

**Problem 1.** (15 points)

- (a) State the Law of Quadratic Reciprocity.  
 (b) The number 8389 is prime. Does the congruence

$$x^2 \equiv -1 \pmod{8389}$$

have a solution? (Explain how you got your answer.)

- (c) The number 8389 is prime. Does the congruence

$$x^2 \equiv 2 \pmod{8389}$$

have a solution? (Explain how you got your answer.)

**Solution.** (a) The Law of Quadratic Reciprocity says that for odd primes  $p$  and  $q$ ,

$$\begin{aligned} \left(\frac{-1}{p}\right) &= \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}, \end{cases} \\ \left(\frac{2}{p}\right) &= \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}, \end{cases} \\ \left(\frac{p}{q}\right) &= \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4}. \end{cases} \end{aligned}$$

(More generally, this is true if  $p$  and  $q$  are any positive odd numbers.)

(b) Since  $8389 \equiv 1 \pmod{4}$ , the first part of quadratic reciprocity tells us that  $\left(\frac{-1}{8389}\right) = 1$ , so the congruence  $x^2 \equiv -1 \pmod{8389}$  has a solution.

(c) Since  $8389 \equiv 5 \pmod{4}$ , the second part of quadratic reciprocity tells us that  $\left(\frac{2}{8389}\right) = -1$ , so the congruence  $x^2 \equiv 2 \pmod{8389}$  does not have a solution.

**Problem 2.** (15 points)

- (a) How many primitive roots are there for the prime  $p = 41$ ?  
 (b) Is 5 a primitive root modulo 31? Explain why or why not.  
 (c) Suppose that  $2 \leq a \leq 18$  and that

$$a^{15} \equiv 1 \pmod{19}.$$

What is the smallest power of  $a$  that is congruent to 1 modulo 19?

~~(In other words, what is the value of the index  $I_{19}(a)$ ?)~~

[The final sentence should have read “In other words, what is the order of  $a$  modulo 19.” Due to this mistake on my part, I did not deduct credit for Problem 2(c).]

**Solution.** (a) There are  $\phi(40) = \phi(8)\phi(5) = 4 \cdot 4 = 16$  primitive roots modulo 41. In general, there are  $\phi(p-1)$  primitive roots modulo  $p$ .

(b) We compute the powers of 5 modulo 31. Thus

$$5^2 \equiv 25 \pmod{31} \qquad 5^3 \equiv 125 \equiv 1 \pmod{31}.$$

Therefore 5 is not a primitive root modulo 31, since it doesn't require the 30<sup>th</sup>-power to get back to 1.

(c) We know that the index of  $a$  divides 18. (In general, working modulo  $p$ , the index of every element divides  $p-1$ .) We are also given that the 15<sup>th</sup>-power of  $a$  is 1 modulo 19, so it follows that the  $\gcd(15, 18)$ <sup>th</sup> power of  $a$  is 1 modulo 19. In other words  $a^3 \equiv 1 \pmod{19}$ . Since we are given that  $a \not\equiv 1 \pmod{19}$  and since 3 is prime, we must have  $I_{19}(a) = 3$ . (In other words, we now know that  $a^3 \equiv 1 \pmod{19}$  and  $a \not\equiv 1 \pmod{19}$ , so we cannot have  $a^2 \equiv 1 \pmod{19}$ , since that would imply that  $a \equiv a^3 \cdot (a^2)^{-1} \equiv 1 \cdot 1 \equiv 1 \pmod{19}$ .)

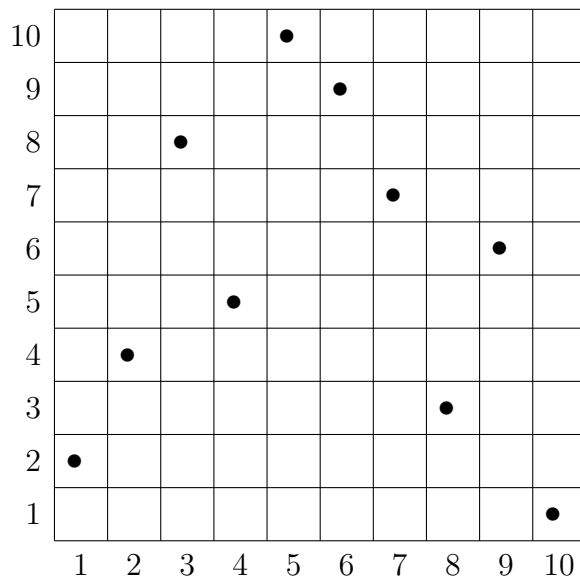
---

**Problem 3.** (10 points) Put 10 dots into the grid to form a 10-by-10 Costas array. (Indicate the method that you use.)

