MATH319 – HOMEWORK SOLUTIONS

HOMEWORK #12

Section 4.3: Problems 1,3
Section 4.4: Problems 1,3

Section 4.3, #1

(a) First $341 = 11 \cdot 31$ and $\gcd(3, 341) = 1$, so we can apply Euler's Theorem. First $\phi(341) = \phi(11)\phi(31) = 10 \cdot 30 = 300$. Using Euler's Theorem we have $3^{340} = 3^{300} \cdot 3^{40} \equiv 3^{40} \bmod 341$. To determine $3^{40} \bmod 341$ we can compute 3^{40} modulo 11 and 31 using Fermat and then use the Chineese Remainder Theorem. First $3^{40} = (3^{10})^4 \equiv 1 \bmod 11$ by Fermat. Next $3^{40} = 3^{30} \cdot 3^{10} \equiv 3^{10} \bmod 31$ by Fermat. Now $3^{10} = (3^3)^3 \cdot 3 \equiv (-4)^3 \cdot 3 = -64 \cdot 3 \equiv -2 \cdot 3 = -6 \equiv 25 \bmod 31$. Since $3^{40} \equiv 1 \bmod 11$ and $3^{40} \equiv 25 \bmod 31$, we can use the Chineese Remainder Theorem to determine the unique solution modulo 341 to the system

$$x \equiv 1 \bmod 11, \qquad x \equiv 25 \bmod 31.$$

Since x is unique it must equal 3^{40}. Here $m_1 = 11, m_2 = 31, M = 341$. This gives $M_1 = 31$ and $M_2 = 11$. We need the inverses x_1 of 31 modulo 11, and x_2 of 11 modulo 31. We find $x_1 = 5$, and $x_2 = 17$. So the solution x of the system is

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 = 1 \cdot 31 \cdot 5 + 25 \cdot 11 \cdot 17 = 4830 \equiv 56 \bmod 341.$$

Thus, $3^{40} \equiv 56 \bmod 341$.

(b) Since $\gcd(7, 100) = 1$ we can apply Euler's Theorem. So $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = 2 \cdot 5 \cdot 4 = 40$. We apply the Division Theorem to the exponent 8^9 and 40. Actually, all we really need is the remainder, that is, $8^9 \bmod 40$. Now $\frac{8^9}{40} = \frac{8^8}{5}$, and $8^8 = (8^2)^4 = 64^4 \equiv (-1)^4 \equiv 1 \bmod 5$. Thus, So 8^9 has a remainder of 8 when divided by 40, that is, $8^9 = 40q + 8$ for some positive integer q. Thus, using Euler we get $7^{8^9} = 7^{40q+8} = (7^{40})^q \cdot 7^8 \equiv 7^8 \bmod 100 = (7^4)^2 = (49^2)^2 = 2401^2 \equiv 1^2 \equiv 1 \bmod 100$.

(c) Again since $\gcd(2, 121) = 1$ we can apply Euler's Theorem. We have $\phi(121) = \phi(11^2) = 11 \cdot 10 = 110$. Apply the Division Theorem to 110 and the exponent 10000. we find $10000 = 110 \cdot 90 + 100$. So $2^{10000} = (2^{110})^{90} \cdot 2^{100} \equiv 1^{90} \cdot 2^{100} = 2^{100} = (2^{10})^{10} = 1024^{10} \equiv 56^{10} = (56^2)^5 = 3136^5 \equiv 111^5 \equiv (-10)^5 = -10^5 = -100 \cdot 10^3 \equiv 21 \cdot 10^3 \equiv 21 \cdot 32 = 672 \equiv 67 \bmod 121$.

∎

Section 4.3, #3 This is similar to the second example of 4.3.2. We write $72 = 8 \cdot 9$, and compute $\phi(8) = \phi(2^3) = 4$, and $\phi(9) = \phi(3^2) = 3 \cdot 2 = 6$. Any n which satisfies $\gcd(n, 72) = 1$ also satisfies $\gcd(n, 4) = 1$ and $\gcd(n, 6) = 1$. Thus we can apply Euler's Theorem which for any n such that $\gcd(72, n) = 1$ gives the system

$$n^4 \equiv 1 \bmod 8, \qquad n^6 \equiv 1 \bmod 9.$$

But using $n^{12} = (n^4)^3$ and $n^{12} = (n^6)^2$ this implies the system

$$n^{12} \equiv 1 \bmod 8, \qquad n^{12} \equiv 1 \bmod 9.$$

But then the Chineese Remainder Theorem implies $n^{12} \equiv 1 \bmod 72$. ∎

Section 4.4, #1 As mentioned in Example 4.4.4, 2 solutions to $x^4 \equiv 1 \bmod 13$ are $x = \pm 1$. By Corollary 4.4.3 there are exactly 4 solutions. Since $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ and ± 1 are clearly solutions to $x^2 \equiv 1 \bmod 13$, it follows again using Corollary 4.4.3 that the other 2 solutions are solutions to the congruence $x^2 \equiv -1 \bmod 13$. One sees easily that $x = \pm 5$ are those two solutions since $(\pm 5)^2 = 25 \equiv -1 \bmod 13$. Thus, the four solution are $\pm 1, \pm 5$, or equivalently $1, 12, 5, 8$. ∎

Section 4.4, #3 By Corollary 4.4.3 the congruence $x^{6k} \equiv 1 \bmod p$ where $p = 6k + 1$ is a prime, has exactly $6k$ solutions, since $6k$ divides $p - 1 = 6k$. Now we factor $x^{6k} - 1 = (x^{3k} - 1)(x^{3k} + 1)$, and and notice that every solution to either of the congruences $x^{3k} \equiv \pm 1 \bmod p$ gives a solution to the congruence $x^{6k} \equiv 1 \bmod p$. Conversely, since p is prime every solution to the congruence $x^{6k} \equiv 1 \bmod p$ must be a solution to one of the congruences $x^{3k} \equiv \pm 1 \bmod p$. Now since $3k$ divides $p - 1 = 6k$ there are exactly $3k$ solutions to the congruence $x^{3k} \equiv 1 \bmod p$. Since there are exactly $6k$ solutions to the congruence $x^{6k} - 1 \equiv 0 \bmod p$, and there are exactly $3k$ solutions to the congruence $x^{3k} - 1 \equiv 0 \bmod p$, there must be exactly $3k$ solutions to the congruence $x^{3k} \equiv -1 \bmod p$. ∎