Fermat's Little Theorem

Reading

- Section 9.1

Practice Problems

9.1 1, 3, 6, 10, 17

Notes

Fermat's Theorem

Fermat's Little Theorem concerns itself with powers of elements modulo a prime number. Let us look at the simple example of $p = 7$, and considering the powers of all nonzero elements, modulo 7. We stop the first time we encounter 1 (because the values will repeat after that point).

$$2^2 = 4, 2^3 = 8 = 1$$
$$3^2 = 9 = 2, 3^3 = 2 \cdot 3 = 6, 3^4 = 6 \cdot 3 = 18 = 4, 3^5 = 4 \cdot 3 = 12 = 5, 3^6 = 5 \cdot 3 = 15 = 1$$
$$4^2 = 16 = 2, 4^3 = 2 \cdot 4 = 8 = 1$$
$$5^2 = 25 = 4, 5^3 = 4 \cdot 5 = 20 = 6, 5^4 = 6 \cdot 5 = 30 = 2, 5^5 = 2 \cdot 5 = 10 = 3, 5^6 = 3 \cdot 5 = 15 = 1$$
$$6^2 = 36 = 1$$

Let us repeat this for different prime moduli: I am listing below only the first power that equals 1:

mod 11:

$$2^{10} = 1, 3^5 = 1, 4^5 = 1, 5^5 = 1, 6^{10} = 1, 7^{10} = 1, 8^{10} = 1, 9^5 = 1, 10^2 = 1$$

So the possible powers are 1,2,5,10.

mod 13:

$$2^{12}, 3^3, 4^6, 5^4, 6^{12}, 7^{12}, 8^4, 9^3, 10^6, 11^{12}, 12^2$$

So the possible powers are 1,2,3,4,6,12.

Starting to notice a pattern?

It looks like the first power that an element becomes equal to 1 is always a divisor of $p - 1$. In particular, if we raise that element to $p - 1$ we will always get 1. This is the essence of Fermat's Little Theorem:

Fermat's Little Theorem

If p is prime and a is relatively prime to p, then $a^{p-1} = 1 \bmod p$.

In general for any a, we have $a^p = a \bmod p$.

This can be used to test that a number is prime, as this property will not hold for most non-prime numbers (there are a few exceptions).

For instance, consider $n = 15$. Let us compute 7^{14} and see if it equals 1.

We have: $7^2 = 49 = 4 \bmod 15$, $7^4 = 4^2 = 16 = 1 \bmod 15$, $7^{12} = (7^4)^3 = 1^3 = 1 \bmod 15$, $7^{14} = 7^{12} \cdot 7^2 = 4 \bmod 15$.

If we had computed 4^{14} instead, we would have found that to be 1, so you often have to try more than one element.

Now we proceed to discuss a proof of Fermat's Little Theorem:

- Recall we have the set of congruence classes (leaving 0 out): $\{\bar{1}, \bar{2}, \ldots \overline{p-1}\}$.
- What happens when we multiply all these by $\bar{a}$? Because multiplication is 1-1, and we can never get 0 as the result, then multiplying by $\bar{a}$ just *rearranges* them.
- So the numbers $\{\bar{a} \cdot \bar{1}, \bar{a} \cdot \bar{2}, \ldots\}$ are exactly the same as $\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$, just in a different order.
- So they should have the exact same product:

$$(\bar{a} \cdot \bar{1}) \cdot (\bar{a} \cdot \bar{2}) \cdots (\bar{a} \cdot \overline{p-1}) = \bar{1} \cdot \bar{2} \cdots \overline{p-1}$$

- Taking out the factors of a from the front we get:

$$\bar{a}^{p-1}(\bar{1} \cdot \bar{2} \cdots \overline{p-1}) = \bar{1} \cdot \bar{2} \cdots \overline{p-1}$$

- By Wilson's theorem, that product is invertible (in fact equal to -1). So we can cancel it out.
- This leaves us with $\bar{a}^{p-1} = 1 \bmod p$.