

# AoPS Volume 2 Solutions

MCKINLEY XIE

August 5, 2021

## Contents

23 Number Theory	1
24 Diophantine Equations	7

## §23 Number Theory

**Exercise 23.1.** Show that if  $a_1 \mid (a, b)$ , then  $\frac{b}{(a, b)} \mid \frac{b}{a_1}$

*Solution.*  $(a, b)$  is a multiple of  $a_1$ , so it's pretty clear. □

**Exercise 23.2.** Compare our  $2 \equiv 20 \pmod{6}$  example to equation (23.2)

*Solution.* It just states  $1 \equiv 10 \pmod{3}$  □

**Exercise 23.3.** Divide out the common factors in the following congruences:

1.  $6a \equiv 6b \pmod{20}$
2.  $23 \equiv 138 \pmod{5}$
3.  $12 \equiv 30 \pmod{9}$

*Solution.* Just regurgitate what we learned in the lesson:

1.  $a \equiv b \pmod{10}$
2.  $1 \equiv 6 \pmod{5}$
3.  $2 \equiv 5 \pmod{3}$

□

**Exercise 23.4.** Solve the congruences.

1.  $1235x + 45 \equiv 9090 \pmod{24}$
2.  $1235x + 45 \equiv 9090 \pmod{11}$
3.  $1235x + 45 \equiv 9087 \pmod{11}$
4.  $1232x + 45 \equiv 9090 \pmod{24}$

*Solution.* Nothing special to see here.

1.

$$1235x + 45 \equiv 9090 \pmod{24}$$

$$1235x \equiv 9045$$

$$247x \equiv 1809$$

$$7x \equiv 9$$

$$7x \equiv 105$$

$$x \equiv 15 \pmod{24}$$

2.

$$1235x + 45 \equiv 9090 \pmod{11}$$

$$247x \equiv 1809$$

$$5x \equiv 5$$

$$x \equiv 1 \pmod{11}$$

3.

$$1235x + 45 \equiv 9087 \pmod{11}$$

$$3x + 1 \equiv 1$$

$$x \equiv 0 \pmod{11}$$

4.

$$1232x + 45 \equiv 9090 \pmod{24}$$

$$1232x \equiv 9045$$

$$8x \equiv 21 \pmod{24}$$

So there is no solution.

**Remark.** You can also just take everything mod 2 to get  $1 \equiv 0 \pmod{2}$

□

**Exercise 23.5.** Solve simultaneously the three congruences  $3x \equiv 4 \pmod{7}$ ,  $4x \equiv 5 \pmod{8}$ , and  $5x \equiv 6 \pmod{9}$

*Solution.* In the first equation,  $x \equiv 6 \pmod{7}$ .

In the second,  $4x \equiv 5 \pmod{8}$  is impossible.

Oops.

□

**Definition.** A **quadratic residue**  $\pmod{m}$  is a number  $n$  such that  $\exists i$  such that  $i^2 \equiv n \pmod{m}$

**Exercise 23.6.** Find all quadratic residues in mod 7, 8, and 9.

*Solution.* We're lazy so we'll just do mod 7. Well, we have  $0^2, 1^2, 2^2$ , and  $3^2 \pmod{7}$ , so 0, 1, 2, and 4.

□

**Exercise 23.7.** What is the most quadratic residues there can be  $\pmod{n}$  for  $n = 2m + 1$ ?

*Solution.* Because every number  $k$  has the same (residue?) as  $n - k$ , our answer is  $m + 1 + 1 = \boxed{m + 2}$  (since 0 goes to itself.)  $\square$

**Exercise 23.10.** Write down and expand the product for  $n = 28$

*Solution.* We have  $(1 + 2 + 4)(1 + 7) = 56$   $\square$

**Exercise 23.11.** Why does this work?

*Solution.* It's like a disguised genfunc!  $\square$

**Exercise 23.12.** Make the product simpler with sum of geometric series

*Solution.*

$$\prod_{i=0}^k \frac{p_i^{e_i+1} - 1}{p_i - 1}$$

Honestly this isn't much simpler.  $\square$

**Exercise 23.13.** These are pretty obviously correct, but I'm not particularly fond of either since they're not very helpful.

**Exercise 23.15.** Show that any perfect number of the form

$$2^k (2^{k+1} - 1)$$

is perfect if  $(2^{k+1} - 1)$  is prime.

This was discovered by Euclid, and *all known perfect numbers have this form.* (In particular, no odd perfect numbers have ever been found.)

