CS30 (Discrete Math in CS), Summer 2021 : Lecture 29

Topic: Numbers: Fermat's Little Theorem

Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.
Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

---

1. **Fermat's Little Theorem.**

We will prove the following theorem remarkable in its own right. Later, we will see how it will lead to an algorithm for public key cryptography.

Theorem 1. Let p be any prime. For any $a \in \mathbb{Z}_p \setminus \{0\}$, $a^{p-1} \equiv_p 1$.

Remark: *Note that the above theorem is for $a \in \mathbb{Z}_p \setminus \{0\}$. For any (larger) a with $\gcd(a,p)$, we get $a^{p-1} \equiv_p (a \bmod p)^{p-1} \equiv_p 1$.*

Remark: *The above allows us to do must "faster" modular exponentiation (at least by hand) when the modulus is prime. For instance, instantiating the above theorem for $a = 3$ and $p = 7$, we get $3^6 \equiv_7 1$. But we also get $3^{60} \equiv_7 1$ by taking the above to power 10 on both sides (note $1^{10} = 1$). And we also get $3^{61} \equiv_7 3 \cdot 3^{60} \equiv_7 3$.*

Proof. The crux of the proof lies in the "dividing out" theorem we did last class. Recall, since every $a \in \mathbb{Z}_p \setminus \{0\}$ has $\gcd(a,p) = 1$, we know that

$$ax \equiv_p ay \Rightarrow x \equiv_p y \tag{1}$$

In particular, if we take two *different* $x, y \in \mathbb{Z}_p \setminus \{0\}$, then $ax \not\equiv_p ay$, that is, $ax \bmod p \neq ay \bmod p$.

Remark: *In other words, if one considers the function $h_a : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p \setminus \{0\}$ defined as $h_a(x) = ax \bmod p$, then h_a is an injective function.*

Furthermore, if we look at the numbers of the form $ax \bmod p$ as x ranges in $\mathbb{Z}_p \setminus \{0\}$, then we must see all the numbers in $\mathbb{Z}_p \setminus \{0\}$. Indeed, for any $y \in \mathbb{Z}_p$, we know that $ax \equiv_p y$ has the solution $x \equiv_p a^{-1}y$ in $\mathbb{Z}_p \setminus \{0\}$.

Remark: *That is, the function h_a defined above is a surjective function. Together with the fact that it is injective, we get it is bijective. That is, h_a is just a* **scrambler** *of the numbers in $\mathbb{Z}_p \setminus \{0\}$.*

Therefore, we get that the following two sets:

$$A = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\} \quad \text{and} \quad B = \{ax \bmod p : x \in A\}$$

are the same.

Example. Let us just illustrate with $p = 7$ and $a = 3$.

x	$ax \bmod p$
1	3
2	1
3	2
4	5
5	1
6	4

Now, since A and B are the same set, we get

$$\prod_{z \in A} z \quad = \quad \prod_{z \in B} z = \prod_{x \in A} h_a(x) = \prod_{x \in A} (ax \bmod p)$$

Taking both sides modulo p, we get

$$\left(\prod_{z \in A} z\right) \quad \equiv_p \quad \left(\prod_{x \in A} (ax)\right) \quad \equiv_p \quad \left(a^{p-1} \cdot \prod_{x \in A} x\right)$$

Let us use the notation $Q \coloneqq (\prod_{z \in A} z)$ (note $Q = (p-1)!$). Then, we get

$$Q \quad \equiv_p \quad a^{p-1} Q \tag{2}$$

Finally, we assert that $\gcd(p, Q) = \gcd(p, (p-1)!) = 1$. This is problem 1(c) in PSet 8. And now, we can again apply (1) on (2) to get $a^{p-1} \equiv_p 1$ (cancel Q from both sides). □

Exercise: *Check if the above would be true if* p *were not a prime but the only restriction was* $\gcd(a, n) = 1$. *In particular, find* a, n *such that* $\gcd(a, n) = 1$ *but* $a^{n-1} \not\equiv_n 1$.

Remark: *After doing the above exercise you should ask yourself : where all is the property that* p *is prime used? If you think about it clearly enough, you will indeed prove that if* $\gcd(a, n) = 1$, *then there is indeed some number* ϕ *such that* $a^{\phi} \equiv_n 1$. *A problem in the UGP explores this.*