Solutions to Assignment 5

9C Euler’s Theorem

49. We know that \( \phi(18) = \phi(2)\phi(3^2) = (2-1)3^2-1(3-1) = 6. \) So by Euler’s Theorem we know that since \((5, 18) = 1, \) then \( 5^{18} \equiv 1 \pmod{18}. \) Thus \( 5 \cdot 5^{18} \equiv 1 \pmod{18}, \) so then \( 5^{18} \) is the inverse of 5 modulo 18.

50. Euler’s Theorem gives us that \( a^{\phi(m)} \equiv 1 \pmod{m}. \) Now we know that \( f = 1 + k\phi(m) \) for some \( k \in \mathbb{Z}. \) So we get
\[
a^f \equiv a^{1+k\phi(m)} \equiv a \cdot (a^{\phi(m)})^k \pmod{m} \\
\equiv a \cdot 1^k \pmod{m} \\
\equiv a \pmod{m}
\]

9F Finding High Powers Modulo \( m \)

82. Note that \( 1729 = 10^3 + 9^3 = (10 + 9)(10^2 - 9 \cdot 10 + 9^2) = 19 \cdot 91 = 19 \cdot 7 \cdot 13 \)

So it is not a prime. Also, since \( \phi(1729) = \phi(7)\phi(13)\phi(19) = 6 \cdot 12 \cdot 18 = 1296 \) and \( (5, 1729) = 1, \) \( 5^{1296} \equiv 1 \pmod{1729}. \) So \( 5^{1728} \equiv 5^{1296} \cdot 5^{432} \equiv 5^{432} \pmod{1729}. \) Now
\[
5^{432} = 25^{216} = 625^{108} = (625^2)^{54} \equiv 1600^{54} = (1600^2)^{27} \equiv 1080^{27} = (1080^3)^9 \equiv 638^9 \equiv (1065^3)^3 \equiv 1 \pmod{1729}
\]

10A RSA cryptography

7. We know that \( m = pq \) and \( \phi(m) = (p-1)(q-1) = pq - p - q + 1 = m - p - m/p + 1 \) So \( p\phi(m) = pm - p^2 - m + p \implies p^2 + (\phi(m) - m - 1)p + m = 0. \) Also note that \( m \) and \( \phi(m) \) are both symmetric in \( p \) and \( q. \) Thus, a quadratic equation \( x^2 + (\phi(m) - m - 1)x + m = 0, \) has both \( p \) and \( q \) as its roots.

11A Groups of Units and Euler’s Theorem

9. \( (1-i)^2 = i, (1-i)^4 = i^2 = -1, (1-i)^8 = (-1)^2 = 1 \)

So the order of \((1-i)\) must be a factor of 8, i.e. 1,2,4 or 8. But we have seen from above that 1,2,4 cannot be the order. So the order of \((1-i)\) is 8.

Since \( a = (1-i) \) has order 8, the elements in the set \( \{1, a, a^2, \ldots, a^7\} \) must be distinct, or else \( a^i = a^j \) for some \( 0 \leq i < j \leq 7 \) implies \( a^{i-j} = 1, \) violating the order of \( a. \) So every unit of \( \mathbb{F}_9 \) (there are 8 of them) must be a power of \( a. \)

Then \( a^i \) will have order \( 8/gcd(i, 8), \) according to a Proposition in the textbook.

11B Subgroups
10. One direction is easy: Suppose $H$ is a subgroup, then for any $h_1, h_2$ in $H$, the product must also be in $H$ by definition. For the other direction, we need to show that if $h \in H$, then $h^{-1} \in H$.

To do so, consider the set $S = \{h, h^2, h^3, \ldots \}$. Since we assume multiplication is closed, every element in $S$ must be in $H$. Also, we know that $G$ is finite, so $H$ is also finite and hence $S$ is also finite. That means there must be some $1 \leq i < j$ such that

$$h^i = h^j$$

In particular, if we consider $h^i$ and $h^j$ as elements in $G$, we have

$$1 = h^i(h^{-1})^i = h^j(h^{-1})^j = h^{j-i}$$

So $1 = h^{j-i} \in S \subset H$, and $h \cdot h^{j-i-1} = 1$. The inverse of $h \in H$ is $h^{j-i-1} \in H$.

11. (i) Note that $[7^2] = [49] = [11]$ and then $[7^3] = [77] = [1]$ in $U_{19}$, so we get $\langle [7] \rangle = \{ [7], [11], [1] \}$.

(ii) Here $[12^2] = ([-7]^2] = [49] = [11], \ [12^3] = [-77] = [-1] = [18], \ [12^4] = [7], \ [12^5] = [-49] = [-11] = [8], \ [12^6] = [77] = [1]$. Thus we have $\langle [12] \rangle = \{ [12], [11], [18], [7], [8], [1] \}$.

(iii) Here $[8^2] = [64] = [7], \ [8^3] = [56] = [-1] = [18], \ [8^4] = [-8] = [11], \ [8^5] = [-64] = [-7] = [12], \ [8^6] = [-56] = [1]$. Thus we see that $\langle [8] \rangle = \{ [8], [7], [18], [11], [12], [1] \}$.

12. Consider $H = \{1, 7, 9, 15 \}$. Note that this set is closed under the operation and that each element is its own inverse. Hence this is a non-cyclic subgroup of $U_{16}$.

11C Cosets and Lagrange’s Theorem

15. (i) $\{1, 7, 11\}, \{2, 14, 3\}, \{4, 9, 6\}, \{5, 16, 17\}, \{8, 18, 12\}, \{10, 13, 15\}$ are distinct cosets. Note that $6 \cdot 3 = 18$.

(ii) $\{1, 12, 11, 18, 7, 8\}, \{2, 5, 3, 17, 14, 16\}, \{4, 10, 6, 15, 9, 13\}$ are distinct cosets. Note that $3 \cdot 6 = 18$.

(iii) $\{1, 5, 6, 11, 17, 9, 7, 16, 4\}, \{2, 10, 12, 3, 15, 18, 14, 13, 8\}$ are distinct cosets. Note that $2 \cdot 9 = 18$.

Extra Questions

1. Using $p = 19, \ q = 23$, and encoding exponent $e = 5$, encode the word "baby". Use $a = 11, \ b = 12, \ . \ . \ , \ z = 36$.

The codes before encryption: 11, 12, 35. To encrypt: Compute

$11^5 \equiv 237 \ (mod\ 19 \cdot 23)$

$12^5 \equiv 179 \ (mod\ 19 \cdot 23)$

$35^5 \equiv 156 \ (mod\ 19 \cdot 23)$

2. Consider an RSA cryptosystem with modulus 7081 and encoding exponent 1789. Using the same alphabet as in the previous problem, decode 5192, 2604, 4222. Show all your work.

First of all 7081 = 97 \cdot 73. So $\phi(7081) = 96 \cdot 72 = 6912$. We need to find $1789^{-1} (mod\ 6912)$, which is 85$(mod\ 6912)$. Therefore for any $a$ such that $(a, 7081) = 1$,

$$(a^{1789})^{85} = a^{1789 \cdot 85} = a^{6912k + 1} \equiv 1 (mod\ 7081)$$

To decode 5192, compute

$5192^{85} \equiv 1615 (mod\ 7081)$

$2604^{85} \equiv 2823 (mod\ 7081)$

$4222^{85} \equiv 1130 (mod\ 7081)$

which gives FERMAT, one of the greatest mathematicians in history!