*Solution.* By our handy-dandy formula, the sum of divisors is equal to

$$(2^{k+1} - 1)(2^{k+1} - 1 + 1)$$

Which is twice our original number, and we're done.  $\square$

**Exercise 23.19.** Find  $6^{1000} \pmod{23}$

*Solution.*  $6^{22} \equiv 1 \pmod{23}$ , so  $6^{990} \equiv 1 \pmod{23}$ . We then bash out  $6^{10} \pmod{23}$  and find that it's equal to  $\boxed{4}$   $\square$

**Exercise 23.20.** Find all possible periods a number can have  $\pmod{23}$

*Solution.* Well,  $a^2$  must be 1, so the period length must be 1, 2, 11, or 22.  $\square$

**Definition.** A **primitive root**  $\pmod{p}$  is a number  $g$  with period  $p - 1$ .

**Exercise 23.21.** Let the divisors of  $p - 1$  be  $d_1, d_2, \dots$ . Prove that if we have a primitive root  $g \pmod{p}$ , then for each  $d_i$  there is an element with period  $d_i$ .

*Solution.* If  $g$  has period  $p - 1$ , then  $g^{\frac{p-1}{d_i}}$  has period  $d_i$ .  $\square$

**Exercise 23.24.** It's just  $p^{k-1}$

**Exercise 23.27.** We get  $(m - 1)! \equiv 0 \pmod{a}$

**Exercise 23.28.** Look at the proof of Wilson's theorem

*Proof.* Consider some primitive root  $g \pmod{p}$ . By the definition of a primitive root,  $\{g^k \mid k \in [p-1]\} = [p-1]$ . So

$$(p-1)! \equiv g^{\frac{p(p-1)}{2}} \pmod{p}$$

But because  $g^p \equiv g(g^{p-1}) \equiv g \pmod{p}$ ,  $g^{\frac{p(p-1)}{2}} \equiv (g^p)^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod{p}$ . Let  $t = g^{\frac{p-1}{2}}$ . Note that

$$t^2 = g^{p-1} \equiv 1 \pmod{p}$$

So  $t^2 - 1 \equiv 0 \pmod{p}$ , and  $t \equiv \pm 1 \pmod{p}$

But because  $t = g^{\frac{p-1}{2}}$ , we can't have  $t \equiv 1$  because the period of  $g$  is  $p-1$  (and  $\frac{p-1}{2} < p-1$ ), so  $t \equiv -1$ , and  $(p-1)! \equiv -1 \pmod{p}$   $\square$

**Problem 373.** Show that for all prime numbers  $p$  greater than 3, 24 divides  $p^2 - 1$  evenly.

*Proof.*  $p^2 - 1 = (p+1)(p-1)$ . If  $p$  is prime then  $p \equiv 1$  or  $p \equiv 3 \pmod{4}$  so  $(p+1)(p-1)$  is divisible by 8. Similarly,  $p \equiv 1$  or  $2 \pmod{3}$  so one of the factors of  $p^2 - 1$  is divisible by 3, and we're done.  $\square$

**Problem 374.** Given that  $n - 4$  is divisible by 5, list which of the following are also divisible by 5:

$$n^2 - 1, n^2 - 4, n^2 - 16, n + 4, n^4 - 1$$

(Mandelbrot #3)

*Solution.* Well, just take everything mod 5.

$n \equiv 1 \pmod{5}$  so  $n^2 - 1$ ,  $n^2 - 16$ ,  $n + 4$ , and  $n^4 - 1$  are all divisible by 5.  $\square$

**Problem 375.** If the same number  $r$  is the remainder when each of the numbers 1059, 1417, and 2312 is divided by  $d$ , where  $d$  is an integer greater than one, find  $d - r$ .

*Solution.* Two pairwise differences between these numbers are 358 and 895. These are both divisible by 179, so  $d$  is 179. Plugging in,  $r$  is 164, so our answer is 15  $\square$

**Problem 376.** Find the sum of all  $x$ ,  $1 \leq x \leq 100$ , such that 7 divides  $x^2 + 15x + 1$ . (Mandelbrot #3)

*Solution.* The condition is equivalent to  $x^2 + x + 1 \pmod{7}$ . We just test all numbers  $\pmod{7}$ . 1 doesn't work, 2 does, 3 doesn't, 4 does, 5 doesn't, and 6 doesn't.

So  $\square$

**Problem 377.** Find the largest integer divisor of  $n^5 - n$

*Solution.* This expression is equal to  $n(n^2 + 1)(n + 1)(n - 1)$ .

Note that if  $n = 2$  then our expression is equal to 30, so our largest integer must be a divisor of 30.

