Homework 5 Solutions

4.2: 2:

a. $321 = 256 + 64 + 1 = (01000001)_2$

b. $1023 = 512 + 256 + 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = (1111111111)_2$. Note that this is 1 less than the next power of 2, 1024, which is $(10000000000)_2$.

c. $100632 = 2^{16} + 2^{15} + 2^{11} + 2^8 + 2^4 + 2^3 = (11000100100011000)_2$.

4.2: 4:

a. $16 + 8 + 2 + 1 = 27$

b. $512 + 128 + 32 + 16 + 4 + 1 = 693$

c. $512 + 256 + 128 + 32 + 16 + 8 + 4 + 2 = 958$

d. $2^{14} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 31775$

4.2: 29: Every positive integer n can be written as the sum of distinct powers of 2, since the binary expansion of n is such an expression (which can be derived algorithmically by adding 1 starting from 0 a total of n times, using standard carry-over rules). Also, every such expression can be written as a binary expansion. Suppose n has two distinct binary expansions x and y, and suppose the largest power of 2 at which they differ is 2^i. Suppose without loss of generality that x contains the term 2^i while y does not. Then $x - y$ contains a positive term of 2^i, while its negative terms sum up to at most $-(2^{i-1} + 2^{i-2} + ... + 4 + 2 + 1) = -\frac{1-2^i}{1-2} = -(2^i - 1)$.

Therefore $x - y \geq 2^i + (1 - 2^i) = 1$, a contradiction since x and y represent the same integer n (meaning that $x - y$ should be equal to 0). Therefore the binary representation – or any way to write an integer as a sum of distinct powers of 2 – is unique. (For the purists: the problem as stated is technically a bit ambiguous; it should have said *nonnegative* integer powers of 2. Can you find a counterexample to uniqueness that uses positive and negative integers?)

4.2: 31: Let $n = (a_k a_{k-1} a_{k-2} ... a_1 a_0)_{10}$ be written in base 10, with each a_i being a digit from 0 to 9. Because $10 \bmod 3 = 1$, we know $10^i \bmod 3 = 1^i \bmod 3 = 1$ for any nonnegative integer i. Then
$n \bmod 3 = (a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10 + a_0) \bmod 3$
$= \big(a_k \cdot (10^k \bmod 3) + a_{k-1} \cdot (10^{k-1} \bmod 3) + ... + a_1 \cdot (10 \bmod 3) + a_0\big) \bmod 3$
$= (a_k + a_{k-1} + ... + a_1 + a_0) \bmod 3.$

Therefore n is divisible by 3 (i.e., $n \bmod 3 = 0$) exactly when the sum of the digits of n is a multiple of 3. In fact, the remainder when n is divided by 3 is the same as that when its digit sum is divided by 3.

4.2: 32: As in the previous problem, let $n = (a_k a_{k-1} a_{k-2} ... a_1 a_0)_{10}$ be written in base 10, with each a_i being a digit from 0 to 9. Because $10 \bmod 11 = -1$, we know $10^i \bmod 11 = (-1)^i \bmod 11 = (-1)^i$ for any nonnegative integer i. Then
$n \bmod 11 = (a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10 + a_0) \bmod 11$
$= \big(a_k \cdot (10^k \bmod 11) + a_{k-1} \cdot (10^{k-1} \bmod 11) + ... + a_1 \cdot (10 \bmod 11) + a_0\big) \bmod 11$
$= ((-1)^k a_k + (-1)^{k-1} a_{k-1} + ... - a_1 + a_0) \bmod 11$
$= (a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)$
Therefore n is divisible by 11 (that is, $n \bmod 11 = 0$) exactly when the difference between the sum of the digits of n in even and odd positions is 0.

