Primitive Roots,Order,Quadratic Residue

Mathmdmb

March 30, 2011

1 About This Note and Notations

In this note,I am going to discuss some facts related to order,primitive root and quadratic residue along with Legendre symbol and Jacobi symbol.We shall first see some basic ideas,and then work on them a bit.All notations I have used are usual,but I have introduced a new notation(probably),as described later(for denoting primitive roots).First let's see some definitions we need.Also if the modulo is not mentioned anywhere,there it is to be considered that the modulo remains same, otherwise the modulo is stated.
Before starting the note,I must remember some of my AoPS friends-amparvardi(Amir Hossein Parvardi),al-mahed(Al-Mahed) and Moonmathpi496(Tarik Adnan Moon) for their and directions to let me know how to create a pdf and comments for improving its structure.When I completed the task os source code,I found the output pdf incomplete,but I just got stuck.I didn't understand why it happened.Later fedja informed me about my typo mistake in putting curly braces.So,I also remember and thank him for letting me know where my mistake was and edit it to finish the pdf.
Here goes some notations I used.
$\star$ $a|b \rightarrow a$ divides b.Alternatively b leaves remainder 0 upon division by a.
$\star$ $a \not| b \rightarrow a$ does not divide b.
$\star$ $a \equiv b \pmod n \rightarrow a$ and b gives the same remainder upon division by n.
$\star$ $\varphi(m) \rightarrow$ Euler's toteint function of m.
$\star$ $gcd(a, b) \rightarrow$the greatest common divisor of a and b.
$\star$ $lcm(a, b) \rightarrow$the least common multiple or the smallest positive integer divisible by a and b.
$\star$ $p \rightarrow$prime.
$\star$ $pr_m = g \rightarrow g$ is a primitive root of m.
$\star$ $h \neq pr_m \rightarrow h$ is never a primitive root of m.
$\star$ $ord_m(a) = x \rightarrow x$ is the order of a modulo m.
$\star$ $qr \rightarrow$ quadratic residue.
$\star$ $qnr \rightarrow$quadratic non-residue.
$\star$ $U_m = \{r_1, r_2, ..., r_{\varphi(m)}\} \rightarrow$ the set of units modulo m,or $r_1, r_2, ..., r_{\varphi(m)}$ are numbers less than m and co-prime to m.
$\star$ $P_{U_m} \rightarrow$the product of the elements of U_m.