We claim that 30 always divides  $n^5 - n$  (for  $n \in \mathbb{Z}$ ).

Clearly one of  $n$  and  $n - 1$  are divisible by 2, so our expression is always divisible by 2. Similarly, one of  $n - 1$ ,  $n$ , and  $n + 1$  are divisible by 3.

Now, suppose that this expression is not divisible by 5 for some  $n$ . That implies that each of  $n - 1, n, n + 1 \not\equiv 0 \pmod{5}$ . That means that  $n$  must be either 2 or 3  $\pmod{5}$ . But  $2^2 + 1 \equiv 3^2 + 1 \equiv 5 \pmod{5}$ , which is a contradiction since  $n$  is not divisible by 5. Because 2, 3, 5 all divide  $n^5 - n$  then  $30 \mid n^5 - n$  and we are done.  $\square$

**Remark 23.29.** Another solution could be to use induction and show that

$$30 \mid ((n+1)^5 - (n+1)) - (n^5 - n)$$

However this is terribly messy and sad.

**Problem 378.** What is the units digit of  $7^{(7^7)}$ ?

*Solution.* By Fermat's theorem we know that  $7^4 \equiv 1 \pmod{10}$ .

Now we need to find  $7^7 \pmod{4}$ .

Well, we know that  $7^2 \equiv 1 \pmod{4}$  so  $7^7 \equiv 3 \pmod{4}$

So our answer is  $\boxed{3}$ . □

**Problem 379.** What is the size of the largest subset  $S$  of  $[50]$  such that no pair of distinct elements of  $S$  has a sum divisible by 7?

*Solution.* Clearly if we have a number  $a \in S$ , we cannot have  $b \equiv -a$ , where  $b \in S$ .

So we just take all  $x \equiv 1, 2, 3 \pmod{7}$ .

We can also throw in a 7, so our answer is  $22 + 1 = \boxed{23}$  □

**Problem 381.** For any integer  $n$  greater than 1, how many prime numbers are there greater than  $n! + 1$  and less than  $n! + n$ ?

*Solution.*  $k \mid n! + k$  for  $k \leq n$ , so our answer is  $\boxed{0}$ . □

**Problem 382.** Find the last three digits of  $9^{105}$ .

*Solution.* This is equivalent to  $3^{210}$ .

$3^{400} \equiv 1 \pmod{1000}$  so  $3^{200} \equiv -1 \pmod{1000}$ .

We then bash out the last three digits of  $3^{10}$ , which are 049, so our answer is  $\boxed{951}$  □

**Problem 383.** What is the least possible value of  $n$  such that

$$\sqrt{\frac{3}{1} \cdot \frac{4}{2} \cdot \frac{5}{3} \cdots \frac{n+2}{n}}$$

is an integer?

*Solution.* This just cancels out to

$$\sqrt{\frac{(n+2) \cdot (n+1)}{2}}$$

Assuming  $n \in \mathbb{Z}$ , then one factor is a perfect square while the other is twice a perfect square. We test small perfect squares until we stumble upon  $\boxed{n = 7}$  □

**Problem 387.** Let  $x$  and  $y$  be integers such that  $2x + 3y$  is a multiple of 17. Show that  $9x + 5y$  must also be a multiple of 17. (USAMTS 1)

*Solution.* Note first that  $-4(2x + 3y) \equiv -8x - 12y \equiv 0 \pmod{17}$ .

So  $17x - 8x + 17y - 12y \equiv 0 \pmod{17}$ , and the rest is trivial. □

**Problem 388.** Note that 1990 can be “turned into a square” by adding a digit on its right, and some digits on its left, i.e.,  $419904 = 648^2$ . Prove that 1991 cannot be turned into a square by the same procedure; i.e., there are no digits  $d, x, y, \dots$  such that  $\dots yx1991d$  is a perfect square. (USAMTS 3)

*Solution.* Suppose there exists a number whose square satisfies the desired property. Let its last two digits be  $a$  and  $b$ . Clearly the second-to-last digit of  $20ab + b^2$  must be a 1. That implies that the tens digit of  $b^2$  is odd, so  $b = 4$  or  $b = 6$ . So we need to find  $a$  such that  $8a + 1 \equiv 1 \pmod{10}$  or  $12a + 3 \equiv 1 \pmod{10}$ , so we have  $10a + b = 04, 46, 54, \text{ or } 96$ . Uhh I dunno COME BACK HERE LATER  $\square$

**Problem 393.** Let  $n$  be an integer. If the tens digit of  $n^2$  is 7, what is the units digit of  $n^2$ ?

*Solution.* Consider  $n^2 \pmod{100}$ .

