CSC165H1: Problem Set 2 Sample Solutions

Due October 23 2019 before 4 pm

Note: solutions are incomplete, and meant to be used as guidelines only. We encourage you to ask follow-up questions on the course forum or during office hours.

1. **[9 marks] mod 3** Prove each of the following statements. You may use the Quotient Remainder Theorem from the course notes.

(a) **[3 marks]** Every integer n satisfies either $9 \mid n^2$ or $3 \mid n^2 - 1$.

Solution

statement:

$$\forall n \in \mathbb{Z}, 9 \mid n^2 \vee 3 \mid n^2 - 1$$

header: Let $n \in \mathbb{Z}$. I want to show that either $9 \mid n^2$ or $3 \mid n^2 - 1$.

body: By the Quotient Remainder Theorem there are integers q and r such that $n = 3q + r$ and $r \in \{0, 1, 2\}$. Consider the three possible cases:

case $r = 0$: Here $n^2 = 9q^2$, so $9 \mid n^2$.

case $r = 1$: Here $n^2 - 1 = 9q^2 + 6q$, which can be factored as $3(3q^2 + 2q)$, so $3 \mid n^2 - 1$.

case $r = 2$: Here $n^2 - 1 = 9q^2 + 12q + 4 - 1$, which can be factored as $3(3q^2 + 4q + 1)$, so $3 \mid n^2 - 1$.

In each of the three possible cases either $9 \mid n^2$ or $3 \mid n^2 - 1$. ■

(b) **[3 marks]** No integer n satisfies $n^2 \equiv 2 \pmod 3$.

Solution

statement: This is the flip side of the previous question.

$$\forall n \in \mathbb{Z}, n^2 \not\equiv 2 \pmod 3$$

header: Let $n \in \mathbb{Z}$. I want to show that $n^2 \not\equiv 2 \pmod 3$.

body: By the Quotient Remainder Theorem there are integers q and r such that $n = 3q + r$ and $r \in \{0, 1, 2\}$. Consider the three possible cases:

case $r = 0$: Here $n^2 = 9q^2 = 3(3q^2) + 0$, so $3 \mid n^2 - 0$. By the contrapositive of the theorem (course notes, proved in lecture) saying linear combinations of multiples are also multiples:

$$3 \nmid 2 \Rightarrow 3 \nmid \left[(n^2 - 0) - (n^2 - 2)\right] \Rightarrow 3 \nmid n^2 - 0 \vee 3 \nmid n^2 - 2$$

The hypothesis is true, and since $3 \mid n^2 - 0$ we must have $3 \nmid n^2 - 2$, that is $n^2 \not\equiv 2 \pmod 3$.

case $r = 1$: Here $n^2 - 1 = 9q^2 + 6q = 3(3q^2 + 2q)$, so $3 \mid n^2 - 1$. By the contrapositive of the theorem mentioned in the last part:

$$3 \nmid 1 \Rightarrow \Big[(n^2-1)-(n^2-2)\Big] \Rightarrow 3 \nmid n^2-2 \vee 3 \nmid n^2-1$$

The hypothesis is true, and since $3 \mid n^2-1$, we must have $3 \nmid n^2-2$, that is $n^2 \not\equiv 2 \pmod 3$.

case $r=2$: Here $n^2-1 = 9q^2+12q+4-1 = 3(3q^2+4q+1)$, so $3 \mid n^2-1$. By the contrapositive of the theorem referred to (twice!) above,

$$3 \nmid 1 \Rightarrow \Big[(n^2-1)-(n^2-2)\Big] \Rightarrow 3 \nmid n^2-2 \vee 3 \nmid n^2-1$$

The hypothesis is true, and since $3 \mid n^2-1$, we must have $3 \nmid n^2-2$, that is $n^2 \not\equiv 2 \pmod 3$.