2 Definitions

Euler's Toteint Function:
Euler's Toteint Function $\varphi(m)$ is the number of numbers less than or equal to m and co-prime to m.That is,$\varphi(m)$ is the number of elements x in the set $\{1, 2, ..., m\}$ for which $gcd(m, x) = 1$.
$m = 6$,in the set $\{1, 2, 3, 4, 5, 6\}$ there are two elements co-prime to m,namely $1, 5$.
It is obvious to see that for $m = p$ a **prime**,$\varphi(p) = p-1$ since every element less than p is co-prime to p.If $m > 1$,this set does not include the element m because then $gcd(m, m) > 1$.Also for $m > 2, \varphi(m)$ is even.This can be shown by **Euclidean Algorithm.**If $gcd(m, a) = 1$ then $gcd(m, m-a) = 1$ too,so the number of elements co-prime to m must be even.We shall use few well-known facts about $\varphi(m), \varphi(m)$ is **multiplicative**,that is, if $gcd(m, n) = 1, \varphi(mn) = \varphi(m)\varphi(n)$, $\varphi(p^a) = p^{a-1}(p-1)$ where p is a prime.And if $gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod m$.
Definition Of Order:
If x is the smallest positive integer such that $a^x \equiv 1 \pmod m$ then x is called the **order** of a modulo m and it is denoted by $ord_m(a) = x$.
Example. $ord_8(3) = 2$.
Definition Of Primitive Root:
If g is a positive integer such that $ord_m(g) = \varphi(m)$ then g is called a **primitive root modulo** m.Let's agree to denote it as $pr_m = g$
Note. This does not mean that there exists a unique pr of m.(Well,then how many are there?)
Definition Of Quadratic Residue:
If $x^2 \equiv a \pmod m$ for some x,then a is called a **quadratic residue** of m and we shortly say a is a **qr** of m,otherwise a is a **quadratic non-residue** of m and say it a is a **qnr** of m shortly.
Example. $2^2 \equiv -1 \pmod 5$,so -1 is a qr of 5.
Definition Of Legendre Symbol:
The Legendre symbol for a positive integer a and a prime $p$is denoted by $(\frac{a}{p})$ and defined as:
⋆ $(\frac{a}{p}) = 0$ if $p|a$
⋆ $(\frac{a}{p}) = 1$ if a is a qr of p
⋆ $(\frac{a}{p}) = -1$ if a is a qnr of p
Properties Of Legendre Symbol:
$P_1 : a \equiv b \Longrightarrow (\frac{a}{n}) = (\frac{b}{n})$
$\mathrm{P}_2 : (\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p$
If $p|a$,it is trivial.Again it is trivial for $p = 2$ too.So, consider $p \not| a, p > 2$ odd.From Fermat's little theorem,we know that if $p \not| a, a^{p-1} \equiv 1 \pmod p$.Take square root on both sides(we can do this as we described before).
Now if $a \equiv x^2$ for some x then $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$
Thus the property holds.This property is called **Euler's Criterion**.
A special case:$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.So $(\frac{-1}{p}) = -1$ if $p \equiv 3 \pmod 4$, 1 otherwise.

P_3.For a prime p,there is exactly $\frac{p-1}{2}$ qr's namely $1^2, ...(\frac{p-1}{2})^2$
P_4.Legendre symbol is multiplicative,that is $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ for all integers a, b and $p > 2$.
P_5.$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
(We are not proving this here.You may read from google or wikipedia for details on the facts I have used here.) Thus $(\frac{2}{p}) = 1$ if $p \equiv \pm 1 \pmod 8$,-1 if $p \equiv \pm 3 \pmod 8$

Definition Of Jacobi Symbol:
Jacobi Symbol is the generalization of Legendre symbol,it is defined for all odd $n > 1$.Thus it becomes Legendre symbol when m is a prime.
$\star$ $(\frac{a}{n}) = 0$ if $gcd(a, n) \neq 1$
$\star$ $(\frac{a}{n}) = \pm 1$ if $gcd(a, n) = 1$.
$\star$ $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$,so $(\frac{a^2}{n}) = 1$ or 0.
$\star$ $(\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})$,so $(\frac{a}{n}) = 1$ or 0.
$\star$ $(\frac{-1}{n}) = 1$ if $n \equiv 1 \pmod 4$,-1 otherwise.

Definition Of Perfect Power In Congruence:
An integer a is called a pefect $k-th$ power of m iff $a^{\frac{\phi(m)}{gcd(\phi(m),k)}} \equiv 1 \pmod m$.

