Solutions to Assignment 7

22.3 Let S be the set of all infinite sequences of 0s and 1s. Show that S is uncountable.

Proof: We use Cantor's diagonal argument. So we assume (toward a contradiction) that we have an enumeration of the elements of S, say as $S = \{s_1, s_2, s_3, \ldots\}$ where each s_n is an infinite sequence of 0s and 1s. We will write $s_1 = s_{1,1}s_{1,2}s_{1,3}\cdots$, $s_2 = s_{2,1}s_{2,2}s_{2,3}\cdots$, and so on; so $s_n = s_{n,1}s_{n,2}s_{n,3}\cdots$. So we denote the mth element of s_n by $s_{n,m}$. Now we create a new sequence $t = t_1t_2t_3t_4\cdots$ of 0s and 1s as follows: $t_n = s_{n,n} - 1$ (so $t_n = 1$ if $s_{n,n} = 0$ and $t_n = 0$ if the $s_{n,n}$ is 1). It is clear that t is an element of S - it is an infinite sequence of 0s and 1s. However, we will now see that t is not in the list above. Suppose that $t = s_k$ for some value of k. Then $t_k = s_{k,k}$, but by construction, $t_k \neq s_{k,k}$, so this is not possible. We conclude that S is not countable.

22.4(a) Let S be the set of all finite subsets of $\mathbb{N}$. Claim: S is countable.

Proof: We will prove this using the result from Proposition 22.4. So we will need to construct a 1-1 function f from S to $\mathbb{N}$. To do this, we first write $p_1, p_2, p_3, \cdots$ for the primes in ascending order. Now, for any finite subset $T \subseteq \mathbb{N}$, start by ordering the elements of T in ascending order, $T = \{t_1, t_2, \ldots, t_n\}$, with $t_1 < t_2 < \cdots < t_n$. Then define $f(T) = p_1^{t_1}p_2^{t_2}\cdots p_n^{t_n}$.

To check that f is 1-1, suppose that $f(T) = f(T')$. Then $p_1^{t_1}p_2^{t_2}\cdots p_n^{t_n} = p_1^{t'_1}p_2^{t'_2}\cdots p_{n'}^{t'_{n'}}$. By the fundamental theorem of arithmetic these two products can only be equal if $n = n'$ (so T and T' have the same number of elements) and each of the corresponding powers is equal, *i.e.*, $t_1 = t'_1$, $t_2 = t'_2$, $\cdots$, $t_n = t'_n$; so, $T = T'$.

22.4(b) Let T be the set of all infinite subsets of $\mathbb{N}$. Show that T is uncountable.

Proof: By Proposition 22.5 the set of all subsets of $\mathbb{N}$ is uncountable (if it were countable, it would have the same cardinality as $\mathbb{N}$). Suppose now that the set T of all infinite subsets of $\mathbb{N}$ were countable. In Part (a) we have shown that the set S of all finite subsets of $\mathbb{N}$ is countable. So by Problem 1(b) we could derive that $S \cup T$ is countable. But $S \cup T$ is the set of all subsets of $\mathbb{N}$, so this leads to a contradiction. We conclude that T is uncountable.

14.1(b) We need to find $0 \leq r \leq 645$ such that $2^{81} \equiv r \mod 645$. Since $645 = 3*5*43$, so an extension of Fermatt's little theorem gives us that $2^{2*4*42} \equiv 1 \mod 645$, so $2^{336} \equiv 1 \mod 645$, but unfortunately that exponent is too large, so we need to use successive squares or other tricks. (The extension of Fermatt's little theorem can be used any time when the power is a product of distinct squares.) So, here is a solution, using squares and some powers of 3: $2^2 \equiv 4 \mod 645$, $2^3 \equiv 8 \mod 645$, $2^9 \equiv 2^3 * 2^3 * 2^3 \mod 645 \equiv 512 \mod 645 \equiv -133 \mod 645$, and $2^{18} \equiv 133^2 \mod 645 \equiv 17,689 \mod 645 \equiv 274 \mod 645$, so $2^{36} \equiv 274^2 \mod 645 \equiv$

$75076 \mod 645 \equiv 256 \mod 645$, $2^{72} \equiv 256^2 \mod 645 \equiv 65,536 \mod 645 \equiv 391 \mod 645 \equiv -254 \mod 645$, and finally, $2^{81} = 2^{72} * 2^9 \equiv (-254) * (-133) \mod 645 \equiv 33,782 \mod 645 \equiv 242 \mod 645$.

14.1(c) To find the last two digits, we need to calculate $3^{124} \mod 100$. (Since $100 = 2^2 * 5^2$, the extensions of Fermatt's Little Theorem don't apply.)

However, a quick method goes as follows: $3^5 = 243 \equiv 43 \mod 100$, and $3^{10} \equiv 43^2 \mod 100 \equiv 1849 \mod 100 \equiv 49 \mod 100$, and $3^{20} \equiv 49^2 \mod 100 \equiv 2401 \mod 100 \equiv 1 \mod 100$; so $3^{124} = 3^{120} * 3^4 \equiv 1 * 81 \mod 100 \equiv 81 \mod 100$.

14.3 (a) $99x \equiv 9x \mod 30$, so we need to solve $9x \equiv 18 \mod 30$ and it is clear that $x \equiv 9 \mod 30$ is a solution.

