Lecture 14

Codes (~~[illegible]~~)

We have proved that there is a unique field of order p^n (p prime). This is called the Galois field of order p^n, written $GF(p^n)$.

We wish to transmit a set of binary words of length 4 (eg. 1101, 0101, 0000) and correct up to 1 error by using $GF(2^3) = GF(8)$.

Since $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ irreducible (check!) it follows that $\mathbb{Z}_2[x]/(x^3+x+1)$ is a field, and since K contains the root α of $p(x)$:

$$K \cong \{ c_2\alpha^2 + c_1\alpha + c_0 ;\ c_i \in \mathbb{Z}_2 \}.$$

This means $|K| = 2^3 \Rightarrow K \cong GF(2^3)$

Computation in K:

$$\alpha^3 + \alpha + 1 = 0 \iff \alpha^3 = -\alpha - 1 \overset{i\,\mathbb{Z}_2}{=} \alpha + 1,$$

and further $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$, $\alpha^3 = \alpha + 1$,

$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha+1) = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$,

$\alpha^6 = \alpha^2 + 1$, $\alpha^7 = 1 = \alpha^0$

We will use polynomials $a_6x^6 + \dots + a_1x + a_0 \in \mathbb{Z}_2[x]$ (the elements of $\mathbb{Z}_2[x]/(x^n-1)$ where $n = 2^3 - 1 = 7$.)

Assume we have the binary word abcd. Then we let $C_I(x) = ax^6 + bx^5 + cx^4 + dx^3$, and compute remainder mod $p(x)$:

$$C_I(x) = q(x)p(x) + C_R(x),$$

where $C_R(x) = rx^2 + sx + t$.

Let $C(x) = C_I(x) + C_R(x) = ax^6 + bx^5 + cx^4 + dx^3 + rx^2 + sx + t$.

Note: $C(x) = C_I(x) + C_R(x) \overset{i\,\mathbb{Z}_2}{=} C_I(x) - C_R(x) = q(x)p(x)$

$$\Rightarrow C(\alpha) = q(\alpha)\underbrace{p(\alpha)}_{=0} = 0$$

Now we transmit coeff. of $C(x)$: abcdrst

Assume we recieve ABCDRST, corresponding to

$$R(x) = Ax^6 + Bx^5 + \dots + Sx + T.$$

Let $E(x) = R(x) - C(x)$.

- No error: $E(x) = 0 \Rightarrow 0 = E(\alpha) = R(\alpha) - \overbrace{C(\alpha)}^{=0}$ $\Rightarrow R(\alpha) = 0$
- One error: $E(x) = x^i \Rightarrow \alpha^i = E(\alpha) = R(\alpha) - \overbrace{C(\alpha)}^{=0}$ $\Rightarrow R(\alpha) = \alpha^i$

where i is the false position in ABCDRST

Ex: We want to send 1101 $\Rightarrow C_I(x) = x^6 + x^5 + x^3$

$\Rightarrow x^6 + x^5 + x^3 = (x^3 + x^2 + x + 1)p(x) + 1 \Rightarrow C_R(x) = 1$

$\Rightarrow C(x) = x^6 + x^5 + x^3 + 1$.

We therefore transmit 1101001. Assume that from noise we receive 1001001 $\Rightarrow$

$R(x) = x^6 + x^3 + 1$.

Now $R(\alpha) = \alpha^6 + \alpha^3 + 1 = (\alpha^2 + 1) + (\alpha + 1) + 1 = \alpha^2 + \alpha + 1 = \alpha^5$

The error is in the position x^5: 1001001

$\Rightarrow$ 1101001 is correct, and the word is 1101.

Note: Using GF(16), we can correct two errors, and so on...

RSA-cryptography

Public Key-system:
- Public encoding alg.
- Secret decoding alg.

The algebra we need:

Lemma (Fermats theorem): p prime, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

Proof: $\mathbb{Z}_p^*$ mult. group of order $p-1$

$$\underset{\text{Cor 7.27}}{\Rightarrow} a^{p-1} = 1 \quad \text{for all } a \in \mathbb{Z}_p^*. \qquad \square$$

Now we do the following:

- Choose p, q primes, $p \neq q$
- $n = pq$
- $k = (p-1)(q-1)$
- Choose d such that $(d, k) = 1$
- e solution of $dx \equiv 1 \pmod k$

Theorem: $b^{de} \equiv b \pmod n$ for all $b \in \mathbb{Z}$

Proof: $p | b \Rightarrow b^{de} \equiv b \equiv 0 \pmod p$

$p \nmid b$: $de \equiv 1 \pmod k \iff de = kt + 1$ for some t

$\Rightarrow b^{de} = b^{kt+1} = b^{(p-1)(q-1)t+1} = (b^{p-1})^{(q-1)t} \cdot b \equiv$

$\equiv 1^{(q-1)t} \cdot b \equiv b \pmod p$

Same principle: $b^{de} \equiv b \pmod q$,

and $p | (b^{de} - b)$, $q | (b^{de} - b) \Rightarrow n = pq | (b^{de} - b)$

$\Rightarrow b^{de} \equiv b \pmod n$

The method: Public encoding key: e and n

Secret decoding key: $(p, q)\, d, k$

To encode a message M, M integer $0 \le M < n$, we compute $K \equiv M^e \pmod{n}$, $0 \le K < n$

To decode K, we compute $M' \equiv K^d \pmod{n}$, $0 \le M' < n$.

Since $M' \equiv K^d \equiv (M^e)^d = M^{de} \underset{\text{Theorem}}{\Longrightarrow} \underline{M' \equiv M}$

Ex: Let $p = 47$, $q = 59$. We get $n = 47 \cdot 59 = 2773$,

$k = 46 \cdot 58 = 2668$, and let $d = 157 \Rightarrow (d, k) = 1$

We solve $157x \equiv 1 \pmod{2668}$, and get $e = 17$

With the alphabet code

A	B	C	$\cdots$
01	02	03	$\cdots$

we get "HA" = 0801. We use the public e and n: $801^{17} \equiv 2480 \pmod{2773}$

Now $K = 2480$ i sent and received.

We now decode with secret key d:

$2480^{157} \equiv 801 \pmod{2773}$, so 0801 = "HA".

Note: To break a RSA-code we need to factorize n!

(Hard problem!)