3 Lemmas and Theorems

Lemma 1::
Let $pr_m = g$,then $g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod m$
Proof:
We may let $m > 2$.Now $g^{\varphi(m)} \equiv 1 \pmod m$.So either g$^{\frac{\varphi(m)}{2}} \equiv -1$ or 1 $\pmod m$.Otherwise m would divide their difference 2,but $m > 2$ as we said.Also $\varphi(m) \geq 2$ is even.Then in the second case,$\frac{\varphi(m)}{2}$ would be a smaller number than $\varphi(m)$ for which $g^{\frac{\phi(m)}{2}} \equiv 1 \pmod m$,contradicting the minimality of $\phi(m)$.Hence,from the definition,$g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod m$
Corollary:
If $g^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m, g \neq pr_m$ or m does not have a primitive root.
Generalization Of The Corollary: If $d > 1$ is a divisor of $\varphi(m)$,such that $a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod m$,then m does not have a primitive root.
Lemma 2::
For every r_i,there exists a unique r_j such that $r_i r_j \equiv a \pmod m$ where a is a qnr of m and $gcd(a, m) = 1$.
Proof:
Of-course $i \neq j$,otherwise $r_i^2 \equiv a \pmod m$ which would imply that a is a qr of m.
Also if $r_i r_j = mq + a, 0 < a < m$.Now r_i, r_j both does not share any common factor other than 1 with m,so does $r_i r_j$ too.Then we get
$gcd(r_i r_j, m) = 1 \Longrightarrow gcd(m, mq + a) = 1 \Longrightarrow gcd(m, a) = 1$.
This means that the remainder of $r_i r_j$ when divided by m lies in the set U_m,that is a is co-prime to m and a qnr of m.Now let's prove that this r_j is unique.
If $r_i \equiv r_j \pmod m, 1 \leq i, j \leq \varphi(m)$,then $m|r_i - r_j$ but $|r_i - r_j| < m$,contradiction.
Corollary:
For $1 \leq k \leq \varphi(m)$,$\{r_k r_1, r_k r_2, ..., r_k r_{\varphi(m)}\}$ is a reduced system of m.
Indeed.
If $r_k r_i \equiv r_k r_j \pmod m$,we have $r_i \equiv r_j \pmod m$.Since $gcd(m, r_k) = 1$ we can divide the congruence relation by r_k.But this yields a contradiction.
So the claim is true.
Lemma 3::
If $pr_m = g$,then $\{g, g^2, ..., g^{\varphi(m)}\}$ is a reduced system of m
Proof:
If $g^i \equiv g^j$ then $g^{j-i} \equiv 1$,since $gcd(m, g) = 1$.But $|j - i| < \varphi(m)$.Contradiction!
Corollary:
$\{1, g, g^2, ..., g^{\varphi(m)-1}\}$ is a reduced system of m.
Lemma 4::
If $ord_m(g) = d$ and $g^n \equiv 1, d|n$
Proof:
Let $n = dq + r, 0 \leq r < d$.we get $g^n \equiv g^{dq+r} \equiv (g^d)^q.g^r \equiv g^r \equiv 1$ but $g^d \equiv 1$ with d smallest where $r < d$.So we must have $r = 0$.
Corollary 1::
If $ord_m(a) = d, d|\varphi(m)$.

Corollary 2::
$\{a, a^2, ..., a^d\}$ is a reduced system of m.
That is,we can use g as a generator of m to produce all the numbers $r_1, r_2, ..., r_{\varphi(m)}$ which are co-prime to m.
Now let's see a theorem.we shall proceed on this theorem later.
Theorem:
The product of the elements of U_m gives remainder -1 upon division by m if m has a primitive root.
Proof:
Let $pr_m = g$,then g is a generator of m with order $\varphi(m)$.Hence,g^i is congruent to exactly one of r_i.Then

