Homework #03, due 2/3/10 = 9.4.3, 9.4.8, 9.4.14, 9.4.18 (use 9.4.17), 9.5.2.

Additional problems recommended for study: 9.4.10, 9.4.12, 9.4.16, 9.4.20, 9.5.1, 9.5.3, 9.5.4, 9.5.7

9.4.3 Show that the polynomial \((x - 1)(x - 2) \cdots (x - n) - 1\) is irreducible over \(\mathbb{Z}[n]\) for all \(n \geq 1\). [If the polynomial factors consider the values of the factors at \(x = 1, 2, \ldots, n\).]

Let \(p(x) = (x-1)(x-2) \cdots (x-n)-1\). To show that \(p(x)\) is irreducible in \(\mathbb{Z}[x]\) for all \(n \geq 1\), we assume \(p(x) = a(x)b(x)\) for some (wlog monic) polynomials \(a(x), b(x) \in \mathbb{Z}[x]\), and we will show this factorization is trivial.

For all \(k \in \{1, \ldots, n\}\) we have \(p(k) = -1 = a(k)b(k)\) so, since \(a(k)\) and \(b(k)\) are integers, they both must be 1 or -1, and they can’t have the same sign, so \(a(x) \neq b(x)\). Thus we have \(1 = (a(k))^2 = (b(k))^2\) for all \(k \in \{1, \ldots, n\}\). Since \(\deg(p) = n = \deg(a(x)) + \deg(b(x))\), the degrees of \(a(x)\) and \(b(x)\) cannot both be strictly larger than \(\frac{n}{2}\), so we may assume one of them has degree no more than \(\frac{n}{2}\). We assume wlog that \(\deg(a(x)) \leq \frac{n}{2}\), hence \(\deg(a^2(x)) \leq n\). Therefore \(p(x) + a^2(x)\) is a polynomial of degree \(n\) that has roots \(1, \ldots, n\). These are distinct roots, so by Prop. 9.9 \(p(x) + a^2(x)\) has \(n\) distinct linear factors \(x-1, x-2, \ldots, x-n\). Now \(p(x) + a^2(x)\) has factor \(x-1\), so \(p(x) + a^2(x) = (x-1)q_1(x)\) for some \(q_1(x) \in \mathbb{Z}[x]\), but \(p(x) + a^2(x)\) has roots 2, \(\ldots, n\) and these aren’t roots of \(x-1\), so they’re roots of \(q_1(x)\), so \(q_1(x)\) has a linear factor \(x-2\), hence \(q_1(x) = (x-2)q_2(x)\), and so on. Thus

\[
p(x) + a^2(x) = (x-1)q_1(x) = (x-1)(x-2)q_2(x) = \cdots = (x-1)(x-2) \cdots (x-n) = p(x) + 1
\]

Note the final equation gives \(a^2(x) = 1\), so the degree of \(a^2(x)\) is actually 0, hence \(a(x)\) is a constant in \(\mathbb{Z}\) whose square is 1, so \(a(x) = \pm 1\) and \(p(x) = \mp b(x)\). Therefore the factorization is trivial.

9.4.8 Prove that \(K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)\) and \(K_2 = \mathbb{F}_{11}/(y^2 + 2y + 2)\) are both fields with 121 elements. Prove that the map which sends
the element \( p(\bar{x}) \) of \( K_1 \) to the element \( p(\bar{y} + 1) \) of \( K_2 \) (where \( p \) is any polynomial with coefficients in \( \mathbb{F}_{11} \)) is well-defined and gives a ring (hence field) isomorphism from \( K_1 \) onto \( K_2 \).