In all three possible cases $n^2 \not\equiv 2 \pmod 3$. ■

(c) **[3 marks]** Every integer n satisfies either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Solution

statement:

$$\forall n \in \mathbb{Z}, n^2 \equiv 0 \pmod 4 \vee n^2 \equiv 1 \pmod 4$$

header: Let $n \in \mathbb{Z}$. I want to show that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

body: By the Quotient Remainder theorem there are integers q and r such that $n = 4q+r$ and $r \in \{0,1,2,3\}$. There are four possible cases to consider:

case $r=0$: Here $n^2-0 = 16q^2 = 4(4q^2)$, so $4 \mid n^2-0$, that is $n^2 \equiv 0 \pmod 4$.

case $r=1$: Here $n^2-1 = 16q^2+8q = 4(4q^2+2q)$, so $4 \mid n^2-1$, that is $n^2 \equiv 1 \pmod 4$.

case $r=2$: Here $n^2-0 = 16q^2+16q+4 = 4(4q^2+4q+1)$, so $4 \mid n^2-0$, that is $n^2 \equiv 0 \pmod 4$.

case $r=3$: Here $n^2-1 = 16q^2+24q+8 = 4(4q^2+6q+2)$, so $4 \mid n^2-1$, that is $n^2 \equiv 1 \pmod 4$.

In all four possible cases $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1$ (mod). ■

2. **[6 marks] more congruence.**

(a) **[3 marks]** Prove that if p_1 and p_2 are distinct primes, and a and b are any integers, then

$$a \equiv b \pmod{p_1p_2} \Leftrightarrow a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2}$$

Solution

statement:

$$\begin{aligned}&\forall a,b,\in \mathbb{Z}, \forall p_1,p_2 \in \mathbb{N},\\ &\qquad Prime(p_1) \wedge Prime(p_2) \wedge p_1 \neq p_2\\ &\qquad \Rightarrow (a \equiv b \pmod{p_1p_2} \Leftrightarrow a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2})\end{aligned}$$

header: Let $a, b \in \mathbb{Z}$ and $p_1, p_2 \in \mathbb{N}$. Assume $Prime(p_1), Prime(p_2)$ and $p_1 \neq p_2$.* I want to show that:

$$a \equiv b \pmod{p_1 p_2} \Leftrightarrow a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2}$$

body: I begin with the $\Rightarrow$ direction of the biconditional:

$$a \equiv b \pmod{p_1 p_2} \Rightarrow a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2}$$

header: Assume $a \equiv b \pmod{p_1 p_2}$, so $\exists k \in \mathbb{Z}, kp_1p_2 = a - b$. Let $k_1 = kp_1$ and let $k_2 = kp_2$. I want to show that $k_1p_2 = a - b = k_2p_1$, so $a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2}$.

body:

$$k_1p_2 = kp_1p_2 = a - b = kp_2p_1 = k_2p_1 \qquad \blacksquare$$

Now for the $\Leftarrow$ direction of the biconditional:

$$a \equiv b \pmod{p}_1 \wedge a \equiv b \pmod{p}_2 \Rightarrow a \equiv b \pmod{p_1 p_2}$$

header: Assume $a \equiv b \pmod{p}_1 \wedge a \equiv b \pmod{p}_2$, so $\exists k_1, k_2 \in \mathbb{Z}, p_1k_1 = a - b = p_2k_2$. I want that $\exists k_3 \in \mathbb{Z}, k_3p_1p_2 = a - b$.

body: By Theorem 2.3 (page 53 course notes), where p_2 and k_2 play the roles of a and b:

$$p_1 \nmid p_2 \wedge p_1 \nmid k_2 \Rightarrow p_1 \nmid p_2k_2$$

The contrapositive of this is:

$$p_1 \mid p_2k_2 \Rightarrow p_1 \mid p_2 \vee p_1 \mid k_2$$

I know $p_1k_1 = p_2k_2$, the hypothesis is true, and since $p_1 \nmid p_2$ (they are distinct primes), that just leaves $p_1 \mid k_2$, so $\exists k_3 \in \mathbb{Z}, p_1k_3 = k_2$, and $k_3p_1p_2 = k_2p_2 = a - b$. Thus $a \equiv b \pmod{p_1p_2}$. $\blacksquare$

* Assume the hypothesis, since otherwise the implication is vacuously true.

(b) **[3 marks]** Prove that if p_1 and p_2 are distinct primes, and a and b are any integers, there exists exactly one integer x that satisfies:

$$x \equiv a \pmod{p_1} \wedge x \equiv b \pmod{p_2} \wedge 0 \leq x \wedge x < p_1p_2$$

Hint: If two different integers x_1 and x_2 satisfy the first two conditions, what can you prove about their remainder $\pmod{p_1p_2}$?

