Fermat's Little Theorem

Theorem

Fermat's Little Theorem.
Let $a \in \mathbb{Z}$. If p is a prime then $a^p \equiv_p a$.

Example:
$2^{13} \equiv_{13} 2$ as 13 is prime.
Check:
$2^4 \equiv_{13} 3$ as $2^4 = 16$ and $16 \equiv_{13} 3$.
$2^{12} = (2^4)^3 \equiv_{13} 3^3 \equiv_{13} 1$ as $3^3 = 27$. i.e
$2^{12} \equiv_{13} 1$.
$2^{13} = 2^{12} * 2 \therefore$
$2^{13} \equiv_{13} 2$.
Also, e.g. $6^{13} \equiv_{13} 6$.

Fermat's Primality Test

From Fermat's Little Theorem we have its contraposition:
Contrapostion of $p \to q$ is $\neg q \to \neg p$

Theorem

Fermat's Test for Primality
If, for some $a \in \mathbb{Z}$, $a^n \not\equiv_n a$ then n is not prime.

Example:
Consider $2^{12} mod\, 12$.
$2^4 \equiv_{12} 4$ as $2^4 = 16$.
$2^{12} = (2^4)^3 \equiv_{12} 4^3 \equiv_{12} 4$ as
$4^3 = 4^2 * 4 \equiv_{12} 4 * 4 \equiv_{12} 4$
$\therefore 2^{12} \not\equiv_{12} 2$
$\therefore$ 12 is not prime.

Exponent and Base

Based of the properties of exponents:
$a^n = (a^{\frac{n}{2}})^2$ if n is even
$a^n = a * a^{n-1}$ if n is odd.
calculating exponents can be done efficiently in 'log n' time. Also, calculating exponents is done efficiently due to calculating in modular arithmetic.
Terminology: In the expression x^y , y is the 'exponent' and x is the 'base'.

Primality counter examples

From Fermat's Primality test:

Theorem

If, for some $a \in \mathbb{Z}$, $a^n \not\equiv_n a$ then n is not prime

We cannot conclude that if $a^n \equiv_n a$ then n is prime.
(In Logic: $\neg P \rightarrow \neg Q \neq P \rightarrow Q$)
Note: Fermat's Little Thm states: if n is prime then $a^n \equiv_n a$.
It is possible for $a^n \equiv_n a$ and n is not prime.
In particular, let $n = 341$.
341 is not prime as $341 = 11 * 31$
but $2^{341} \equiv_{341} 2$.
i.e. $2^{341} \equiv_{341} 2$ and 341 is not prime.
Since Fermat's Primality is true for some $a \in \mathbb{Z}$ we could try another value.
Since $3^{341} \equiv_{341} 168$ and so $3^{341} \not\equiv_{341} 3$ then 341 is not prime.

Carmichael Numbers

Carmichael Numbers

While Fermat's Primality test works for 341 if we use 3^{341}, the test does not work for the number, 561. 561 is a **Carmichael number.**
A **Carmichael number**, n, is a composite (i.e. not prime) number that satisfies the property $a^n \equiv_n a$.
While rare, there are an infinite number of Carmichael numbers.
The only **Carmichael numbers** less that 2000 are 561, 1105 and 1729.
The **Carmichael number** $561 = 3 * 11 * 17$, $1105 = 5 * 13 * 17$, $1729 = 7 * 13 * 19$.
The **Carmichael numbers** are counter examples to Fermat's Primality test.

Carmichael Numbers (Cont'd)

The number 561 is not prime as $561 = 3 * 11 * 17$

For any integer, a, we have that $a^{561} \equiv_{561} a$, even though 561 is not prime.

Due to the rarity of **Carmichael numbers** and that other tests can be applied, Fermat's Primality Test may be used to check if a number is **possibly prime**.

If a number, n, satisfies $a^n \equiv_n a$ then there is very high probability, but not certainty, that the number, n, is prime.

From Wikipedia

The Carmichael number 1729 is known as the Hardy–Ramanujan number after a famous anecdote of the British mathematician G. H. Hardy regarding a visit to the hospital to see the Indian mathematician Srinivasa Ramanujan. In Hardy's words:
" I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."

1729
$= 1^3 + 12^3$
$= 9^3 + 10^3$

Fermat's Little Theorem

Checking Fermat's Little Theorem: $a^p \equiv_p a$ **where** p **is prime.**

Check $3^7 \equiv_7 3$.
For $p = 7$ and $a = 3$, consider the product:
$(3 *_7 1) *_7 (3 *_7 2) *_7 (3 *_7 3) *_7 (3 *_7 4) *_7 (3 *_7 5) *_7 (3 *_7 6)$.
As $*_7$ is associative and commutative, this product is the same as:

$$3^6 *_7 1 *_7 2 *_7 3 *_7 4 *_7 5 *_7 6$$

Fermat's Little Theorem (Cont'd)

Also, for
$(3 *_7 1) *_7 (3 *_7 2) *_7 (3 *_7 3) *_7 (3 *_7 4) *_7 (3 *_7 5) *_7 (3 *_7 6)$.
we can calculate for each k, $3 *_7 k$

k	1	2	3	4	5	6
$3 *_7 k$	3	6	2	5	1	4

$\therefore$
$(3 *_7 1) *_7 (3 *_7 2) *_7 (3 *_7 3) *_7 (3 *_7 4) *_7 (3 *_7 5) *_7 (3 *_7 6)$
$= 3 *_7 6 *_7 2 *_7 5 *_7 1 *_7 4$
$= 1 *_7 2 *_7 3 *_7 4 *_7 5 *_7 6$

Fermat's Little Theorem (Cont'd)

$\therefore$

$$3^6 *_7 1 *_7 2 *_7 3 *_7 4 *_7 5 *_7 6 = 1 *_7 2 *_7 3 *_7 4 *_7 5 *_7 6$$

Since 7 is prime: for $k \in \{1 \ldots 6\}$, $gcd(k, 7) = 1$.
Cancelling on both sides we get

$$3^6 \equiv_7 1$$

$\therefore$ multiplying both sides by 3,

$$3^7 \equiv_7 3$$

Check: $3^7 = 2187 = 7 * 312 + 3$.

