# Number Theory 2: Fermat's Theorem (Draft)
# (Last revision Nov 27, 2015)

## Fermat's Theorem

In this lecture we focus again on the properties of integers modulo a prime. Let $p$ be a prime and consider numbers $0, 1, ..., p-1$, namely all possible remainders modulo $p$. As we discussed earlier, we can think of this set as an algebraic system, with arithmetic operations of addition and multiplication modulo $p$. For example, for $p = 7$, if we compute all results modulo 7, we have $4 + 5 = 2$, $4 \cdot 5 = 6$, etc. We have also discussed inverses modulo $p$. For example, the inverse of 5 modulo 7 is 3, because $5 \cdot 3 \equiv 1 \pmod 7$.

We can also consider computing powers, $a^x \operatorname{rem} p$, for $a \in \{1, 2, ..., p-1\}$ and any non-negative integer $x$. This raises some interesting questions. If we compute the sequence of numbers $a^0, a^1, a^2, ...$, all taken modulo $p$, this gives us an infinite sequence with all numbers in the finite range $\{1, 2, ..., p-1\}$. Will this sequence visit all numbers in this range? Will this sequence have a pattern? In particular, will it be periodic?

As it turns out, yes, if $p$ is prime then this sequence will be periodic, namely it will repeat itself every $p-1$ steps, and each block of $p-1$ consecutive elements of this sequence is a permutation of $\{1, 2, ..., p-1\}$. This follows from the following theorem.

**Theorem 1** *(Fermat's Little Theorem) Let $p$ be a prime number and let $a \in \{1, 2, ..., p-1\}$. Then $a^{p-1} \equiv 1 \pmod p$.*

*Proof:* Fix our $a$, and consider the sequence of the numbers

$$a \cdot 1\,,\ a \cdot 2\,,\ ...\,,\ a \cdot (p-1) \tag{1}$$

computed modulo $p$.

We claim that all these numbers are different. The proof of this claim is by contradiction. Suppose that there are two different $x, y \in \{1, 2, ..., p-1\}$, for which $ax \equiv ay \pmod p$. Without loss of generality, assume $x > y$. (Otherwise we can swap $x$ and $y$.) This gives us that $a(x-y) \equiv 0 \pmod p$, which is equivalent to saying that $a(x-y) = kp$ for some integer $p$. On the left-hand side we have an integer that is a product of two numbers, $a$ and $x-y$, both smaller than $p$, so it does not have $p$ in its factorization. But on the right-hand side, we have an integer that has $p$ in its factorization, so this equation cannot be true, giving us our contradiction.

So now we know that all numbers in the sequence (1) are different (remember that we compute them modulo $p$). This sequence has $p-1$ different numbers, all in the range $1, 2, ..., p-1$, so the sequence must be simply a permutation of $1, 2, ..., p-1$. Therefore if we multiply these numbers, we get

$$(a \cdot 1) \cdot (a \cdot 2)\,,\ ...\,,\ \cdot(a \cdot (p-1)) \equiv 1 \cdot 2 \cdot ... \cdot (p-1) \pmod p$$

We can cancel all numbers $1, 2, ..., p-1$ from this equation (multiplying both sides by their inverses), which leaves us with

$$a^{p-1} \equiv 1 \pmod p,$$

completing the proof of the theorem. □

**Example 1.** Consider $p = 7$ and $a = 3$. Then Fermat's theorem says that $3^{7-1} = 3^6 \equiv 1 \pmod 7$. Indeed, computing modulo 7, $3^6 = 9^3 = 2^3 = 8 = 1$.

Fermat's Theorem has some interesting applications, the most notable of which is for the correctness of the RSA (that we will discuss later). We can also use it to compute inverses and powers, as explained below.

**Application to computing inverses.** The statement of Fermat's theorem suggests that it should be useful to computing inverses. We have $a^{p-1} \equiv 1 \pmod{p}$. But we can write $a^{p-1}$ as $a \cdot a^{p-2}$. This gives us that

$$a \cdot a^{p-2} \equiv 1 \pmod{p}$$

But this implies that $a^{p-2} \equiv a^{-1} \pmod{p}$, that is $a^{p-2} \operatorname{rem} p$ is exactly the inverse of $a$ modulo $p$.

For example, to compute $3^{-1} \pmod{7}$, we can compute $3^5 \operatorname{rem} 7$. Computing modulo 7, this gives us $3^{-1} = 3^5 = 3 \cdot 9^2 = 3 \cdot 2^2 = 3 \cdot 4 = 12 = 5$. This is indeed correct, because $3 \cdot 5 \equiv 1 \pmod{7}$.

**Application to computing powers.** Let $p$ be prime and $a \in \{1, 2, ..., p-1\}$. Suppose we want to compute $a^x \operatorname{rem} p$, for some large $x$. We can do this using the squaring algorithm, but Fermat's theorem could also significantly reduce the computation. Let $z = x \operatorname{rem} (p-1)$, and write $x$ as $x = r(p-1) + z$. Then, computing modulo $p$, we have

$$a^x = a^{r(p-1)+z} = (a^{p-1})^r \cdot a^z = a^z.$$

Since $z$ is much smaller than $x$, this can save us a lot of computation.

For example, to compute $3^{40954327098} \pmod{11}$, we can proceed as follows (all calculations modulo 11):

$$\begin{aligned} 3^{40954327098} &= 3^{10 \cdot 4095432709} \cdot 3^8 \\ &= 3^8 = 9^4 = 81^2 = 4^6 = 16 = 5. \end{aligned}$$

Just to make sure though: this trick is legal only if $p$ is prime.