A1. Define the *right derivative* of a function f at x = a to be the following limit if it exists.

$$\lim_{h \to 0^+} \frac{f(a+h) - f(a)}{h}, \text{ where } h \to 0^+ \text{ means}$$

h approaches 0 only through positive values.

#### Statements

- (1) If f is differentiable at x = a then f has a right derivative at x = a.
- (2) f(x) = |x| has a right derivative at x = 0.
- (3) If f has a right derivative at x = a then f is continuous at x = a.
- (4) If f is continuous at x = a then f has a right derivative at x = a.
- (1) True. Obvious from the definition of the derivative.
- (2) True. Right derivative is 1.
- (3) False. Consider the floor function at integer values.
- (4) False. Take  $x \sin \frac{1}{x}$  made continuous at 0.

A2. Suppose a rectangle EBFD is given and a rhombus ABCD is inscribed in it so that the point A is on side ED of the rectangle. The diagonals of ABCD intersect at point G. See the indicative figure below.



### Statements

- (5) Triangles CGD and DFB must be similar.
- (6) It must be true that  $\frac{AC}{BD} = \frac{EB}{ED}$ .
- (7) Triangle CGD cannot be similar to triangle AEB.
- (8) For any given rectangle EBFD, a rhombus ABCD as described above can be constructed.
- (5) True. Both are right angled and  $\angle FBD = \angle BDA = \angle GDC$ .
- (6) True. G bisects AC and BD. Use the similarity of CGD with  $DEB \simeq DFB$ .
- (7) False. They are similar when ABC is equilateral, which is possible.
- (8) False.  $ED \ge AD = AB \ge EB$  (hypotenuse), so need  $ED \ge EB$ .

A3. This question is about complex numbers.

### **Statements**

(9) The complex number  $(e^3)^i$  lies in the third quadrant.

(10) If  $|z_1| - |z_2| = |z_1 + z_2|$  for some complex numbers  $z_1$  and  $z_2$ , then  $z_2$  must be 0.

(11) For distinct complex numbers  $z_1$  and  $z_2$ , the equation  $|(z - z_1)^2| = |(z - z_2)^2|$  has at most 4 solutions.

(12) For each nonzero complex number z, there are more than 100 numbers w such that  $w^{2023} = z$ .

(9) False. Second quadrant. The argument of  $e^{3i}$  is 3 radian, which is just under  $172^{\circ}$ .

(10) False. Take  $z_2 = rz_1$  with r real and  $-1 \le r < 0$ .

(11) False.  $|(z-z_1)^2| = |z-z_1|^2$ , so z is equidistant from  $z_1$  and  $z_2$ . Solutions form a line.

(12) True. There are 2023 such w. Letting  $\frac{z}{|z|} = e^{i\theta}$ ,  $w = |z|^{\frac{1}{2023}} e^{\frac{i(2\pi k+\theta)}{2023}}$ ,  $k = 0, 1, \dots, 2022$ .

### A4. Statements

(13)

$$\lim_{x \to 0} e^{\frac{1}{x}} = +\infty.$$

(14)

$$\lim_{x \to \infty} \frac{\ln x}{x^{100}} < \lim_{x \to \infty} \frac{\ln x}{x^{\frac{1}{100}}}$$

(15) For any positive integer n,

$$\int_{-n}^{n} x^{2023} \cos(nx) dx < \frac{n}{2023}.$$

(16) There is no polynomial p(x) for which there is a single line that is tangent to the graph of p(x) at exactly 100 points.

(13) False. Limit from the left is 0.

(14) False. Both limits are 0. The numerator  $\ln x$  is dominated by any positive power of x.

(15) True. The function  $x^{2023}\cos(nx)$  is odd so by symmetry the integral is 0.

(16) False. For p(x) with exactly 100 multiple roots the X-axis is such a line. (This is essentially the only way: if y = ax + b is such a line for a polynomial q(x), then the X-axis is such a line for the polynomial q(x) - ax - b, which must have exactly 100 multiple roots.)

(17)  $4 < \sqrt{5 + 5\sqrt{5}}$ . (18)  $\log_2 11 < \frac{1 + \log_2 61}{2}$ . (19)  $(2023)^{2023} < (2023!)^2$ . (20)  $92^{100} + 93^{100} < 94^{100}$ .