Cancelling

Recall: if a and n are relatively prime (i.e. $gcd(a, n) = 1$) then
if $a * x \equiv_n a * y$ then $x \equiv_n y$.
i.e. we can 'divide across' or 'cancel' the 'a' .
Taking the Contrapositive (From Logic: $p \rightarrow q = \neg q \rightarrow \neg p$) we get, when $gcd(a, n) = 1$,
if $x \not\equiv_n y$ then $a * x \not\equiv_n a * y$

Proof 'Fermat's Little Theorem', $a^p \equiv_p a$

Proof Fermat's Little Theorem

Since p is prime, we consider 2 cases:

- $gcd(a, p) = p$ (i.e. $p|a$)

or

- $gcd(a, p) = 1$, (i.e. a and p are relatively prime).

- **Case** $gcd(a, p) = p$ i.e. $p|a$ i.e. $a \, mod \, p = 0$.

$a \, mod \, p = 0$
$a \equiv_p 0$
then
$0^p \equiv_p 0$
i.e.
$a^p \equiv_p a$

More briefly, when $a \equiv_p 0$ then $0^p \equiv_p 0$.

Lemma

Lemma

Let p be a prime. For an integer, a, such that $gcd(a, p) = 1$, the sequence of numbers
$1 *_p a,\ 2 *_p a,\ 3 *_p a, \ldots (p-1) *_p a$ is a permutation of
$1, 2, 3 \ldots p-1$
i.e. as sets
$\{1 *_p a,\ 2 *_p a,\ 3 *_p a, \ldots (p-1) *_p a\} = \{1, 2, 3 \ldots p-1\}$
Note that for $gcd(a, p) = 1$, if $x \not\equiv_p y$ then $a * x \not\equiv_p a * y$

Lemma proof

Proof Lemma:
Since $gcd(a, p) = 1$, then $a \not\equiv_p 0$. Let $k \in \{1, 2 \ldots p - 1\}$
$\therefore\ gcd(k, p) = 1$.
For each $k \in \{1, 2, 3 \ldots p - 1\}$, $k *_p a \in \mathbb{Z}_p$ and all of
$1 *_p a$, $2 *_p a \ldots (p - 1) * a$ are different,
as if $i *_p a = j *_p a$ then, by cancellation of a, $i = j$, i.e. if $i \neq j$
then $i *_p a \neq j *_p a$.
$\therefore\ \{1 *_p a,\ 2 *_p a,\ 3 *_p a, \ldots (p - 1) *_p a\} = \{1, 2, 3 \ldots p - 1\}$
i.e. $1 *_p a$, $2 *_p a$, $3 *_p a, \ldots (p - 1) *_p a$ is a permutation of
$1, 2, 3 \ldots p - 1$.

Proof: Fermat's Little Theorem.

- **Case** $gcd(a, p) = 1$ i.e. a and p are relatively prime.

Theorem

For prime, p, $a^p \equiv_p p$ *when* $gcd(a, p) = 1$*.*

Proof.

Assume p is a prime, show $a^p \equiv_p a$.
From Lemma,
$\{1 *_p a,\ 2 *_p a,\ 3 *_p a, \ldots (p-1) *_p a\} = \{1, 2, 3 \ldots p-1\}$
$\therefore$ the products of these elements are equal i.e.
$(1 *_p a) *_p (2 *_p a) *_p (3 *_p a), \cdots *_p (p-1) *_p a$
$= 1 *_p 2 *_p 3 \cdots *_p (p-1)$
i.e.
$(1 * a) * (2 * a) * \cdots * ((p-1) * a) \equiv_p 1 * 2 * 3 * \cdots * (p-1)$ $\square$

Proof Cont'd

Proof.

but

$(1*a)*(2*a)*\cdots*(p-1)*a = a^{p-1}*(1*2*3*\cdots*(p-1))$

$\therefore\ a^{p-1}*(1*2*3*\cdots*(p-1)) \equiv_p 1*2*3*\cdots*(p-1)$

$\therefore\ a^{p-1}*(1*2*3*\cdots*(p-1)) - (1*2*3*\cdots*(p-1)) \equiv_p 0$

i.e. $\therefore\ (a^{p-1}-1)*(1*2*3*\cdots*(p-1))$ is divisible by p.

Since $p \not| 1$ and $p \not| 2$ ... $p \not| (p-1)$ then $p | (a^{p-1}-1)$ i.e.

$a^{p-1} - 1 \equiv_p 0$ i.e.

$a^{p-1} \equiv_p 1$

Multiplying both sides by, a, we get

$a^p \equiv_p a$

$\square$

This proof is attributed to Ivory in 1806.