International Journal of Sciences

Research Article Volume 11 – December 2022 (12)

Quadratic Residuacity: Intro to Advance Number Theory

Maher Ali Rusho

Abstract: This is the second paper of Number Theory for Math Olympiad enthusiast . Number Theory is the basement of Mathematics and it is followed in INTERNATIONAL MATH OLYMPIAD syllabus . Students are asked various types of question here equivalently . In the first paper "A Case Study Of Special Types of congruences and it's solution" I discuss special type of quadratic residuacity. And it's congruence of second degree in one unknown with prime modulo.

Introduction:
In this paper we discuss the congruence of second degree with prime modulo P which is

$$x^2 \equiv a(modp); p \nmid a$$

If it has solution , then a is the remainder of some squares when divided by p . We say that a is the quadratic residue of P . Otherwise a is called a quadratic non residue of p . Our aim is to determine which integers are the quadratic residues of the given prime p which are non residue of p .

Quadratic residue and non residue :
Let P be an odd prime and a is a quadratic residue modulo p, then $x1^2 \equiv a(modp); p \nmid a$. If x=p -x1 then x is also a quadratic residue modulo p . If $(a,p) = 1$ and the congruence $x^2 \equiv a(modp)$ is solvable then it has exactly 2 solution . Let p be an odd prime and (a,p)=1 then either $a^(p-1)/2 \equiv 1(modp)$ or $a^(p-1)/2 \equiv -1(modP)$

If p is an odd prime then the congruence $x^(p-1)/2 \equiv 1(modp)$ has exactly
$X \equiv 1^2, 2^2, 3^2, - - - - - - [(P-1)/2]^2$
Has exactly $(p-1)/2$ solution and the congruent has solution if and only if $(a^p - 1/2 \equiv 1)$(mod p) and no solution if the modulo is -1.

And the interesting property is the product of two quadratic residues/non residues of p is quadratic residue . The product of a quadratic residue and non residue of p is quadratic non-residue of p .

This can be easily proved . Let, a1 and a2 be two quadratic residues of p , then
$a1^(p-1)$ is congruent to 1 mod p and a2^(p-1)/2 is congruent to 1 mod p . Then multiplying both we get $(a1a2)^(p-1)/2$ is congruent to 1 modulo p. Similarly the above two both can be proved .

Legendre symbol:
Let P be an odd prime and a is an integer then the Legendre symbol (a/p) is defined as

$$\begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Postulate of lagendra symbol

1. If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. $\left(\frac{a^2}{p}\right) = 1$
4. $\left(\frac{1}{p}\right) = 1$
5. $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv -1 \pmod 4 \end{cases}$
6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ **(The Law of Quadratic Reciprocity)**

Src : http://mathcenter.oxford.emory.edu/site/math125/legendresSymbolProperties/

Theorem 5.1 (Unique Factorization into Ideal Primes). Every element of Z[ζp] factors uniquely as a product of (ideal and actual) primes.

The finiteness condition can be established once again through a norm, which maps each element of Z[ζp] to the product of all its images under the different embeddings of Q(ζp) (the field of fractions of Z[ζp]) into C. Enough of unique factorization is then recaptured to proceed with the arithmetic almost as usual.

Among other things, Kummer used his ideal prime numbers to es- tablish a variant of Lam´e's argument for Fermat's Last Theorem. The argument does run, however, into certain subtle technical difficulties and does not work for an arbitrary prime. Kummer listed a set of two conditions that p would have to satisfy to be able to deduce the n = p case of Fermat's Last Theorem using this approach. He even informed the Berlin Academy that he "had reason to believe" that p = 37 did not satisfy them (it does not; see [7]). On the other

Published at: http://www.ijsciences.com/pub/issue/2022-12/
DOI: 10.18483/ijSci.2639; Online ISSN: 2305-3925; Print ISSN: 2410-4477

Maher Ali Rusho (Correspondence)
+

hand, Kummer considered his proof of Fermat's Last Theorem for the so-called regular primes a by-product of his research into higher reciprocity laws, not the main interest of his development. (Src: https://www.math.uwaterloo.ca/~dmckinno/Papers/Gauss.pdf)

Now let's solve some problems with this:

3.3 IMO 2008

Prove that there are infinitely many positive integers n such that n2 + 1 has a
2n
Solution Let p be a prime, p = 8k+1. Note that 4−1 ≡ 6k+1 (modp).
prime divisor greater than 2n +
√
Choose n = 4k − a, 0 ≤ a < 4k. Then (p−1 − a)2 + 1 ≡ 0 (mod p) is equivalent 2
to4−1+a+a2+1≡0 (modp),soa(a+1)≡−6k−2≡2k−1 (modp).But
a(a+1) is even and positive, so a(a+1) ≥ 10k. We have that (a+1)2 > a(a+1) ≥
10k>p,so n= p+1 −(a+1)< p+1 −√p< p+1 −√2n,so2n+2√2n−1>p. 222

Note that this result is a bit stronger than the initial inequality. Solution support : https://www.math.cmu.edu/~cargue/arml/archive/19-20/number-theory-at-11-24-19.pdf
3.6