We want to find  $10a + b$  such that  $2ab + (\text{the tens digit of } b^2) = 7$ .

Clearly the tens digit of  $b^2$  must be odd, so  $b = 4$  or  $b = 6$ , so our units digit must be  $\boxed{6}$ .  $\square$

**Problem 394.** Prove that none of the numbers  $a_n = 1001001 \cdots 1001$  is prime, where  $n = 2, 3, 4, \dots$  denotes the number of occurrences of the digit 1 in  $a_n$ .

*Solution.* Define a function  $f(x, n)$  as

$$f(x, n) = \sum_{k=0}^{n-1} x^k = \frac{x^{n-1} - 1}{x - 1}$$

Conveniently,  $a_n = f(1000, n) = \frac{10^{3n+1} - 1}{(10-1)(111)}$ .

Now, consider only odd  $n$ , since  $2 \mid n \implies a_2 \mid a_n$ .

If  $n$  is odd then  $a_n = \frac{1000^{n+1} - 1}{999} = \frac{(1000^{\frac{n+1}{2}} + 1)(1000^{\frac{n+1}{2}} - 1)}{999}$ , and for  $n > 1$  this is clearly not prime, and we're done.  $\square$

**Remark.** I hate my proof. Hopefully there's something better.

**Problem 395.** Let  $p$  be a prime number. Prove that there exists an integer  $a$  such that  $p \mid a^2 - a + 3 \iff \exists b$  such that  $p \mid b^2 - b + 25$ .

*Solution.* The problem statement is equivalent to proving that

$\exists a$  such that  $a(a-1) \equiv -3 \pmod{p} \iff \exists b$  such that  $b(b-1) \equiv -25 \pmod{p}$

I'm not sure how to progress.  $\square$

**Problem 396.** Each of the numbers  $x_1, x_2, \dots, x_n$  equals 1 or -1, and

$$x_1x_2x_3x_4 + x_2x_3x_4x_5 + \cdots + x_{n-2}x_{n-1}x_nx_1 + x_{n-1}x_nx_1x_2 + x_nx_1x_2x_3 = 0$$

Prove that  $4 \mid n$ .

*Solution.* We first note that  $\square$

**Problem 398.** Find the positive integer  $m$  such that the polynomial  $p^3 + 2p + m$  divides  $p^{12} - p^{11} + 3p^{10} + 11p^3 - p^2 + 23p + 10$ .

*Solution.* We plug in 0 and find that  $m \mid 30$ .

We plug in 1 and find that  $m + 3 \mid 66$ , so  $m = 3, 8, 19, 30, 63$

So clearly  $m = 3$  or  $m = 30$ . We plug in  $p = 2$  to get  $2048 + 3072 + 88 - 4 + 46 + 30 = 5120 + 84 + 46 + 30 = 5280$ , and our possible divisors are 15 or 42.

42 doesn't work so our answer is  $\boxed{m = 3}$ .  $\square$

**Problem 399.** Prove that, for all positive integer pairs  $(a, b)$  where  $b > 2$ ,  $2^b - 1$  does not evenly divide  $2^a + 1$ .

*Solution.* Suppose  $\exists k \in \mathbb{Z}$  such that  $k(2^b - 1) = 2^a + 1$ .

Note that  $2^{b-a}(2^a + 1) = 2^b + 2^{b-a} > 2^b - 1$ , so  $k < 2^{b-a}$ .

But  $(2^{b-a} - 1)(2^a + 1) = 2^b - 2^a - 1 < 2^b - 1$ , so  $k > 2^{b-a} - 1$ .

This is absurd since  $k$  cannot be between two integers, so we're done.  $\square$

**Problem 400.** Let  $d$  be any positive integer not equal to 2, 5, or 13. Show that one can find distinct  $(a, b)$  in the set  $\{2, 5, 13, d\}$  such that  $ab - 1$  is not a perfect square.

*Solution.* Suppose there exists integers  $x, y, z$  such that

$$x^2 = 2d + 1$$

$$y^2 = 5d + 1$$

$$z^2 = 13d + 1$$

Then  $y^2 - x^2 = 3d$ ,  $z^2 - y^2 = 8d$ , and  $z^2 - x^2 = 11d$ .  $\square$

**Problem 401.** Let  $a$  and  $b$  be integers and  $n$  a positive integer. Prove that

$$n! \mid b^{n-1}a(a+b)(a+2b)\cdots(a+(n-1)b)$$

**Problem 402.** Prove that a positive integer is a sum of at least two consecutive positive integers if and only if it is not a power of two.

## §24 Diophantine Equations