4.3: 4:

a. $39 = 3 \cdot 13$

b. $81 = 3^4$

c. 101 is prime

d. $143 = 11 \cdot 13$

e. $289 = 17^2$

f. $899 = 29 \cdot 31$

4.3: 10: Suppose $2^m + 1$ is an odd prime – which guarantees that $m \geq 1$ – and suppose by way of contradiction that $p \neq 2$ is a prime number dividing m. Let $k = \frac{m}{p}$, so $m = pk$. Note that $(2^k + 1)(2^{k(p-1)} - 2^{k(p-2)} + 2^{k(p-3)} - ... - 2^k + 1) = \big(2^{kp} - 2^{k(p-1)} + 2^{k(p-2)} - ... + 2^k\big) + \big(2^{k(p-1)} - 2^{k(p-2)} + 2^{k(p-3)} - ... + 1\big)$, which telescopes to $2^{kp} + 1 = 2^m + 1$. In other words, we've found a factorization of $2^m + 1$. Because $1 \leq k < m$, we know $2 \leq 2^k + 1 < 2^m + 1$, so this is a proper factorization of $2^m + 1$ (i.e., not just $1 \cdot (2^m + 1)$). This is a contradiction, so m had no odd prime factors, and so $m = 2^n$ for some nonnegative integer n. Note that we required p to be odd in order for the second term of our factorization to end with $-2^k + 1$; if p were even, it would end with $+2^k - 1$, meaning the product would telescope to $2^{kp} - 1$, not $2^{kp} + 1$ like we needed.

4.3: 11: Suppose by way of contradiction that $\log_2 3 = \frac{a}{b}$ for some positive integers a and b (note that $\log_2 3$ is positive, so this is valid). Then $3 = 2^{a/b}$. Taking both sides to the bth power, we see $3^b = 2^a$. But this is a contradiction – the only prime dividing the left-hand side is 3 (which it does, since $b \geq 1$) and the only prime dividing the right-hand side is 2 (which is also does, since $a \geq 1$). Therefore $\log_2 3$ is irrational.

4.3: 12: For any positive integer n, consider the integer $(n+1)!+i$ for every $2 \leq i \leq n+1$. Note that $(n+1)!+i = i \cdot \left(\frac{(n+1)!}{i} + 1\right)$ is a factorization of $(n+1)!+i$ into smaller integers, since $i \geq 2$ and by the definition of factorial, $(n+1)!$ is divisible by any integer between 2 and $n+1$. Therefore each such integer is composite, yielding n consecutive composite integers.

4.3: 13: 3, 5, and 7 work.

4.3: 16(b,d):

b. Because $\gcd(17, 85) = 17$, these integers are not relatively prime.

d. Every pair of these integers has gcd 1, so these integers are relatively prime (you could also write out their prime factorizations – easy since all but 18 is already prime – and note that no prime appears in more than one factorization).

4.3: 18(a,b):

a. The positive divisors of 6 are 1, 2, 3, and 6. Adding these all up except for the 6 yields 6, so 6 is perfect. Similarly, the positive divisors of 28 are 1, 2, 4, 7, 14, and 28. Adding these up except for the 28 yields 28, so 28 is perfect.

b. Suppose $2^p - 1$ s prime. The positive divisors of $2^{p-1}(2^p - 1)$, apart from itself, are 1, 2, 4, 8, ..., 2^{p-2}, 2^{p-1} together with $(2^p - 1), 2 \cdot (2^p - 1), 4 \cdot (2^p - 1), ..., 2^{p-2}(2^p - 1)$. The sum of all these divisors is
$(1+2+4+...+2^{p-1})+(2^p-1)(1+2+4+...+2^{p-2}) = 2^p-1+(2^p-1)(2^{p-1}-1) = (2^p-1)2^{p-1}$.
Therefore $2^{p-1}(2^p - 1)$ is a perfect number.

4.3: 20(a,b):

a. $2^7 - 1 = 127$, which is prime

b. $2^9 - 1 = 511$, which factors as $7 \cdot 73$ and thus is not prime.

4.3: 24(a,b):

a. Take the minimum exponents of each primes in the prime factorizations: the gcd is $2^2 \cdot 3^3 \cdot 5^2$.

b. By similar reasoning, the gcd is $2 \cdot 3 \cdot 11$. Note that the prime 5 only appears in the first factorization, so its minimum exponent is 0 (think of there as being a 5^0 in the second factorization), and similarly for 11, 13, and 17.

4.3: 26(a,b):

a. Take the maximum exponent of the primes in the prime factorizations: the lcm is $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$.

b. By similar reasoning, the lcm is $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$. These numbers are relatively prime, so their lcm is simply their product (and their gcd is 1).