A very useful lemma
Suppose that the positive integer a is not a perfect square. Then (ap) = −1 for infinitely many primes p.
Solution Let's say that it's not true. This means that there exists a number
r such that for every prime q > r, (aq) = 1. Because a is not a perfect square,
we can write a = x2 p1 p2 ...pk where p1 , p2 ...pk are primes in increasing order.
Let's take a prime p > r, p ≡ 5 (mod 8). We have that (a) = (p1)(p2)...(pk). pppp
If pi is odd, (pi) = (p) (from Quadratic Reciprocity Law). If p1 = 2, (2) = p pi p
(−1)p2−1 =−1.(a)=(p)...(p)or(a)=−(p)...(p).Wecantaker ,r ,...,r 8 p p1 pk p p2 pk 22 k
residues (mod p2,p3...pk) such that (r2)...(rk) is 1 or −1 as we wish. By Chinese p2 pk
Remainders Theorem there are infinitely numbers t with t ≡ 5 (mod 8),t ≡ ri (mod pi), 2 ≤ i ≤ k. Now we look at progression t + l8p2p3...pk. By Dirichlet's Theorem there are infinitely many prime q in this sequence and we take q > r. We have that (a/q) = 1 but as we've already discussed we can select r2,r3...rk such that (a/q) = −1, contradiction.

3.7 2015 Iran Team Selection Test

Let b1 < b2 < b3 < ... be the sequence of all natural numbers which are sum of squares of two natural numbers. Prove that there exists infinite natural numbers like m which bm+1 − bm = 2015 .
Solution For any i , 1 ≤ i ≤ 2014 we can find infinitely many primes p such that p ≡ 3 (mod 8) and (10072+i) = −1 (10072 + i is not a perfect square,
p
so the second part follows easily from problem 6 and first part follows from
Chinese Remainders Theorem and Dirichlet's Theorem). Now, we choose prime
numbers p1,p2...,p2014 such that pi ≡ 3 (mod 8) and (10072+i) = −1. There is pi
a number x such that x ≡ pi − i (mod p2i) for any 1 ≤ i ≤ 2014 (by Chinese Remainders Theorem). We will prove that there are infinitely many numbers a

such that the number a2 + 10072 is of the form x + kp21p2...p2014 for some k.
If we note y = a2 +10072, we see that y and y+2015 can be written as sum
of squares of two natural numbers and y + i, 1 ≤ i ≤ 2014, cannot because
y+i ≡ pi (modp2i). To prove this, we see that (x−10072) = 1, so there is a pi
number xi with x2i ≡ x − 10072 (mod pi). We can find a numbers ti such that p2i |(xi + piti)2 − (x − 10072) (this is equivalent to finding a number ti such that
+ 2xiti and that's easy because pi does not divide xi, otherwise pi would divide x − 10072 and pi would divide 10072 + i and we can avoid this by choosing pi very large). We denote by ri the residue of xi + piti (mod p2i). By Chinese Remaindes Theorem we can find infinitely many numbers a such thata≡ri (modp2i),1≤i≤2014,this means thata2 ≡x−10072 (modp2i), 1 ≤ i ≤ 2014 ⇒ a2 + 10072 = x + kp21p2...p2014 for some k and that's all.

Conclusion:

IF you really want more problem to see and learn how to solve then please visit this website: https://www.math.cmu.edu/~cargue/arml/archive/19-20/number-theory-at-11-24-19.pdf

Number theory is earlier developed and one of the deepest root in unsolved math .

"**If the theory of numbers could be employed for any practical and obviously honourable purpose, if it could be turned directly to the furtherance of human happiness or the relief of human suffering, as physiology and even chemistry can, then surely neither Gauss nor any other mathematician would have been so foolish as to decry or regret such applications. But science works for evil as well as for good; and both Gauss and lesser mathematicians may be justified in rejoicing that there is one science at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.**"
— G.H. Hardy, A Mathematician's Apology

References:

1. Dusan Djukic: Quadratic Congruences, www.imocompedium.com
2. Titu Andreescu and Dorin Andrica. Number Theory: Structures,Examples and Problems. Springer, 2009

1. Keith Conrad:Examples of Mordell's Equation:http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/mordelleqn1.pdf
2. Xu Jiagu.Lecture Notes on Mathematical Olympiad Courses, For Senior Section,Volume 2, World Scientific
3. http://www.artofproblemsolving.com
4. Titu Andreescu. Mathematical Reflections, the first two years. XYZ Press, 2011
5. Laurentiu Panaitopol and Alexandru Gica. Probleme de aritmetica si teoria nu-merelor.Idei de rezolvare, Editura Gil
6. Advance theory of numbers book written by Prof.Dr.M.Fazlur Rahaman
7. Taken quote form : https://www.goodreads.com/quotes/tag/number-theory
8. Src : http://mathcenter.oxford.emory.edu/site/math125/legendresSymbolProperties/
9. https://en.wikipedia.org/wiki/Legendre_symbol