Homework 7
Due: Monday, July 12th at 11:59pm EDT

All homeworks are due the Monday after their release at 11:59pm EDT on Gradescope.

Please do not include any identifying information about yourself in the handin, including your Banner ID.

Be sure to fully explain your reasoning and show all work for full credit. We recommend checking out the sample proofs on the course website to see the level of rigor for which we’re looking.

Problem 1

Saturn and its moon Titan want to establish a secure communication channel to discuss who the impostor moon is without any eavesdroppers. They want to use a cryptosystem that is both simple and effective and have decided to use the RSA cryptosystem as a result. Saturn publishes the product of primes \( n = 1963 \) and the public key \( e = 49 \).

a. Titan wants to send nonsense along the communication channel to test the system out. Encrypt the random word ‘SAND’ by encrypting each letter separately by using the encoding of \( A = 1 \), \( B = 2 \), \ldots , \( Z = 26 \). Your answer should be a sequence of numbers.

b. In a moment of weakness, Saturn leaked the private key \( d = 1249! \). Decrypt the most recent series of messages sent by Titan:

\[(1224, 1344, 1305, 1, 407)\]

Note: Saturn and Titan are using the same encoding as used in part (a) for encoding letters. As such, your answer should be a sequence of letters that Titan originally encoded.
c. Suppose the impostor moon has found two integers $x$ and $y$ such that $x^2 \equiv y^2 \pmod{n}$, but $x \not\equiv \pm y \pmod{n}$. Show how it can use this to find the prime factors of $n$, which we’ll denote by $p$ and $q$.

**Hint:** What does $n$ divide?

d. Saturn has regained its senses and has chosen the new public key $e_2 = 101$. However, the impostor moon has duped them once again and stolen the corresponding private key, $d_2 = 1301$. The impostor now knows of two pairs of public and private keys, $(e, d)$ and $(e_2, d_2)$ that both work for $n$. Show how these two pairs alone allow the impostor moon to compute the prime factors $p$ and $q$ of $n$.

**Hint:** What congruence relation holds for both pairs?

### Problem 2

Answer the following questions, explaining the reasoning behind your result.

a. Saturn has a total of 82 moons. Out of this total, 24 of them are regular satellites whose orbits are not greatly inclined relative to Saturn’s equatorial plane. The rest are non-regular satellites.

Saturn decides to bring four moons on a trip. If it picks one regular satellite and three non-regular satellites, how many distinct groups of moons can Saturn bring on a trip?

b. Saturn’s moon Rhea is playing with Morse code. The symbols in Morse code are represented by variable-length sequences of dots and dashes (more formally, dits or dahs). For example, the letter A = –•, and the number 1 = • – – – – –. How many different symbols can Rhea represent by sequences of seven or fewer dots and dashes?

c. Saturn’s moon Titan is making bracelets. It has nine charms to include on its bracelets: a clover, a rainbow, a heart, a shooting star, a horseshoe, a balloon, a blue moon, a pot-o-gold and a leprachaun hat. If each bracelet uses seven charms and does not use a charm more than once, how many distinct bracelets can Titan make with its nine charms?

**Note:** The charms are able to slide over the clasp of the bracelet! However, the charms also have an ‘orientation’. This means that flipping the order of the charms (which is equivalent to wearing the bracelet the other way around) counts as a new distinct pattern.

d. Saturn’s moon Enceladus is playing with a deck of cards. There are 52 cards in a deck, 13 for each of the four suits. It repeatedly draws 5 cards randomly, sees what they are, and then puts them back. In how many ways can Enceladus draw a set of five cards with at least four diamonds and exactly one pair?
e. It’s been a long time since a family photo has been taken. Saturn asks all of its moons to pick a spot in a line in front of its camera. However, all 24 of the regular satellites have been in a fight, and refuse to sit next to each other. In how many ways can Saturn arrange its 82 moons for a photo if respecting this constraint?

Problem 3

Please Read: For the purposes of this problem, you may assume the existence of a bijection between paths on a grid and strings of letters/digits that represent the moves that are chosen along the paths. This means that you are allowed to represent paths by strings that represent sequences of moves.

For example, let \( l \) = left-move and \( u \) = up-move. Then the path in a Cartesian grid from \((0,0)\) to \((0,1)\) to \((-1,1)\) can be represented by the string ‘ul’.

a. On a \( 4 \times 4 \) square grid dots, how many paths of length six connect the lower left-hand corner dot to the upper right-hand corner dot (dot \( a \) to dot \( b \))? The length of a path is the number of hops between points on that path. A hop can be a move up, move down, move left, or move right. Explain your reasoning.

