Number Theory Notes

Ernesto Diaz

October 21, 23 2019

DATE October 21, 2019

Euler's Theorem Says that $a^{\varphi(n)} \equiv$1 (mod n) so this equation has a solution if b is the smallest positive integer such that $a^b \equiv 1$ (mod n) we call b the (multiplicative) order of a (mod m) write this as $ord_m(a) = b$ the book calls this a belongs to the exponent b(mod m)

Definition: if $ord_m(a) = b$ we call a a primitive root mod m.

Example: Consider powers of 3(mod 10),

$$3^1 \equiv 3(mod10)$$
$$3^2 \equiv 9(mod10)$$
$$3^3 \equiv 27 \equiv 7(mod10)$$
$$3^4 \equiv 81 \equiv 1(mod10)$$

So $ord_{10}(3) = 4 = \varphi(10)$, 3 is a primitive root (mod 10).

Theorem: If $ord_m(a) = b$ and $a^r \equiv 1$(modn) then $n \mid r$.

Proof: Suppose it didn't ($n \nmid r$) us division with remainder to write r=qb+s where $0 \leq s \leq b$, q has to be at least 1 sonce q=0 $\Rightarrow r < h$ $1 \equiv a^r \equiv a^{qb+s} \equiv (a^{qb})a^s \equiv (1)a^s$(modn) so $a^s \equiv$(mod n) since s¡h this contradicts $ord_m(a) = b$

Theorem: If g is a primitive root (mod n) they $g^1, g^2, \ldots, g^{\varphi(m)}$ is reduced residue system (mod n).

Proof:

Proof. Any reduced residue system (mod m) has size $\varphi(m)$ so it suffices to show $g^i \not\equiv g^j$(mod m) if 1$\leq i < j \leq \varphi(m)$

Suppose for contradiction $g^i \equiv g^j$(mod m) $1 \leq i < j \leq \varphi(m)$ this means $m \mid (g^j - g^i)$, $g^j - g^i = g^i(g^{j-i} - 1)$, so $m \mid g^i(g^{j-i} - 1)$, gcd(m,g^i)=1 since g is a primitive root (mod n). so $m \mid (g^{j-i} - 1) \iff g^{j-i} \equiv 1$ (mod n). $1 \leq j - i < \varphi(m)$

This contradicts g being a primitive root since $ord_m(g) \leq j - i < \varphi(m)$ $\square$

Theorem: if $ord_m(a) =$ h and gcd(h,k)=d then $ord_m(a^k)$=h/k

Example: $ord_{10}(3) = \varphi = 4$, k = 2, gcd(4,2) = 2, $ord_{10}(9) = ord_{10}(3^2) = ord_{10}(3^k) = 2 = 4/2$.

Proof. Call $h_1 =$ h/d and $k_1 =$ k/d.

Our goal is to get $ord_m(a^k) = h_1$

suppose $ord_m(a^k) =$ j, this means $a^{kj} = (a^k)^j \equiv 1$ (mod n)

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

by out first theorem $h \mid kj \iff$ hq = kj $\iff$ dh_1q = dk_1j $\iff$ h_1q = k_1j $\iff$ so $h_1 \mid k_1 j$. Since gcd(h_1, k_1 =1, so $h_1 \mid j$.
Now consider $(a^k)^{h_1} \equiv a^{kh_1} \equiv (a^{h_1 dk_1}) \equiv (a^{hk_1}) \equiv (a^h)^{k_1} \equiv (1)^{k_1}$ (mod m).
So $j \mid h_1$. This tells us that j = h_1 = h/d $\square$

Corollary: If g is a primitive root (mod m), then g^k is a primitive root mod(m) if and only if gcd(k,φ)=1.
Example : m=10, 3 is a primitive root φ(10)= 4, gcd(3,4) =1 so $3^3 \equiv$ 7(mod 10) is also a primitive root,

$$\begin{aligned}
7^1 &\equiv 7(mod 10) \\
7^2 &\equiv 49 \equiv 9(mod 10) \\
7^3 &\equiv 63 \equiv 3(mod 10) \\
7^4 &\equiv 21 \equiv 1(mod 10)
\end{aligned}$$

Corollary: If g is a primitive root(mod m) then g^{-1} is alos a primitive root (mod m)
Theorem: if m has at least one primitive root g then it has exactly $\varphi(\varphi(m))$ many distinct primitive roots.