Solution

statement:

$$\begin{aligned}
&\forall a, b \in \mathbb{Z}, \forall p_1, p_2 \in \mathbb{N}, Prime(p_1) \wedge Prime(p_2) \wedge p_1 \neq p_2 \\
&\Rightarrow \exists x \in \mathbb{Z}, x \equiv a \pmod{p_1} \wedge x \equiv b \pmod{p_2} \wedge 0 \leq x \wedge x < p_1p_2 \\
&\qquad \wedge \forall y \in \mathbb{Z}, (y \equiv a \pmod{p_1} \wedge y \equiv b \pmod{p_2} \wedge 0 \leq y \wedge y < p_1p_2 \Rightarrow y = x)
\end{aligned}$$

header: Let $a, b \in \mathbb{Z}, p_1, p_2 \in \mathbb{N}$. Assume $Prime(p_1) \wedge Prime(p_2) \wedge p_1 \neq p_2$. From problem set #1 I know there exists $x' \in \mathbb{Z}, x' \equiv a \pmod{p_1} \wedge x' \equiv b \pmod{p}_2$. By the Quotient

Remainder theorem I know there exists unique integers q, x such that:

$$x = x' - qp_1p_2 \wedge 0 \leq x < p_1p_2,$$

i.e. x is the unique remainder of x' modulo p_1p_2. I want to show that:

$$x \equiv a \pmod{p_1} \wedge x \equiv b \pmod{p_2} \wedge \forall y \in \mathbb{Z}, \\ (y \equiv a \pmod{p_1} \wedge y \equiv b \pmod{p_2} \wedge 0 \leq y \wedge y < p_1p_2 \Rightarrow y = x)$$

[*]

body: Since $x' \equiv a \pmod{p_1}$ we know there exists $k_1 \in \mathbb{Z}, p_1k_1 = x' - a$. so substituting $qp_1p_2 + x$ for x' (from the Quotient Remainder theorem), I have:

$$p_1k_1 = qp_1p_2 + x - a \Rightarrow p_1(k_1 - qp_2) = x - a,$$

so $x \equiv a \pmod{p_1}$. ■

Similarly I know $\exists k_2 \in \mathbb{Z}, k_2p_2 = x' - b$, so substituting $qp_1p_2 + x$ for x' I have:

$$p_2k_2 = qp_1p_2 + x - b \Rightarrow p_2(k_2 - qp_1) = x - b,$$

so $x \equiv b \pmod{p_2}$. ■

It remains to prove:

$$\forall y \in \mathbb{Z}, (y \equiv a \pmod{p_1} \wedge y \equiv b \pmod{p_2} \wedge 0 \leq y \wedge y < p_1p_2 \Rightarrow y = x)$$

header: Let $y \in \mathbb{Z}, y \equiv a \pmod{p_1} \wedge y \equiv b \pmod{p_2} \wedge 0 \leq y \wedge y < p_1p_2$. I want to show $y = x$.

body: Since $y \equiv a \pmod{p_1}$ and $a \equiv x \pmod{p_1}$, by the lemma used in my solution for 3(c) in problem set #1, $y \equiv x \pmod{p_1}$. Similarly, $y \equiv x \pmod{p_2}$. Using the result from the previous part of this question, this implies $y \equiv x \pmod{p_1p_2}$. This means that $p_1p_2 \mid y - x$, so $\exists k_3 \in \mathbb{Z}, k_3p_1p_2 = y - x$. I will show that $k_3 = 0$

$$\begin{aligned} k_3p_1p_2 &= y - x \\ k_3p_1p_2 + x &= y \\ k_3 &< 1 \qquad \# \; y < p_1p_2 \wedge x \geq 0 \text{ by assumption} \\ k_3 &> -1 \qquad \# \; y \geq 0 \wedge x < p_1p_2 \text{ assumption} \\ k_3 &= 0 \\ x = y & \quad ■ \end{aligned}$$

[*] By choice of x I already know $0 \leq x < p_1p_2$

3. **[9 marks] alternations...**

For each of the following statements, decide whether you believe it is true or false. If you believe it is true, prove the statement. If you believe it is false, negate the statement and prove the negation.

You need to approach each part seriously. There are no marks for "proving" a false statement true, or "proving" a true statement false.