4.3: 28: We factor: $1000 = 2^3 5^3$ and $625 = 5^4$. Thus $\gcd(1000, 625) = 5^3$ and $\text{lcm}(1000, 625) = 2^3 5^4$. Therefore $\gcd(1000, 625) \cdot \text{lcm}(1000, 625) = 2^3 5^7 = 1000 \cdot 625$. When dealing with large numbers like this, it's much easier to leave everything as prime factorizations.

4.3: 30: Let the two (positive) integers be a and b. We know $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$, so $\text{lcm}(a, b) = \frac{ab}{\gcd a,b} = \frac{2^7 3^8 5^2 7^{11}}{2^3 3^4 5} = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$

4.3: 32(c): $\gcd(123, 277) = \gcd(277 \bmod 123, 123) = \gcd(31, 123) = \gcd(31, 123 \bmod 31) = \gcd(31, 30) = \gcd(31 \bmod 30, 30) = \gcd(1, 30) = 1$. At each step we replace the larger integer by its remainder when divided by the smaller integer. (We could also have noted that the larger number, 277, is prime, so the gcd must be 1.)

4.3: 36: Suppose a and b are positive integers. We're going to use the following formula:

$$2^a - 1 = (2^b - 1)\left(2^{a-b} + 2^{a-2b} + 2^{a-3b} + ... + 2^{a-\lfloor \frac{a}{b} \rfloor b}\right) + \left(2^{a \bmod b} - 1\right)$$

but first let's see where it comes from:
In order to find $(2^a - 1) \bmod (2^b - 1)$, we're going to subtract off multiples of $2^b - 1$ from $2^a - 1$ and see what's left. First we can subtract 2^{a-b} multiples of $(2^b - 1)$. We're left with $(2^a - 1) - 2^{a-b}(2^b - 1) = 2^{a-b} - 1$. Now subtract off 2^{a-2b} multiples of $(2^b - 1)$ from what's left to now be left with $(2^{a-b} - 1) - 2^{a-2b}(2^b - 1) = 2^{a-2b} - 1$. As long as the exponent $a - b$, $a - 2b$, $a - 3b$, ... is nonnegative we can keep doing this.

What will be left when we can't keep doing it any more? $2^{a-ib} - 1$, where $i = \lfloor \frac{a}{b} \rfloor$. But $a - \lfloor \frac{a}{b} \rfloor b = a \bmod b$; in words, this is subtracting off as many copies of b as possible from a, which is exactly what mod is defined to do. Thus we're left with $2^{a \bmod b} - 1$. This is reflected in the above equation.

Finally, note that $a \bmod b < b$, so $2^{a \bmod b} - 1 < 2^b - 1$, and so the answer $(2^a - 1) \bmod (2^b - 1)$ really is $2^{a \bmod b} - 1$.

4.3: 37: Let a and b be positive integers with $a \geq b$. To compute the gcd of a and b, the Euclidean algorithm uses the fact that $\gcd(a, b) = \gcd(a \bmod b, b)$. Thus

$$\gcd(2^a - 1, 2^b - 1) = \gcd((2^a - 1) \bmod (2^b - 1), 2^b - 1) = \gcd(2^{a \bmod b} - 1, 2^b - 1)$$

By similar logic, $\gcd(2^{a \bmod b} - 1, 2^b - 1) = \gcd(2^{b \bmod (a \bmod b)} - 1, 2^{a \bmod b} - 1)$ (by plugging in "a" $= b$ and "b" $= a \bmod b$ into what we already proved.)

But this mimics the path of the Euclidean algorithm. In the end the Euclidean algorithm produces $\gcd(a, b)$, so by following this chain of reasoning down we'll eventually end up with $\gcd(2^{\gcd(a,b)} - 1, 2^{\gcd(a,b)} - 1) = 2^{\gcd(a,b)} - 1$, as desired. Note: to give a more precise proof of this result we'd need something called "strong induction," which you'll learn about later, and formalizes this idea of proving a result for larger numbers by relying on the result being true for smaller numbers.

