1. Prove that $7^m - 1$ is divisible by 6 for all positive integers $m$ (try this both inductively and using equivalence classes).

**Solution**  
There are two ways to do this. One way: notice that $7 \equiv 1 \pmod{6}$, thus $7^m \equiv 1 \pmod{6}$ for any $m$ (applying the known result that “if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$” $m - 1$ times), and thus $7^m - 1 \equiv 0 \pmod{6}$. This implies $7^m - 1$ is divisible by 6.

Alternatively you can do a direct proof by induction:
**Base case:** $m = 1$, $7^1 - 1 = 6$ which is obviously divisible by 6.

**Inductive step:** Assume $7^m - 1$ is divisible by 6 for some $m \geq 1$ (inductive hypothesis). Then $7^{m+1} - 1 = 7^m - 7 + 6 = 7(7^m - 1) + 6$. But $7^m - 1$ is divisible by 6 (by the inductive hypothesis) and so is 6, so $7^{m+1} - 1$ is also divisible by 6. Hence proved by induction.

2. [6 points] Pascal’s triangle is a sequence of rows, where each entry is formed by adding the two adjacent entries from the previous row:

1  
1 1  
1 2 1  
1 3 3 1  
1 4 6 4 1  

If we let $P_{n,k}$ stand for the $k$th entry in the $n$th row of Pascal’s triangle, then $P_{n,k}$ is given by the formulas

$$P_{1,1} := 1, \quad P_{n,0} := 0 \quad \text{for all } n, \quad \text{and } P_{n+1,k} := P_{n,k-1} + P_{n,k} \quad \text{if } n \geq 1.$$

*Prove by induction on $n$ that for all $n \geq 1$, for all $k$ with $1 \leq k \leq n$, $P_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.*

**Note:** The definition of $n!$ is $0! := 1$ and $n! := n \cdot (n-1)!$ for all $n \geq 1$.

**Solution**  
Proof by induction. Let $P(n)$ be the statement $\forall k \in [1..n], \ P_{n,k} = \binom{n}{k}$.

$P(1)$ is true, because the only $k \in [1..1]$ is $k = 1$, and $P_{1,1} = 1$ and $\binom{1}{1} = 1!/0! = 1$.

Now, assume $P(n)$; we wish to show $P(n + 1)$. Choose an arbitrary $k$. We have

$$P_{n+1,k} = P_{n,k-1} + P_{n,k} \quad \text{by definition}$$

$$= \binom{n}{k-1} + \binom{n}{k} \quad \text{by definition}$$

$$= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \quad \text{by definition}$$

$$= \frac{n!k + (n-k+1)}{k!(n-k+1)!} \quad \text{putting things over a common denominator}$$

$$= \frac{n!(n+1)}{k!(n+1-k)!} \quad \text{algebra}$$

$$= \binom{n+1}{k} \quad \text{by definition}$$

as required.
3. Prove the following claim using induction: for any \( n \geq 0 \), \( \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \)

**Solution**  
**Base case:** when \( n = 0 \), the left hand side is \( 2^0 = 1 \) and the right hand side is \( 2^2 - 1 = 1 \), and they are clearly the same.

**Inductive step:** Choose an arbitrary \( n \) and assume that \( \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \) (this is the inductive hypothesis).

We wish to show that \( \sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1 \). We compute:

\[
\begin{align*}
\sum_{i=0}^{n+1} 2^i &= \sum_{i=0}^{n} 2^i + 2^{n+1} \\
&= (2^{n+1} - 1) + 2^{n+1} \\
&= 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1
\end{align*}
\]

as required.

4. The Fibonacci numbers \( F_0, F_1, F_2, \ldots \) are defined inductively as follows:

\[
F_0 = 1 \\
F_1 = 1 \\
F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2
\]

That is, each Fibonacci number is the sum of the previous two numbers in the sequence. Prove by induction that for all natural numbers \( n \) (including 0):

\[
\sum_{i=0}^{n} F_i = F_{n+2} - 1
\]

**Solution**  
Let \( P(n) \) be the statement “\( \sum_{i=0}^{n} F_i = F_{n+2} - 1 \). We must show \( P(0) \) and \( P(n+1) \) assuming \( P(n) \).

To see \( P(0) \), note that \( \sum_{i=0}^{0} F_i = F_0 = 1 \), while \( F_{0+2} - 1 = F_0 + F_1 - 1 = 1 + 1 - 1 = 1 \). Since they are the same, \( P(0) \) holds.

