math115A hw7

Jonas Chen

October 10, 1000

https://www.youtube.com/watch?v=m-puDTc02sE

Problem 1

> Find the index of 5 relative to each of the primitive roots of 13. [Hint: Recall that 2 is a primitive root modulo 13. To find the other primitive roots, use the the table that was written down in class.]

Solution

The primitive roots of 13 are 2,6,7,11

Then the index of 5 relative to 2 modulo 13 is the smallest k such that $5 \equiv 2^k \pmod{13}$

(a) The powers 1…9 of $2 \pmod{13}$ are congruent to $2, 4, 8, 3, 6, 12, 11, 9, 5$ respectively. Therefore $\operatorname{ind}_2(5) = 9$

(b) The powers 1…9 of $6 \pmod{13}$ are congruent to $6, 10, 8, 9, 2, 12, 7, 3, 5$ respectively. Therefore $\operatorname{ind}_6(5) = 9$

(c) The powers 1…3 of $7 \pmod{13}$ are congruent to $7, 10, 5$ respectively. Therefore $\operatorname{ind}_7(5) = 3$

(d) The powers 1…3 of $11 \pmod{13}$ are congruent to $11, 4, 5$ respectively. Therefore $\operatorname{ind}_{11}(5) = 3$

Problem 2

> Find a primitive root modulo 11, and construct a table of indices relative to this primitive root. Use your table to solve the following congruences:
>
> (a) $7x^3 \equiv 3 \pmod{11}$
>
> (b) $3x^4 \equiv 5 \pmod{11}$
>
> (c) $x^8 \equiv 10 \pmod{11}$

Solution

Note that $\phi(11) = 10$ Also note that 2 is a primitive root mod 11 since $2^{10} \equiv 1 \pmod{11}$ (and no other powers smaller than 10 satisfy the congruence)

Taking powers of $2 \pmod{11}$ we can obtain the following table:

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2(a)$	10	1	8	2	4	9	7	3	6	5

(a)

Checking to see how many potential solutions (if there exist any) we see that $(3, 10) = 1$ and $3^{10} \equiv 1 \pmod{11}$ by fermat's little theorem. Therefore there is exactly one solution

$$\begin{aligned} 7x^3 &\equiv 3 \pmod{11} \\ \mathrm{ind}_2(7) + 3\mathrm{ind}_2(x) &\equiv \mathrm{ind}_2(3) \pmod{10} \\ 7 + 3\mathrm{ind}_2(x) &\equiv 8 \pmod{10} \\ 3\mathrm{ind}_2(x) &\equiv 1 \pmod{10} \end{aligned}$$

implies that $\mathrm{ind}_2(x) \equiv 7$ so that we have the solution $x \equiv 7 \pmod{11}$

(b) Checking to see (how many potential) solutions there are we see that $(4, 10) = 2$ and $5^5 \equiv (5^2)(5^2)(5) \equiv 1 \pmod{11}$. Therefore there are 2 solutions

$$3x^4 \equiv 5 \pmod{11}$$
$$\mathrm{ind}_2(3) + 4\mathrm{ind}_2(x) \equiv 4 \pmod{10}$$
$$8 + 4\mathrm{ind}_2(x) \equiv 4 \pmod{10}$$
$$4\mathrm{ind}_2(x) \equiv -4 \equiv 6 \pmod{10}$$

Which implies that $\mathrm{ind}_2(x) \equiv 9$ and $\mathrm{ind}_2(x) \equiv 4 \pmod{10}$ so that the solutions are $x \equiv 5, x \equiv 6 \pmod{11}$

(c) Checking to see how many potential solutions there could be: $(10, 8) = 2$ and $10^5 \equiv (100)^2(100)^2 100 \equiv 1 \pmod{11}$

$$x^8 \equiv 10 \pmod{11}$$
$$8\mathrm{ind}_2(x) \equiv \mathrm{ind}_2(10) \pmod{10}$$
$$8\mathrm{ind}_2(x) \equiv 5 \pmod{10}$$

But this is not solvable therefore the original congruence has no solution

Problem 3

> The following is a table of indices for integers modulo 17 relative to the primitive root 3:
>
> | a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
> |---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
> | $\mathrm{ind}_3(a)$ | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |
>
> Use this table to solve the following congruences:
>
> (a) $x^{12} \equiv 13 \pmod{17}$
> (b) $8x^5 \equiv 10 \pmod{17}$
> (c) $9x^8 \equiv 8 \pmod{17}$
> (d) $7^x \equiv 7 \pmod{17}$

Solution

(a)

$$x^{12} \equiv 13 \pmod{17}$$
$$12\mathrm{ind}_2(x) \equiv \mathrm{ind}_3(13) \pmod{16}$$
$$12\mathrm{ind}_3(x) \equiv 4 \pmod{16}$$

which means that $\mathrm{ind}_3(x) \equiv 7, 3, 11, 15 \pmod{16}$ so that we have solutions $x \equiv 11, 10, 7, 6 \pmod{17}$

Confirming the number of solutions $(\phi(17), 12) = 4$ and $13^4 \equiv \left(13^2\right)^2 \equiv 16^2 \equiv 1 \pmod{17}$ (has 4 solutions if solvable)

