math115A hw8

Jonas Chen

October 10, 1000

Problem 1

> Prove that the quadratic congruence
>
> $$6x^2 + 5x + 1 \equiv 0 \pmod{p}$$
>
> has a solution modulo every prime p even though the equation $6x^2 + 6x + 1 = 0$ has no solutions in the integers.

Solution

No idea

Although for $p = 2$ the congruence can be solved with $x \equiv 1 \pmod{2}$ and $p = 3$ the congruence has a solution also $x \equiv 1 \pmod{3}$

Problem 2

> Show that 3 is a quadratic residue modulo 23, but is a non-residue modulo 31

Solution

$(23-1)/2 = 11$ and $3^{11} \equiv \left(3^3\right)^3 \cdot 3^2 \equiv (4)^3 \cdot 3^2 \equiv 18 \cdot 9 \equiv 1 (\operatorname{mod} 23)$ therefore 3 is a quadratic residue modulo 23 by Euler's criterion

$(31-1)/2 = 15$ and $3^{15} = \left(3^3\right)^5 \equiv (-4)^5 \equiv 30 \equiv -1 (\operatorname{mod} 31)$ and therefore 3 is a quadratic non-residue modulo 31 by Euler's criterion

Theorem: **Euler's criterion**

> Suppose that p is an odd prime, and let $a \in \mathbb{Z}$ satisfy $(a, p) = 1$
>
> Then a is a quadratic residue mod p
>
> $$\text{if and only if } a^{(p-1)/2} \equiv 1 \pmod{p}$$

Problem 3

> Given that a is a quadratic residue modulo the odd prime p , prove the following:
>
> (a) a is not a primitive root of p
>
> (b) The integer $p - a$ is a quadratic residue or non-residue modulo p according as $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$
>
> (c) If $p \equiv 3 \pmod{4}$ then $x \equiv \pm a^{(p+1)/4} \pmod{p}$ are the solutions of the congruence $x^2 \equiv a \pmod{p}$

Solution

(a) Since a is a quadratic residue mod p then by Euler's criterion $a^{(p-1)/2} \equiv 1 \pmod{p}$ and since $\frac{p-1}{2} < p - 1 = \phi(p)$ then it follows that a is not a primitive root of p

(b) Note that $(p-a)^{(p-1)/2} \equiv (-a)^{(p-1)/2} \equiv (-1)^{(p-1)/2}(a)^{(p-1)/2} \equiv (-1)^{(p-1)/2}$ where the last equivalence holds by Euler's criterion.

If $p \equiv 1 \pmod{4}$ then $p = 4k + 1$ then $\frac{p-1}{2}$ will be even and $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ so that $p - a$ is a quadratic residue modulo p. Similarly if $p \equiv 3 \pmod{4}$ then $p = 4k + 3$ making $(p-1)/2$ odd so that $p - a$ is a quadratic non-residue modulo p

(c) Substituing x into $x^2 \equiv a \pmod{p}$ we have $\left(\pm a^{(p+1)/4}\right)^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} a \equiv 1a \equiv a \pmod{p}$

Problem 4

> If $p = 2^k + 1$ is a prime, show that every quadratic non-residue modulo p is a primitive root modulo p

Solution

Let a be a quadratic non-residue mod p then by Euler's criterion the following equivalences are the same:

$$a^{(p-1)/2} \equiv -1 (\operatorname{mod} p)$$
$$a^{(2^k)/2} \equiv -1 (\operatorname{mod} p)$$
$$a^{2^{k-1}} \equiv -1 (\operatorname{mod} p)$$
$$a^{2^k} \equiv 1 (\operatorname{mod} p)$$

First one by euler's criterion, second one by def of p and fourth one by squaring both sides of second one

Note that $a^{\phi(p)} = a^{p-1} = a^{2^k}$ therefore we would like to show that the order of a is at most 2^k

Suppose there exists some $z < 2^k$ such that $a^z \equiv 1 (\operatorname{mod} p)$

Case 1: z is not a power of 2. Note that $a^{2^k} \equiv 1 (\operatorname{mod} p)$ implies that the order of a divides 2^k (the divisors of 2^k are also powers of 2), then z cannot be the order of a

Case 2: z is a power of 2 then z has the form 2^l where $l < k$ but notice that if we repeatedly square the congruence (specifically: $k - l - 1$ times) $a^{2^l} \equiv 1 (\operatorname{mod} p)$ that will eventually obtain $a^{2^{k-1}} \equiv 1 \operatorname{mod} p$ but from above we also know that $a^{2^{k-1}} \equiv -1 (\operatorname{mod} p)$ therefore z cannot be the order of a