- (17) True.  $16 < 5 + 5\sqrt{5}$  as  $11 < 5\sqrt{5}$  as 121 < 125. Taking square roots preserves order.
- (18) True.  $2^{2\log_2 11} = 121 < 2^{1+\log_2 61} = 122$ . Taking  $\log_2$  preserves order.
- (19) True. Pair numbers on the RHS symmetrically. n(2024 n) > 2023 for n = 1, ..., 2023.
- (20) True. Divide by 92<sup>100</sup> and use binomial theorem for  $(1+x)^{100}$  with  $x = \frac{1}{92}$  and  $x = \frac{2}{92}$ .

A6. For a sequence  $a_i$  of real numbers, we say that  $\sum a_i$  converges if  $\lim_{n \to \infty} \left( \sum_{i=1}^n a_i \right)$  is finite. In this question all  $a_i > 0$ .

## Statements

- (21) If  $\sum a_i$  converges, then  $a_i \to 0$  as  $i \to \infty$ .
- (22) If  $a_i < \frac{1}{i}$  for all *i*, then  $\sum a_i$  converges.
- (23) If  $\sum a_i$  converges, then  $\sum (-1)^i a_i$  also converges.
- (24) If  $\sum a_i$  does not converge, then  $\sum i \tan(a_i)$  cannot converge.
- (21) True.
- (22) False. Take  $a_i = \frac{1}{2i}$
- (23) True. Given  $a_i$  are all positive, so  $\sum_{i=1}^{n} (-1)^i a_i$  remains a Cauchy sequence.
- (24) False. Take all  $a_i = \pi$ .

## $\textbf{Continued} \longrightarrow$

# A7. Statements

(25) To divide an *integer* b by a *nonzero integer* d, define a quotient q and a remainder r to be *integers* such that b = qd + r and |r| < |d|. Such integers q and r always exist and are both unique for given b and d.

(26) To divide a polynomial b(x) by a nonzero polynomial d(x), define a quotient q(x) and a remainder r(x) to be polynomials such that b = qd + r and degree(r) < degree(d). (Here b(x) and d(x) have real coefficients and the 0 polynomial is taken to have negative degree by convention.) Such polynomials q(x) and r(x) always exist and are both unique for given b(x) and d(x).

(27) Suppose that in the preceding question b(x) and d(x) have rational coefficients. Then q(x) and r(x), if they exist, must also have rational coefficients.

(28) The least *positive* number in the set  $\{(a \times 2023^{2020}) + (b \times 2020^{2023})\}$  as a and b range over all *integers* is 3.

(25) False. For r > 0, we can increase quotient by 1 and make remainder negative.

(26) True.  $q_1d + r_1 = q_2d + r_2$  gives  $(q_1 - q_2)d = r_2 - r_1$ . Compare degrees.

(27) True. Uniqueness and the long division procedure ensure this.

(28) False. It is the gcd of  $2023^{2020}$  and  $2020^{2023}$ , which is 1.

**A8.** You play the following game with three fair dice. (When each one is rolled, any one of the outcomes 1, 2, 3, 4, 5, 6 is equally likely.) In the first round, you roll all three dice. You remove every die that shows 6. If any dice remain, you roll all the remaining dice again in the second round. Again you remove all dice showing 6 and continue.

# Questions

(29) Let the probability that you are able to play the second round be  $\frac{a}{b}$ , where a and b are integers with gcd 1. Write the numbers a and b separated by a comma. E.g., for probability  $\frac{10}{36}$  you would type 5,18 with no quotations, space, full stop or any other punctuation.

(30) Let the probability that you are able to play the second round but not the third round be  $\frac{c}{d}$  where c and d are integers with gcd 1. Write only the integer c as your answer. E.g., for probability  $\frac{34}{36}$  you would type 17 with no quotations, space or any other punctuation.

(29) The probability is  $1 - (\frac{1}{6})^3 = \frac{215}{216}$ , so 215,216 is the answer.

(30) The probability is  $\frac{1115}{66}$  by the calculation below, so 1115 is the answer.