First we note that \( x^2 + 1 \) is quadratic and has no roots in the ground field \( \mathbb{F}_{11} \) since, calculating modulo 11, we have

\[
\begin{align*}
(0)^2 + 1 &= 1 \\
(1)^2 + 1 &= 2 \\
(2)^2 + 1 &= 5 \\
(3)^2 + 1 &= 10 \\
(4)^2 + 1 &= 6 \\
(5)^2 + 1 &= 4 \\
(6)^2 + 1 &= 4 \\
(7)^2 + 1 &= 6 \\
(8)^2 + 1 &= 10 \\
(9)^2 + 1 &= 2 \\
(10)^2 + 1 &= 2
\end{align*}
\]

It follows by Prop. 9.10 that \( x^2 + 1 \) is irreducible in \( \mathbb{F}_{11}[x] \). The elements of the quotient field \( K_1 = \mathbb{F}_{11}[x]/(x^2 + 1) \) are \( ax + b + P \), where \( P = (x^2 + 1) \) and \( a, b \in \mathbb{F}_{11} \).

By Exercise 9.2.3, \( F[x]/(f(x)) \) is a field when \( f \in F[x] \) is irreducible, and by Exercise 9.2.2, \( F[x]/(f(x)) \) has \( q^n \) elements if \( |F| = q \) and \( \deg(f) = n \). In this case we have \( F = \mathbb{F}_{11} \) so \( q = 11 \), and \( f(x) = x^2 + 1 \) so \( n = 2 \), and the number of elements in \( K_1 \) is therefore \( q^n = 11^2 = 121 \).

(Strong of the proof goes like this: if \( a + bx + P = c + dx + P \) for some \( a, b, c, d \in \mathbb{F}_{11} \), then \( a-c+(b-d)x \in P \), hence \( a-c+(b-d)x = p(x)q(x) \) for some \( q(x) \in \mathbb{F}_{11}[x] \). If \( b - d \neq 0 \) then

\[
1 = \deg(a - c + (b - d)x) = \deg(p(x)q(x))
\]

\[
= \deg(p(x)) + \deg(q(x)) = 2 + \deg(q(x)) \geq 2,
\]

a contradiction, so \( b = d \). But then \( a-c \in P \), hence \( a-c = p(x)q'(x) \) for some \( q'(x) \in \mathbb{F}_{11}[x] \). If \( a-c \neq 0 \) then \( 0 = \deg(a-c) = \deg(p(x)q'(x)) = \deg(p(x)) + \deg(q'(x)) = 2 + \deg(q'(x)) \geq 2 \), a contradiction, so \( a = c \). Thus, each element of \( \mathbb{F}_{11}[x]/P \) has the form \( a + bx + P \) for uniquely determined \( a, b \in \mathbb{F}_{11} \).

Define a map \( \varphi \) from \( \mathbb{F}_{11}[x] \) to \( \mathbb{F}_{11}[y] \) by \( \varphi(p(x)) = p(y + 1) \) for every \( p(x) \in \mathbb{F}_{11}[x] \). Then \( \varphi \) is a ring homomorphism because

\[
\varphi(p(x)q(x)) = p(y + 1)q(y + 1) = \varphi(p(x))\varphi(q(x))
\]
\[
\varphi(p(x) + q(x)) = p(y + 1) + q(y + 1) = \varphi(p(x)) + \varphi(q(x))
\]
The map $\varphi$ can be described as “substitute $y+1$ for $x$”. This map has an inverse $\varphi^{-1}$ which may be described as “substitute $x-1$ for $y$”, that is, for all $q(y) \in \mathbb{F}_{11}[y]$ we let $\psi(q(y)) = q(x-1)$, so that $\psi(\varphi(p(x))) = \psi(p(y+1)) = p((x-1)+1) = p(x)$ and $\varphi(\psi(q(y))) = \varphi(q(x-1)) = q((y+1)-1) = q(y)$, so $\varphi = \varphi^{-1}$. This shows that $\varphi$ is actually a ring isomorphism. Note that $\varphi(x^2+1) = (y+1)^2 + 1 = y^2 + 2y + 2$. Corresponding elements in isomorphic rings generate corresponding ideals, so the image of the principal ideal $(x+1) \subseteq \mathbb{F}_{11}[x]$ under $\varphi$ is the ideal $(y^2+2y+1) \subseteq \mathbb{F}_{11}[y]$. Consequently the quotients by corresponding ideals are isomorphic, so

$$K_1 = \mathbb{F}_{11}[x]/(x^2+1) \cong \mathbb{F}_{11}/(y^2+2y+2) = K_2.$$

**9.4.14** Factor each of the two polynomials $x^8 - 1$ and $x^6 - 1$ into irreducibles over each of the following rings. (a) $\mathbb{Z}$ (b) $\mathbb{Z}/2\mathbb{Z}$ (c) $\mathbb{Z}/3\mathbb{Z}$.