4.3: 40(f): The Euclidean algorithm performs the following steps:

$$\begin{aligned}
323 &= 2 \cdot 124 + 75 \\
124 &= 1 \cdot 75 + 49 \\
75 &= 1 \cdot 49 + 26 \\
49 &= 1 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}$$

Thus the gcd is 1 (323 and 124 were relatively prime). To find a linear combination of 323 and 124 that equals 1 as per Bezout's theorem, we'll work backwards, each time solving for the remainder (the added number on the right of the equation) and plugging it into what we already have:

$$\begin{aligned}
&1 = 3 - 1 \cdot 2 \\
&1 = 3 - 1 \cdot (23 - 7 \cdot 3) = 8 \cdot 3 - 23 \\
&1 = 8 \cdot (26 - 1 \cdot 23) - 23 = 8 \cdot 26 - 9 \cdot 23 \\
&1 = 8 \cdot 26 - 9 \cdot (49 - 1 \cdot 26) = 17 \cdot 26 - 9 \cdot 49 \\
&1 = 17 \cdot (75 - 1 \cdot 49) - 9 \cdot 49 = 17 \cdot 75 - 26 \cdot 49 \\
&1 = 17 \cdot 75 - 26 \cdot (124 - 1 \cdot 75) = 43 \cdot 75 - 26 \cdot 124 \\
&1 = 43 \cdot (323 - 2 \cdot 24) - 26 \cdot 124 = 43 \cdot 323 - 112 \cdot 124
\end{aligned}$$

Therefore $43 \cdot 323 - 112 \cdot 124 = 1$.

4.4: 2: $937 \cdot 13 \bmod 2436 = 12181 \bmod 2436 = (2436 \cdot 5 + 1) \bmod 2436 = 1$, so 937 is an inverse of 13 mod 2436.

4.4: 4: Because $2 \cdot 9 = 18$ and $18 \bmod 17 = 1$, 9 is an inverse of 2 mod 17.

4.4: 6(a,c):

a. The Euclidean algorithm to compute $\gcd(17, 2)$ performs the following step:

$$17 = 8 \cdot 2 + 1$$

The next gcd is $\gcd(2,1)$, which is just 1. Therefore $1\cdot 17 - 8\cdot 2 = 1$, so (taking both sides mod 17) $(-8)\cdot 2 = 1$. Therefore -8 is an inverse of 2 mod 17. Note that $-8+17=9$ is also an inverse of 2 mod 17, as is $-8+2\cdot 17 = 26$, etc.

c. The Euclidean algorithm to compute $\gcd(233,144)$ performs the following steps:

$$\begin{aligned}
233 &= 1\cdot 144\cdot 2 + 89\\
144 &= 1\cdot 89 + 55\\
89 &= 1\cdot 55 + 34\\
55 &= 1\cdot 34 + 21\\
34 &= 1\cdot 21 + 13\\
21 &= 1\cdot 13 + 8\\
13 &= 1\cdot 8 + 5\\
8 &= 1\cdot 5 + 3\\
5 &= 1\cdot 3 + 2\\
3 &= 1\cdot 2 + 1
\end{aligned}$$

The next gcd is $\gcd(2,1)$, which is just 1. We compute the Bezout coefficients of 233 and 144 as follows, working backwards plugging each line into the line beneath it, starting by solving for 2 in the second-to-last line to get $2 = 5 - 1\cdot 3$ (see the solution to 4.2:40). For simplicity I'll omit the 1's:

$$\begin{aligned}
&1 = 3 - 2\\
&1 = 3 - (5-3) = 2\cdot 3 - 5\\
&1 = 2\cdot(8-5) - 5 = 2\cdot 8 - 3\cdot 5\\
&1 = 2\cdot 8 - 3\cdot(13-8) = 5\cdot 8 - 3\cdot 13\\
&1 = 5\cdot(21-13) - 3\cdot 13 = 5\cdot 21 - 8\cdot 13\\
&1 = 5\cdot 21 - 8\cdot(34-21) = 13\cdot 21 - 8\cdot 34\\
&1 = 13\cdot(55-34) - 8\cdot 34 = 13\cdot 55 - 21\cdot 34\\
&1 = 13\cdot 55 - 21\cdot(89-55) = 34\cdot 55 - 21\cdot 89\\
&1 = 34\cdot(144-89) - 21\cdot 89 = 34\cdot 144 - 55\cdot 89\\
&1 = 34\cdot 144 - 55\cdot(233-144) = 89\cdot 144 - 55\cdot 233
\end{aligned}$$

Therefore $89\cdot 144 - 55\cdot 233 = 1$. Taking this mod 233, we see that $89\cdot 144 \bmod 233 = 1$, so 89 is an inverse of 144 mod 233.