$g.g^2...g^{\varphi(m)} \equiv r_1 r_2 ... r_{\varphi(m)}$
$\Longrightarrow r_1...r_{\varphi(m)} \equiv g^{\frac{\varphi(m)(\varphi(m)+1)}{2}}$
$\Longrightarrow r_1...r_{\varphi(m)} \equiv \{g^{\frac{\varphi(m)}{2}}\}^{\varphi(m)+1}$
Now since $\varphi(m)$ even,$\varphi(m)+1$ is odd.So using lemma 1,we get
$r_1...r_{\varphi(m)} \equiv (-1)^{\frac{\varphi(m)}{2}+1} \equiv -1 \pmod m$
Thus the theorem is proved.The converse is also true.
Theorem:
$P_{U_m} \equiv \pm 1 \pmod m$.
Proof:
According to lemma 3,there is a unique r_j for every r_i in U_m such that $\mathrm{r}_i r_j \equiv a$,$a$ is a co-prime qnr of m.Also for distinct i's we shall get distinct j's.Therefore,we may pair up all $\varphi(m)$ elements of U_m such that:
$r_1 r_2 ... r_{\varphi(m)} \equiv a.a...a(\frac{\varphi(m)}{2})$ times.Then $P_{U_m} \equiv \pm 1 \pmod m$.
Now from lemma 1,if there exists a $pr_m = g$,then $P_{U_m} \equiv -1$,else $P_{U_m} \equiv 1$.
Therefore,this is an **iff** theorem.
Corollary:
We know from Euclidean Algorithm that $gcd(a, m) = gcd(a, m-a)$.Also $gcd(m, 1) = gcd(m, m-1) = 1$
For this reason we can rearrange U_m in increasing order.Then obviously
$r_1 = 1, r_{\varphi(m)} = m-1, r_{\phi(m)-1} = m - r_2, ..., r_{\frac{\varphi(m)}{2}} + 1 = m - r_{\frac{\varphi(m)}{2}}$.
We note that $r_{\varphi(m)} \equiv -r_1, r_{\varphi(m)-1} \equiv -r_2, ...$
And P_{U_m} becomes $r_1 r_2 ... r_{\varphi(m)} r_{\frac{\varphi(m)}{2}+1} ... r_{\varphi(m)} \equiv a^{\frac{\varphi(m)}{2}}$ from which it follows that
$r_1 r_{\varphi(m)} r_2 . r_{\varphi(m)-1} .... r_{\frac{\varphi(m)}{2}} r_{\frac{\varphi(m)}{2}+1} \equiv (-1) r_1^2 . (-1) r_2^2 .... (-1) r^2_{\frac{\varphi(m)}{2}} \equiv a^{\frac{\varphi(m)}{2}}$

We shall make further progress on this,but before that we need some other lemmas.
Lemma 5::
If $k > 2, m = 2^k$ has no primitive root.
Proof:
Let $gcd(a, 2^k) = 1$,then a odd.We know that $a^2 \equiv 1 \pmod{2^3}$,or $2^3 | a^2 - 1$
So,using the identity $a^2 - b^2 = (a+b)(a-b)$ repeatedly,

$a^{2^{k-2}}-1=(a^{2^{k-3}}+1)(a^{2^{k-3}}-1)=(a^{2^{k-3}}+1)(a^{2^{k-4}}+1)....(a^2-1)$
We infer that $a^{2^{k-2}}\equiv 1 \pmod m \Longrightarrow a^{\frac{\varphi(2^k)}{2}}\equiv 1 \pmod{2^k}$ which shows that $m=2^k$ has no primitive roots.(Note that $2,4$ have primitive roots namely $1,3$ because in the identity above we needed $k-2>0$.)
Lemma 6:
$m=2^k l, l>1$ odd has no primitive roots.
Proof:
Let $gcd(a,m)=1$.Then from euler's function,$a^{2^{k-1}}\equiv 1 \pmod{2^k}, a^{\varphi(l)}\equiv 1 \pmod l$.
Note that from the identity $a-1|a^n-1$,we get that $a^{2^{k-1}}-1, a^{\phi(l)}-1|a^{lcm(2^{k-1},\varphi(l))}-1$
We conclude that $a^{lcm(2^{k-1},\phi(l))}\equiv 1 \pmod{2^k l}$
Now since $\varphi(l)$ even,so $gcd(2^{k-1},\varphi(l))=2^r$ for some natural n.Then applying the fact $ab=gcd(a,b).lcm(a,b)$ to the congruence above,we get that $a^{\frac{2^{k-1}\varphi(l)}{2^r}}\equiv 1 \Longrightarrow a^{\frac{\varphi(m)}{2}}\equiv 1 \pmod m$,(after raising to power r on both sides).
From the corollary of lemma 1,we can say that m does not possess a primitive root.And as a corollary,we get the following theorem:
Theorem:
The only values of m having primitive roots are $m=2,4,p^k,2p^k$ where p is an odd prime and k is a positive integer.
Corollary 1:
If $m=m_1m_2, gcd(m_1,m_2)=1$ with $m_1,m_2>2$ then m does not have any primitive root.
Corollary 2:
If m has two different prime factors than m has primitive root only for $m=2p^k$

