Euler's Theorem Proof

Start with a set of values from to 1 to n, where each value does NOT share a common factor with n. Thus, the set has $\phi(n)$ values in it.

Example: n = 15, S = {1,2,4,7,8,11,13,14}

Pick any a such that gcd(a, n) = 1. Let a = 7

T = {7, 14, 28, 49, 56, 77, 91, 98} (all values in S multiplied by a)

= {7, 14, 13, 4, 11, 2, 1, 8}

S = { a_1, $a_{2, ..., a_{\phi(n)}}$}

T = { aa_1, $aa_{2, ..., aa_{\phi(n)}}$}

We want to prove that the values in the set T are all equivalent to the values in the set S mod n.

Since gcd(a, n) = 1 and gcd(a_i, n) = 1, gcd(aa_i, n) = 1, for any of the a_i.

So, all the values in the set T have gcd 1 with n. We know that there are phi(n) unique values that could be in the set T, reduced mod n, so S and T are equivalent if and only if all the values in T are unique mod n.

We will prove that all the values in the set T are unique mod n via proof by contradiction.

Assume to the contrary that there are two items in T that are equivalent mod n. Let these items be aa_i and aa_j,where a_i != a_j mod n.

$$aa_i \equiv aa_j (mod\ n)$$

$$aa_i - aa_j \equiv 0 (mod\ n)$$

$$a(a_i - a_j) \equiv 0 (mod\ n)$$

Thus, n | (a)(a_i – a_j).

If gcd(a, b) = 1, and a | bc, then a | c.

Since gcd(a, n) = 1, and we know that n | (a a_i – a_j), it follows that n | (a_i – a_j). But the problem is that 1 <= a_i, a_j <= n-1, and 1 <= |a_i-a_j| <= n-2. But this contradicts the given info that n | (a_i – a_j). Since we've reached a contradiction, it follows that our initial assumption was incorrect. But if no two values in the set T are equivalent mod n, that means they all unique mod n and that the sets S and T are equivalent, mod n.

Since the sets are equivalent mod n, the product of all the elements in both sets must be equivalent mod n:

$$\prod_{i=1}^{\phi(n)} aa_i \equiv \prod_{i=1}^{\phi(n)} a_i\ (mod\ n)$$

$$\prod_{i=1}^{\phi(n)} aa_i - \prod_{i=1}^{\phi(n)} a_i \equiv 0(mod\ n)$$

$$[\prod_{i=1}^{\phi(n)} a_i](a^{\phi(n)} - 1) \equiv 0(mod\ n)$$

Thus, $n|\left[(a^{\phi(n)} - 1)\prod_{i=1}^{\phi(n)} a_i\right]$

What do we know about the thing in yellow and its relationship to n? GCD(a_i, n) = 1, so what does this mean about gcd(n, $\prod_{i=1}^{\phi(n)} a_i$)??? THIS GCD IS 1!!!

If gcd(a, b) = 1 AND a | bc, then a | c.

Since **about gcd(n, $\prod_{i=1}^{\phi(n)} a_i$) = 1, it follows that** $n|\left[(a^{\phi(n)} - 1)\right]$.

$$a^{\phi(n)} - 1 \equiv 0\ (mod\ n)$$

$$a^{\phi(n)} \equiv 1\ (mod\ n)$$

What is the remainder when 30^{180} is divided by 77?

N = 77, phi(n) = phi(7 x 11) = (7-1)(11-1) = 6 x 10 = 60,

Gcd(30, 77) = 1, so Euler's theorem says $30^{60} \equiv 1$ mod 77

$30^{180} = (30^{60})^3 \equiv 1^3 \equiv 1$ (mod 77)

Let's say I asked for 30^{182} is divided by 77?

$30^{182} = (30^{60})^3(30^2) \equiv 1^3(900) \equiv 53$ (mod 77)

DISCRETE LOG PROBLEM

We know that for all primes p, and values a such that gcd(a, p) = 1, $a^{p-1} \equiv 1 \bmod p$.

Another interesting question is what happens as we exponentiate a mod p?

p = 17

a = 5

Power	0	1	2	3	4	5	6	7	8
Answer	1	5	8	6	13	14	2	10	16

Power	9	10	11	12	13	14	15	16
Answer	12	9	11	4	3	15	7	1

Each number, from 1 to p-1 appears exactly once. But, the order of the values looks pretty random.

In regular mathematics, a logarithm is the inverse function of the exponent, so in regular math when I ask you what is $\log_2 64$, I am asking you the question, what is x such that $2^x = 64$?

For integer mathematics, we can ask a similar question. I can ask, what is the discrete log base 5 of 3, mod 17? So this really means, what is the value of x such that $5^x \equiv 3 \pmod{17}$?

It turns out that no one knows how to solve this problem quickly!!!

A LOT OF THE SECURITY OF PUBLIC KEY CRYPTO IS BASED ON THE FACT THAT THIS PROBLEM IS DIFFICULT TO SOVLE QUICKLY!!!

(Note: RSA encryption's security is based on the fact that we don't know how to factor an integer quickly…)

Almost always, these things represent what we call one way functions…these are functions that are easy to calculate forward, but hard to calculate backwards. So, it's easy for me to calculate a^x mod p. But if you give me the value of a^x mod p, it's hard for to to figure out what x is. It's easy to multiply two numbers a and b. But if you give me the product ab, it's hard for me to figure out what a and b are.

What happened with 5 mod 17 isn't always going to happen. Consider a = 2 for p = 17:

p = 17

a = 2

Power	0	1	2	3	4	5	6	7	8
Answer	1	2	4	8	16	15	13	9	1

Power	9	10	11	12	13	14	15	16
Answer	2	4	8	16	15	13	9	1

Notice that this repeats faster and not every number from 1 to 16 shows up in yellow!!!

There is a special name given to values of a such that when you raise a to each power up to p-1, you get each integer from 1 to p-1 exactly once. That name is a “primitive root”, also, I will call it a generator.

So, 5 is a primitive root mod 17 and is a generator mod 17, because when you take 5 and raise it to each power upto 16, you get each integer from 1 to 16 exactly once.

What is the period for a = 2? (How long before the list of exponent answers repeats) 8

Why does 8 make a lot more sense for the period than 9?

ALL CYCLE LENGTHS WHEN EXPONENTIATING AN ARBITRARY A (MOD P) MUST DIVIDE EVENLY INTO P-1.