Fermat and Euler's Theorems

theorem

Fermat's Theorem is often called Fermat's "little" Theorem to distinguish it from his more famous "Last" theorem.

The theorem says that for any prime number p and any integer $1 < a < n$

$$a^p \bmod p = a$$

Two equivalent statements are

$$a^{p-1} \bmod p = 1$$

$$(a^p - a) \bmod p = 0$$

The second statement is what we use in analyzing the RSA method, and the third is used in the combinatorial proof of the theorem.

Examples:

```
2^3 mod 3 =   8 mod 3 = 2
2^5 mod 5 =  32 mod 5 = 2
3^5 mod 5 = 243 mod 5 = 3
```

Consider $p = 7$

```
1^6        1 mod 7 = 1
2^6 =     64 mod 7 = 1
3^6 =    729 mod 7 = 1
```

```
4^6 =  4096 mod 7 = 1
5^6 = 15625 mod 7 = 1
6^6 = 46656 mod 7 = 1
```

Here is a table from Laws of Cryptography for $p = 13$, which computes such powers more efficiently (by computing mod p at each step).

p	a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
13	2	***2***	***4***	***8***	***3***	***6***	***12***	***11***	***9***	***5***	***10***	***7***	***1***
13	3	***3***	***9***	***1***	3	9	1	3	9	1	3	9	1
13	4	***4***	***3***	***12***	***9***	***10***	***1***	4	3	12	9	10	1
13	5	***5***	***12***	***8***	***1***	5	12	8	1	5	12	8	1
13	6	***6***	***10***	***8***	***9***	***2***	***12***	***7***	***3***	***5***	***4***	***11***	***1***
13	7	***7***	***10***	***5***	***9***	***11***	***12***	***6***	***3***	***8***	***4***	***2***	***1***
13	8	***8***	***12***	***5***	***1***	8	12	5	1	8	12	5	1
13	9	***9***	***3***	***1***	9	3	1	9	3	1	9	3	1
13	10	***10***	***9***	***12***	***3***	***4***	***1***	10	9	12	3	4	1
13	11	***11***	***4***	***5***	***3***	***7***	***12***	***2***	***9***	***8***	***10***	***6***	***1***
13	12	***12***	***1***	12	1	12	1	12	1	12	1	12	1

Table 1.4 Fermat's Theorem for $p = 13$.

`www.cs.utsa.edu/~wagner/lawsbookcolor/laws.pdf`

Let's do the calculation for $a = 7, p = 13$:

```
7**1  =                 7
7**2  = 49 - 3(13)  = 10
7**3  = 70 - 5(13)  =  5
7**4  = 35 - 2(13)  =  9
7**5  = 63 - 4(13)  = 11
7**6  = 77 - 5(13)  = 12
7**7  = 84 - 6(13)  =  6
```

```
7**8  = 42 - 3(13) =  3
7**9  = 21 - 1(13) =  8
7**10 = 56 - 4(13) =  4
7**11 = 28 - 2(13) =  2
7**12 = 14 - 1(13) =  1
```

As the theorem says, we cycle around to $7^{12} \bmod 13 = 1$. The number 7 is called a *generator* because its powers generate all the values in the field Z_{13}.

$2, 6$ and 11 are also generators for Z_{13}.

Other values for a have shorter repeats (2, 3, 4 or 6 long). The lengths of such runs must be divisors of 12 so that they can cycle around after 12 rounds.

proofs of Fermat's Theorem

Fermat didn't actually prove his theorem. Euler proved something more general, the theorem we introduce below, and Fermat is a specific case of that.

There is a beautiful combinatorial proof called the "necklace proof". Here is a write-up:

`http://scienceblogs.com/evolutionblog/2010/04/15/a-combinatorial-proof-of-ferma/`

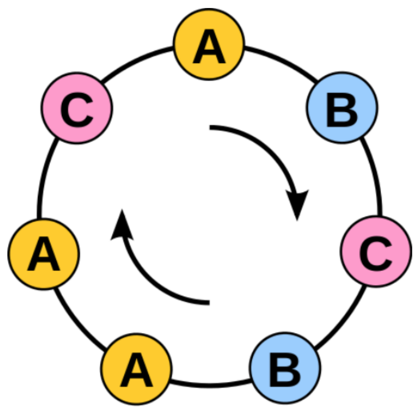
combinatorial proof

We construct a necklace of p beads, choosing from a different colors. We start by threading beads onto a linear piece of string.

Since we can choose any one of a colors, p times, there are a^p possible sequences.

However, we wish to exclude arrangements where all the beads have the same color There are a of these and so the number of arrangements is $a^p - a$.

Now, join the ends of the string. As a cycle, each shifted sequence becomes indistinguishable from the others. There are p such cyclic shifts for each linear arrangement. For example, any cyclic permutation of $ABCBAAC$ looks the same:



Therefore, the total number of arrangements is reduced by a factor of p.

$$n = \frac{a^p - a}{p}$$

The key observation is that n, the number of different arrangements, is clearly an integer. So we have that

$$a^p - a = np$$

If we take the modulus of both sides (mod p) we have the result we seek.

$$(a^p - a) \bmod p = 0$$

□

proof by induction

This proof is just as simple. We claim that

$$a^p \bmod p = a$$

The base case is $1^p \bmod p = 1$, which is obviously true.

