Erikson Sodergren CS462-01

1. Reducible polynomials degree<2 are x, x+1, x^2+x+1. Products of degree 5 MUST use one of these, along with something of degree 3 or 4.
    a. $x^5+x^4+1 = (x^2+x+1)(x^3+x+1)$
    b. x^5+x^3+1 = irreducible.
    c. $x^5+x^4+x^2+1 = (x+1)(x^4+x+1)$ -- reducible
2. Generators are bolded
    a. a mod 29

        order of 2 mod 29 is 28
        order of 3 mod 29 is 28
        order of 4 mod 29 is 14
        order of 5 mod 29 is 14
        order of 6 mod 29 is 14
        order of 7 mod 29 is 7
        order of 8 mod 29 is 28
        order of 9 mod 29 is 14
        order of 10 mod 29 is 28
        order of 11 mod 29 is 28
        order of 12 mod 29 is 4
        order of 13 mod 29 is 14
        order of 14 mod 29 is 28
        order of 15 mod 29 is 28
        order of 16 mod 29 is 7
        order of 17 mod 29 is 4
        order of 18 mod 29 is 28
        order of 19 mod 29 is 28
        order of 20 mod 29 is 7
        order of 21 mod 29 is 28
        order of 22 mod 29 is 14
        order of 23 mod 29 is 7
        order of 24 mod 29 is 7
        order of 25 mod 29 is 7
        order of 26 mod 29 is 28
        order of 27 mod 29 is 28
        order of 28 mod 29 is 2

    b. a mod 30 -- most never become 1.

        order of 2 mod 30 is nonexistant
        order of 3 mod 30 is nonexistant
        order of 4 mod 30 is nonexistant
        order of 5 mod 30 is nonexistant
        order of 6 mod 30 is nonexistant
        order of 7 mod 30 is 4

order of 8 mod 30 is nonexistant
order of 9 mod 30 is nonexistant
order of 10 mod 30 is nonexistant
order of 11 mod 30 is 2
order of 12 mod 30 is nonexistant
order of 13 mod 30 is 4
order of 14 mod 30 is nonexistant
order of 15 mod 30 is nonexistant
order of 16 mod 30 is nonexistant
order of 17 mod 30 is 4
order of 18 mod 30 is nonexistant
order of 19 mod 30 is 2
order of 20 mod 30 is nonexistant
order of 21 mod 30 is nonexistant
order of 22 mod 30 is nonexistant
order of 23 mod 30 is 4
order of 24 mod 30 is nonexistant
order of 25 mod 30 is nonexistant
order of 26 mod 30 is nonexistant
order of 27 mod 30 is nonexistant
order of 28 mod 30 is nonexistant
order of 29 mod 30 is 2

c. a mod 31

order of 2 mod 31 is 5
order of 3 mod 31 is 30
order of 4 mod 31 is 5
order of 5 mod 31 is 3
order of 6 mod 31 is 6
order of 7 mod 31 is 15
order of 8 mod 31 is 5
order of 9 mod 31 is 15
order of 10 mod 31 is 15
order of 11 mod 31 is 30
order of 12 mod 31 is 30
order of 13 mod 31 is 30
order of 14 mod 31 is 15
order of 15 mod 31 is 10
order of 16 mod 31 is 5
order of 17 mod 31 is 30
order of 18 mod 31 is 15
order of 19 mod 31 is 15
order of 20 mod 31 is 15
order of 21 mod 31 is 30