Since z cannot exist, then 2^k is the order of $a \operatorname{mod} p$ which means that a is a primitive rood $\operatorname{mod} p$

Theorem: **properties of the Legendre symbol**

> Let p be an odd prime and let $a, b \in \mathbb{Z}$ with $(a, p) = (b, p) = 1$
>
> (i) If $a \equiv b (\operatorname{mod} p)$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
>
> (ii) $\left(\frac{a^2}{p}\right) = 1$
>
> (iii) $\left(\frac{a}{p}\right) \equiv a^{p-1/2} (\operatorname{mod} p)$
>
> (iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
>
> (v) $\left(\frac{1}{p}\right) = 1$ and $\left(-\frac{1}{p}\right) = (-1)^{p-1/2}$

Problem 5

> Find the value of the following Legendre symbols:
>
> (a) $(19/23)$
> (b) $(-23/59)$
> (c) $(-72/131)$

Solution

(a) $(19/23) = (-4/23) = (-1/23)(4/23) = -1$

since $(-1/23) = (-1)^{(23-1)/2} = (-1)^{11} = -1$

(b) $(-23/59) = (36/59) = 1$

(c) $(-72/131) = (9/131)(-8/131) = (1)(-1/131)(8/131) = (-1)(2/131) = 1$ where $(-1/131) = (-1)^{65} = -1$ and $(2/131) = 2^{65} \equiv -1 (\operatorname{mod} 131)$

Lemma: **Gauss's Lemma**

> Let p be an odd prime, and suppose $a \in \mathbb{Z}$ with $(a, p) = 1$
>
> Let n denote the number of integers in the set $S = \left\{a, 2a, 3a, ..., \frac{p-1}{2}a\right\}$ whose smallest positive residue $\bmod p$ exceeds $\frac{p}{2}$
>
> Then $\left(\frac{a}{p}\right) = (-1)^n$

Problem 6

> Use Gauuss's Lemma to compute each of the following Legendre symbols (i.e., in terms of the notation that we used in class, find the integer n in Gauss's Lemma for which $\left(\frac{a}{p}\right) = (-1)^n$)
>
> (a) $(8/11)$
> (b) $(7/13)$
> (c) $(5/19)$

Solution

(a) We can compute $\frac{p-1}{2} = 5$ smallest positive residues in the set $\{8, 16, 24, 32, 40\}$ which are $\{8, 5, 2, 10, 7\}$ since 3 of these numbers are larger than $\frac{p}{2}$ then $(8/11) = (-1)^3 = -1$

(b) Similar to (a) the smallest positive residues in the set $\{7, 14, 21, 28, 35, 42\}$ are $\{7, 1, 8, 2, 9, 3\}$ then $n = 3$ and $(7/13) = -1$

(c) Similar to (a) and (b) the smallest positive residues in the set $\{5, 10, 15, 20, 25, 30, 35, 40, 45\}$ are $\{5, 10, 15, 1, 6, 11, 16, 2, 7\}$ therefore $n = 4$ and $(5/19) = 1$

Definition: Legendre symbol

Let p be an odd prime, with $(a, p) = 1$

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue } \bmod p \\ -1 \text{ if a is a quadratic non-residue} \end{cases}$$

Problem 7

> (a) Let p be an odd prime, and suppose that a is an integer with $(a, p) = 1$. Show that the diophantine equation
>
> $$x^2 + py + a = 0$$
>
> has an integral solution if and only if $(-a/p) = 1$
>
> (b) Determine whether of not the Diophantine equation
>
> $$x^2 + 7y - 2 = 0$$
>
> has a solution in the integers

Solution

(a)

Mod p the diophantine equation is equivalent to $x^2 \equiv -a (\bmod p)$

Therefore there is a solution iff $-a$ is a quadratic residue $\bmod p$ iff $(-a/p) = 1$

(b) Mod 7 the equation is equivalent to $x^2 \equiv 2 (\bmod 7)$

Since $(2/7) = 2^3 \equiv 1 (\bmod 7)$ this implies that 2 is a quadratic residue $\bmod 7$ and therefore there exists an x such that the diophantine equation holds (i.e. solution exists)

Lemma

> if a is a quadratic residue mod p , then a is not a primitive root mod p
> (the contrapositive holds as well)

