Fermat's Little Theorem

Theorem

n^7-n is a multiple of 7, for $n=1,2,3,\ldots$

for example 153^7-153 is a multiple of 7

Proof (by induction)

part 1:

If $n=1$ then $n^7-n=0$

So n^7-n is a multiple of 7 when $n=1$

part 2:

If n^7-n is a multiple of 7 when $n=k$ then:

k^7-k is a multiple of 7, so $k^7-k=7r$ for some integer r

Now $(k+1)^7-(k+1)=(k^7+7k^6+21k^5+35k^4+35k^3+21k^2+7k+1)-(k+1)$

So $(k+1)^7-(k+1)=(k^7-k)+(7k^6+21k^5+35k^4+35k^3+21k^2+7k)$

So $(k+1)^7-(k+1)=7r+7(k^6+3k^5+5k^4+5k^3+3k^2+k)$

So $(k+1)^7-(k+1)$ is a multiple of 7

So n^7-n is a multiple of 7 when $n=k+1$

Note: our proof worked because the coefficients in the binomial theorem: $7,21,35,35,21,7$ are all multiples of 7

A typical coefficient is: $(7C3)=\dfrac{7\times6\times5\times4\times3\times2\times1}{(3\times2\times1)(4\times3\times2\times1)}$

After lots of cancelling, we are left with a positive integer. The 7 on the top of the fraction can't be cancelled out by numbers on the bottom of the fraction because 7 is prime. So $(7C3)$ must be a multiple of 7

In general:

If p is prime then all the coefficients in the expansion of $(k+1)^p$ will be a multiple of p (apart from the 1's at each end)

In general:

Fermat's Little Theorem (FLT) for prime number p and $n=1,2,3,\ldots$

n^p-n is a multiple of p

We can prove this for prime number p as we proved it above for prime number 7

Now:

n^7-n is a multiple of 7, so $n(n^6-1)$ is a multiple of 7

So:

if n is not a multiple of 7 then n^6-1 is a multiple of 7

So we can rephrase:

Fermat's Little Theorem (FLT) for prime number p and $n=1,2,3,\ldots$

$n^{(p-1)}-1$ is a multiple of p provided n is not a multiple of p

We can rephrase using mod arithmetic:

Fermat's Little Theorem (FLT) for prime number p and $n=1,2,3,\ldots$

$n^p-n=0,mod\ p$ so $n^p=n,mod\ p$

Or:

$n^{(p-1)}-1=0,mod\ p$ so $n^{(p-1)}=1,mod\ p$ provided n is not a multiple of p

We will now use FLT to evaluate expressions of the form $a^b,mod\ p$ where p is prime. Such expressions can be tricky to evaluate if a is large or b is large. Luckily there are two theorems that can help us.

Theorem

If $a=A,mod\ p$ then $a^n=A^n,mod\ p$ where $n=1,2,3,\ldots$

(this theorem is true whether p is prime or not)

for example $273=3,mod\ 5$ so $273^{24}=3^{24},mod\ 5$

Proof

See section, Modular Arithmetic

Theorem

If $a=A,mod\ p-1$ then $n^a=n^A,mod\ p$ where $n=1,2,3,\ldots$ and n is not a multiple of p

(this theorem is only true if p is prime)

for example $387=3,mod\ 4$ so $97^{387}=97^3,mod\ 5$

Proof

We will show that:

$153=3,mod\ 6$ so $n^{153}=n^3,mod\ 7$

You can prove the general result in the same way.

$n^6 = 1, mod\ 7$ from FLT where $n = 1, 2, 3, \ldots$ and n is not a multiple of p

So

$$n^{153} = n^{(6\times 25)+3} = n^{(6\times 25)} \times n^3 = (n^6)^{25} \times n^3 = 1^{25} \times n^3 = 1 \times n^3 = n^3, mod\ 7$$

Example

Evaluate $2518^{10}, mod\ 17$

Now:

$2518 = 2, mod\ 17$ so $2518^{10} = 2^{10}, mod\ 17$

And:

$2^{10} = 1024 = 4, mod\ 17$

Example

Evaluate $3^{220}, mod\ 19$

Now:

$220 = 4, mod\ 18$ so $3^{220} = 3^4, mod\ 19$

And:

$3^4 = 81 = 5, mod\ 19$

Example

Evaluate $875^{302}, mod\ 13$

Now:

$875 = 4, mod\ 13$ so $875^{302} = 4^{302}$

Now:

$302 = 2, mod\ 12$ so $4^{302} = 4^2, mod\ 13$

And:

$4^2 = 16 = 3, mod\ 13$

We will now use FLT to find the last digit of numbers of the form a^b

Note:

If $N = 32748$ then $N = 32740 + 8 = (3274 \times 10) + 8$ so $N = 8, mod\ 10$

Finding the last digit of N is the same as finding $N, mod\ 10$

Note:

If $N=7, mod\,10$ then $N=10k+7$ for some positive integer k

So:

$N=2(5k+3)+1$ so $N=1, mod\,2$

And:

$N=5(2k+1)+2$ so $N=2, mod\,5$

We can repeat these calculations for $N=1,2,3,4,5,6,8,9, mod\,10$ to get this table.

$N, mod\,10$	0	1	2	3	4	5	6	7	8	9
$N, mod\,2$	0	1	0	1	0	1	0	1	0	1
$N, mod\,5$	0	1	2	3	4	0	1	2	3	4

So if we know $N, mod\,2$ and $N, mod\,5$ we can find $N, mod\,10$

for example, if $N=0, mod\,2$ and $N=3, mod\,5$ then $N=8, mod\,10$

Example

Find the last digit of 13^{270}

mod 2

13^{270} is odd so $13^{270}=1, mod\,2$

mod 5

a) $13=3, mod\,5$ so $13^{270}=3^{270}, mod\,5$

b) $270=2, mod\,4$ so $3^{270}=3^2=9=4, mod\,5$

iii) Now $13^{270}=1, mod\,2$ and $13^{270}=4, mod\,5$ so from the table $13^{270}=9, mod\,10$

So the last digit of 13^{270} is 9

In 1640, Fermat announced FLT. In1978, Rivest, Shamir and Adleman announced the RSA encryption system. RSA encryption relies on FLT. It has many applications. For example, if enables us to buy stuff online.

See chapter: Encryption

see Exercise

Another proof of FLT

Show that

$(a+b)^7-(a^7+b^7)$ is a multiple of 7

Show that

$(a+b+c)^7-(a^7+b^7+c^7)$ is a multiple of 7

Show that

$(a+b+c+d+...)^7-(a^7+b^7+c^7+d^7+...)$ is a multiple of 7

If there are n numbers $a,b,c,d\ldots$ and we set them all equal to 1 then

n^7-n is a multiple of 7

etc

Yet another proof of FLT

Take any number from $1,2,3,4,5,6$ and write down its first six multiples

for example, take the number 3

$1\times3=3,mod7$ $2\times3=6,mod7$ $3\times3=2,mod7$

$4\times3=5,mod7$ $5\times3=1,mod7$ $6\times3=4,mod7$

These multiples are just $1,2,3,4,5,6$ in a different order.

Hint: If $n\times3=m\times3$ then $n=m$ Why?

So $(1\times3)\times(2\times3)\times(3\times3)\times(4\times3)\times(5\times3)\times(6\times3)=1\times2\times3\times4\times5\times6$

So $1\times2\times3\times4\times5\times6\times3^6=1\times2\times3\times4\times5\times6$

$3^6=1,mod7$

etc

EXERCISE

1) Show that:

n^5-n is a multiple of 10 for $n=1,2,3,\ldots$

2) Find:

$7465^5,mod7$

3) Find:

$18^{163},mod41$

4) Find the last digit of:

8^{154}

SOLUTIONS

1) 10 is not prime so we cannot use FLT directly, but ...

$n^5 - n$ is a multiple of 5 by FLT

If n is even then $n^5 - n$ is a multiple of 2

If n is odd then $n^5 - n$ is a multiple of 2

Either way $n^5 - n$ is a multiple of 2 and a multiple of 5 and hence a multiple of 10.

2) $7465 = 3, mod\, 7$ so $7465^5 = 3^5 = 243 = 5, mod\, 7$

3) $163 = 3, mod\, 40$ so $18^{163} = 18^3 = 5832 = 10, mod\, 41$

4)

i) mod 2

a) 8^{154} is even so $8^{154} = 0, mod\, 2$

ii) mod 5

a) $8 = 3, mod\, 5$ so $8^{154} = 3^{154}, mod\, 5$

b) $154 = 2, mod\, 4$ so $3^{154} = 3^2 = 9 = 4, mod\, 5$

iii) from the table

$8^{154} = 4, mod\, 10$ so the last digit of 8^{154} is 4