AUTHORS

NOTICE TO AUTHORS

MATH SURVEY is the annual student journal of the Stuyvesant High School Mathematics Department. Students are invited to submit papers written during research courses or programs, as well as synopses of subjects learned in school or in private study. Written material need not represent original theory, but may instead summarize or explain a subject. Appropriate subjects include all aspects of mathematics and computer science not encountered in the standard high school curriculum. Papers written during the freshman year must be accompanied by a brief recommendation from the directing researcher or faculty member.

Each paper submitted to MATH SURVEY will be read by a faculty referee, who will convey notice through the editor of whether the paper has been accepted, and if so, what improvements are to be required; these may be mathematical or stylistic. The editorial staff reserves the right to alter final submitted drafts in point of style, wording, and layout.

Our readers expect a high level of both scholarship and exposition. To be a good candidate, and article should first contain important and challenging mathematical ideas. The writing should be clear and straightforward, so that the content may speak for itself. Sufficient background should be given so that a non-expert may learn and profit from each article.

Authors should submit their work in the LaTeX markup language if possible. Other submissions will be rendered in LaTeX at the discretion of the editors. To learn our formatting style, as well as how to properly cite other published materials, please examine the present volume.

All submissions should be sent to the Faculty Advisor.

Contents

1 Editor's Notes

Dear Reader,

Since 1927, the Math Survey has been the official publication of the Mathematics Department, produced by the efforts of students of Stuyvesant High School. The Math Survey Staff is honored to continue this longstanding tradition.

I would like to thank the Math Survey Staff for all of their hard work to make this publication possible. I would also like to thank the many individuals who contributed their works to the Math Survey. In addition, on behalf of the entire Math Survey Staff, I would also like to thank our faculty advisor, Mr. Aziz Jumash, for his support and guidance in the publication of this journal and Ms. Ferrara, Ms. Zhang, and the math department for their support.

Without further ado, enjoy!

Sincerely,

Jon Lu

Editor

2 Foreword

By Jan Siwanowicz

Jan K. Siwanowicz is an alumni of Benjamin Cardozo High School and was a former member of the New York City Math Team. Some of his problem solving successes include winning a bronze medal in the 1994 International Math Olympiad and being named a Putnam Fellow for the 2001 William Lowell Putnam Undergraduate Competition. Today, he continues his involvement with problem solving and helps the New York City Math Team.

When I was working at the HCSSiM program in the summer of 1999, a senior staff member was polling the instructors, asking "what do you like about mathematics?" When she shared the answers afterwards, they were all different, and while I do not remember them all, I do recall my reply.

"I value that mathematics rewards the consideration of concepts from different points of view."

The same question was asked of me on several different occasions, and I have always given the same answer. I would do so today, as well. The idea of constantly trying to look for a different point of view is a part of me, it drives me when I am working on math problems and when I am teaching, it shapes my analysis and empathy. It makes me stronger and wiser, even if it creates a paradoxical doubt as to why has my answer to the above question not changed after all this time.

But the doubt of confidence in your correctness that is created when looking for different points of view is a good type of doubt. Perhaps it is what we sometimes need more of, a caution that there is always room for improvement. I have gradually come to believe that the number

of absolutes in life lies in the single digits, and while the rejection of absolutes is a strange idea coming from a math nerd like myself, it perhaps is not so strange if you consider the constant hunger for different points of view.

Mathematics essentially cannot be mastered in its whole. There simply is not enough time to review all of the knowledge that the subject has accumulated. However, no one person needs to know all of the intricacies of all fields. Research today is done by teams of people, with modern technology taking collaboration to new heights, with teams of scientists from all over the globe working as if they were in the same location. The idea of being open to different points of view shapes collaboration as well, bridging gaps between cultures and languages, but also to different backgrounds, not only professional but also organizational and social. It allows us to have faith in members of our team who are masters in fields we have not had time to study and makes a modern collaborative team greater than the sum of its parts.

I am grateful that mathematics taught me to accept the possibility of existence of concepts I have not considered before, to see things in many different lights, and to have faith in others to show me things I have not seen before. While I have accepted that I will not master the knowledge of all of mathematics, I am happy to have found a way of learning that embodies what I believe is the spirit of mathematics. I wonder what will I learn today?

3 The Chicken McNugget Theorem

By Calvin Lee

Background

This problem, also known as the Postage Stamp Problem, supposedly arose when a mathematician was buying Chicken McNuggets at McDonalds. Back then, the packages held either 9 or 20 pieces. The question was: what is the largest number of McNuggets that is impossible to buy? The answer, as it turns out, is 151. The Chicken McNugget Theorem generalizes this; if the boxes held a or b pieces, with a and b relatively prime, the largest unattainable number is given by:

$$ab - a - b$$

An extension of the theorem gives the number of unattainables:

$$\frac{(a-1)(b-1)}{2}$$

In this paper, we will prove both of these facts rigorously.