4.4: 8: Let $\gcd(a,m) = d \geq 2$ and suppose by way of contradiction that that $ab \bmod m = 1$. Then for some integer k, $ab + km = 1$. Now d divides both a and m, so d divides ab, and so d divides $ab + km$. But d does not divide 1, a contradiction. Thus a has no inverse (i.e., b) mod m.

For example, let $a = 9$ and $m = 12$. Then $\gcd(a, m) = 3$, and multiplying 9 by anything mod 12 always gives an answer that's divisible by 3, which 1 isn't. So there's no way to multiply 9 by anything and take the result mod 12 to get 1.

4.4: 10: The problem should say: use the inverse of 2 modulo 17 found in 6a. Multiply both sides by the inverse of 2 modulo 17, which we found to be 9 (or -8, if you prefer):

$$9 \cdot 2x \equiv 9 \cdot 7 \bmod 17$$

Using the associative rule and doing a bit of arithmetic,
$(9 \cdot 2)x \equiv 12 \bmod 17$, so $1x \equiv 12 \bmod 17$, and so $x \equiv 12 \bmod 17$. Check that this works in the original equation.

4.4: 12(b): We found that 89 is an inverse of 144 mod 233 (i.e., $89 \cdot 144 \equiv 1 \bmod 3$). Multiply on both sides by 89:

$$89 \cdot 144x \equiv 89 \cdot 4 \bmod 233$$

So $1x \equiv 123 \bmod 233$, and so $x \equiv 123 \bmod 233$.

4.4: 16:

a. The pairs are: $2 \cdot 6 \equiv 1 \bmod 11$, $3 \cdot 4 \equiv 1 \bmod 11$, $5 \cdot 9 \equiv 1 \bmod 11$, and $7 \cdot 8 \equiv 1 \bmod 11$. Each pair consists of two numbers that are each other's inverses mod 11.

   We could also prove this with a bit less trial and error: we know that any number between 1 and 10 must have an inverse mod 11 (because all such numbers are relatively prime to 11, since 11 is prime), and if b is the inverse of a mod 11 then a is also the inverse of b. The only question is if a number can be its own inverse: you can check that for mod 11, the only numbers that are their own inverses are 1 and 10 (which is $\equiv -1 \bmod 11$). This is often the case modulo prime numbers: can you figure out exactly when?

b. Let's group together the factors nicely:

   $$10! \equiv 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 1 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) \equiv -1 \bmod 11$$

4.4: 20: Because the moduli are relatively prime, the Chinese Remainder Theorem guarantees a unique solution modulo $3 \cdot 4 \cdot 5 = 60$. Let $m_1 = 3$, $m_2 = 4$, and $m_3 = 5$ be the respective moduli and $a_1 = 2$, $a_2 = 1$, and $a_3 = 3$ be as in the proof of the Chinese Remainder Theorem (page 278; refer to it for the notation of this construction). Then $M_1 = 20$, $M_2 = 15$, and $M_3 = 12$ (the products of all the other moduli). An inverse of 20 modulo 3 is $y_1 = 2$, an inverse of 15 modulo 4 is $y_2 = 3$, and an inverse of 12 modulo 5 is $y_3 = 3$.

Then $a_1M_1y_1+a_2M_2y_2+a_3M_3y_3 \bmod (m_1m_2m_3) = 2\cdot 20\cdot 2+1\cdot 15\cdot 3+3\cdot 12\cdot 3 \bmod (3\cdot 4\cdot 5) = 80+45+108 \bmod 60 = 53$. Therefore any integer $x \equiv 53 \bmod 60$ (i.e., $x = 53+60k$ for any integer k) is a solution of this system of congruences.