(a) $\mathbb{Z}$: First we note that

$$x^8 - 1 = (x^4)^2 - 1 = (x^4 + 1)(x^4 - 1)$$

$$= (x^4 + 1)(x^2 + 1)(x^2 - 1)$$

$$= (x^4 + 1)(x^2 + 1)(x + 1)(x - 1)$$

Next we show that the factors $x^4 + 1$, $x^2 + 1$, $x + 1$, and $x - 1$ are all irreducible in $\mathbb{Z}[x]$. In Example (3), p. 310, following Cor. 14 in Section 9.4, the polynomial $p(x) = x^4 + 1 \in \mathbb{Z}[x]$ was shown to be irreducible in two steps. First, by the Eisenstein Criterion, applied with prime 2 to the polynomial $p(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, we know that $p(x+1)$ is irreducible in $\mathbb{Z}[x]$. Second, if there were a nontrivial factorization $p(x) = a(x)b(x)$, with $a(x), b(x) \in \mathbb{Z}[x]$, $1 \leq \deg(a(x)) < 4$, and $1 \leq \deg(b(x)) < 4$, then we would have $p(x+1) = a(x+1)b(x+1)$ where $1 \leq \deg(a(x+1)) < 4$ and $1 \leq \deg(b(x+1)) < 4$, contradicting the irreducibility of $p(x+1)$. The factor $x^2 + 1$ has no roots in $\mathbb{Z}$ and is quadratic, hence is irreducible by Prop. 9.10. Finally, the linear factors $x + 1$ and $x - 1$ are irreducible.

A factorization of $x^6 - 1$ into irreducibles in $\mathbb{Z}[x]$ is

$$x^6 - 1 = (x^3)^2 - 1 = (x^3 + 1)(x^3 - 1)$$

$$= (x^2 - x + 1)(x + 1)(x^2 + x + 1)(x - 1)$$
The linear factors $x + 1$ and $x - 1$ are irreducible. Let $p(x) = x^2 - x + 1$. Then
\[
p(x + 1) = (x + 1)^2 - (x + 1) + 1 = x^2 + 2x + 1 - x - 1 + 1 = x^2 + x + 1
\]
\[
p(x + 2) = (x + 2)^2 - (x + 2) + 1 = x^2 + 4x + 4 - x - 2 + 1 = x^2 + 3x + 3
\]
Now $x^2 + 3x + 3$ is irreducible in $\mathbb{Z}[x]$ by the Eisenstein Criterion, since prime 3 does not divide the leading coefficient 1, but does divide the lower order coefficients (3 and 3), and its square $3^2 = 9$ does not divide the constant 3. If $p(x)$ had a nontrivial factorization into nonconstant polynomials, say $p(x) = a(x)b(x)$, this would yield a nontrivial factorization $p(x + 2) = a(x + 2)b(x + 2)$, contradicting the irreducibility of $p(x + 2)$, so $p(x)$ is irreducible. A nontrivial factorization of $p(x + 1)$, say $p(x + 1) = c(x)d(x)$, would yield a nontrivial factorization $p(x + 2) = c(x + 1)d(x + 1)$, contradicting the irreducibility of $p(x + 2)$, so $p(x + 1)$ is also irreducible. This shows that the two quadratic factors in the factorization of $x^6 - 1$ are irreducible in $\mathbb{Z}[x]$.

