Solutions to HW #4

7.3: #3 Since $\varphi(25) = 20$, we must check that 2 has order 20. By the primitivity test, we check that $2^{10} \equiv -1 \mod 25$ and $2^4 \equiv 16 \mod 25$ are both not equal to 1.

7.3: #10 If we use the baby-step big step method with $g = 3$, $N = 101$, and $h = 2$ $n = 11$ we have modulo 101

$$(g^0, g^1, \ldots, g^{11}) = (1, 3, 9, 27, 81, 41, 22, 66, 97, 89, 65, 94)$$

and

$$(hg^0, hg^{-n}, \ldots, hg^{-n^2}) = (2, 43, 66, 5, 57, 64, 63, 92, 59, 6, 28, 97)$$

so that $g^7 \equiv 2 * g^{-22} \mod 101$ or $2 \equiv g^{29} \mod 101$, so $\log_3(2) = 29$.

7.3: #13 Note here that $x$ must be invertible modulo $m$. Let $x = se$ and $s = rf$, so $e = \log_s(x)$ and $f = \log_r(s)$. Since $x = r^e f$ and primitive elements have order $\varphi(m)$, we have

$$\log_r(x) \equiv ef = \log_s(x)\log_r(s) \mod \varphi(m).$$

9.1: #4: 23 is prime and $GCD(3, 23) = 1$ so FLT says

$$3^{1000} \equiv 3^{22*45+10} \equiv 3^{10} \equiv 8 \mod 23.$$ 

13.1: #2: $18^{48} \equiv 1 \mod 49$. (This can be verified from Euler’s theorem, $\varphi(49) = 42$ and $GCD(18, 49) = 1$. $18^{48} \equiv 18^6 \equiv 1 \mod 49$ since $18^3 \equiv 1$.)

13.1 #6: $14^{64} \equiv 1 \mod 65$. (Again by Euler’s theorem, $GCD(14, 65) = 1$ and $\varphi(65) = 48$ so $14^{64} \equiv 14^{16} \equiv 1 \mod 65$. since $14^2 \equiv 1$.)

E0: By trial division we must check divisibility by all primes $\sqrt{100} = 10$. These primes are 2, 3, 5, 7, so this is true.

E1: (a) $\varphi(690)/690 = 176/690$.

(b) Since 15 divides 690, the answer is $\varphi(15) = 2 * 4 = 8$. Since 40 does not divide 690, the answer is 0.

(c) The primes dividing 690 are 2, 3, 5, and 23. 2 is not primitive because $2^{690/3} \equiv 1 \mod 691$. However $b = 3$ passes this test.

(d) Use baby-step giant-step with $n = 27$, $g = 3$, $h = 2$, $N = 691$,

$$(1, 3, 9, 27, 81, 243, 38, 114, 342, 335, 314, 251, 62, 186, 558, 292, 185, 555, 283, 158, 474, 40, 120, 360, 389, 476, 46, 138)$$
and
(2, 618, 50, 441, 559, 660, 155, 607, 420, 664, 135, 16, 611, 400,
73, 326, 443, 549, 19, 596, 475, 389, 128, 51, 436, 584, 535, 89)

so \(g^{24} = 2 \ast g^{-27 \ast 21} \) or \( \log_3(2) = 591 \).

For Method 2, use 690 = 2 * 3 * 5 * 23, and the CRT.

Let \( x = \log_3(2) \). Then, if \( x = x_0 + 2 \ast x_1 \), \( 0 \leq x_0 \leq 1 \),
\( -1 \equiv 2^{690/2} \equiv 3^{690/2 \ast x_0} \) implies \( x_0 = 1 \).

If \( x = y_0 + 3 \ast y_1 \), \( 0 \leq y_0 \leq 2 \), \( 1 \equiv 2^{690/3} \equiv 3^{690/3 \ast y_0} \) implies \( y_0 = 0 \).

If \( x = z_0 + 5 \ast z_1 \), \( 0 \leq z_0 \leq 4 \), \( 3 \equiv 2^{690/5} \equiv 3^{690/5 \ast z_0} \equiv 132^{z_0} \) implies \( z_0 = 1 \).

If \( x = w_0 + 23 \ast w_1 \), \( 0 \leq w_0 \leq 22 \), \( 379 \equiv 2^{690/23} \equiv 3^{690/23 \ast y_0} \equiv 271^{w_0} \) implies \( w_0 = 16 \).

The CRT solution is \( x \equiv 591 \mod 690 \).

E2: Since 4 divides 101 which is prime, the roots of this polynomial are all elements of order 1 (1), order 2 (-1), and order 4 (10 and -10) so
\( x^4 - 1 = (x^2 - 1) \ast (x^2 + 1) = (x - 1) \ast (x + 1) \ast (x - 10) \ast (x + 10) \).

E3: This never occurs. Proof: Let \( x \) be primitive and suppose that \( x^e \) is another primitive element. Then we must have \( GCD(e, p - 1) = 1 \), so \( e \) is odd. Then the product is \( x \ast x^e = x^{e+1} \), and 2 divides \( GCD(e + 1, p - 1) \), so \( x^{e+1} \) is not primitive.

E4: Note that \( x^4 - 1 = (x^2 + 1) \ast (x^2 - 1) \) so that \( x^2 + 1 \equiv 0 \mod p \) has a solution exactly when \( (Z/p)^x \) has an element of order 4. This occurs exactly when 4 divides \( p - 1 \) namely \( p \equiv 1 \mod 4 \).

E5: \( 2^{23376} \equiv 1 \mod 23377 \). However \( 2^{23376/2} \equiv 15907 \mod 23377 \) is not 1 or -1, so the Miller-Rabin test proves that 23377 is NOT prime.

E6: (a) It looks like this \( X \) passes the Miller-Rabin test with base 7, so we can say \( X \) is at least probably prime. Can we use the knowledge of \( 7^{(X-1)/3} \) to say more? Since \( X > 1000 \) and we have \( 722 < X \), so \( 7^{(X-1)/3} \neq 1 \mod X \). The only primes dividing \( X - 1 \) are 2 and 3, so the Lucas test says \( X \) is prime since 7 has order \( X - 1 \).

(b) Let’s try the Pocklington-Lehmer criterion with \( K = 2^c \) and \( U = 5^d \). Since \( c \geq 3d \) we have \( K \geq U \). The only prime dividing \( K \) is \( q = 2 \). Note that we do have \( 7^{Y-1} \equiv 1 \mod Y \). Try \( b_q = 7 \), so is \( GCD(7^{(Y-1)/2} - 1, Y) = 1? \) Since \( GCD(7^{(Y-1)/2} - 1, Y) = GCD(-2, Y) = 1 \), yes. So \( Y \) is prime.

(c) \( Z \) is composite because \( 3706 \neq \pm 1 \mod Z \) is a square root of 1.