 $\begin{array}{lll} P(3 \mbox{ dice left after first round}) & \times & P(\mbox{all 3 remaining dice show 6 in round 2}) + \\ P(2 \mbox{ dice left after first round}) & \times & P(\mbox{both remaining dice show 6 in round 2}) + \\ P(1 \mbox{ die left after first round}) & \times & P(\mbox{the remaining die shows 6 in round 2}) + \\ \end{array}$ 

$$= \left(\frac{5}{6}\right)^3 \times \left(\frac{1}{6}\right)^3 + 3\left(\frac{5}{6}\right)^2 \left(\frac{1}{6}\right) \times \left(\frac{1}{6}\right)^2 + 3\left(\frac{5}{6}\right) \left(\frac{1}{6}\right)^2 \times \left(\frac{1}{6}\right).$$

**A9.** Two lines  $\ell_1$  and  $\ell_2$  in 3-dimensional space are given by

 $\ell_1 = \{(t-9, -t+7, 6) \mid t \in \mathbb{R}\} \text{ and } \ell_2 = \{(7, s+3, 3s+4) \mid s \in \mathbb{R}\}.$ 

# Questions

(31) The plane passing through the origin and not intersecting either of  $\ell_1$  and  $\ell_2$  has equation ax + by + cz = d. Write the value of |a + b + c + d| where a, b, c, d are integers with gcd = 1.

(32) Let r be the smallest possible RADIUS of a circle that has a point on  $\ell_1$  as well as a point on  $\ell_2$ . It is given that  $r^2$  (i.e., the SQUARE of the smallest radius) is an integer. Write the value of  $r^2$ .

(31) (1, -1, 0) and (0, 1, 3) are the direction vectors of the given lines. (3, 3, -1) is a common perpendicular to both direction vectors. So 3x + 3y - z = 0 is an equation for the desired plane. Thus the answer is |3 + 3 - 1 + 0| = 5.

(32) Each of the two mentioned points must be the only intersection of such a circle with the respective line. The segment joining these points must be perpendicular to both  $\ell_1$  and  $\ell_2$  and is a diameter of any specified circle. Taking a general point on each line, a vector representing the segment joining the two points is (16 - t, s + t - 4, 3s - 2). Solving

$$(16 - t, s + t - 4, 3s - 2) \cdot (1, -1, 0) = 0$$
 and  $(16 - t, s + t - 4, 3s - 2) \cdot (0, 1, 3) = 0$ 

gives s = 0, t = 10. So  $(2r)^2 = (16 - 10)^2 + (10 - 4)^2 + (-2)^2 = 76$ . Thus the answer is 19.

A10. Consider the part of the graph of  $y^2 + x^3 = 15xy$  that is strictly to the right of the Y-axis, i.e., take only the points on the graph with x > 0.

## Questions

(33) Write the least possible value of y among considered points. If there is no such real number, write NONE (without any spaces or quotation marks or any other punctuation).

(34) Write the largest possible value of y among considered points. If there is no such real number, write NONE (without any spaces or quotation marks or any other punctuation).

(33) Regarding the equation as a quadratic in y gives  $y = \frac{1}{2}(15x \pm \sqrt{225x^2 - 4x^3})$ . So there is a y-value for every  $x \le \frac{225}{4}$ . We also have y > 0 for x > 0 since in that case  $15x > \sqrt{225x^2 - 4x^3}$ . As  $x \to 0$ , y also  $\to 0$ , so there is no minimum y-value.

(34) On the closed interval  $[0, \frac{225}{4}]$ , each sign in the formula for y gives a continuous function. So y must have a maximum, which cannot occur at x = 0 as y > 0 for x > 0. So we inspect y-values for the endpoint  $x = \frac{225}{4}$  and for any critical points. Differentiating implicitly,  $\frac{dy}{dx} = 0$  precisely when  $3x^2 = 15y$  for (x, y) on the graph. This gives only the point (50, 500). As 500 > (y-value at  $x = \frac{225}{4}$ ), the answer is 500. One can also argue without considering  $x = \frac{225}{4}$  at all. Plot the graph to see that there is no "endpoint".

## Part B solutions

**B1.** [11 points] We want to find *odd* integers n > 1 for which n is a factor of  $2023^n - 1$ .

- (a) Find the two smallest such integers.
- (b) Prove that there are infinitely many such integers.

**Solution**: (a) 2023 is 1 mod 3, so n = 3 works. Similarly using modular arithmetic one checks that 5 and 7 do not work but 9 does. (b) If n = k works so does n = 3k by induction:  $2023^{3k}-1 = (2023^k-1)(2023^{2k}+2023^k+1) = ($ multiple of k)(multiple of 3) as each summand in the second factor is 1 mod 3. Thus all powers of 3 satisfy the required condition.