(a) **[3 marks]**

$$\forall e \in \mathbb{R}^+, \exists d \in \mathbb{R}^+, \forall x \in \mathbb{R}, |x| < d \Rightarrow |7x| < e$$

Solution

statement: The statement is true, so I need to prove:

$$\forall e \in \mathbb{R}^+, \exists d \in \mathbb{R}^+, \forall x \in \mathbb{R}, |x| < d \Rightarrow |7x| < e$$

header: Let $e \in \mathbb{R}^+$. Let $d = e/7$. Let $x \in \mathbb{R}$. Assume $|x| < d$, where $|x|$ is:

$$|x| = \begin{cases} -x & \text{if } x < 0 \\ x & \text{if } x \geq 0 \end{cases}$$

I want to show $|7x| < e$.

body: Consider two cases:

$$\begin{aligned} x < 0 \wedge |x| < d \Rightarrow -x &< d \\ -7x &< 7d \\ |7x| &< 7d = e \qquad \# d = e/7 \wedge 7x < 0 \Rightarrow |7x| = -7x \\ x \geq 0 \wedge |x| < d \Rightarrow x &< d \\ 7x &< 7d \\ |7x| &< 7d = e \qquad \# d = e/7 \wedge 7x \geq 0 \Rightarrow |7x| = 7x \end{aligned}$$

In either of the two possible cases $|7x| < e$. ■

(b) **[3 marks]**

$$\exists d \in \mathbb{R}^+, \forall e \in \mathbb{R}^+, \forall x \in \mathbb{R}, |x| < d \Rightarrow |7x| < e$$

Solution

statement: The claim is false, so I need to prove its negation:

$$\forall d \in \mathbb{R}^+, \exists e \in \mathbb{R}^+, \exists x \in \mathbb{R}, |x| < d \wedge |7x| \geq e$$

header: Let $d \in \mathbb{R}^+$. Let $e = x = d/7$. I want to show that $|x| < d$ and $|7x| \geq e$.

body:

$$\begin{aligned} 1/7 &< 1 \\ d/7 &< d \\ x = |x| &< d \qquad \# \, x = d/7 \geq 0 \Rightarrow x = |x| \\ 7x = d &> d/7 = e \qquad \# \, x = e = d/7 \\ |7x| &\geq e \quad ■ \end{aligned}$$

(c) **[3 marks]**

$$\forall d \in \mathbb{R}^+, \exists e \in \mathbb{R}^+, \forall x \in \mathbb{R}, |x| < d \Rightarrow |7x| < e$$

Solution

statement: The statement is true. I will prove:

$$\forall d \in \mathbb{R}^+, \exists e \in \mathbb{R}^+, \forall x \in \mathbb{R}, |x| < d \Rightarrow |7x| < e$$

header: Let $d \in \mathbb{R}^+$. Let $e = 7d$. Let $x \in \mathbb{R}$. Assume $|x| < d$, so either $x < 0$ and so $|x| = -x < d$, or $x \geq 0$, so $|x| = x < d$. I want to show that $|7x| < e$.

body: I have two possibilities to check:

$$\begin{array}{rcll}
\text{case } x < 0 \Rightarrow |x| = -x & < & d & \\
-7x & < & 7d & \\
|7x| & < & 7d = e & \# \, 7x < 0 \Rightarrow |7x| = -7x < 7d \\
\text{case } x \geq 0 \Rightarrow |x| = x & < & d & \\
7x & < & 7d & \\
|7x| & < & 7d = e & 7x \geq 0 \Rightarrow |7x| = 7x < 7d
\end{array}$$

In both of the possible cases $|7x| < e$. ■

4. **[6 marks] a prime example...**

Euclid proved that there are infinitely many prime numbers, and this is the approach used in the course notes Theorem 2.3. In the questions below you may use Exercise 2.19 on modular arithmetic, and the divisibility of linear combinations.

(a) **[3 marks]** Prove there are infinitely many primes congruent to 5 (mod 6). **Hint:** Think about the **technique** of Theorem 2.3 in the course notes, and also that there are other arithmetic manipulations other than adding one, such as multiplying by 5.

