Sketch of Lecture 21

Fri, 3/6/2020

Example 125. (bonus challenge!) Find the smallest (pseudo)prime with 100 decimal digits, all of which are 1 or 2.

(Send me an email by 3/15 with the prime, and how you found it, to collect a bonus point. Earn an extra bonus point if you can find it using a single line of Sage code [artificial concatenations not allowed].)

AES

Finite fields

Example 126. We have already seen xor in several cryptosystems. Note that a single xor operation as in the one-time pad or stream ciphers provides no diffusion.

When designing a cipher it may be nice to replace xor of N bit blocks with an operation that does provide some diffusion.

- A tiny amount of diffusion is provided by instead using addition modulo 2^N.
  Due to carries, one bit flip in the input can propagate to more than one bit flipped in the output.
- More diffusion can be achieved using operations (multiplication/inversion) in finite fields like $\mathrm{GF}(2^N)$.
  [We only need to make sure in our design that we don't multiply with zero.]

A **field** is a set of elements which can be added/subtracted as well as multiplied/divided by according to the usual rules.

In particular, a field always has distinguished elements 0 and 1, which are the neutral elements with respect to addition and multiplication, respectively.

Example 127.

- The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ all are fields, which you have seen before. They contain infinitely many elements.
- The integers $\mathbb{Z}$ are not a field because, for instance, 3 is not invertible (since $\frac{1}{3}$ is not an integer itself). Quotients of integers (rational numbers!) are a field.
  Since addition/subtraction and multiplication work as they should, $\mathbb{Z}$ is what is called a **ring**.
- Polynomials are not a field (they are a ring like $\mathbb{Z}$). Quotients of polynomials (rational functions!) are a field.

Cryptographic applications require finite structures. Correspondingly, our focus will be on **finite fields**, that is, fields consisting of only a finite number of elements.

Example 128. Let p be a prime. The residues modulo p form a field, often denoted as $\mathrm{GF}(p)$.

GF is short for **Galois field**, which is another word for finite field.

Note that we can divide by any element! (Except the zero residue but, of course, we can never divide by 0).

Example 129. The residues modulo 21 (or any other composite number) are not a field.

We can add/subtract and multiply these numbers, but we cannot always divide. Specifically, we cannot divide by elements like $3, 6, 7, \ldots$ even though these are nonzero (we can, of course, never divide by zero).

Note. We have already seen that this seemingly slight deficiency has "terrible" consequences. For instance, the quadratic equation $x^2 = 1$ has more than the two solutions $x = \pm 1$ modulo 21 (namely, ± 8 as well).

AES is built upon byte operations (in contrast to DES, which is built on bit operations). Each of the 2^8 bytes represents one of the 2^8 elements of the finite field $\mathrm{GF}(2^8)$.

Note. We do not yet know what $\mathrm{GF}(2^8)$ is. It cannot be the residues modulo 2^8, because we just observed that the residues modulo n are a field only if n is prime.

To construct the finite field $\mathrm{GF}(p^n)$ of p^n elements, we can do the following:

- Fix a polynomial $m(x)$ of degree n, which is irreducible modulo p (i.e. cannot be factored modulo p).
- The elements of $\mathrm{GF}(p^n)$ are polynomials modulo $m(x)$ modulo p.

We will discuss the irreducibility condition on $m(x)$ next time. For now, see Example 132.

Comment. Actually, all finite fields can be constructed in this fashion. Moreover, choosing different $m(x)$ to construct $\mathrm{GF}(p^n)$ does not really matter: the resulting fields are always isomorphic (i.e. work in the same way, although the elements are represented differently). That justifies writing down $\mathrm{GF}(p^n)$, since there is exactly one such field.

Example 130. AES is based on representing bytes as elements of the field $\mathrm{GF}(2^8)$. It is constructed using the polynomial $x^8 + x^4 + x^3 + x + 1$ (which is indeed irreducible mod 2).

From bits to polynomials. For instance, the polynomial $x^7 + x^4 + x$ corresponds to the bits 10010010 while $x^6 + 1$ corresponds to 01000001.

Example 131. The polynomial $x^2 + x + 1$ is irreducible modulo 2, so we can use it to construct the finite field $\mathrm{GF}(2^2)$ with 4 elements.

(a) List all 4 elements, and make an addition table. Then realize that this is just xor.

(b) Make a multiplication table.

(c) What is the inverse of $x + 1$?

Solution.

(a) The four elements are $0, 1, x, x + 1$.

For instance, $(x + 1) + x = 2x + 1 = 1$ (in $\mathrm{GF}(2^2)$, since we are working modulo 2). The full table is below.

Each of the four elements is of the form $ax + b$, which can be represented using the two bits ab (for instance, $(10)_2$ represents x and $(11)_2$ represents $x + 1$).

Then, addition of elements $ax + b$ in $\mathrm{GF}(2^2)$ works in the same way as xoring bits ab.

(b) For instance, $(x + 1)^2 = x^2 + 2x + 1 \equiv x^2 + 1 \equiv (x + 1) + 1 \equiv x$.

Here, the key is to realize that reducing modulo $x^2 + x + 1$ is the same as saying that $x^2 = -x - 1$, i.e. $x^2 = x + 1$ in $\mathrm{GF}(2^2)$. That means all polynomials of degree 2 and higher can be reduced to polynomials of degree less than 2.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

(c) We are looking for an element y such that $y(x + 1) = 1$ in $\mathrm{GF}(2^2)$. Looking at the table, we see that $y = x$ has that property. Hence, $(x + 1)^{-1} = x$ in $\mathrm{GF}(2^2)$.

Example 132. What if we proceed as in the previous example but used $m(x) = x^2 + 1$ instead?

Solution. The addition table would be the same. The multiplication table would be different and a crucial difference would be that $(x + 1) \cdot (x + 1) = x^2 + 2x + 1 \equiv x^2 + 1 \equiv 0$, which implies that $x + 1$ cannot be invertible. That means our construction is not a field.

Comment. Note how, here, $m(x)$ factors modulo 2 as $x^2 + 1 \equiv (x + 1)(x + 1)$. Hence the condition of irreducibility in the construction of $\mathrm{GF}(p^n)$ is violated.