SOLUTIONS FOR MIDTERM 2

1. The prime divisors of $29-1=28$ are 2 and 7. Thus 5 is a primitive root modulo 29 if and only if $5^{\frac{28}{7}=4} \neq 1$ modulo 29 and $5^{\frac{28}{2}=14} \neq 1$ modulo 29.

$5^4=(5^2)^2=25^2=(-4)^2=16\neq 1$ modulo 29, but $5^{14}=(5^2)^7=25^7=(-4)^7=-(2^2)^7=-2^{14}=-2^5\cdot 2^5\cdot 2^4=-32\cdot 32\cdot 16=-3\cdot 3\cdot 16=-3\cdot 48=-3\cdot 19=-57=1$ modulo 29.

Thus $5^{14}=1$ modulo 29. Hence 5 is NOT a primitive root modulo 29.

2. Answer: x^3+1.

3a. A polynomial of degree ≤ 3 is irreducible over $\mathbb{Z}/3$ if and only if it has no linear factors, i.e. no roots in $\mathbb{Z}/3$. There are just three elements in $\mathbb{Z}/3$, namely, 0, 1 and 2. Since $p(0)=2\neq 0, p(1)=1\neq 0$ and $p(2)=2\neq 0$, none of the elements of $\mathbb{Z}/3$ are roots of $p(x)$. This proves that $p(x)$ is irreducible.

3b. $(2\bar{x}+1)(\bar{x}+2)=2\bar{x}^2+5\bar{x}+2=2(-\bar{x}-2)+5\bar{x}+2=3\bar{x}-2=1$. I used $\bar{x}^2=-\bar{x}-2$ because $p(\bar{x})=\bar{x}^2+\bar{x}+2=0$. Answer: $a=0, b=1$.

3c. It follows from 3b that $(\bar{x}+2)^{-1}=2\bar{x}+1$.

3d. The only prime divisor of $9-1=8$ is 2. Thus $\bar{x}$ is a primitive root if and only if $\bar{x}^{\frac{8}{2}=4}\neq 1$ modulo $p(x)$. The remainder of x^4 upon division by $p(x)$ is $2\neq 1$. Thus $\bar{x}$ IS a primitive root.

4. Linearly dependent over $\mathbb{F}_2$ because $(1,1,0)+(1,0,1)+(0,1,1)=(0,0,0)$. But linearly independent over $\mathbb{F}_3$ because $c_1(1,1,0)+c_2(1,0,1)+c_3(0,1,1)=(0,0,0)$ implies $c_1+c_2=0; c_1+c_3=0; c_2+c_3=0$. The first equation implies $c_1=-c_2$ and the third implies $c_3=-c_2$. Plugging these into the second equation we get $-2c_2=0$ which implies $c_2=0$ since $-2\neq 0$ in $\mathbb{F}_3$. Hence $c_1=c_3=-c_2=0$, i.e. the only possible linear dependency relation is the trivial one.

5a. $\gcd(x^3+x^2+4x+2, x^6-1)=x^2+4x+1$. Thus a generating matrix with linearly independent rows is

$$G=\begin{bmatrix}1&4&1&0&0&0\\0&1&4&1&0&0\\0&0&1&4&1&0\\0&0&0&1&4&1\end{bmatrix}.$$

5b. $\dim C=6-\deg(x^2+4x+1)=6-2=4$.

5c. $\frac{x^6-1}{x^2+4x+1}=x^4+x^3+4x+4$. Reversing coefficients, $h(x)=1+x+4x^3+4x^4$. Thus a check matrix with linearly independent rows is

$$H=\begin{bmatrix}1&1&0&4&4&0\\0&1&1&0&4&4\end{bmatrix}.$$