Solution

statement: Define the set of all primes congruent to 5 (mod 6) as P. I will prove:

$$|P| = \infty$$

... by assuming, for the sake of contradiction, its negation:

$$\exists n \in \mathbb{N}, |P| = n$$

header: Let $n \in \mathbb{N}$ such that $|P| = n$,that is $P = \{p_1, p_2, \ldots, p_n\}$, where each p_i is prime and congruent to $5 \pmod 6$. I want to show that this leads to a contradiction.

body: Consider the number

$$m = 6(p_1 \times p_2 \times \cdots \times p_n) - 1 = 6(p_1 \times p_2 \times \cdots \times p_n - 1) + 5$$

Let $j = (p_1 \times p_2 \times \cdots \times p_n - 1)$, and $m = 6j + 5$. Also notice that each $p_i \in P$ does divide $6(p_1 \times p_2 \times \cdots \times p_n)$ but does not divide m, since

$$p_i \mid 6(p_1 \times p_2 \times \cdots \times p_n) \wedge p_i \mid 6(p_1 \times p_2 \times \cdots \times p_n) - 1 \Rightarrow p_i \mid 1 \ldots$$

... since linear combinations of multiples are also multiples. Also $m > 1$, since one of the p_i is 5, so m can be no smaller than $6 \times 5 - 1 = 29$. This means that m has one or more prime factors, and none of them are elements of P. I want to show that at least one of the prime factors is congruent to $5 \pmod 6$.

Let $p \in \mathbb{N}$ be some prime factor of m. By the Quotient Remainder Theorem p there are integers q, r such that $p = 6q + r$, and there are six possibilities to consider, depending on the value of r (which must be in the interval $[0, 6)$.

case $p = 6q + 0$: There are no primes divisible by 6.

case $p = 6q + 2 = 2(3q + 1)$: This prime is even, so it cannot be a factor of $6j + 5 = 2(3j + 2) + 1$, an odd number.

case $p = 6k + 3 = 3(2q + 3)$: This is a multiple of 3, whereas $m = 6j + 5 = 3(2j + 1) + 2$ has remainder 2 when divided by 3.

case $p = 6q + 4 = 2(3q + 2)$: This prime is even, so it cannot be a factor of $6j + 5$, an odd number.

case $p = 6k + 1$: This is one of two possible cases to consider.

case $p = 6k + 5$: This is the second of two possible cases to consider.

If all prime factors of m were congruent to $1 \pmod 6$, their product m would also be congruent to 1.* That means that m has at least one prime factor congruent to $5 \pmod 6$. $\rightarrow\leftarrow$ Contradiction! Set P was assumed to contain all prime numbers congruent to $6 \pmod 5$, and no factors of m are also elements of P.

Since assuming P to be finite leads to a contradiction, that assumption is false and P has infinitely many elements. ■

*Proof by induction, using Exercise 2.19(3)

(b) **[3 marks]** Prove or disprove that for any natural number n there is a natural number m that is not prime, is larger than n, and with $m \equiv 5 \pmod 6$.

Solution

statement: The claim is true, so I will prove:

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, \neg Prime(m) \wedge m > n \wedge m \equiv 5 \pmod 6$$

header: Let $n \in \mathbb{N}$. Let $m = 30(n + 1) + 5$. I want to show that:

$$\neg Prime(m) \wedge m > n \wedge m \equiv 5 \pmod 6$$

body:

$$
\begin{array}{rcl}
m = 30(n+1) + 5 = 5(6(n+1)+1) & \Rightarrow & 5 \mid m \\
1 < 5 \wedge 5 < m & \# & n \geq 0 \Rightarrow m \geq 35 \\
\neg Prime(m) & \# & \text{definition of } Prime(m) \\
29n & \geq & 0 \qquad \# \, n \geq 0 \\
29n + 35 > 29n & \geq & 0 \\
29n + n + 35 = 30n + 35 = m & > & n \\
m - 5 = 6(5(n+1)) & \Rightarrow & 6 \mid m - 5 \\
m & \equiv & 5 \pmod 6 \qquad \blacksquare
\end{array}
$$

5. **[3 marks] subsets** If a set S has n elements, how many subsets of size 4 does it have? Investigate this for sets of size 0, 1, 2, 3, 4, and 5, then make a conjecture. Prove your conjecture using simple induction. You may **not** use any external facts or techniques from combinatorics, but you **may** assume (without proof) the fact that a set with n elements has $n(n-1)(n-2)/6$ subsets of size 3.