Now let's get back to the corollary of the converse theorem we proved which stated that
$(-1)^{\frac{\varphi(m)}{2}}r_1^2r_2^2.....r_{\frac{\varphi(m)}{2}}^2\equiv a^{\frac{\varphi(m)}{2}} \pmod m$
.We consider $m>2$ has a primitive root,$m=p^k$ or $m=2p^k$
In both cases,if $p\equiv 1 \pmod 4$ then $\varphi(m)=p^{k-1}(p-1)$ which is divisible by 4 implying that $r_1^2r_2^2...r_{\frac{\varphi(m)}{2}}^2\equiv -1$
If $p\equiv 3 \pmod 4$, then $r_1^2r_2^2...r_{\frac{\varphi(m)}{2}}^2\equiv 1 \pmod m$
So, using Jacobi symbol in the previous result we find that if $m=p^k, p$ odd,then $r_1^2r_2^2...r_{\frac{\varphi(m)}{2}}^2\equiv -1 \pmod m$ when $(\frac{-1}{m})=1$.Else $r_1^2r_2^2...r_{\frac{\varphi(m)}{2}}^2\equiv 1$.
If $m\equiv 1 \pmod 4$,then $r_1^2r_2^2...r_{\frac{\varphi(m)}{2}}^2\equiv -1 \Longrightarrow i\equiv r_1r_2...r_{\frac{\varphi(m)}{2}} \pmod m$ where $i^2\equiv -1 \pmod m$.
Also,$r_1^2r_2^2...r_{\frac{\varphi(m)}{2}}^2\equiv -1\equiv r_1r_2...r_{\varphi(m)}\Longrightarrow r_1r_2...r_{\frac{\varphi(m)}{2}}\equiv r_{\frac{\varphi(m)}{2}+1}.....r_{\phi(m)}\equiv i \pmod m$
In other words if $r_1,r_2,....,r_{p^{k-1}(p-1)}$ are positive integers such that no r_i have a prime factor p,then $p^k|r_{\frac{p^{k-1}(p-1)}{2}+1}....r_{p^{k-1}(p-1)}-r_1r_2..r_{\frac{p^{k-1}(p-1)}{2}}$
Special Case: When $k=1$,we get $r_i=i$ for $1\le i\le\varphi(p)=p-1$ and then

$p|(p-1)....\frac{p+1}{2} - 1.2....\frac{p-1}{2}$.
So let $p = 2k+1$,it becomes $p|\frac{(p-1)!}{k!} - k!$.
You can work on it more yourself and develop these properties further.