**B2.** [12 points] Let  $\mathbb{Z}^+$  denote the set of *positive* integers. We want to find *all* functions  $g: \mathbb{Z}^+ \to \mathbb{Z}^+$  such that the following equation holds for any m, n in  $\mathbb{Z}^+$ .

$$g(n+m) = g(n) + nm(n+m) + g(m)$$

Prove that g(n) must be of the form  $\sum_{i=0}^{d} c_i n^i$  and find the precise necessary and sufficient condition(s) on d and on the coefficients  $c_0, \ldots, c_d$  for g to satisfy the required equation.

**Solution**: Setting m = 1 gives g(n + 1) - g(n) = n(n + 1) + g(1). Apply this repeatedly starting with n = 1 to get  $g(n) = ng(1) + \sum_{i=1}^{n-1} i^2 + i$ , which works out to  $ng(1) + \frac{1}{3}(n^3 - n)$ . Set g(1) to be an arbitrary positive integer k and verify that the resulting formula satisfies the given condition for all m, n. Thus  $g(n) = \frac{1}{3}n^3 + kn$  with  $k = (any positive integer) - \frac{1}{3}$ .

**B3.** [13 points] Suppose that for a given polynomial  $p(x) = x^4 + ax^3 + bx^2 + cx + d$ , there is exactly one *real* number r such that p(r) = 0.

- (a) If a, b, c, d are rational, show that r must be rational.
- (b) If a, b, c, d are integers, show that r must be an integer.

Possible hint: Also consider the roots of the derivative p'(x).

**Solution**: (a) The multiplicity of the root r must be either 2 or 4. In the latter case  $p(x) = (x-r)^4 = x^4 - 4rx^3 + 6r^2x^2 - 4r^3x + r^4$ . As 4r is a rational, so is r. If the multiplicity is 2 then the two non-real roots are complex conjugates and r is the only repeated root of p(x). So r is the only common root (whether real or not) of p(x) and p'(x) AND r is a simple root of the polynomial p'(x). So gcd(p,p') = x - r by looking at complete factorization of p(x) and p'(x) into linear terms (including complex roots). As p(x) and p'(x) have rational coefficients, so does their gcd by looking at each step of the division algorithm. (The preceding three sentences deserve careful consideration.) Therefore r must be rational.

(b) It is standard that a rational root of a monic polynomial with integer coefficients must be an integer. (Proof: write a rational root  $r = \frac{m}{n}$  with gcd(m, n) = 1, substitute into the polynomial, clear powers of n in the denominators and deduce that n cannot be divisible by any prime because that prime would then need to divide m as well. So  $n = \pm 1$ .) **B4.** [14 points] There are *n* students in a class and no two of them have the same height. The students stand in a line, one behind another, in no particular order of their heights.

- (a) How many different orders are there in which the shortest student is not in the first position *and* the tallest student is not in the last position?
- (b) The *badness* of an ordering is the largest number k with the following property. There is at least one student X such that there are k students taller than X standing ahead of X. Find a formula for  $g_k(n)$  = number of orderings of n students with badness k.

Example: The ordering 64 61 67 63 62 66 65 (the numbers denote heights) has badness 3 as the student with height 62 has three taller students (with heights 64, 67 and 63) standing ahead in the line and nobody has more than 3 taller students standing ahead.

Possible hints for (b): It may be useful to first count orderings of badness 1 and/or to find  $f_k(n)$  = the number of orderings of n students with badness less than or equal to k.

**Solution**: (a) There are (n-1)! + (n-1)! - (n-2)! orderings with the shortest student first or the tallest student last or both. So the desired number = n! - 2(n-1)! + (n-2)!, i.e.,  $(n-2)!(n^2 - 3n + 3)$ . Alternatively, first order all but the shortest and the tallest students in (n-2)! ways. The number of ways to insert the shortest and then the tallest is (n-2)(n-1) + 1. (What is the extra 1 for?)

(b) Following both the hints, first consider badness 1 and use induction. Leave out the shortest student and order the remaining n-1 students with badness 1. The shortest student can now go in place 1 or 2. There is one more possibility where the n-1 students have 0 badness (i.e., are in increasing order) and the shortest student goes in place 2. Inductively one gets the formula  $g_1(n) = 2^{n-1} - 1$  (valid even for n = 1, giving  $g_1(1) = 0$ ).