Solution

Sets of size 0, 1, 2, 3 have 0 subsets of size 4. Sets of size 4 have 1 subset (themself) of size 4. Sets of size 5 have 5 subsets of size 4 (one for each possibility of omitting an element). My conjecture is that the number of subsets of size 4 for a set of size n is $n(n-1)(n-2)(n-3)/24$.

statement: Denote the set of all sets as $\mathcal{S}$. Define the predicate $C(S, n)$: "S has n subsets of size 4," for $S \in \mathcal{S}$ and $n \in \mathbb{N}$. Then our statement becomes:

$$\forall n \in \mathbb{N}, \forall S \in \mathcal{S}, |S| = n \Rightarrow C(S, n(n-1)(n-2)(n-3)/24)$$

header: Define $P(n) : \forall S \in \mathcal{S}, |S| = n \Rightarrow C(S, n(n-1)(n-2)(n-3)/24)$. I will prove by simple induction that $\forall n \in \mathbb{N}, P(n)$.

base case $P(0)$: The only set with 0 elements is the empty set, which has 0 subsets of size $0 = 0(0-1)(0-2)(0-3)/24$, so $P(0)$ is verified.

inductive step: Let $n \in \mathbb{N}$. Assume $P(n)$. Let $S \in \mathcal{S}$, and assume $|S| = n+1$. I want to show that S has $(n+1)(n)(n-1)(n-2)$ subsets of size 4.

Since S has $n+1 > 0$ elements, we can distinguish one element and call it x. The size-4 subsets of S that do **not** include x as an element are also size-4 subsets of $S - \{x\}$, a set of size n. By the inductive hypothesis $P(n)$, $S - \{x\}$ has $n(n-1)(n-2)(n-3)/24$ size-4 subsets. Each of the size-4 subsets of S that **do** include x as an element are formed by a size-3 subset of $S - \{x\}$ unioned with set $\{x\}$. We know there are $n(n-1)(n-2)/6$ such subsets. Counting all of these yields:

$$\begin{aligned}\frac{n(n-1)(n-2)(n-3)}{24}+\frac{n(n-1)(n-2)}{6} &= \frac{n(n-1)(n-2)(n-3)}{24}+\frac{4n(n-1)(n-2)}{24}\\ &= \frac{(4n+n(n-3))(n-1)(n-2)}{24}\\ &= \frac{(4+n-3)n(n-1)(n-2)}{24}\\ &= \frac{(n+1)n(n-1)(n-2)}{24} \qquad \blacksquare\end{aligned}$$

6. **[3 marks] number representation** Read Theorem 4.1 carefully. It claims there is at least one binary representation for any natural number. The base case explicitly gives one representation for the natural number 0. Trace through the proof to see what binary representation it guarantees for the natural number 5. What is the representation? Explain.

Solution

Theorem 4.1 guarantees that the sum

$$0\times 2^3+1\times 2^2+0\times 2^1+1\times 2^0$$

I will explain this step-by-step using the following the following short-hand: **BR(n)** is the binary representation guaranteed by Theorem 4.1 for natural number n.

step 1: In the proof, since 5 is odd and greater than 0, we go to the inductive step and follow the odd case, which tells us that BR(5) is built using BR(2) by:

$$\mathsf{BR(5)}=2\times\mathsf{BR(2)}+1\times 2^0$$

This step also specifies that BR(5) has one more term than BR(2).

step 2: To find BR(2) I go again to the inductive step and follow the even case, which says that BR(2) is built using BR(1) by:

$$\mathsf{BR(2)}=2\times\mathsf{BR(1)}+0\times 2^0$$

This step also specifies that BR(2) has one more term than BR(1). Substituting this into BR(5) yields:

$$\mathsf{BR(5)}=2\times\mathsf{BR(2)}+1\times 2^0=4\times\mathsf{BR(1)}+0\times 2^1+1\times 2^0$$

step 3: To find BR(1) I go to the inductive step and follow the odd case, which says BR(1) is built using BR(0) by:

$$\mathsf{BR(1)}=2\times\mathsf{BR(0)}+1\times 2^0$$

This step also specifies that BR(1) has one more term than BR(0). Substituting this into our emerging representation of BR(5) yields:

$$\mathsf{BR(5)}=4\times\mathsf{BR(1)}+0\times 2^1+1\times 2^0=8\times\mathsf{BR(0)}+1\times 2^2+0\times 2^1+1\times 2^0$$

step 4: To find BR(0) I go to the base case and note that $\mathsf{BR}(0) = 0 \times 2^0$. Substituting this into our emerging representation BR(5) yields:

$$\mathsf{BR}(5) = 8 \times \mathsf{BR}(0) + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

Notice this representation has 4 bits, with the left-most a 0! This is what a precise reading of the proof of Theorem 4.1 yields: one of the infinitely many binary representations of 5. Responding to this, Theorem 4.2 assures us that there is a unique representation of any positive natural number with 1 being the left-most digit.