4.4: 22: We write $x = 3+6a$ for some integer a. Then $3+6a \equiv 4 \bmod 7$, so $6a \equiv 1 \bmod 7$. Thus $a \equiv 6 \bmod 7$ (which we could do by trial and error, or by multiplying by the inverse of $6 \mod 7$, which happens to also be 6). Thus $a = 6+7b$ for some integer b. Plugging back in, this means $x = 3+6(6+7b) = 9+42b$. Thus $x \equiv 39 \bmod 42$ (and any such x is a valid solution to the system of congruences).

4.4: 32: We want an integer x such that $x \equiv 0 \bmod 5$ and $x \equiv 1 \bmod 3$. Let's solve this by back-substitution: We know $x = 5a$ for some integer a. Then $5a \equiv 1 \bmod 3$, which simplifies to $2a \equiv 1 \bmod 3$. Thus $a \equiv 2 \bmod 3$, so $a = 2+3b$ for some integer b. Back-substituting, we see $x = 5(2+3b) = 10+15b$. Thus any integer $x \equiv 10 \bmod 15$ has these properties, and these are all such integers.

4.4: 34: By Fermat's little theorem, since 41 is prime we know that for any integer a not divisible by 41 we have $a^{41-1} \equiv 1 \bmod 41$, so $23^{40} \equiv 1 \bmod 41$. We can write $1000 = 40\cdot 25$, so

$$23^{1002} \equiv \left(23^{40}\right)^{25} \cdot 23^2 \bmod 41 = 1^{25} \cdot 23^2 \bmod 41 = 37$$

Intuitively, we're group together 40 copies of 23 at a time, each such grouping just giving a multiplication by 1 according to Fermat's little theorem.

4.4: 38(a): By Fermat's little theorem, since 3 is relatively prime to each of 5, 7, and 11 (they are all prime), we know $3^4 \equiv 1 \bmod 5$, $3^6 \equiv 1 \bmod 7$, and $3^{10} \equiv 1 \bmod 11$. Therefore

$$3^{302} \equiv (3^4)^{75} \cdot 3^2 \equiv 1^{75} \cdot 3^2 \equiv 4 \bmod 5$$

$$3^{302} \equiv (3^6)^{50} \cdot 3^2 \equiv 1^{50} \cdot 3^2 \equiv 2 \bmod 7$$

$$3^{302} \equiv (3^{10})^{30} \cdot 3^2 \equiv 1^{30} \cdot 3^2 \equiv 9 \bmod 11$$

4.4: 40: Let n be a positive integer. We'll show individually that $n^7 - n$ is divisible by 7, by 3, and by 2, which implies that it is divisible by 42. By Fermat's little theorem, $n^7 \equiv n \bmod 7$ (note that even if n is divisible by 7 this still holds). Therefore $n^7 - n$ is divisible by 7. Also, $n^3 \equiv n \bmod 3$, so $n^3 \equiv n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \equiv n^3 \equiv n \bmod 3$, and thus $n^3 - n$ is divisible by 3. Finally, n^7 has the same parity as n, so $n^7 - n$ is even, meaning that 2 divides $n^7 - n$ (we could also have done this using the fact that $n^2 \equiv n \bmod 2$ just as we did for 3). Because $n^7 - n$ is divisible by 2, 3, and 7, which are all relatively prime, $n^7 - n$ is divisible by $2 \cdot 3 \cdot 7 = 42$.

4.4: 54: Let's compute the powers of 2 modulo 19. To do this, we start with 1 (i.e., 2^0) and keep multiplying by 2 until we get back where we started:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2^n mod 19	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2

This hits all the integers between 1 and 18, so 2 is a primitive root of 19. Note that $2^{18} \equiv 1 \bmod 19$ and $2^{19} \equiv 2 \bmod 19$, as expected by Fermat's little theorem.

4.4: 55: Because $2^{16} \equiv 5 \bmod 19$, the discrete logarithm of 5 is 16, and because $2^{14} \equiv 6 \bmod 19$, the discrete logarithm of 6 is 14. Note that the discrete logarithm is very much not an increasing function, unlike the regular log function.