To see \( P(n+1) \), first assume \( P(n) \). We have

\[
\begin{align*}
\sum_{i=0}^{n+1} F_i &= \sum_{i=0}^{n} F_i + F_{n+1} \\
&= F_{n+2} - 1 + F_{n+1} \\
&= F_{n+1+2} - 1
\end{align*}
\]

as required.

5. Prove by induction that for any integer \( n \geq 3 \), \( n^2 - 7n + 12 \) is non-negative.

**Solution**  
Let \( P(n) \) be the statement “\( n^2 - 7n + 12 \) is non-negative.” We must show \( P(3) \), and for any \( n \geq 3 \), \( P(n+1) \) assuming \( P(n) \).

To see \( P(3) \), note that \( 3^2 - 7 \cdot 3 + 12 = 0 \geq 0 \).
Now, assume $n \geq 3$ and $P(n)$; we want to show $P(n+1)$. Well,

$$
(n+1)^2 - 7(n+1) + 12 = n^2 + 2n + 1 - 7n - 7 + 12
$$

$$
= (n^2 - 7n + 12) + (2n + 1 - 7)
$$

$$
\geq 2n + 1 - 7 \quad \text{by } P(n)
$$

$$
\geq 0 \quad \text{since } n \geq 3
$$

6. Chapter 5 of MCS has a bunch of good induction exercises (and you can find even more by searching)

7. Suppose that Alice sends the message $a$ to Bob, encrypted using RSA. Suppose that Bob’s implementation of RSA is buggy, and computes $k^{-1} \mod 4\phi(m)$ instead of $k^{-1} \mod \phi(m)$. What decrypted message does Bob see? Justify your answer.

**Solution** Alice transmits $a^k \mod m$ to Bob, who then computes $(a^k)^{k^{-1}} \mod m$. Because Bob miscomputed $k^{-1}$, we know that $kk^{-1} \equiv 1 \mod 4\phi(m)$. In other words, $kk^{-1} = 1 + t \cdot 4\phi(m)$ for some $t$. Therefore Bob receives

$$
(a^k)^{k^{-1}} \equiv a^{1 + 4t\phi(m)}
$$

$$
\equiv a \cdot a^{4t\phi(m)}
$$

$$
\equiv a \cdot (a^{\phi(m)})^{4t}
$$

$$
\equiv a \cdot 1^{4t}
$$

$$
\equiv a \mod m
$$

8. (a) What are the units of $\mathbb{Z} \mod 12$?

**Solution** A unit in a set of numbers is a number that has an inverse. In the set $\mathbb{Z}_{12} = \{0, [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$, the units are $[1], [5], [7],$ and $[11]$. In general, $[n]$ is a unit mod $m$ if $n$ and $m$ are relatively prime.

(b) What are their inverses?


(c) What is $\phi(12)$?

**Solution** By definition of $\phi$, $\phi(12)$ is the number of units mod 12. Since there are 4 units, $\phi(12) = 4$.

9. Use Euler’s theorem and repeated squaring to efficiently compute $8^n \mod 15$ for $n = 5$, $n = 81$ and $n = 16023$. Hint: you can solve this problem with 4 multiplications of single digit numbers. Please fully evaluate all expressions for this question (e.g. write 15 instead of 3 \cdot 5).
Solution  We use the fact that $8^{\varphi(15)} = 1 \mod 15$. $\varphi(15) = (3-1)(5-1) = 8$ [multiplication #1], so we can reduce all of the exponents mod 8. We then use repeated squaring to compute $8^2$:

\[
\begin{align*}
[8]^2 &= [64] = [4] & \text{[multiplication #2]} \\
\end{align*}
\]

We can then use these to compute the powers of $[8]$:

\[
\begin{align*}
\end{align*}
\]

10. In this problem, we are working mod 7, i.e. $\equiv$ denotes congruence mod 7 and $[a]$ is the equivalence class of $a$ mod 7.

(a) What are the units of $\mathbb{Z}_7$? What are their inverses?

Solution

- [1]'s inverse is [1]
- [2]'s inverse is [4]
- [3]'s inverse is [5]
- [4]'s inverse is [2]
- [5]'s inverse is [3]
- [6]'s inverse is [6]

(b) Compute $2^{393}$.

Solution  $2^{393} = ([2]^3)^{131} = [1]^{131} = [1]$

11. (a) Recall Bézout’s identity from the homework: for any integers $n$ and $m$, there exist integers $s$ and $t$ such that $\gcd(n, m) = sn + tm$. Use this to show that if $\gcd(k, m) = 1$ then $[k]$ is a unit of $\mathbb{Z}_m$.