The binomial theorem gives this expansion for

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$$

All terms on the right-hand side except the first and last have p as a factor, so mod p each is just zero. We have

$$(a+1)^p \bmod p = (a^p + 1) \bmod p$$

For the inductive step, we may assume that $a^p \bmod p = a$, so this becomes

$$(a+1)^p \bmod p = (a+1) \bmod p$$

which completes the proof.

□

consequence

A consequence of this theorem is that the sequence $a^1,\ a^2,\ a^3 \ldots a^{p-1}$ repeats, so the sequence $a^p, a^{p+1} \ldots a^{2p-1}$ consists of exactly the same values.

As the source says:

Because a to a power x mod p always starts repeating after the power reaches $p-1$, one can reduce the power mod $p-1$ and still get the same answer."

Thus no matter how big the power x in

$$a^x \bmod p$$

then let

$$y = x \bmod (p-1)$$

and so

$$a^x \bmod p = a^y \bmod p$$

For example, mod 13:

$$a^{29} \bmod 13 = a^{29 \bmod 12} \bmod 13$$

$$= a^5 \bmod 13$$

Of course, it is possible that the sequence may repeat even more quickly, as we saw with the table above.

Euler

Euler's totient function $\phi(n)$ is defined like so:

$$\phi(n) = n \prod (1 - \frac{1}{p_i})$$

where the p_i are the prime factors of n.

For a prime number p, this is just $\phi = p - 1$.

For a product of primes pq, $\phi(p,q) = (p-1)(q-1) = \phi(p)\ \phi(q)$.

For three factors, $n = pqr$:

$$\phi(n) = \phi(p)\ \phi(q)\ \phi(r)$$

In number theory, ϕ gives the count of the positive integers up to a given integer n that are relatively prime to n, where the only common factor is 1. In fact, for the factorization $n = pq$, p and q need be only *relatively prime.*

Examples:

```
 n  co-prime     phi
 4 1,3           2
 6 1,5           1 x 2 = 2
 8 1,3,5,7
10 1,3,7,9       1 x 4 = 4
12 1,5,7,11      ?
```

We need a rule for when the prime factor is repeated. That rule is

$$\phi(p^a) = p^a - p^{a-1}$$

So for the table above

$$\phi(4) = 2^2 - 2^1 = 2$$

$$\phi(8) = 2^3 - 2^2 = 4$$

$$\phi(12) = \phi(3)\phi(4) = 2(2^2 - 2^1) = 4$$

And in general:

$$n = p \cdot q^2 \cdot r^3$$

$$\phi(n) = (p^1 - p^0)(q^2 - q^1)(r^3 - r^2)$$

theorem

Relevant to the study of cryptography, Euler's Theorem says that for an integer $1 < a < p$:

$$a^{\phi(n)} \bmod n = 1$$

As we said above, if n is prime the formula for ϕ reduces to

$$\phi(n) = n - 1$$

so then

$$a^{n-1} \bmod n = 1$$

Fermat's Theorem is thus seen to be a special case of Euler's Theorem, when n is prime.

We will not prove Euler's formula. See Chapter 3 of this wonderful book for more about $\phi(n)$.

`https://www.whitman.edu/mathematics/higher_math_online/`

cryptography

Here we are particularly interested in the situation where n has two large prime factors p and q and then:

$$\phi(n) = pq\ (1 - \frac{1}{p})(1 - \frac{1}{q}) = (p-1)(q-1)$$

Furthermore, we have defined encryption followed by decryption in public key cryptography as $m^{ed} \bmod n = m$. We would like to show that this follows as a consequence of our definitions.

From now on, we write ϕ for $\phi(n)$. Recall that d is defined to be the multiplicative inverse of e mod ϕ.

Write out what's given:

$$\phi = (p-1)(q-1)$$

$$m^{\phi} \bmod n = 1$$

$$ed \bmod \phi = 1$$

Our chained encryption/decryption is $(m^e)^d \bmod n$ or:

$$m^{ed} \bmod n$$

My source says: "similar to Fermat's Theorem, arithmetic in the exponent is taken mod ϕ."

The idea is that since

$$m^{\phi} \bmod n = 1$$

if we are computing any *other* power of m, say ed, we need only compute to the power of ed mod ϕ, because beyond that, the sequence just repeats.

We saw the repetition for Fermat's Theorem; it happens here as well, even though n is not prime. However, it is required that m be coprime to n.

As a counter-example, take $n = 6 = 2 * 3$. Then $\phi = 2$.

Now, $5^2 = 25 = 1 \bmod 6$.

But $4^2 = 16 \bmod 6 = 4$. Thus, 4 to *any* power mod 6 is 4!. The difference is that 4 is not coprime to 6, but 5 is.

For the big example, we have m to the power ed and then mod pq, and we reduce the power to be ed mod ϕ since $\phi = (p-1)(q-1)$.

(Assuming m has no common divisors with n):

$$m^{ed} \bmod n = m^{ed} \bmod pq$$

$$= m^{ed \bmod \phi} \bmod pq$$

But of course $ed \bmod \phi = 1$ so this is just m.

Furthermore, $m^{ed} = m^{de}$, hence the ability to encrypt first with the private key and then decrypt with the public one.