(For those of you eager to impress, $mn - m - n$ is the Frobenius number of the set $\{m, n\}$.)

Some Notation

Throughout this article, all variables are assumed to be integers unless otherwise stated.

If b is a multiple of a, we write $a|b$. For example, $9|72$ and $13|1001$. The statement $a|b$ is read *a divides b* and implies that $\frac{b}{a}$ is an integer and that $a \leq b$.

The remainder when a is divided by b is denoted by $a \bmod b$ and is always an integer r with $0 \leq r < b$. For example $100 \bmod 7 = 2$. Notice that if $r = a \bmod b$, then $b|(a - r)$. (In the

example, we see that $7|98$).

This is not to be confused with the statement $a \equiv c \bmod b$, which is read *a is congruent to c modulo b*, which means that $b|(a-c)$ (or equivalently $a \bmod b = c \bmod b$). This is less strict than the statement $a = c \bmod b$, which means that $0 \leq a < b$ *and* $a \equiv c \bmod b$.

Finitely Many?

Just to get a feel for the problem, we will go ahead and first prove (using tools that are useful later) that if a and b are relatively prime, then there are only finitely many unattainable numbers. Note that if a and b share a divisor d, then any number of the form $ax + by$ will be divisible by d; therefore the infinitely many numbers not divisible by d cannot be attained. This is why, for the rest of the paper, we require that a and b be relatively prime.

To prove that there are only finitely many unattainable numbers, we will show that any number $N \geq 2ab$ is attainable. Since $N = 2ab$ is attainable from $x = b$ and $y = a$, we will only consider $N > 2ab$. Since a and b are relatively prime, there is a unique number $0 \leq I_a < b$ such that $I_a a \equiv 1 \bmod b$.

Exercise: See if you can prove this statement for yourself! A proof is provided later.

Similarly, define I_b such that $I_b b \equiv 1 \bmod a$ and $0 \leq I_b < a$. Then if we define $x' = NI_a \bmod b$ and $y' = NI_b \bmod a$, we have:

$$(x'a + y'b) \equiv (NI_a)a \equiv N \bmod b$$

$$(x'a + y'b) \equiv (NI_b)b \equiv N \bmod a$$

$$x'a + y'b \equiv N \bmod ab$$

The last step only holds because a and b are relatively prime. Note that $x' < b$ and $y' < a$, so

the LHS is less than $2ab$. Since $N > 2ab$, we can define the positive integer $U = N - (x'a + y'b)$. Then U is a multiple of ab; define the positive integer $j = \frac{U}{ab}$. Then $jab = N - (x'a + y'b)$, so

$$N = x'a + y'b + jab = (x' + jb)a + (y')b$$

This is our solution, which we will denote by $(\overline{x}, \overline{y})$. $\overline{x} = x' + jb$ is positive integer, and $\overline{y} = y'$ is an integer between 0 and $a - 1$, inclusive. Also notice that this is unique. (All other positive solutions will have $y \geq a$). This demonstrates that every number above $2ab$ is attainable.

But What About $N < 2ab$?

All of this is useful for the next part, where we analyze the unattainable N, which are obviously less than $2ab$. The above still generates a solution $(\overline{x}, \overline{y})$. However, since $N < 2ab$, U is not necessarily positive, and thus $j < 0$ is possible. So $\overline{x} = x' + jb$ may not be positive. I claim that an integer is unattainable if and only if $\overline{x} < 0$.

First, consider what happens when $\overline{x} \geq 0$. $\overline{y}$ is always nonnegative, so the solution $(\overline{x}, \overline{y})$ is a solution, like before, and N is attainable. So N is unattainable only if $\overline{x} < 0$.

Now we assume $\overline{x} < 0$ and prove that $N = \overline{x}a + \overline{y}b$ is unattainable. To do so, we suppose for the sake of contradiction that there exists a solution of positive integers $(\underline{x}, \underline{y})$ that satisfies $N = \underline{x}a + \underline{y}b$. Then we have

$$0 = \overline{x}a + \overline{y}b - (\underline{x}a + \underline{y}b) = (\overline{x} - \underline{x})a + (\overline{y} - \underline{y})b \Rightarrow (\underline{x} - \overline{x})a = (\overline{y} - \underline{y})b$$

The LHS is divisible by a. Since a and b are relatively prime, this means that $\overline{y} - \underline{y} = k_1 a$ for some integer (not necessarily positive) k_1. Similarly, we have $\underline{x} - \overline{x} = k_2 b$, where k_2 is positive (since clearly the LHS is positive). Substituting gives

$$(k_2 b)a = (k_1 a)b \Rightarrow k_2 = k_1$$

Therefore k_1 is positive, so $\underline{y} = \overline{y} - k_1 a$. But since $\overline{y} < a$ (recall its definition), we have

$$\underline{y} = \overline{y} - k_1 a \leq \overline{y} - a < 0$$

This contradicts our original assumption that $\underline{y}$ was positive; therefore, we are done.