Proof. Since g is a primitive root $g^1, g^2, \ldots, g^{\varphi(m)}$ form a reduced residue system, so every primitive root is one of these numbers.
g^i is a primitive root if and only if gcd(i,φ=1. count the number of i$\in$ $1, 2, \ldots, \varphi(m)$ with gcd(i,φ=1 this count is $\varphi(\varphi(m))$ $\square$

Example: $\varphi(\varphi(10)) = \varphi(4)) = \varphi(2^2) = 2$, 10 has 2 primitive roots 3 and 7.

DATE October 23, 2019

Theorem: if p is prime then there exists a primitive root (mod p). Note: This means that some a(mod p) has $ord_p(a) = \varphi$(p) = p-1.

By our theorem there are $\varphi(\varphi(m))$ many primitive roots. Recall that the order of any element will divide p-1 since $a^{p-1} \equiv$ 1(mod p) (Fermat's little theorem).

if $ord_p(a) =$ r, then $r \mid p$ for each $h \mid p-1$, let N(h) = {1$\leq a \leq p \mid ord_p(a) = h$}

Example: p=7

a	1	2	3	4	5	6
$ord_p(a)$	1	3	6	3	6	2

$\sum_{i=1}^{\infty} N(h) =$ p - 1

Claim: N(h) is either 0 or φ(h)

If no element has order h then N(h)=0

so suppose at least one element a(mod p) has $ord_p(a) = h$

consider rots of $x^n - 1 \equiv$0 (mod p) $\iff$ $x^n \equiv$ 1(mod p)

this has at most h (distinct) roots (mod p) by Lagrange's Theorem, $a^1, a^2, \ldots, a^h$ are all roots of this equation.

pick one a^i, plug it in $(a^i)^n - 1 \equiv (a^n)^i - 1 \equiv 1^i$ -1 (mod p)

these are all distinct so all of the elements with order h(mod p) are contained in $\{a^1, a^2, \ldots, a^h\}$

Recall: The order of a^i is h/gcd(i,h) since the order of a is h.

so we need ot count i $\in \{1, 2, \ldots, h\}$ with gcd(i,h) = 1

this is φ(n) by definition.

N(h) =

$$\begin{cases} 0 & \text{Nothing has order h} \\ \varphi(n) & \text{Something has order h} \end{cases}$$

N(h) $\leq \varphi(n)$

p-1 = $\sum_{h|p-1} N(h) \leq \sum_{h|p-1} \varphi(h)$

Recall: $\sum_{d|n} \varphi(n) =$ n

Since both sides of this inequality are p-1 we must have N(h) = φ(h) for all h. So N(p-1) = $\varphi(p-1) \geq 1$.

Since N(p-1) ¿ 0, there exists an element with order p-1 which is a primitive root by definition

Proof Complete.

How many primes are there?

One Answer: Infinitely Many! proved by Euclid.

Proof. Suppose there is a finite list of primes $p_1, p_2, \ldots, p_k$, where p_k us the last one.
Compute N=$p_1 * p_2 * \cdots * p_k$
Product of all primes.
what are the prime factors of N+1?
This number can't be divisible by any of $p_1, p_2, \ldots, p_k$, so it is either prime or divisible by a prime not in our list. $\square$

Note: if $p_1 * p_2 * \cdots * p_k$, are the first k primes it isn't necessarily true that $(p_1 * p_2 * \cdots * p_k)$+1 is a prime.
Define: π(x) = the number of primes less than or equal to x.
Example $\pi(10) = 4$, $\pi(11) = 5$, $\pi(12) = 5$
Theorem:

$$\lim_{x \to \infty} \varphi(x) = \infty$$

Proof: Proof for this is the same proof as Euclid's proof above.