(b): $\mathbb{Z}/2\mathbb{Z}$. This ring is the 2-element field $\mathbb{F}_2$, whose only elements are 0 and 1, and in which we have $-1 = 1$, so the previous factorizations can be written
\[
x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x + 1)
\]
\[
x^6 - 1 = (x^2 + x + 1)(x + 1)(x^2 + x + 1)(x + 1)
\]
Note that $(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1$, and $(x^2 + 1)(x^2 + 1) = x^4 + 2x^2 + 1 = x^4 + 1$, so we can continue to factor $x^8 - 1$, obtaining
\[
x^8 - 1 = (x^4 + 1)(x^2 + 1)(x + 1)(x + 1) = (x + 1)^8
\]
On the other hand, $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, so a factorization of $x^6 - 1$ into irreducibles over $\mathbb{Z}/2\mathbb{Z}$ is the same as it was over $\mathbb{Z}$, namely
\[
x^6 - 1 = (x^2 + x + 1)(x + 1)(x^2 + x + 1)(x + 1)
\]
GAP that confirms these results:
gap> r:=PolynomialRing(GF(2),"x");
GF(2)[x]
gap> x:=IndeterminatesOfPolynomialRing(r)[1];
x
gap> Factors(x^8-1);Factors(x^6-1);
[ x+Z(2)^0, x+Z(2)^0, x+Z(2)^0, x+Z(2)^0,
  x+Z(2)^0, x+Z(2)^0, x+Z(2)^0, x+Z(2)^0 ]
[ x+Z(2)^0, x+Z(2)^0, x^2+x+Z(2)^0, x^2+x+Z(2)^0 ]

(c): $\mathbb{Z}/3\mathbb{Z}$. This ring is the 3-element field $\mathbb{F}_3$, in which $-1 = 2$. The factorizations of $x^8 - 1$ and $x^6 - 1$ into irreducibles are

$$x^8 - 1 = (x + 1)(x + 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$$
$$x^6 - 1 = (x + 1)(x + 1)(x + 1)(x + 2)(x + 2)(x + 2)$$

These results were obtained by the following calculation in GAP:

gap> r:=PolynomialRing(GF(3),"x");
GF(3)[x]
gap> IndeterminatesOfPolynomialRing(r);
[ x ]
gap> x:=IndeterminatesOfPolynomialRing(r)[1];
x
gap> Factors(x^8-1);Factors(x^6-1);
[ x+Z(3)^0, x-Z(3)^0, x^2+Z(3)^0, x^2+x-Z(3)^0, x^2-x-Z(3)^0 ]
[ x+Z(3)^0, x+Z(3)^0, x+Z(3)^0, x-Z(3)^0, x-Z(3)^0, x-Z(3)^0 ]

9.4.18 Show that $6x^5 + 14x^3 - 21x + 35$ and $18x^5 - 30x^2 + 120x + 360$ are irreducible in $\mathbb{Q}[x]$.

We may use Exercise 9.4.17, which is the extended version of the Eisenstein Criterion that was proved in class.

Let $p(x) = 6x^5 + 14x^3 - 21x + 35$. Then $p(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein’s Criterion using prime 7, which does not divide the leading coefficient 6, does divide the remaining coefficients 14, $-21$, and 35, but it square $7^2 = 49$ does not divide the constant 35. Suppose $p(x)$ is reducible in $\mathbb{Q}[x]$, say $p(x) = A(x)B(x)$ for some $A(x), B(x) \in \mathbb{Q}[x]$. Note that $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, so by Prop. 9.5 (Gauss’s Lemma) there are rationals $r, s \in \mathbb{Q}$ such that $p(x) = rA(x)sB(x)$,
Let \( q(x) = 18x^5 - 30x^2 + 120x + 360 \). Then \( q(x) \) is irreducible by Eisenstein’s Criterion using prime 5, which does not divide the leading coefficient 18, does divide the remaining coefficients \(-30, 120, \) and \(360, \) but \(5^2 = 25\) does not divide the constant \(360\). By Prop. 9.5 (Gauss’s Lemma), \( q(x) \) is also irreducible in \( \mathbb{Q}[x] \), as was argued for \( p(x) \) above.

9.5.2 For each of the fields in Exercise 6 of Section 4 exhibit a generator for the (cyclic) multiplicative group of nonzero elements.