**Solution.** If  $p$  is prime, we can use primitive roots to build a  $(p-1)$ -by- $(p-1)$  Costas array. We first need to find a primitive root modulo 11. Let's try  $g = 2$ .

$$\begin{array}{lll} 2^1 \equiv 2 \pmod{11} & 2^2 \equiv 4 \pmod{11} & 2^3 \equiv 8 \pmod{11} \\ 2^4 \equiv 5 \pmod{11} & 2^5 \equiv 10 \pmod{11} & 2^6 \equiv 9 \pmod{11} \\ 2^7 \equiv 7 \pmod{11} & 2^8 \equiv 3 \pmod{11} & 2^9 \equiv 6 \pmod{11} \\ 2^{10} \equiv 1 \pmod{11} & & \end{array}$$

So 2 is a primitive root modulo 11. We fill in the Costas array as follows: In the  $i$ <sup>th</sup> column, we put a dot in the  $(2^i \bmod 11)$ <sup>th</sup> row. This gives the Costas array



**Problem 4.** (10 points) Suppose that  $\left(\frac{a}{b}, \frac{c}{d}\right)$  is a solution in rational numbers to the equation

$$x^3 + y^3 = 7,$$

where the fractions  $\frac{a}{b}$  and  $\frac{c}{d}$  are written in lowest terms with positive denominators. Prove that  $b = d$ .

**Solution.** The fractions  $\frac{a}{b}$  and  $\frac{c}{d}$  satisfy the equation

$$\left(\frac{a}{b}\right)^3 + \left(\frac{c}{d}\right)^3 = 1.$$

Multiply by  $b^3d^3$  to clear the denominators,

$$a^3d^3 + c^3b^3 = b^3d^3.$$

It follows from this equation that  $b^3 \mid a^3d^3$ . (To see that  $b^3$  divides  $a^3d^3$ , we just need to rewrite the equation as  $a^3d^3 = b^3(d^3 - c^3)$ .) But  $\gcd(a, b) = 1$ , since the fraction  $a/b$  is written in lowest terms. Therefore  $b^3 \mid d^3$ , from which it follows that  $b \mid d$ .

Similarly, rewriting the equation as  $c^3b^3 = d^3(b^3 - a^3)$  shows that  $d^3 \mid c^3b^3$ . The assumption that the fraction  $c/d$  is in lowest terms means that  $\gcd(c, d) = 1$ , so  $d^3 \mid b^3$ , and hence  $d \mid b$ .

We have now shown that  $b$  and  $d$  are positive integers satisfying both  $b \mid d$  and  $d \mid b$ . Therefore  $b = d$ .

(If you want to be more formal about this last step, write  $d = bu$  and  $b = dv$  for some (positive) integers  $u$  and  $v$ . Substituting the first

into the second gives  $b = dv = buv$ , and canceling  $b$  gives  $uv = 1$ . Since  $u$  and  $v$  are positive integers, the only possibility is  $u = v = 1$ .

**Problem 5.** 10 (10 points) Find a solution to the congruence

$$x^{23} \equiv 5 \pmod{91}.$$

(*Hint.* 91 is not prime.) **Be sure to show your work.**

No credit will be given for an answer with no work. Your solution should indicate the steps that one uses to solve any congruence of the form  $x^e \equiv b \pmod{pq}$  if you know the primes  $p$  and  $q$ .

Here are a few computations, some of which may be useful for solving this problem.

$$\begin{array}{lll} 22 \cdot 29 \equiv 1 \pmod{91} & 23 \cdot 4 \equiv 1 \pmod{91} & 5 \cdot 73 \equiv 1 \pmod{91} \\ 25 \cdot 49 \equiv 1 \pmod{72} & 23 \cdot 47 \equiv 1 \pmod{72} & 5 \cdot 29 \equiv 1 \pmod{72} \\ 5^1 \equiv 5 \pmod{91} & 5^2 \equiv 25 \pmod{91} & 5^4 \equiv 79 \pmod{91} \\ 5^8 \equiv 53 \pmod{91} & 5^{16} \equiv 79 \pmod{91} & 5^{32} \equiv 53 \pmod{91} \\ 5^1 \equiv 5 \pmod{72} & 5^2 \equiv 25 \pmod{72} & 5^4 \equiv 49 \pmod{72} \\ 5^8 \equiv 25 \pmod{72} & 5^{16} \equiv 49 \pmod{72} & 5^{32} \equiv 25 \pmod{72} \end{array}$$

**Solution.** The first step is to factor  $91 = 7 \cdot 13$ . Then the value of Euler's phi function is  $\phi(91) = \phi(7)\phi(13) = 6 \cdot 12 = 72$ .

The second step is to find the inverse of 23 modulo 72. In other words, solve

$$23d \equiv 1 \pmod{72}.$$

In general, this is done using the extended Euclidean algorithm. However, the problem gives this information,  $d = 47$ .

The third step is to compute  $5^{47} \pmod{91}$ . This is done by the square-and-multiply algorithm. So we write 47 in binary as

$$47 = 32 + 8 + 4 + 2 + 1.$$

Then using the values provided in the problem,

$$\begin{aligned} 5^{47} &= 5^{32} \cdot 5^{8} \cdot 5^4 \cdot 5^2 \cdot 5^1 \\ &\equiv 53 \cdot 53 \cdot 79 \cdot 25 \cdot 5 \pmod{91} \\ &\equiv 27738875 \pmod{91} \\ &\equiv 73 \pmod{91}. \end{aligned}$$

Therefore

$$x = 73 \text{ is a solution to } x^{23} \equiv 5 \pmod{91}$$