![Diagram of a 4x4 grid with dots and a path from a to b.]

b. Now consider a generalized Cartesian grid with height and width equal to \( n \geq 1 \), an \((n+1) \times (n+1)\) grid of dots. Here we label the lower left-hand corner dot by \((0,0)\) and the upper right-hand corner dot by \((n,n)\). How many paths of shortest length go from the \((0,0)\) dot to the \((n,n)\) dot? Explain your reasoning.

c. Now, holes have appeared in the grid at every point \((x,y)\) such that \( x < y \). With the same rules as before, how many paths of shortest length go from \((0,0)\) to \((n,n)\) without hitting the holes in the grid? Explain your reasoning. **Hint:** Consider the diagonal where \( x + 1 = y \). If a path crosses this diagonal, is it valid? What can you say about the path up until it crosses the diagonal, and the rest of the path?

d. Another Cartesian grid has height \( n - 1 \) and width \( n + 1 \), but has holes in the grid at every point \((x,y)\) such that \( x \leq y \), except for \((0,0)\). Prove that this new grid has the same number of valid paths as the one in part (c) by proving the existence of a bijection between them.

Note: Drawing a diagram to familiarize yourself with valid paths can be helpful. Diagrams are an acceptable supplement to a proof, but never a replacement for one.
Mind Bender (Extra Credit)

Note: This question brings together a lot of the content we have covered so far, so we hope it gives you a deeper understanding of the content!

Consider the set $M_0 = \{0, 1, \ldots, m - 1\}$, and the corresponding equivalence relation $R_m^*$ on $M_0$ defined by

$$\{(x, y) \mid \exists a, b \in \mathbb{Z}^+, \text{ such that } x^a \equiv y^b \pmod{m}\}.$$

Consider the prime factorization of $m = p_1^{a_1}p_2^{a_2} \cdots p_n^{a_n}$ for distinct primes $p_1, \ldots, p_n$. Let us define the set $F = \{p_1, p_2, \ldots, p_n\}$. Let $E \subseteq \mathcal{P}(M_0)$ be the set of equivalence classes of $R_m^*$.

Define the function $f : \mathcal{P}(F) \mapsto E$ by

$$f(\{q_1, \ldots, q_k\}) = [q_1 \times q_2 \times \cdots \times q_k]_{R_m^*}$$

In words, $f$ maps a subset of the prime factors of $m$ to the equivalence class containing their product. As an example, we will look at $m = 30 = 2 \times 3 \times 5$. We then have that $F = \{2, 3, 5\}$, and:

- $f(\emptyset) = \{1, 7, 11, 13, 17, 19, 23, 29\}$
- $f(\{2\}) = \{2, 4, 8, 14, 16, 22, 26, 28\}$
- $f(\{3\}) = \{3, 9, 21, 27\}$
- $f(\{5\}) = \{5, 25\}$
- $f(\{2, 3\}) = \{6, 12, 18, 24\}$
- $f(\{2, 5\}) = \{10, 20\}$
- $f(\{3, 5\}) = \{15\}$
- $f(\{2, 3, 5\}) = \{0\}$

To get you thinking: what kinds of patterns do you see in these equivalence classes? Make sure to pay special attention to $f(\emptyset)$ and $f(F)$.

a. Give an example of an $m$ where $f(F)$ is not just the set $\{0\}$. What property must $m$ have to make $f(F) = \{0\}$?

b. Consider two distinct subsets of $F$, $Q_1$ and $Q_2$, and define

$$q_1^* = \prod_{q \in Q_1} q$$
$$q_2^* = \prod_{q \in Q_2} q.$$
Prove that \((q_1^*, q_2^*) \notin R^*_m\), concluding that \(f\) is injective. Why is that equivalent to injectivity?\footnote{If you have never seen this notation before, big Pi notation (\(\Pi\)) is used just like big Sigma notation (\(\Sigma\)), except it is used for \textbf{products} instead of for \textbf{sums}.}

c. Consider some arbitrary element

\[ x = cq_1^{b_1} q_2^{b_2} \ldots q_k^{b_k} \]

where \(Q = \{q_1, \ldots, q_k\} \subseteq F\), \(\gcd(c, m) = 1\), all \(b_i\) are positive, and \(x \in M_0\). Prove that \(x \in f(Q)\), concluding that \(f\) is surjective. Why is that equivalent to surjectivity?

\textbf{Note:} You may assume the following result without proof. For \(Q = \{q_1, \ldots, q_k\}\) and positive exponents \(\lambda_1, \ldots, \lambda_k\),

\[
\left( q_1 q_2 \ldots q_k, q_1^{\lambda_1} q_2^{\lambda_2} \ldots q_k^{\lambda_k} \right) \in R^*_m.
\]

d. What can we conclude about the function \(f\), and what do you think this says about the relative size of \(\mathcal{P}(F)\) and \(E\)?

e. Show that \(R^*_m\) has exactly two equivalence classes if \(m\) is prime, and show what they are.