Exercise 9.4.6 asks for fields of order \( (a)\ 9, \ (b)\ 49, \ (c)\ 8, \) and \( (d)\ 81, \) exhibited in the form \( F[x]/(f(x)) \) where \( F \) is field and \( f \in F[x] \).

(a) For a field \( F[x]/(f(x)) \) of order 9, let \( F = \mathbb{F}_3 \) and let \( f \) be the irreducible quadratic polynomial \( f(x) = x^2 + 1 \in \mathbb{F}_3[x] \). The elements \( F[x]/(f(x)) \) have the form \( ax + b + (f) \), where \( a, b \in \{0, 1, 2\} \). The multiplicative group of \( F[x]/(f(x)) \) is generated by \( x + 2 + (f) \), as is shown in the table of calculations below, where we write simply “\( ax+b\)” instead of “\(ax+b+(f)\)”. With this notational convention, observe that in \( F[x]/(f(x)) \) we have \( x^2 + 1 = 0 \) (more precisely, \( x^2 + 1 + (f) = (f) \)), so \( x^2 = -1 = 2 \).

\[
\begin{align*}
(x + 2)^1 &= x + 2 \\
(x + 2)^2 &= x^2 + 4x + 4 = 2 + x + 1 = x \\
(x + 2)^3 &= (x + 2)x = x^2 + 2x = 2x + 2 \\
(x + 2)^4 &= (2x + 2)(x + 2) = 2x^2 + 6x + 4 = 2(2) + 1 = 2 \\
(x + 2)^5 &= 2(x + 2) = 2x + 1 \\
(x + 2)^6 &= (2x + 1)(x + 2) = 2x^2 + 5x + 2 = 2(2) + 2x + 2 = 2x \\
(x + 2)^7 &= 2x(x + 2) = 2x^2 + 4x = 2(2) + x = x + 1 \\
(x + 2)^8 &= (x + 1)(x + 2) = x^2 + 3x + 2 = 2 + 2 = 1
\end{align*}
\]

(b) To get a field \( F[x]/(f(x)) \) of order 49, we choose \( F = \mathbb{F}_7 \) so that \( q = |\mathbb{F}_7| = 7 \), and we let \( f \) be any one of the 21 irreducible quadratic polynomials in \( \mathbb{F}_7[x] \). Then \( n = 2 \) and the order of \( F[x]/(f(x)) \) is \( q^n = 7^2 = 49 \). The 21 quadratic irreducible polynomials in \( \mathbb{F}_7[x] \) are
organized in the following table according to the 7 linear substitutions, “substitute \( x + n \) for \( x \).”

<table>
<thead>
<tr>
<th>( \varphi(x) )</th>
<th>( x^2 + 1 )</th>
<th>( x^2 + 2 )</th>
<th>( x^2 + 4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \varphi(x+1) )</td>
<td>( x^2 + 2x + 2 )</td>
<td>( x^2 + 2x + 3 )</td>
<td>( x^2 + 2x + 5 )</td>
</tr>
<tr>
<td>( \varphi(x+2) )</td>
<td>( x^2 + 4x + 5 )</td>
<td>( x^2 + 4x + 6 )</td>
<td>( x^2 + 4x + 1 )</td>
</tr>
<tr>
<td>( \varphi(x+3) )</td>
<td>( x^2 + 6x + 3 )</td>
<td>( x^2 + 6x + 4 )</td>
<td>( x^2 + 6x + 6 )</td>
</tr>
<tr>
<td>( \varphi(x+4) )</td>
<td>( x^2 + x + 3 )</td>
<td>( x^2 + x + 4 )</td>
<td>( x^2 + x + 6 )</td>
</tr>
<tr>
<td>( \varphi(x+5) )</td>
<td>( x^2 + 3x + 5 )</td>
<td>( x^2 + 3x + 6 )</td>
<td>( x^2 + 3x + 1 )</td>
</tr>
<tr>
<td>( \varphi(x+6) )</td>
<td>( x^2 + 5x + 2 )</td>
<td>( x^2 + 5x + 3 )</td>
<td>( x^2 + 5x + 5 )</td>
</tr>
</tbody>
</table>

