Problem Set 5

Due: Wednesday, May 3, by 11:59pm

Instructions

Solutions submission. You must submit your solution via Gradescope. In particular:

- Submit a single PDF file in Gradescope containing the written solution to all the regular tasks in the homework.
- The extra credit is submitted separately in Gradescope

Task 1 – Modding Off [15 pts]

a) Compute $3^{293} \bmod 100$ using the efficient modular exponentiation algorithm.
Show all intermediate results.

b) How many multiplications does the algorithm use for this computation? (Assume that we do not need to perform a multiplication to calculate $3^1 = 3$ since we know that $x^1 = x$ for any x.)

c) The integer 3^{293} has 140 digits, so calculating $3^{293} \bmod 100$ by first calculating 3^{293} and then reducing it modulo 100 would require storing a 140-digit number.

If we calculate $3^{293} \bmod 100$ as in part (a), with each of the modular multiplications $(a \times b) \bmod 100$ performed by calculating the integer $a \times b$ and then reducing it modulo 100, what is the largest number of decimal digits that could appear in any number computed by any step of this computation?

Task 2 – Game, Set, Match [14 pts]

Prove that for all sets A, B, and C we must have:

$$(B \setminus A) \cup (C \setminus A) = (B \cup C) \setminus A.$$

Task 3 – We've Got the Power [16 pts]

Prove or disprove the following statements:

a) For any two sets S and T, we must have:

$$\mathcal{P}(S \cap T) = \mathcal{P}(S) \cap \mathcal{P}(T).$$

b) For any two sets S and T, we must have:

$$\mathcal{P}(S \cup T) = \mathcal{P}(S) \cup \mathcal{P}(T) \cup \mathcal{P}(S \cap T).$$

Task 4 – Keeping up with the Cartesians **[15 pts]**

Let B and C be non-empty sets.

a) Prove that if A is also non-empty then we must have $(A \times B = A \times C) \to B = C$.

b) Is the conclusion of part a) true if A is empty? Why or why not?

Task 5 – Induction Cooking **[20 pts]**

Prove that for every $n \in \mathbb{N}$, the following equality is true:

$$0 \cdot 2^0 + 1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2.$$

Task 6 – Inductive Bias **[20 pts]**

Let $x \in \mathbb{R}$ satisfy $x > 0$. Prove, by induction, that $(2+x)^{n+1} > 2^{n+1} + n2^n x$ holds for all $n \in \mathbb{N}$.

Task 7 – Extra Credit: RSA and modular exponentiation

We know that we can reduce the *base* of an exponent modulo m before multiplying or powering $\pmod{m}$: That is, $a^k \equiv (a \text{ mod } m)^k \pmod{m}$. But the same is not true of the exponent itself! That is, we cannot write $a^k \equiv a^{k \text{ mod } m} \pmod{m}$. This is easily seen to be false in general. Consider, for instance, that 2^{10} mod $3 = 1$ but $2^{10 \text{ mod } 3}$ mod $3 = 2^1$ mod $3 = 2$.

The correct law for the exponent is more subtle. We will prove it in steps....

a) Let $R = \{n \in \mathbb{Z} : 1 \leqslant n \leqslant m-1 \wedge \gcd(n,m) = 1\}$. Define the set $aR = \{ax \text{ mod } m : x \in R\}$. Prove that $aR = R$ for every integer $a > 0$ with $\gcd(a,m) = 1$.

b) Consider the products modulo m of all the elements in R and of all the elements in aR. By comparing those two expressions, conclude that for all $a \in R$ we have $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m) = |R|$.

c) Use the last result to show that, for any $b \geqslant 0$ and $a \in R$, we have $a^b \equiv a^{b \text{ mod } \phi(m)} \pmod{m}$.

d) Now, prove the following two facts about the function ϕ above. First, if p is prime, then $\phi(p) = p-1$. Second, for any positive integers a and b with $\gcd(a,b) = 1$, we have $\phi(ab) = \phi(a)\phi(b)$.

e) The two facts from part d) imply that, if p and q are primes, then $\phi(pq) = (p-1)(q-1)$., along with part c), prove the **Fact:** on Slide 26 about RSA from Lecture 12, and complete the proof of correctness of the algorithm?