Solution  If $\gcd(k, m) = 1$ then $1 = sk + tm$. Reducing this equation mod $m$ gives $[1] = [s][k] + [t][0] = [s][k]$. Therefore, $[k]$ has an inverse (namely $[s]$); and is thus a unit.

(b) Use part (a) to show that if $p$ is prime, then $\phi(p) = p - 1$.

Solution  Since $p$ is prime, everything less than $p$ is relatively prime to $p$, except for 0. There are $p - 1$ such numbers, and thus $p - 1$ units.

(c) Use Euler’s theorem to compute $3^{38} \mod 37$ (note: 37 is prime).
12. Bob the Bomber wishes to receive encrypted messages from Alice the Accomplice. He generates a public key pair \( m = 21 \) and \( k = 5 \). Luckily, you have access to an NSA supercomputer that was able to factor 21 into \( 7 \cdot 3 \).

(a) Use this information to find the decryption key \( k^{-1} \).

Solution  \( \varphi(37) = 36, \) so \( [3]^{38} = [3]^2 = [9] \mod 37. \)

(b) Without changing \( m \), what other possible keys \( k \) could Bob have chosen? Find the decryption keys for those keys as well.

Solution  By inspection, the units of \( \mathbb{Z}_{12} \) are \([1], [5], [7], \) and \([11]\) (all other numbers share a factor with 12). Experimentally, they are all their own inverses. Note that \([1]\) is not a smart key choice, but we accepted it.

(c) Alice encrypts a secret message \( \text{msg} \) using Bob’s public key \( (k = 5) \), and sends the ciphertext \( c = 4 \). What was the original message?

Solution  We must compute \([4][5] = [45]\). We see \([4^2] = [16]\); squaring this gives \([4^4] = [(4^2)^2] = [256] = [4]_{21}. \) Thus \([45] = [4 \cdot 4^4] = [16]. \)

13. Which of the following does RSA depend on? Explain your answer briefly.

(a) Factoring is easy and testing primality is hard.

(b) Factoring is hard and testing primality is easy.

(c) Both factoring and testing primality are hard.

(d) Both factoring and testing primality are easy.

Solution  RSA depends on (b), that factoring is hard and testing primality is easy. The public key in RSA is the product of two large primes. We couldn’t generate public keys if testing primality wasn’t easy. On the other hand, we could easily decrypt encrypted messages if factoring was easy (because in that case, given a public key, which is the product of two large primes could easily compute the secret – the two factors, and that’s what we need to know to decrypt.

14. (a) Let \( m \) and \( n \) be integers greater than 1. Show that the function \( f : \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m \) given by \( f : ([a]_m, [b]_n) \rightarrow [a + b]_m \) is not necessarily well defined. [Hint: you just need an example here.]

Solution  Consider \( m = 2, n = 3 \). Then \([1]_m = [3]_m \) and \([1]_n = [4]_n \), but \([1 + 3]_m = [0]_m \) while \([3 + 4]_m = [1]_m \).

(b) Show that \( f \) is well defined if \( m|n \).

Solution  Suppose \( m|n \). Then \( n = mc \) for some \( c \). Suppose also that \([a]_m = [a']_m \) (so that \( a = a' + md \) for some \( d \)) and \([b]_n = [b']_n \) (so that \( b = b' + ne \)).

Then
\[
(a + b) = (a' + md) + (b' + ne) = a' + b' + md + mce = a' + b' + m(d + ce)
\]

Thus \([a + b]_m = [a' + b']_m \).
We define a set $S$ of functions from $\mathbb{Z}$ to $\mathbb{Z}$ inductively as follows:

**Rule 1.** For any $n \in \mathbb{Z}$, the translation (or offset) function $t_n : x \mapsto x + n$ is in $S$.

**Rule 2.** For any $k \neq 0 \in \mathbb{Z}$, the scaling function $r_k : x \mapsto kx$ is in $S$.

**Rule 3.** If $f$ and $g$ are elements of $S$, then the composition $f \circ g \in S$.

**Rule 4.** If $f \in S$ and $f$ has a right inverse $g$, then $g$ is also in $S$.

In other words, $S$ consists of functions that translate and scale integers, and compositions and right inverses thereof.

