quiz 09.1 Solution

(1) Using the alphabet $GF(13)$ find a generator matrix for a Reed-Solomon code correcting any 5 bit errors. (Use primitive root 2 mod 13.)

To correct any e bit errors, the minimum distance must be at least $2 \cdot e + 1$. Thus, to correct any 5 bit errors, we should take designed distance $2 \cdot 5 + 1 = 11$. Thus, we take generating polynomial

$$g(x) = (x-2)(x-2^2)(x-2^3)(x-2^4)\dots(x-2^{11-2})(x-2^{11-1})$$

The length of any RS code using alphabet $GF(13)$ is 13-1, so this code will have length 12. Multiplying together these linear factors gives

$$g(x)$$

$$= x^{10} + 8x^9 + 5x^8 + 10x^7 + 6x^6 + 4x^5 + 3x^4 + 9x^3 + 12x^2 + 7x + 11$$

Inserting the coefficients in ascending order into a 2-by-12 matrix, padding at the right with 0's in the first line and cycling over until the constant coefficient bumps against the right edge, gives the generating matrix

$$\begin{pmatrix} 11 & 7 & 12 & 9 & 3 & 4 & 6 & 10 & 5 & 8 & 1 & 0 \\ 0 & 11 & 7 & 12 & 9 & 3 & 4 & 6 & 10 & 5 & 8 & 1 \end{pmatrix}$$

Alternatively, one might also try a little trick to reduce the computational load. Since

$$x^{12} - 1 = (x-2^1)(x-2^2)\dots(x-2^{13-1})$$

The check polynomial $h(x)$ is the coefficient-reversed form of $(x^{12}-1)/g(x)$. Using the factored expression saves work: $h(x)$ is simply (the coefficients-reversed form of) the leftover factors from $x^{12}-1$ after the factors from $g(x)$ are removed:

$$h(x) = (\text{reversed...}\ )(x-2^{11})(x-2^{13-1}) = (\text{reversed...})x^2 + 5x + 7 = (\text{reversed...})1 + 5x + 7x^2$$

Thus, the generator polynomial is perhaps best computed by dividing $x^{12}-1$ by (re-reversed) $h(x)$, obtaining

$$g(x) = \frac{x^{12}-1}{x^2+5x+7}$$

$$= x^{10} + 8x^9 + 5x^8 + 10x^7 + 6x^6 + 4x^5 + 3x^4 + 9x^3 + 12x^2 + 7x + 11$$

It is not clear which is easier, the division, or simply multiplying out.

(2) Show that the binary fifth-degree polynomial 101001 (with coefficients in descending order) is irreducible.

We do this by trial division. That is, we know that if there is a divisor $d(x)$ of 101001 with

$$0 < \deg(d) < \deg(101001) = 5$$

then in fact there is a divisor with

$$0 < \deg(d) \le \deg(101001)/2$$

Thus, we need only consider possible divisors of degrees 1 and 2, since degrees are integers. Further, we need only consider irreducible divisor candidates. There are two polynomials of degree 1, x and $x+1$. From class (or another family of trial divisions) among the 4 quadratic polynomials there is only one irreducible, x^2+x+1. Thus, we have only 3 trial divisions to do to verify irreducibility. Division by x gives remainder 1, as does division by $x+1$. Division by x^2+x+1 gives $x+1$, which is not 0. Thus, 101001 is indeed irreducible.

(3) Find an element of order 63 in $GF(2^6)$, where $GF(2^6)$ is modeled as $\mathbf{F}_2[x]$ mod 1010111 where those are the coefficients in descending order.

Let $P(x) = 1010111$ construed as the coefficients in descending order. Implicit in the question is the apparent fact that $P(x)$ is irreducible, or else polynomials modulo $P(x)$ wouldn't be a field. In light of the facts mentioned in the notes, namely the analogue of Fermat's little theorem for finite fields, we know that for any polynomial g not divisible by P, $g^{63} = 1 \bmod P$. So to check whether or not a given candidate g is a primitive element, we need to compute $g^{63/3}$ and possibly $g^{63/7} \bmod P$ since 3,7 are the two primes dividing 63. In this example, the polynomial $g(x) = x$ is not primitive, because $x^{21} = 1 \bmod P$. But it does turn out that $x + 1$ is primitive, because neither $(x + 1)^{21}$ nor $(x + 1)^9$ is 1 mod P. The fast exponentiation computations to compute $(x+1)^9$ and $(x+1)^{21} \bmod 1010111$ are

$$\begin{array}{ccc} x+1 & 9 & 1 \\ x+1 & 8 & x+1 \\ x^2+1 & 4 & x+1 \\ x^4+1 & 2 & x+1 \\ x^3+x & 1 & x+1 \\ x^3+x & 0 & x^4+x^3+x^2+x \end{array}$$

$$\begin{array}{ccc} x+1 & 21 & 1 \\ x+1 & 20 & x+1 \\ x^2+1 & 10 & x+1 \\ x^4+1 & 5 & x+1 \\ x^4+1 & 4 & x^5+x^4+x+1 \\ x^3+x & 2 & x^5+x^4+x+1 \\ x^4+x+1 & 1 & x^5+x^4+x+1 \\ x^4+x+1 & 0 & x^5+x^3+x^2+x+1 \end{array}$$

showing that $x + 1$ to these powers is not 1, so it is a primitive element.

(4) Model the finite field $\mathbf{F}_{32} = GF(32)$ as $\mathbf{F}_2[x]/f(x)$, where $f(x)$ is the polynomial with coefficients 101001 in descending order. Find the multiplicative inverse of 1011, again interpreted as a polynomial with coefficients in descending order.

Use the extended Euclidean algorithm applied to polynomials $g(x) = 1011$ and $f(x) = 101001$ to obtain polynomials $a(x)$ and $b(x)$ so that $a(x)f(x) + b(x)g(x) = 1$. Looking at the latter relation modulo $f(x)$ gives $b(x)$ as a multiplicative inverse of $g(x)$ modulo $f(x)$. Executing the extended Euclidean algorithm:

$$\begin{aligned} (x^5+x^3+1) + (x^2)(x^3+x+1) &= x^2+1 \\ (x^3+x+1) + (x)(x^2+1) &= 1 \\ (x^2+1) + (x^2+1)(1) &= 0 \end{aligned}$$

$$\begin{aligned} 1 &= (1)(x^3+x+1) + (x)(x^2+1) \\ &= (1)(x^3+x+1) + (x)[(x^5+x^3+1) + (x^2)(x^3+x+1)] \\ &= (x)(x^5+x^3+1) + (x^3+1)(x^3+x+1) \end{aligned}$$

Thus, by the earlier comment about expressions of the form $as + bt = 1$, the multiplicative inverse of 1011 modulo 101001 is $x^3 + 1$.