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 and $\phi(13) = 12$

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

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) $7x^3 \equiv 3 (\operatorname{mod} 11)$
>
> (b) $3x^4 \equiv 5 (\operatorname{mod} 11)$
>
> (c) $x^8 \equiv 10 (\operatorname{mod} 11)$

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
$\operatorname{ind}_3(a)$	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) $x^{12} \equiv 13 (\operatorname{mod} 17)$
> (b) $8x^5 \equiv 10 (\operatorname{mod} 17)$
> (c) $9x^8 \equiv 8 (\operatorname{mod} 17)$
> (d) $7^x \equiv 7 (\operatorname{mod} 17)$

Solution

Problem 4

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

Solution

Problem 5

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

Solution

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