(b)

$$8x^5 \equiv 10 \pmod{17}$$
$$\mathrm{ind}_3(8x^5) \equiv \mathrm{ind}_3(10) \pmod{16}$$
$$\mathrm{ind}_3(8) + 5\mathrm{ind}_3(x^{)} \equiv \mathrm{ind}_3(10) \pmod{16}$$
$$10 + 5\mathrm{ind}_3(x) \equiv 3 \pmod{16}$$
$$5\mathrm{ind}_3(x) \equiv -7 \equiv 9 \pmod{16}$$

which means that $\mathrm{ind}_3(x) \equiv 5 \pmod{16}$ and the solutions is $x \equiv 5 \pmod{17}$ Confirming the number of solutions, we see that $(\phi(17), 5) = 1$

(c) $9x^8 \equiv 8 \pmod{17} \Rightarrow \mathrm{ind}_3(9) + 8\mathrm{ind}_3(x) \equiv \mathrm{ind}_3(8) \pmod{16} \Rightarrow 2 + 8\mathrm{ind}_3(x) \equiv 10 \pmod{16} \Rightarrow$ $8\mathrm{ind}_3(x) \equiv 8 \pmod{16}$ so that $\mathrm{ind}_3(x) \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$ with corresponding solutions $x \equiv 3, 10, 5, 11, 14, 7, 12, 6 \pmod{17}$
Confirming the number of solutions, $(\phi(17), 8) = 8$

(d)

$$7^x \equiv 7 \pmod{17}$$
$$x\mathrm{ind}_3(7) \equiv \mathrm{ind}_3(7) \pmod{16}$$
$$x(11) \equiv 11 \pmod{16}$$

And we have a solution $x \equiv 1 \pmod{17}$

Problem 4

> Find the remainder when $3^{24} \cdot 5^{13}$ is divided by 17. [Hint: use the theory of indices]

Solution

Note that 3 is a primitive root mod 19

We sould like to solve for x in the following congruence:

$$3^{24} \cdot 5^{13} \equiv x (\operatorname{mod} 17)$$
$$24 \operatorname{ind}_3(3) + 13 \operatorname{ind}_3(5) \equiv \operatorname{ind}_3(x) (\operatorname{mod} 16)$$
$$24 + 65 \equiv \operatorname{ind}_3(x) (\operatorname{mod} 16)$$
$$8 + 1 = 9 \equiv \operatorname{ind}_3(x) (\operatorname{mod} 16)$$

And we can see by the table in problem 3 that $3^9 \equiv 14 (\operatorname{mod} 17)$ therefore the remainder is 14

Problem 5

> Show that the congruence $x^3 \equiv 3 \pmod{19}$ has no solutions, while the congruence $x^3 \equiv 11 \pmod{19}$ has three distinct solutions.

Solution

For the first congruence, $(\phi(19), 3) = 3$ and

$$3^{\frac{18}{3}} = 3^6 \equiv \left(3^3\right)^2 \equiv (27)^2 \not\equiv 1 \pmod{19}$$

therefore no solutions

For the second congruence, $(\phi(19), 3) = 3$ and

$$11^6 \equiv \left(11^3\right)^2 \equiv \left(11^2 \cdot 11\right)^2 \equiv (7 \cdot 11)^2 = (77)^2 \equiv 1 \pmod{19}$$

therefore there are exactly 3 distinct solutions

Problem 6

> Granville, Exercise 8.1.1
>
> (a) Prove that 337 is not a square (that is, the square of an integer) by reducing it mod 5
>
> (b) Prove that 391 is not a square by reducing it mod 7
>
> (c) Prove that there do not exist integers x and y for which $x^2 - 3y^2 = -1$, by reducing any solution mod 3.

Solution

(a) $337 = 335 + 2 \equiv 2 (\operatorname{mod} 5)$ but 2 is not in the table of quadratic residues $(\operatorname{mod} 5)$ Therefore there does not exist an x such that $337 = x^2 \equiv 2 (\operatorname{mod} 5)$

(b) $391 = (10)^3 + 91 \equiv 3^3 + 7 \equiv 27 + 7 \equiv 34 \equiv 6 (\operatorname{mod} 7)$ but 6 is not in the table of quadratic residues (mod 7) therefore there does not exist an x such that $391 = x^2 \equiv 6 (\operatorname{mod} 7)$

(c)

Let $x, y \in \mathbb{Z}$

First we can use two facts:

$-3y^2 \equiv 0 (\operatorname{mod} 3)$ and

$x^2 \equiv a (\operatorname{mod} 3)$ if and only if $a = 1 + 3k$ for some integer k

The second fact is true since $a \in \mathbb{Z}$ is a quadratic residue $\operatorname{mod} p$ if for $(a, p) = 1$ and it holds that $a^{(p-1)/2} \equiv 1 (\operatorname{mod} p)$

Here we have $(p - 1)/2 = 1$ so that $a^1 \equiv 1 (\operatorname{mod} p)$ Therefore a must have the form $a = 1 + 3k$

Combining the above two congruence we have that $x^2 - 3y^2 \equiv a$ i.e. $x^2 - 3y^2 \equiv 1 + 3k - 0 (\operatorname{mod} 3) (\dagger)$

Let $x^2 = 1 + 3k$ then from the original equation we can obtain $y = \frac{1+x^2}{3}$ and substituting gives

$$\frac{1 + (3k + 1)^2}{3} = \frac{3(3k^2 + 2k) + 2}{3} = y$$

But the above implies that $3 \nmid y$ which contradicts the fact that $y = \frac{1+x^2}{3}$ is an integer, therefore $y \neq 0$ and $(\dagger)$ does not hold

the conlclusion is that for any choice of $x \in \mathbb{Z}$, the integer $y \in \mathbb{Z}$ does not exists such that $x^2 - 3y^2 = -1$

□