Solutions to Assignment 10

17C P.369

25. By Lagrange’s interpolation, let

\[ g(x) = x(x-1)(x+1) \]

with

\[ h_{-1}(x) = x(x-1)/(-1)(-1-1) = \frac{x(x-1)}{2} \]
\[ h_0(x) = (x+1)(x-1)/(0+1)(0-1) = -(x-1)(x+1) \]
\[ h_1(x) = x(x+1)/(1)(1+1) = \frac{x(x+1)}{2} \]

The required function is

\[ f(-1)h_{-1}(x) + f(0)h_0(x) + f(1)h_1(x) = \frac{1}{2}x(x-1) + x(x+1) = \frac{x}{2}[x-1 + 2x + 2] = \frac{x(3x+1)}{2} \]

19A P.391

10. \( 11^2 = 121 = 2 \times 61 - 1, \ 3^5 = 243 = 4 \times 61 - 1, \ 13^3 = 2197 = 36 \times 61 + 1 \)

To find a primitive root, we need an element of order \( (61-1) = 60 \). From above, we know 11 has order 4, 9 has order 5 (since 3 has order 10), 13 has order 3. So

\[ 11 \times 9 \times 13 = 1287 \equiv 6(\text{mod}61) \]

has order \( lcm(3, 4, 5) = 60 \).

11. First of all, note that 401 is prime. Since 30 has order 16, 5 has order 25. If 6 is of order less than 400, then the order must be \( 2^a5^b \), with either \( a < 4 \) or \( b < 2 \) (or both). Suppose the former holds, then

\[ 30^{2^a \times 25} = 5^{2^a \times 25} \times 6^{2^a \times 25} \equiv 1 \times 1 \equiv 1(\text{mod}401) \]

But then \( 16|\left(2^a \times 25\right) \), with \( a < 4 \), which is a contradiction. Suppose the latter holds, then

\[ 1 \equiv 30^{16 \times 2^b} = 5^{16 \times 2^b} \times 6^{16 \times 2^b} \equiv 5^{16 \times 2^b} \times 1 = 1(\text{mod}401) \]

i.e. \( 1 \equiv 5^{16 \times 2^b}(\text{mod}401) \). Then \( 25|(16 \times 2^b) \), which is again a contradiction. Hence \( a = 4 \) and \( b = 2 \) and the order of 6 is 400.

12. \( 33^2 \equiv -1(\text{mod}109) \), and 3 has order 27. So

\[ (-1)^{27} \equiv (33^2)^{27} = 3^{54} \times 11^{54}(\text{mod}109) \]
\[ -1 \equiv 11^{54}(\text{mod}109) \]

So any factor of 54 cannot be the order of 11, i.e. the order can only be 4, 12, 36, 108. Suppose the order is 4, then \( 1 \equiv 33^4 = 11^4 \times 3^4 \equiv 1 \times 3^4(\text{mod}109) \). However, it is known that 3 has order 27, which gives a contradiction. And similarly for the case of order 12, 36. Hence the order must be 108.

23A P.483

4. We know \( \alpha^2 + \alpha + 2 = 0 \) in \( F_3 \). So \( \alpha^2 = -\alpha - 2 = 2\alpha + 1 \)

(i) \( (\alpha + 1)(\alpha + 2) = \alpha^2 + 3\alpha + 2 = \alpha^2 + 2 = (-\alpha - 2) + 2 = -\alpha \).
(ii) Note that every polynomial in terms of $\alpha$ can be reduced into a linear one by the equation above. Suppose $a\alpha + b$ is an inverse of $2\alpha + 1$. Then

$$1 = (a\alpha + b)(2\alpha + 1) = 2a\alpha^2 + (a + 2b)\alpha + b = 2a(-\alpha - 2) + (a + 2b)\alpha + b = (2b - a)\alpha + (b - 4a)$$

So

$$2b - a = 0$$

$$b - 4a = b - a = 1$$

Adding the equations, we get $3b - 2a = 2a = a = 1$. And hence $b = 2$. So the inverse is $\alpha + 2$.

(iii) $\alpha^6 = (2\alpha + 1)^3 = 8\alpha^3 + 12\alpha^2 + 6\alpha + 1 = 2\alpha^3 + 1$. Now

$$\alpha^6 = 2\alpha^3 + 2\alpha + 1 = 2\alpha(2\alpha + 1) + 1 = 4\alpha^2 + 2\alpha + 1 = 2\alpha + 1 + 2\alpha + 1 = \alpha + 2$$

(iv) From (ii) and (iii), $\alpha^6(2\alpha + 1) = (\alpha + 2)(2\alpha + 1) = 1$. So

$$\alpha^7(2\alpha + 1) = \alpha$$

and from the quadratic relation $\alpha^2 + \alpha + 2 = 0$, $\alpha(\alpha + 1) = -2 = 1$. So

$$\alpha^7(2\alpha + 1)(\alpha + 1) = \alpha(\alpha + 1) = 1$$

This means $(2\alpha + 1)(\alpha + 1) = 2\alpha^2 + 1 = 2(2\alpha + 1) + 1 = \alpha$ is the inverse of $\alpha^7$.

**ALTERNATIVELY**, note that $F_3[\alpha]$ is a field with 9 elements. The nonzero elements in the field forms a group of 8 elements. Hence $\beta^8 = 1$ by the abstract Lagrange’s theorem for all elements $\beta$, including $\alpha$.

5. Note that the polynomial $p(x)$ is irreducible. Therefore $F_3[\alpha]$ is a field with 9 elements. So in particular $a + b\alpha$, with $a, b \in \{0, 1, 2\}$ are the 9 elements. Also, note that $\alpha^2, \alpha^4 \neq 1$ so the order of $\alpha$ is 8. So the powers of $\alpha, \alpha^i, i \in \{1, \ldots, 8\}$ are the 8 units in the field. The inverse of $\alpha^i$ is $\alpha^{8-i}$.

6. Again, check that $g(x) = x^3 + 2x + 2$ is irreducible in $F_3[x]$. So $F = F_3(\alpha)$ is a field. Now factor theorem says in $F[x]$, $(x - \alpha)|g(x)$. Also, note that

$$(\alpha^3)^3 + 2(\alpha^3) + 2 = (-2\alpha - 2)^3 + 2(-2\alpha - 2) + 2 = \alpha^3 + 1 + 2\alpha + 2 + 2 = (-2\alpha - 2) + 2\alpha + 2 = 0$$

Hence $g(\alpha^3) = 0$, and by factor theorem $(x - \alpha^3)|g(x)$. Similarly, check $g(\alpha^9) = 0$ and hence $(x - \alpha^9)|g(x)$. From these, we conclude that

$$g(x) = (x - \alpha)(x - \alpha^3)(x - \alpha^9)$$

**Primitive Root Handout**

The use of commutativity boils down to the first line of the proof of Lemma 1:

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1$$