Proof: follows from Euler's criterion

suppoe that a is a quadratic residue then $a^{(p-1)/2} \equiv 1 (\operatorname{mod} p)$ but $\phi(p) = p - 1 > (p - 1)/2$ therefore a cannot have order $\phi(p)$ and is therefore not a primitive root mod p

□

Theorem

> Let p be an odd prime, then
> $$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 (\operatorname{mod} 8) \vee p \equiv 7 (\operatorname{mod} 8) \\ -1 \text{ if } p \equiv 3 (\operatorname{mod} 8) \vee p \equiv 5 (\operatorname{mod} 8) \end{cases}$$

Proof: From class

□

Problem 8

> Prove that 2 is not a primitive root modulo any prime of the form $p = 3 \cdot 2^n + 1$ except when $p = 13$

Solution

For $n = 1$ we have $p = 7$ and we can note that $(2/7) = 1$ since $2^3 \equiv 1 (\operatorname{mod} 7)$, therefore we know that 2 is a quadratic residue mod p and therefore 2 is not a primitive root modulo p

For $n = 2$ we have $p = 13$ and we showed that 2 is a primitive of root modulo 13 before. (note that $(2/13) = -1$)

For $n \geq 3$ we can see that $p = 3 \cdot 8 \cdot 2^{n-3} + 1 \Rightarrow p \equiv 1 (\operatorname{mod} 8)$ and by the above theorem $\left(\frac{2}{p}\right) = 1$ therefore 2 is a quadratic residue modulo p and therefore 2 is not a primitive root modulo p for $n \geq 3$

Conclusion is that claim holds for all n such that $n \geq 1 \wedge n \neq 13$

Problem 9

> For a prime $p \equiv 7 \pmod 8$ show that $p \mid 2^{(p-1)/2} - 1$

Solution

By the above theorem from class we have that $(2/p) = 1$ which implies that 2 is a quadratic residue modulo p and by euler's criterion $2^{(p-1)/2} \equiv 1 \pmod p \Rightarrow 2^{(p-1)/2} - 1 \equiv 0 \pmod p \Rightarrow p \mid 2^{(p-1)/2} - 1$

Problem 10

> (a) Suppose that p is an odd prime, and that a and b are integers such that $(ab, p) = 1$ Prove that at least one of $a, b,$ or ab is a quadratic residue modulo p
>
> (b) Show that, for some choice of $n > 0$ p divides
>
> $$(n^2 - 2)(n^2 - 3)(n^2 - 6)$$

Solution

(a) Consider the Legendre symbol $(ab/p) = (a/p)(b/p)$

If both a and b are quadratic non-residues $\bmod p$ then $(ab/p) = (-1)(-1) = 1$ so that ab is a quadratic residue modulo p.

If ab is a quadratic nonresidue $\bmod p$ then $(ab/p) = -1 = (1)(-1) = (-1)(1)$ which means either $(a/p) = 1 \vee (b/p) = 1$ so that one of a, b is a quadratic residue $\bmod p$

(b) Want to show: $(n^2 - 2)(n^2 - 3)(n^2 - 6) \equiv 0 (\bmod p)$ for all p there exist some n to satisfy this congruence

This is true if p divides at least one $(n^2 - 2), (n^2 - 3), (n^2 - 6)$ which further implies that the claim holds if at least one of $2, 3, 6$ is a quadratic residue $\bmod p$

Applying the result in part (a), we know that as long as p is coprime to a product of two integers from the set $\{2, 3, 6\}$ that one of those integers is a quadratic residue or their product is a quadratic residue $\bmod p$

If $p = 2$ or $p = 3$ then the coprime condition does not hold, and we have to manually check if some n exists.

For $p = 2$, set $n = 1$ then the expression becomes $(-1)(-2)(-5) = -10 \equiv 0 (\bmod 2)$

For $p = 3$ set $n = 3$ then the expression becomes $(7)(6)(3) = 126 \equiv 0 (\bmod 3)$

For the case that $p > 3$ consider that since p is odd, then p must be coprime to $6 = 2 \cdot 3$ For $p = 5$ this is easy to see. And for $p \geq 7$ we can see that p has factors $1, p$ and 6 has factors $1, 2, 3, 6$ but $p > 6$ so their only shared factor is 1

To summarize, since $(2 \cdot 3, p) = 1$ for any $p > 3$ then at least one of $2, 3, 6 = 2 \cdot 3$ is a quadratic residue $\bmod p$

Therefore one of the following is true: $n^2 - 2 \equiv 0, n^2 - 3 \equiv 0, n^2 - 6 \equiv 0$ all $\bmod p$ and the claim follows.