4 Some Congruences On Primes

In this section,we shall basically see whether a particular number can be the primitive root or not of a prime.Also is an integer is a perfect power modulo p.Let's consider $1 < a < p-1$ in all cases.The modulo p will be taken throughout the whole section if not stated,otherwise the modulo is stated everywhere.
Claim 1:
If $p \equiv 1 \pmod 4$,then $a^a \equiv 1 \pmod p$ has at least one solution.
Example.$p = 13 = 4.3+1, 3^3 \equiv 1 \pmod{13}$
Proof:
We will show that $a = \frac{p-1}{4}$ works here.So let,$n = \frac{p-1}{4}$.
Then $4n = p-1 \equiv -1 \pmod p, \Longrightarrow n \equiv \frac{-1}{4} \equiv (\frac{i}{2})^2 \pmod p$ where $i^2 \equiv -1 \pmod p$ and the existence of such i is guaranteed by P_2 of Legendre symbol in the section **Definitions**.
Consider two cases:
Case 1:$p \equiv 5 \pmod 8$,then from Legendre symbol,we get $(\frac{2}{p}) = -1, 2^{\frac{p-1}{2}} \equiv -1$.Also $i^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv -1 \pmod 8$.These two imply that $a^a \equiv (\frac{i}{2})^{\frac{p-1}{2}} \equiv \frac{-1}{-1} \equiv 1$.
Case 2:$p \equiv 1 \pmod 8$,then similarly we get $2^{\frac{p-1}{2}} \equiv 1$.Also $i^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv 1$.
Thus it is true for both cases.
Corollary 1:
$\frac{p-1}{4} \neq pr_p$ if $p \equiv 1 \pmod p$.
This follows directly from the generalization of the corollary of lemma 1.
Corollary 2:
$a = \frac{p-1}{4}$ is a perfect $4-th$ power of p. It is straight forward from the definition since $\varphi(p) = p-1$.
Claim 2:
Take $p \equiv 3 \pmod 8$.Then $a^a \equiv 1$ has at least one solution.
Example.$p = 11, a = 5, 5^5 \equiv 1 \pmod{11}$
Proof:
Several examples convince us that we should take $a = \frac{p-1}{2}$ this time.Let's try.
Note that 2 is a qnr of p yielding $(\frac{2}{p}) = -1, 2^{\frac{p-1}{2}}$.Moreover,$(p-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1$ yielding $a^a \equiv \frac{-1}{-1} \equiv 1$. Hence,the conclusion follows.
Corollary 1:
$a = \frac{p-1}{2}$ is a perfect square of $p \equiv 3 \pmod 8$.
Corollary 2:
$a = \frac{p-1}{2} \neq pr_p$ for $p \equiv 3 \pmod 8$.

Claim 3:
Let $n = \frac{p+1}{2}$, be positive integer where $p \equiv -1 \pmod 8$.Then $n^{n-1} \equiv 1$.
Example.$p = 7, n = 4, 4^3 \equiv 1 \pmod 7$.
Proof:
$p \equiv -1 \pmod 8 \implies (\frac{2}{p}) = 1 \implies 2^{\frac{p-1}{2}} \equiv 1 \equiv 2^{p-1} \implies \frac{1}{2^{\frac{p-1}{2}}} \equiv 1$.
The rest is to just see that $n = \frac{p+1}{2} \equiv \frac{1}{2}$ and $n^{n-1} \equiv (\frac{1}{2})^{\frac{p-1}{2}} \equiv 1$.
Corollary 1:
$a = \frac{p+1}{2}$ is a perfect square of $p \equiv -1 \pmod 8$.
Corollary 2:
$a = \frac{p+1}{2} \neq pr_p$ for $p \equiv -1 \pmod 8$.
Claim 4:
Let $\frac{p+1}{4} = n$ be a positive integer.We want to show that $n^{\frac{p-3}{4}} \equiv \pm 2$.
Proof:
$4n = p + 1 \equiv 1 \pmod 8 \implies n \equiv \frac{1}{4} \equiv \frac{1}{2})^2$.
Therefore,we may say that,$\frac{1}{\sqrt{n}} \equiv 2$.
Since $\frac{p-3}{4} = \frac{p-1}{2} - \frac{1}{2}$,using this we get $n^{\frac{p-3}{4}} \equiv n^{\frac{p-1}{2}}.\frac{1}{\sqrt{n}} \equiv (\frac{1}{2})^{\frac{p-1}{2}}.2 \equiv \pm 2$,as desired.
Corollary:
$\star$ 1.If $(\frac{2}{p}) = 1$ or $p \equiv -1 \pmod 8$,then $n^{\frac{p-3}{4}} \equiv 2$.
$\star$ 1.If $(\frac{2}{p}) = -1$ or $p \equiv 3 \pmod 8$,then $n^{\frac{p-3}{4}} \equiv -2$.
I am ending the section with a question.
Question. Does there always exist an a such that $a^a \equiv 1$ for all p?
Well,we have proved this existence for all $p \equiv 1 \pmod 4, p \equiv 3 \pmod 8$ above.Then we just need to consider the case when $p \equiv -1 \pmod 8$.