**Claim:** \( \mathbb{F}_7/(x^2 + 1) \) is generated by \( x + 3 = x + (x^2 + 1) \). From \( x^2 + 1 = 0 \) we have \( x^2 = -1 = 6 \), so we can derive a rule for raising \( x + 3 \) to powers in \( \mathbb{F}_7/(x^2 + 1) \). If \( ax + b \) is a power of \( x + 3 \), we get the next power as follows:

\[
(ax + b)(x + 3) = ax^2 + (3a + b)x + 3b = (3a + b)x + (6a + 3b)
\]

Using GAP, I computed the powers of \( x + 3 \), and obtained these results, which prove that \( x + 3 \) is indeed a generator.

\[
\begin{align*}
(x + 3)^1 &= x + 3 & (x + 3)^2 &= 6x + 1 \\
(x + 3)^3 &= 5x + 4 & (x + 3)^4 &= 5x \\
(x + 3)^5 &= x + 2 & (x + 3)^6 &= 5x + 5 \\
(x + 3)^7 &= 6x + 3 & (x + 3)^8 &= 3 \\
(x + 3)^9 &= 3x + 2 & (x + 3)^{10} &= 4x + 3 \\
(x + 3)^{11} &= x + 5 & (x + 3)^{12} &= x \\
(x + 3)^{13} &= 3x + 6 & (x + 3)^{14} &= x + 1 \\
(x + 3)^{15} &= 4x + 2 & (x + 3)^{16} &= 2 \\
(x + 3)^{17} &= 2x + 6 & (x + 3)^{18} &= 5x + 2 \\
(x + 3)^{19} &= 3x + 1 & (x + 3)^{20} &= 3x \\
(x + 3)^{21} &= 2x + 4 & (x + 3)^{22} &= 3x + 3 \\
(x + 3)^{23} &= 5x + 6 & (x + 3)^{24} &= 6 \\
(x + 3)^{25} &= 6x + 4 & (x + 3)^{26} &= x + 6
\end{align*}
\]
(c) For a field $F[x]/(f(x))$ of order 8, let $F = \mathbb{F}_2$ and let $f$ be the irreducible cubic polynomial $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. The multiplicative group of $\mathbb{F}_3[x]/(x^3 + x + 1)$ has 7 elements, and since 7 is prime it follows that every non-zero element of the field will generate the multiplicative group. In particular, $x$ generates, as is explicitly shown by the following calculations. First note that since $x^3 + x + 1 = 0$, we get $x^3 = -x - 1 = x + 1$ (all modulo 2), so

\begin{align*}
x^1 &= x \\
x^2 &= x^2 \\
x^3 &= x + 1 \\
x^4 &= x^2 + x \\
x^5 &= x^3 + x^2 = x^2 + x + 1 \\
x^6 &= x^3 + x^2 + x = x^2 + 1 \\
x^7 &= x^3 + x^2 = x + 1 + x = 1
\end{align*}

(d) For a field $F[x]/(f(x))$ of order 81, let $F = \mathbb{F}_3$ and let $f$ be the irreducible quartic polynomial $f(x) = x^4 + x + 2 \in \mathbb{F}_3[x]$. Let $P = (f) \subseteq$
The elements $F[x]/(f(x))$ have the form $ax^3 + bx^2 + cx + d + P$, where $a, b, c, d \in \{0, 1, 2\}$. The multiplicative group of $F[x]/(f(x))$ is generated by $x + P$. The 80 powers of $x + P$ are shown in the table below, which has only “$ax^3 + bx^2 + cx + d$” instead of “$ax^3 + bx^2 + cx + d + P$”.