order of 22 mod 31 is 30

order of 23 mod 31 is 10

order of 24 mod 31 is 30

order of 25 mod 31 is 3

order of 26 mod 31 is 6

order of 27 mod 31 is 10

order of 28 mod 31 is 15

order of 29 mod 31 is 10

order of 30 mod 31 is 2

3. $(x^3+x+1)*(x^3+x^2+1) = x^6+x^5+x^4+3x^3+x^2+x+1 = x^6+x^5+x^4+x^3+x^2+x+1$
    a. $x^6+x^5+x^4+x^3+x^2+x+1$ mod $P(x^4+x+1)$
    b. $x^4 = x+1$ mod P, $x^5= x^2+x$ mod P, $x_6 = x^3+x^2$ mod P
    c. $x^6+x^5+x^4+x^3+x^2+x+1$ mod P $= (x^3+x^2)+(x^2+x)+(x+1)+x^3+x^2+x+1 = x^2+x$
4. $(x^7+x^6+x^3+x^2)^{-1} = x^4+x^3+x+1$, $P(x^8+x^4+x^3+x+1)$
    a. $(x^4+x+1) * (x^4+x^3+x+1) = x^8+x^7+2x^5+3x^4+x^3+x^2+2x+1 = x^8+x^7+x^4+x^3+x^2+1$
    b. $x^8 = x^4+x^3+x+1$ mod P
    c. $x^8+x^7+x^4+x^3+x^2+1$ mod P $= (x^4+x^3+x+1)+x^7+x^4+x^3+x^2+1 = x^7+x^2+x$
5. $(x^7+x^6+x+1) * (x^5+x^4+x+1) = x^{12}+2x^{11}+x^{10}+x^8+2x^7+x^6+2x^5+2x^4+x^2+2x+1$
    a. $x^{12}+x^{10}+x^8+x^6+x^2+1$, $P(x^8+x^4+x^3+x+1)$
    b. $x^8 = x^4+x^3+x+1$ mod P, $x^{10} = x^6+x^5+x^3+x^2$ mod P, $x^{12}= x^8+x^7+x^5+x^4$ mod P
    c. $((x^4+x^3+x+1)+x^7+x^5+x^4)+(x^6+x^5+x^3+x^2)+(x^4+x^3+x+1)+x^6+x^2+1$
    d. $x^7+x^4+x^3$
6.

i	q	r	s	t
0		$x^8+x^4+x^3+x+1$	1	0
1	x^2+x	$x^6+x^5+x^4+x$	0	1
2	x	$x^5+x^4+x^2+x+1$		x^2+x
3	x	$x^4+x^3+x^2$		x^3+x^2+1
4	x	x^3+x^2+x+1		$x^4+x^3+x^2$
5	x^2+x+1	x		$x^5+x^4+x^2+1$
6		**1**		$\mathbf{x^7+x^4+x^2+x+1}$

Find r_2		x^2+x
	$\vert$	____
$x^6+x^5+x^4+x$	$\vert$	$x^8+x^4+x^3+x+1$
	-	$x^8+x^7+x^6+x^3 = x^7+x^6+x^4+x$
	-	$x^7+x^6+x^5+x^2 = x^5+x^4+x^2+x+1$

Find r_3		x
$x^5+x^4+x^2+x+1$	$\vert$	____
	$\vert$	$x^6+x^5+x^4+x$
	-	$x^6+x^5+x^3+x^2+x = x^4+x^3+x^2$

Find r_4		x
$x^4+x^3+x^2$	$\vert$	____
	$\vert$	$x^5+x^4+x^2+x+1$
	-	$x^5+x^4+x^3 = x^3+x^2+x+1$

Find r_5		x
x^3+x^2+x+1	$\vert$	____
	$\vert$	$x^4+x^3+x^2$
	-	$x^4+x^3+x^2+x = x$
	-	

Find r_6		x^2+x+1
x	$\vert$	____
	$\vert$	x^3+x^2+x+1
	-	$x^3 = x^2+x+1$

	-	$x^2 = x+1$
	-	$x = 1$

<table>
<tr><td>Find r_7</td><td></td><td></td></tr>
<tr><td></td><td>|</td><td>____</td></tr>
<tr><td></td><td>|</td><td>x</td></tr>
<tr><td></td><td>-</td><td></td></tr>
</table>