**Note:** This semester, we made a bigger distinction between the elements of an inductively defined set and the meaning of an inductively defined set. We probably would have phrased this question as follows: Let $S$ be given by

$$s \in S ::= t_n \mid r_k \mid s_1 \circ s_2 \mid \text{rinv } s$$

and inductively, let the function defined by $s$ (written $F_s : \mathbb{Z} \to \mathbb{Z}$) be given by the rules

$F_{t_n}(x) ::= x + n$, $F_{r_k}(x) ::= ks$, $F_{s_1 \circ s_2}(x) ::= F_{s_1} \circ F_{s_2}$ and let $F_{\text{rinv } s} ::= g$ where $g$ is a right inverse of $F_s$.

(a) [1 point] Show that the function $f : x \mapsto 3x + 17$ is in $S$.

**Solution** By rule 1, the function $t_{17} : x \mapsto x + 17$ is in $S$, and by rule 2, $r_3 : x \mapsto 3x$ is in $S$. By rule 3, therefore, $t_{17} \circ r_3 : x \mapsto 3x + 17$ is in $S$.

(b) Use structural induction to prove that for all $f \in S$, $f$ is injective. You may use without proof the fact that the composition of injective functions is injective.

**Solution** We must show that all functions formed with each of the rules are injective. Let $P(s)$ be the statement $s$ is injective.

$P(t_k)$ holds, because $t_k$ has a two sided inverse $t_{-k}$, and is therefore injective.

$P(r_k)$ holds, because we required that $k \neq 0$. Therefore, if $kx_1 = kx_2$, we can cancel $k$ to find $x_1 = x_2$.

$P(f \circ g)$ holds, assuming $P(f)$ and $P(g)$, because the composition of injections is an injection.

If $g$ is the right inverse of $f$, then $P(g)$ holds, because $g$ has a left-inverse (namely $f$) and is therefore injective.

(c) Give a surjection $\phi$ from $S$ to $\mathbb{Z}$ (proof of surjectivity not necessary). Remember that this surjection must map a function to an integer, and for every integer there must be a function that maps to it.

**Solution** Let $\phi(s) ::= s(0)$. This is a surjection, because $t_n(0) = 0 + n = n$, so for any $n$ there exists $s \in S$ (namely $t_n$) with $\phi(s) = n$.

16. Draw a finite automaton (DFA, NFA or $\epsilon$-NFA) with alphabet $\{a, b\}$ to recognize strings of the form $x_1x_2x_3 \cdots$ where each $x_i$ is either “ab” or “ba”.

6
17. Build a deterministic finite automaton that recognizes the set of strings of 0’s and 1’s, that only contain a single 0 (and any number of 1’s). Describe the set of strings that lead to each state.

Solution

18. (a) In lecture, we proved that if \([a]_m\) is a unit, then \([a]_m^{\varphi(m)} = [1]\).

Use this to show that \([a^b]_m := [a^b]_m\) is well defined.

Solution

Suppose \([b] = [b']\). Then \(b = b' + km\) for some \(k\). Therefore,

\[
[a^b]_m = [a^{b'+km}]_m = [a^{b'}(a^{\varphi(m)})^k] = [a^{b'}][a^{\varphi(m)}]^k = [a^{b'}][1]^k = [a^{b'}]
\]

by assumption

(b) Use Euler’s theorem to prove that if \(p\) is prime, then \([a]^p_p = [a]_p\) (whether \([a]_p\) is a unit or not).

Solution

Since \(p\) is prime, we have \(\varphi(p) = p - 1\). If \([a]_p\) is a unit, then Euler’s theorem says that \([a]_p^{p-1} = [1]\); multiplying both sides by \([a]\) gives \([a]^p_p = [a]\).

If \([a]_p\) is not a unit, then \(gcd(a,p) \neq 1\); this means that \(a\) and \(p\) share a common factor, which can only happen if \(a\) is a multiple of \(p\). In this case, \([a]_p = [0]\), and \([0]^p_p = [0]\).

19. Give a DFA that accepts strings in \(\{0,1\}^*\) if and only if they contain at most one 0 and an even number of 1’s. For each state, describe the strings that reach that state.
Solution

\[ \begin{array}{ccc}
q_0 & \rightarrow & q_1 \\
0 & \rightarrow & 0 \\
1 & \rightarrow & 1 \\
\text{start} & \rightarrow & q_0 \\
q_0 & \rightarrow & q_1 \\
0 & \rightarrow & 0 \\
1 & \rightarrow & 1 \\
q_1 & \rightarrow & q_2 \\
0 & \rightarrow & 0 \\
1 & \rightarrow & 1 \\
q_2 & \rightarrow & q_2 \\
0 & \rightarrow & 0 \\
\end{array} \]

If \( \hat{\delta}(q_0, x) = q_{0e} \) then \( x \) has no 0’s and an even number of 1’s.
If \( \hat{\delta}(q_0, x) = q_{0o} \) then \( x \) has no 0’s and an odd number of 1’s.
If \( \hat{\delta}(q_0, x) = q_{1e} \) then \( x \) has one 0 and an even number of 1’s.
If \( \hat{\delta}(q_0, x) = q_{1o} \) then \( x \) has one 0 and an odd number of 1’s.
If \( \hat{\delta}(q_0, x) = q_{2e} \) then \( x \) has two or more 0’s and an even number of 1’s.
If \( \hat{\delta}(q_0, x) = q_{2o} \) then \( x \) has two or more 0’s and an odd number of 1’s.

