{-1}g + fm$$
$$\equiv rg + fm \mod q$$

An important note:

$$rg + fm < \sqrt{q/2}\,\sqrt{q/2} + \sqrt{q/2}\,\sqrt{q/4} < q$$

by the choices of r, g, f and m

Hence

$$a = rg + fm \bmod q = rg + fm$$

so the writing of $a = rg + fm$ is not just mod q, it holds exactly

Alice computes

$$b = f^{-1}a = f^{-1}(rg + fm)$$

$$= f^{-1}fm = m \bmod q = m$$

since $m < q$

Ex. Alice picks $q = 400$ ($\sqrt{q} = 20$) and $f = 7$, $g = 11$. Note $\gcd(7, 400 \cdot 11) = 1$, $f < \sqrt{200}$, $10 < g < \sqrt{200}$.

Alice computes $f^{-1} \bmod q = 343$.

and $h = f^{-1} g \bmod q = 173$

She make h and q public

but g and f are her private keys.

Bob is to send message $m = 5$. He also picks $r = 2$
Note $0 < m < 10$ and $0 < r < \sqrt{200}$

He computes ciphertext

$$e = rh + m \bmod q = 351$$

and send e to Alice

Alice computes

$$a = fe \bmod q = 57$$
$$b = f^{-1} a \bmod q = 8 \cdot 57 \bmod 11 = 5$$

Note that a was computed mod q and b was computed mod q. Also

$$f^{-1} \bmod q = 343$$
$$f^{-1} \bmod q = 8$$

Finally we see

$$b \bmod q = 5 = m.$$

Now we come to the part that previews how lattices could arise.

Eve knows the public key (q, h) She looks for integers F, G with

$$Fh = G \bmod q$$

where F and G are around $\sqrt{q}$. Recall $fh = g \bmod q$ in Alices private key so F and G are of this type It is likely that (F, G) will serve as a decription key

$$Fh = G \bmod q \rightarrow$$
$$Fh = G + qR \text{ for some } R$$

Before describing Gauss' idea let's see the point.

The vector we are looking for is short by the way we defined the problem with all the inequalities. The vectors we have that are a basis for the lattice can be replaced by other vectors that are a basis for the lattice and they (or at least one of them is shorter) we hope the solution is the shortest vector in the lattice. The very pretty geometrical idea is that the basis vectors give rise to a parallelogram of a certain area. When we change basis in the following way (described next) the new parallelogram has the same area as the old one. If the second set of vectors are shorter than the first set and give the same area, then the new vectors are more orthogonal than the old ones. So we look for a

new set that is more orthogonal. That is what the algorithm does. It is Gram-Schmitt but with integer coefficents which complicates things. The ideas work in all dimensions, not just 2. The major algorithm for doing this is the L.L.L (Lenstra, Lenstra, Lovac's) algorithm.

Back to the process where we have

$$Fh = G \bmod q$$

$$Fh = G + qR$$

$$F(1, h) = R(0, q) = (F, G)$$

Write this as a integer vector problem (<u>lattice problem</u>)

$$F(1,h) - R(0,q) = (F, G)$$

Eve knows vectors $(1,h), (0,q)$ each of length about $\sqrt{q}$. The important fact in all lattice problems is that coefficents need to be integers.

Letting $v_1 = (1,h)$ $v_2 = (0,q)$ find integers a, b such that $w = av_1 + bv_2$ and w has length about $\sqrt{q}$.

Eve needs to find a short vector in set $av_1 + bv_2$; a, b integers (short because length $\sim \sqrt{q}$). This looks like a linear algebra problem, except the coefficients need to be integers

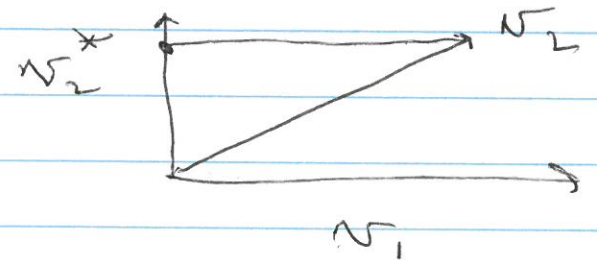
Since this is a 2 dimensional problem, there are quick solutions, due to GAUSS.

GAUSS REDUCTION IN DIM. 2

Suppose that L is a 2 dimensional lattice with basis v_1, v_2. Assume $|v_1| < |v_2|$. We try to make v_2 smaller by subtracting a multiple of v_1. Standard linear algebra says compute

$$v_2^* = v_2 - \frac{v_1 \cdot v_2}{|v_1|^2} v_1$$

Which is othogonal to v_1



(projection problem of v_2 onto othogonal complement of v_1)

v_2^* is shorter than v_2.

Unfortunately it is not in the lattice determined by v_1 and v_2 since the coefficent $\frac{v_1 \cdot v_2}{|v_1|^2}$ is probably not an integer

What is done is approximate v_2^* by taking the

closest integer to $\frac{v_1 \cdot v_2}{|v_1|^2}$ in place of $\frac{v_1 \cdot v_2}{|v_1|^2}$

If v_2^* is longer then v_1 stop. Otherwise swap v_2^* and v_1 and repeat the process until completion

Ex $v_1 = (16586820, 65354729)$
$v_2 = (16513996, 63934647)$
$|v_1| > |v_2|$ SWAP

$v_1 = (16513996, 63934647)$
$v_2 = (16586820, 65354729)$
$\left\lfloor \frac{v_1 \cdot v_2}{|v_1|^2} \right\rceil = \lfloor 10.2221 \rceil = 10$

$v_2^* = v_2 - m v_1 = (1446860, 1420089)$
v_2^* replaces v_2 and we have
v_1, v_2^*

IF YOU CONTINUE 6 STEPS

$v_1 = (2280, -1001)$
$v_2 = (-1324, -2376)$
$\lceil v_1 \cdot v_2 \rfloor = 0$ so v_1, v_2 are

close to orthogonal
v_1 is the shorter, so it is
the shortest vector in the
lattice. (probably)

PYTHON, SAGE