(b) We first find the highest common factor of 91 and 143 by the Euclidean algorithm:

$$\begin{aligned} 143 &= 91 + 52 \\ 91 &= 52 + 39 \\ 52 &= 39 + 13 \\ 39 &= 3 * 13 \end{aligned}$$

So $(143, 91) = 13$. However, 84 is not an integer multiple of 13, so $91x \equiv 84 \mod 143$ does not have a solution according to Proposition 14.6.

(c) We list the squares mod 5: $0^2 \equiv 0 \mod 5$, $1^2 \equiv 1 \mod 5$, $2^2 \equiv 4 \mod 5$, $3^2 \equiv 4 \mod 5$, $4^2 \equiv 1 \mod 5$. We conclude that there are no solutions for $x^2 \equiv 2 \mod 5$.

(d) Putting $0, 1, 2, 3, 4$ into the equation $x^2 + x + 1 \mod 5$ gives us $1, 3, 2, 3, 1$ respectively. We see that $x^2 + x + 1 \equiv 0 \mod 5$ has no solutions.

(e) You may check that $x \equiv 2 \mod 7$ and $x \equiv 4 \mod 7$ are solutions.

15.1 (a) Since 11 is prime and does not divide 3, we can apply Fermatt's little theorem, and we get that $3^{10} \equiv 1 \mod 11$. So $3^{301} = (3^{10})^{30} * 3 \equiv 1 * 3 \mod 11 \equiv 3 \mod 11$.

13 is also prime and does not divide 5, so by Fermatt's little theorem, $5^{12} \equiv 1 \mod 13$. We calculate that $5^{110} = (5^{12})^9 5^2 \equiv 1 * 25 \mod 13 \equiv 12 \mod 13$.

(b) Note that $42 = 7 * 3 * 2$, a product of distinct squares. By Fermatt's little theorem, $n^p \equiv n \mod p$ for any prime p. So $n^7 \equiv n \mod 7$; also, $n^3 \equiv n \mod 3$, and therefore $n^7 = n^3 * n^3 * n \equiv n * n * n \mod 3 \equiv n \mod 3$; finally, n^7 is even if and only if n is even, so $n^7 \equiv n \mod 2$. We conclude then that $n^7 - n$ is a multiple of 7, a multiple of 3, and a multiple of 2. Since 7, 3, and 2 are distinct prime numbers, this implies that $n^7 - n$ is a multiple of 42.

15.7 (a) Solve $x^3 \equiv 2 \mod 29$. Use the Euclidean algorithm for 28 and 3:

$$28 = 9 * 3 + 1$$

So $1 = 28 - 9 * 3 = 28 - 3 * 28 + 28 * 3 - 9 * 3 = -2 * 28 + 19 * 3$. So by the recipe from Proposition 15.2, the solution is $x \equiv 2^{19} \mod 29 \equiv 26 \mod 29$. $(x \equiv x * (x^{28})^2 \mod 29 \equiv (x^3)^{19} \mod 29 \equiv 2^{19} \mod 29)$

(c) Solve $x^{11} \equiv 2 \mod 143$. Note that $143 = 11 * 13$, so we want to apply the recipe from Proposition 15.3/. We start by applying the Euclidean algorithm to 11 and $10 * 12 = 120$: $120 = 10 * 11 + 10$, and $11 = 10 + 1$, so $1 = 11 - 10 = 11 - (120 - 10 * 11) = 11 * 11 - 120$. So the solution is $x \equiv 2^{11} \mod 143 \equiv 46 \mod 143$.

16.2 **(a)** WHEREAREYOU is first translated into numbers as

$$2308051805011805251521,$$

by using $A = 01$, $B = 02$ and so on up to $Z = 26$.

Since $N = 143$, we divide 2308051805011805251521 into 11 two digit numbers: 23, 08, 05, 18, 05, 01, 18, 05, 25, 15, 21.

Since $e = 11$ and $N = 143$, each number is encoded by raising it to the eleventh power, mod 143. We do this as follows:

n	n mod 143	n^2 mod 143	n^4 mod 143	n^8 mod 143	n^e mod 143
23	23	100	133	100	56
08	8	64	92	27	96
05	5	25	53	92	60
18	18	38	14	53	73
05	5	25	53	92	60
01	1	1	1	1	1
18	18	38	14	53	73
05	5	25	53	92	60
25	25	53	92	27	25
15	15	82	3	9	59
21	21	12	1	1	109

So, 23, 08, 05, 18, 05, 01, 18, 05, 25, 15, 21 encodes to 56, 96, 60, 73, 60, 01, 73, 60, 25, 59, 109

(b)

We need to find prime numbers p and q such that $p * q = 143$. The number 143 factors into $11 * 13$, so we take $p = 11$ and $q = 13$. Then $(p - 1)(q - 1) = 10 * 12 = 120$.

Using the expanded Euclidean algorithm, we solve $1 = 11 * d - (p - 1)(q - 1)c$ and get $d = 11$ (since $11 * 11 - 120 = 121 - 120 = 1$).

To decode the string 12, 59, 14, 114, 59, 14 we need to solve each number raised to the power of $d = 11$, mod 143.

n	n mod 143	n^2 mod 143	n^4 mod 143	n^8 mod 143	n^d mod 143
12	12	1	1	1	12
59	59	49	113	42	15
14	14	53	92	27	14
114	114	126	3	9	4
59	59	49	113	42	15
14	14	53	92	27	14

So 12, 59, 14, 114, 59, 14 decodes into 12, 15, 14, 04, 15, 14, which when we use our initial tranlation of 1 = A, 2 = B and so on, gives us LONDON.