Induction to find  $f_k(n)$  is easier. Leave out the shortest student and order the remaining n-1 students with badness at most k. To maintain badness at most k, out of the n available slots for the shortest student, the allowed ones are precisely  $1, 2, \ldots, \min(k+1, n)$ . So  $f_k(n+1) = f_k(n) \min(k+1, n)$ . Answer:  $f_k(n) = n!$  if  $n \leq k+1$  and  $f_k(n) = k!(k+1)^{n-k}$  if  $n \geq k+1$ . (The formulas agree for n = k+1.)

Now  $g_k(n) = f_k(n) - f_{k-1}(n)$ . This works out to 0 if  $n \le k$  (as expected) and for  $n \ge k$ , one gets  $g_k(n) = k! ((k+1)^{n-k} - k^{n-k})$ .

**B5.** [15 points] Throughout this question every mentioned function is required to be a differentiable function from  $\mathbb{R}$  to  $\mathbb{R}$ . The symbol  $\circ$  denotes composition of functions.

- (a) Suppose  $f \circ f = f$ . Then for each x, one must have  $f'(x) = \_$  or  $f'(f(x)) = \_$ . Complete the sentence and justify.
- (b) For a non-constant f satisfying  $f \circ f = f$ , it is known and you may assume that the range of f must have one of the following forms:  $\mathbb{R}, (-\infty, b], [a, \infty)$  or [a, b]. Show that in fact the range must be all of  $\mathbb{R}$  and deduce that there is a unique such function f. (Possible hints: For each y in the range of f, what can you say about f(y)? If the range has a maximum element b what can you say about the derivative of f?)
- (c) Suppose that  $g \circ g \circ g = g$  and that  $g \circ g$  is a non-constant function. Show that g must be onto, g must be strictly increasing or strictly decreasing and that there is a unique such increasing g.

**Solution**: (a) f'(f(x))f'(x) = f'(x) for each x by chain rule, so f'(x) = 0 or f'(f(x)) = 1.

(b) (Argument taken from the answer by Dan Shved to <u>question 365363</u> on stackexchange.) For each y = f(x) in the range, f(y) = f(f(x)) = f(x) = y, so f is the identity function on the range. Therefore it is enough to show that the range is all of  $\mathbb{R}$ . As the range is given to be an interval (a proof is given below), at each y in the range, f'(y) = 1 by direct calculation. Note that if the range has endpoint(s), this derivative calculation is one sided at such a point. We will show that the range does *not* have an endpoint on either side. If the range interval has a left/right endpoint f(c) = c, then f has a minimum/maximum value at c, so it must be true that f'(c) = 0. (Recall that the *domain* is all of  $\mathbb{R}$ , so Fermat's theorem applies at x = c.) This contradicts the earlier calculation of a one-sided derivative at c being 1. So the range cannot be of the form  $(-\infty, b], [a, \infty)$  or [a, b] and must be all of  $\mathbb{R}$ .

(c) By applying g to the given equation,  $g \circ g \circ g \circ g = g \circ g$ . So if  $g \circ g$  is non-constant, it has to be the identity by part (b), i.e., g is its own inverse. In particular, being invertible, g is onto and one-to-one. Due to continuity, being one-to-one implies that g is monotonic. (This is standard. If g is one-to-one and not monotonic, we have some a, b, c for which a < b < c and WLOG g(a) < g(c) < g(b) by replacing g with its reflection in one/both axes if necessary. By the intermediate value theorem, we have  $d \in (a, b)$  with g(c) = g(d), giving a contradiction to g being one-to-one.) If g is increasing, g(x) < x implies x = g(g(x)) < g(x)and vice versa, so the only possibility is g(x) = x.

