CS 30 | Prof. Amit Chakrabarti
Fall 2019 | Computer Science Dept
Discrete Mathematics | Dartmouth College

Problem Set for Unit 6

Here are some problems about **modular exponentiation** and modular arithmetic in general, now that we've developed the subject quite a bit. Before working on this problem set, you will need to have read the corresponding lecture notes posted on the course website. Some of these problems ask you to write out proofs for things mentioned without proof in the lecture notes. In such cases, you can't just cite the lecture notes to say that the result has been proved in class (since it hasn't).

By now you are familiar with what needs to be submitted towards graded homework and when.

The symbols $\mathbb{N}, \mathbb{N}^+, \mathbb{Z}, \mathbb{Z}_m, \mathbb{Q}$, and $\mathbb{R}$ have their usual meanings. The lecture notes define $\mathbb{Z}_m^*$ and $\phi(m)$.

PS6-1

Consider arithmetic modulo 30, in the domain $\mathbb{Z}_{30}$. For each of the following numbers, find

- ***a.*** its inverse modulo 30;
- ***b.*** the smallest positive power of the number that is congruent to 1 modulo 30.

Some of your answers might be "does not exist."

$$1,\ 10,\ 13,\ 19,\ 27,\ 29\,.$$

PS6-2 ^{HW}

Let $p, n, a \in \mathbb{Z}$ be such that p is a prime and $p \nmid a$. Prove that $a^n \equiv a^{n \bmod (p-1)} \pmod{p}$. [4 points]

Let's introduce an important piece of mathematical vocabulary. Consider a set S and an operation "op" on elements on S. We say that S is closed under "op" if the result of applying "op" to elements of S always produces an element of S. The concept is best understood through concrete examples.

- The set $\mathbb{N}$ is closed under the *addition* operation, because if $x, y \in \mathbb{N}$, then $x + y \in \mathbb{N}$.
- Similarly, $\mathbb{N}$ is closed under *multiplication*.
- However, $\mathbb{N}$ is not closed under *subtraction*, because there do exist $x, y \in \mathbb{N}$ such that $x - y \notin \mathbb{N}$.
- On the other hand, the larger set $\mathbb{Z}$ is indeed closed under subtraction.

PS6-3

Prove that $\mathbb{Z}_m^*$ is closed under multiplication modulo m, for all $m \in \mathbb{N}^+$.

PS6-4

Let's generalize Fermat's Little Theorem using a proof along the lines of that given in the lecture notes. Take an arbitrary integer $m \geq 2$ and $a \in \mathbb{Z}_m^*$.

- ***a.*** Prove that $f_a(x) = ax \bmod m$ is a bijection from $\mathbb{Z}_m^*$ to $\mathbb{Z}_m^*$. A fully rigorous proof will need to use ***PS6-3***.
- ***b.*** Using the above result and the Inverse Existence Theorem, prove that $a^{\phi(m)} \equiv 1 \pmod{m}$.
- ***c.*** What does the previous congruence say when m is a prime?

PS6-5 ^{HW}

Let $m \in \mathbb{Z}$ with $m \geq 2$ and $a \in \mathbb{Z}_m^*$. Consider the infinite sequence $P_{m,a}$ of nonnegative powers of a modulo m:

$$P_{m,a} := (a^0 \bmod m,\ a^1 \bmod m,\ a^2 \bmod m,\ a^3 \bmod m,\ \ldots)\,.$$

For instance, $P_{7,3} = (1,3,2,6,4,5,1,3,2,6,4,5,1,3,\ldots)$. Notice that this sequence is *periodic*, i.e., it consists of a finite-length block repeated infinitely often. In this case, the block is $(1,3,2,6,4,5)$. Since this block is six elements long and it's the shortest such block, we say the sequence has period 6.

Another example: $P_{11,5} = (1,5,3,4,9,1,5,3,4,9,1,5,\ldots)$. Again this is a periodic sequence. The shortest block whose repetition generates $P_{11,5}$ is $(1,5,3,4,9)$, so the period is 5.

a. The sequence $P_{m,a}$ always starts with the number 1. Prove that 1 will reappear in the sequence.

b. Prove that $P_{m,a}$ is always a periodic sequence.
Hint: Sometimes the period is 1.

c. Prove that the period of $P_{m,a}$ is at most m.

d. Is every integer in the interval $[1,m]$ equal to the period of some sequence $P_{m,a}$, or are some integers in $[1,m]$ forbidden from being periods? Why? [3+3+3+1 points]
Hint: Play around with some examples for a small value of m, such as $m = 6$.

PS6-6
Let p and q be two distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

PS6-7 ***HW***
Let p be a prime.

a. Suppose $p \geq 5$. Prove that the numbers in the set $S := \{a \in \mathbb{N} : 2 \leq a \leq p-2\}$ can be partitioned into pairs[1] such that the two numbers in each pair are inverses of one another, modulo p.
Hint: You'll want to review your work in ***PS5-9*** ***HW*** and use some of its results here.

b. Using the above, work out the value of $(p-1)! \bmod p$.

c. Hence, prove that for *all* primes p, we have $p \mid (p-1)!+1$. This is called Wilson's Theorem. [4+2+1 points]

PS6-8
Prove that for all composite numbers m, we have $m \nmid (m-1)!+1$.
Hint: Try dividing $(m-1)!$ by m for some small example cases.

PS6-9
Let $a, b, n \in \mathbb{N}^+$.

a. Prove that if $a \mid n$ and $b \mid n$, then $\text{lcm}(a,b) \mid n$.
Review your work in ***PS5-6*** ***HW*** and rewrite things in terms of $\gcd(a,b)$, then make use of LCT.

b. Using the above result repeatedly, prove that if $p_1, p_2, \ldots, p_k$ are distinct primes and each $p_i \mid n$, then the product $p_1 p_2 \cdots p_k \mid n$.

PS6-10 ***HW***
Prove that $\forall\, n \in \mathbb{Z}$: $2730 \mid n^{13} - n$. [7 points]
Hint: Use the result of ***PS6-9***. In your submission it's okay to use that result without writing up its proof.

[1] This means that every element of S occurs in exactly one of the pairs.