20. In this question we formalize the usual algorithm for adding numbers represented in base \( b \).

Let \( \Sigma = \{0, 1, \ldots, b-1\} \).

(a) Give an inductive definition of the base \( b \) interpretation function \( n : \Sigma^* \rightarrow \mathbb{N} \). Check that if \( b = 2 \) then \( n(110) = 6 \).

Solution

\[ n(\varepsilon) := 0 \text{ and } n(xa) := bn(x) + a. \] If \( b = 2 \) we have

\[ n(101) = 2n(11) + 0 \]
\[ = 2(2n(1) + 1) \]
\[ = 2(2(2n(\varepsilon) + 1) + 1) \]
\[ = 2(0 + 1) + 1 \]
\[ = 2(3) = 6 \]

(b) Consider the following inductive definition of a function

\[ add : \Sigma^* \times \Sigma^* \times \{0, 1\} \rightarrow \Sigma^* \]
given by

\[ add(\varepsilon, \varepsilon, c) := \varepsilon c \]
\[ add(xd, \varepsilon, c) := add(x, \varepsilon, q)r \text{ where } q = quot(d + c, b) \text{ and } r = rem(d + c, b) \]
\[ add(\varepsilon, xd, c) := add(\varepsilon, x, q)r \text{ where } q = quot(d + c, b) \text{ and } r = rem(d + c, b) \]
\[ add(xd, ye, c) := add(x, y, q)r \text{ where } q = quot(d + e + c, b) \text{ and } r = rem(d + e + c, b) \]

Note: you know this algorithm well; \( c \) stands for “carry”.

Prove that \( n(add(x, y, c)) = n(x) + n(y) + c. \) If multiple cases are substantially similar, you may say so instead of repeating the proof.

Solution

Let \( P(x, y) \) be the statement \( n(add(x, y, c)) = n(x) + n(y) + c. \)
We must show \( P(\varepsilon, \varepsilon), P(\varepsilon, xa), P(xa, \varepsilon) \) and \( P(xa, yb) \).
In the \( P(\varepsilon, \varepsilon) \) case, we have \( n(add(\varepsilon, \varepsilon, c)) = n(\varepsilon c) = c = n(\varepsilon) + n(\varepsilon) + c. \)
In the $P(xa, \varepsilon)$ case, we first assume $P(x, \varepsilon)$. We have

\[
\begin{align*}
\n(\text{add}(xa, \varepsilon, c)) &= n(\text{add}(x, \varepsilon, q)) r \\
&= bn(\text{add}(x, \varepsilon, q)) + r \quad \text{definition of } n \\
&= bn(x) + bn(\varepsilon) + qb + r \quad \text{by } P(x, \varepsilon) \\
&= bn(x) + 0 + a + c \quad \text{by definition of quotient and remainder} \\
&= n(xa) + 0 + c \quad \text{by definition of } n \\
&= n(xa) + n(\varepsilon) + c \quad \text{by definition of } n \\
\end{align*}
\]

as required.

The $P(\varepsilon, xa)$ case is identical.

Now, to see $P(xa, yd)$, we first assume $P(x, y)$, $P(xa, y)$ and $P(x, yd)$. We have

\[
\begin{align*}
\n(\text{add}(xa, yd, c)) &= n(\text{add}(x, y, \text{quot}(a + d + c, b)) \text{rem}(a + d + c, b)) \quad \text{definition of } \text{add} \\
&= bn(\text{add}(x, y, \text{quot}(a + d + c, b)) \text{rem}(a + d + c, b)) + \text{rem}(a + d + c, b) \quad \text{definition of } n \\
&= bn(x) + bn(y) + b \text{quot}(a + d + c, b) + \text{rem}(a + d + c, b) \quad \text{by } P(x, y) \\
&= bn(x) + bn(y) + a + d + c \quad \text{definition of quotient and remainder} \\
&= n(xa) + n(yd) + c \quad \text{definition of } n \\
\end{align*}
\]