For completeness, here is a proof of the fact that you were asked to assume in part (b), namely that the range of f must be of the form  $\mathbb{R}, (-\infty, b], [a, \infty)$  or [a, b]: As f is continuous, if f(p) < r < f(q) then r is also in the range by intermediate value theorem. So the range must be one of the intervals (m, M) or (m, M] or [m, M) or [m, M], where m is the greatest lower bound of the range (possibly  $m = -\infty$ ), M is the least upper bound of the range (possibly  $M = \infty$ ), and it is understood that if m and/or M is not finite then only the open interval makes sense on the corresponding side. It remains to show that if either of m and M is finite, it must belong to the range. Now f(m + h) = m + h for small enough h > 0. (Recall that the function is non-constant so  $m \neq M$ .) So  $\lim_{h\to 0^+} f(m + h) = \lim_{h\to 0^+} m + h = m$ . At the same time, because f is continuous, the same limit must be f(m), so f(m) = m and thus m is in the range of f. For M, take limit from the left  $\left(\lim_{h\to 0^-} f(M + h), \text{ etc.}\right)$ 

**B6.** [15 points] Starting with any given positive integer a > 1 the following game is played. If a is a perfect square, take its square root. Otherwise take a + 3. Repeat the procedure with the new positive integer (i.e., with  $\sqrt{a}$  or a + 3 depending on the case). The resulting set of numbers is called the trajectory of a. For example the set  $\{3, 6, 9\}$  is a trajectory: it is the trajectory of each of its members.

Which numbers have a finite trajectory? Possible hint: Find the set

 $\{n \mid n \text{ is the smallest number in some trajectory } S\}.$ 

If you wish, you can get partial credit by solving the following simpler questions.

- (a) Show that there is no trajectory of cardinality 1 or 2.
- (b) Show that  $\{3, 6, 9\}$  is the only trajectory of cardinality 3.
- (c) Show that for any integer  $k \ge 3$ , there is a trajectory of cardinality k.
- (d) Find an infinite trajectory.

Solution: Let S = a trajectory, n = the smallest number in S. Note that  $1 \notin S$ , so  $n > \sqrt{n}$ . (a) |S|=1 implies  $n = \sqrt{n}$ , so n = 1, which is impossible. As  $n > \sqrt{n}$ , n cannot be a perfect square. So |S| = 2 implies  $S = \{n, n+3\}$  and  $n+3 = n^2$ , which cannot happen for n > 1. (b) Similarly |S| = 3 implies  $S = \{n, n+3, n+6\}$  and  $n+6 = n^2$ , which gives n = 3. (c) To get any finite cardinality repeatedly square 6 (or 9) and add these numbers to  $\{3, 6, 9\}$ . (d)  $(3k)^2 = 9k^2$  is 0 mod 3. Next,  $(3k+1)^2 = 9k^2 + 6k + 1$  and  $(3k+2)^2 = 9k^2 + 12k + 4$  are

 $1 \mod 3$ . As all squares are 0 or  $1 \mod 3$ , any S containing a 2 mod 3 number is infinite.

Claim: For a trajectory S with smallest number n, exactly one of the following two happens.

- 1. No square occurs after n in the trajectory. Hence n is 2 mod 3 and S is infinite.
- 2. A square does occur after n and n = 3. Hence S is finite.

Proof of the claim: The smallest number in S cannot be a square, so let  $k^2 < n < (k+1)^2$ . Assuming a square occurs after n, we will show that n = 3. The first encountered square after n is at most  $(k+3)^2$  (e.g., make cases depending on what k and n are mod 3.) So  $k^2 < n \le k+3$ , but  $k^2 < k+3$  only for k = 1, 2. Hence  $n < (k+1)^2 \le 9$ . Now n cannot be 2, 5, 8 because adding 3 repeatedly to these will never give a square. And n cannot be 4, 6, 7 because in each case one gets a smaller number by playing the game (respectively 2, 3, 2). So n = 3 is the only possibility. For the second sentence in case 1, note that repeatedly adding 3 to n will eventually give a square if and only if n is 0 or 1 mod 3.

Main answer: If a number in S is / is not divisible by 3, then the same is true for all numbers in S (check this). If the initial number a is a multiple of 3, then so is n, and hence we must be in case 2 of the claim. If a is not a multiple of 3, then nor is n, so  $n \neq 3$  and we must be in case 1. Thus multiples of 3 are precisely the numbers with finite trajectories.

**Notes**: (1) The above pattern was discovered earlier by Stephan Wagner. See problem 1 in IMO 2017 for a slightly different formulation. (2) The analysis in the solution generalizes naturally if 3 is replaced in the game by any prime p. (Why prime?) What happens for p = 2? For p = 5? For p = 7? In general?