| $x^1$ | $x^2$ | $x^3$ | $x^4$ | $x^5$ | $x^6$ | $x^7$ | $x^8$ | $x^9$ | $x^{10}$ | $x^{11}$ | $x^{12}$ | $x^{13}$ | $x^{14}$ | $x^{15}$ | $x^{16}$ | $x^{17}$ | $x^{18}$ | $x^{19}$ | $x^{20}$ | $x^{21}$ | $x^{22}$ | $x^{41}$ | $x^{42}$ | $x^{43}$ | $x^{44}$ | $x^{45}$ | $x^{46}$ | $x^{47}$ | $x^{48}$ | $x^{49}$ | $x^{50}$ | $x^{51}$ | $x^{52}$ | $x^{53}$ | $x^{54}$ | $x^{55}$ | $x^{56}$ | $x^{57}$ | $x^{58}$ | $x^{59}$ | $x^{60}$ | $x^{61}$ | $x^{62}$ |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| $x$   | $x^2$ | $x^3$ | $2x + 1$ | $2x^2 + x$ | $2x^3 + x^2$ | $x^3 + x + 2$ | $x^2 + x + 1$ | $x^3 + x^2 + x$ | $x^3 + x^2 + 2x + 1$ | $x^3 + 2x^2 + 1$ | $2x^3 + 1$ | $2x + 2$ | $2x^2 + 2x$ | $2x^3 + 2x^2$ | $2x^3 + x + 2$ | $x^2 + 2$ | $x^3 + 2x$ | $x^3 + 2x$ | $2x^2 + 2x + 1$ | $2x^2 + 2x + 1$ | $2x^3 + 2x^2$ | $2x^3 + 2x^2 + x$ | $2x^3 + 2x^2 + x + 2$ | $2x^3 + x^2 + 2$ | $x^3 + 2x$ | $x^3 + 2x + 1$ | $2x^2 + 1$ | $2x^3 + x$ | $x^2 + x$ | $x^3 + x^2$ | $x^3 + 2x + 1$ | $x^3 + 2x + 1$ | $2x^3 + 2x^2 + 1$ | $x^3 + 2x^2 + 2x$ | $x^3 + 2x^2 + 2x + 1$ | $2x^3 + 2x^2 + 1$ |
\[
x^{23} = x^3 + x + 1 \\
x^{24} = x^2 + 1 \\
x^{25} = x^3 + x \\
x^{26} = x^2 + 2x + 1 \\
x^{27} = x^3 + 2x^2 + x \\
x^{28} = 2x^3 + x^2 + 2x + 1 \\
x^{29} = x^3 + 2x^2 + 2x + 2 \\
x^{30} = 2x^3 + 2x^2 + x + 1 \\
x^{31} = 2x^3 + x^2 + 2x + 2 \\
x^{32} = x^3 + 2x^2 + 2 \\
x^{33} = 2x^3 + x + 1 \\
x^{34} = x^2 + 2x + 2 \\
x^{35} = x^3 + 2x^2 + 2x \\
x^{36} = 2x^3 + 2x^2 + 2x + 1 \\
x^{37} = 2x^3 + 2x^2 + 2x + 2 \\
x^{38} = 2x^3 + 2x^2 + 2 \\
x^{39} = 2x^3 + 2 \\
x^{40} = 2 \\
x^{63} = 2x^3 + 2x + 2 \\
x^{64} = 2x^2 + 2 \\
x^{65} = 2x^3 + 2x \\
x^{66} = 2x^2 + x + 2 \\
x^{67} = 2x^3 + x^2 + 2x \\
x^{68} = x^3 + 2x^2 + x + 2 \\
x^{69} = 2x^3 + x^2 + x + 1 \\
x^{70} = x^3 + x^2 + 2x + 2 \\
x^{71} = x^3 + 2x^2 + x + 1 \\
x^{72} = 2x^3 + x^2 + 1 \\
x^{73} = x^3 + 2x + 2 \\
x^{74} = 2x^2 + x + 1 \\
x^{75} = 2x^3 + x^2 + x \\
x^{76} = x^3 + x^2 + x + 2 \\
x^{77} = x^3 + x^2 + x + 1 \\
x^{78} = x^3 + x^2 + 1 \\
x^{79} = x^3 + 1 \\
x^{80} = 1
\]