Therefore, any number of the form $N = \overline{x}a + \overline{y}b$ is unattainable if and only if $\overline{x} < 0$. We also, of course, must have $\overline{y} < a$ (this comes from the definition of $\overline{y}$). Notice that the maximum unattainable integer N occurs when $\overline{x}$ and $\overline{y}$ are both maximized; this happens at $\overline{x} = -1$ and $\overline{y} = a - 1$, in which case we have

$$N = -1(a) + (a-1)b = ab - a - b$$

We have successfully proved the theorem! Now we prove its extension, namely that the number of unattainable numbers is

$$\frac{1}{2}(a-1)(b-1)$$

To prove this, consider the $(a-1)(b-1) - 2$ integers from 1 to $ab - a - b - 1$. Take any one of them, L, and define $M = ab - a - b - L$. Both M and L are part of the range we are considering. If L is attainable, then $\overline{x} \geq 0$. So:

$$M = ab - a - b - (\overline{x}a + \overline{y}b) = (-1 - \overline{x})a + (a - y - 1)b$$

Since $0 \leq y \leq a - 1$, $a - y - 1 \geq 0$; since $\overline{x} \geq 0$, $-1 - \overline{x} < 0$. If we express $M = \overline{x'}a + \overline{y'}b$, the ordered pair $(\overline{x'}, \overline{y'})$ is unique if we must have $0 \leq \overline{y'} < a$. Therefore, $(\overline{x'}, \overline{y'}) = (-1-\overline{x}, a-y-1)$, since $M = \overline{x'}a + \overline{y'}b$ and $0 \leq \overline{y'} \leq a - 1$. Therefore $\overline{x'} < 0$ and M is unattainable.

The reverse holds: if M is unattainable, then $\overline{x'} \leq -1$, so $\overline{x} = -1 - x \geq 0$; this makes L attainable (the y's work out exactly the same; they are never a concern).

Therefore, there is a 1-to-1 correspondence between unattainable numbers and attainable numbers (if we only concern ourselves with the $(a-1)(b-1)-2$ integers from 1 to $ab-a-b-1$). So half of those integers are unattainable, and we have

$$\frac{(a-1)(b-1)-2}{2}+1=\frac{(a-1)(b-1)}{2}$$

unattainable numbers. (The plus 1 is needed because the biggest unattainable number, $ab-a-b$, is not in the range we considered). Notice that this must be an integer; since a and b are relatively prime, at least one is odd.

Appendix

Earlier in the paper, you were presented with the following statement as an exercise: given that a and b are relatively prime, there exists a number I_a such that

$$I_a a \equiv 1 \bmod b$$

To prove this, we proceed by contradiction; suppose that the claim is false. Then consider the sequence

$$a, 2a, 3a, 4a, \cdots, (b-1)a$$

Since a and b are relatively prime, none of those numbers is a multiple of b. Consider a new sequence consisting of the remainders when these numbers are divided by b. Since none of the numbers in this new sequence is 0 or 1 mod b, there only $b-2$ possible distinct numbers that could occur in this sequence. However, the sequence has $b-1$ terms. By the Pigeonhole Principle (also known as the Box Principle or Dirichlet's Box Principle), the sequence must have at least one repeated number. So two of its values are the same; suppose they are in

positions k_1 and k_2, where $k_1 \geq k_2$. Then

$$k_1 a \bmod b = k_2 a \bmod b \Rightarrow k_1 a \equiv k_2 a \bmod b \Rightarrow k_1 a - k_2 a \equiv 0 \bmod b \Rightarrow a(k_1 - k_2) \equiv 0 \bmod b$$

But $k_1 - k_2$ is an integer between 0 and $b-1$, so $a(k_1 - k_2)$ is a member of the original sequence. But none of the members of the sequence are divisible by b. So we have a contradiction, thus proving the original statement.

Works Cited

`www.artofproblemsolving.com/Wiki/index.php/Chicken_McNugget_Theorem`.

4 The Totient Function and its Properties

Based on an article by Eric Kolbusz

Rewritten by Calvin Lee

Edited by Richard Yip, Calvin Lee, Gideon Leeper, and Annique Wong

A Note to the Reader

This article has been adapted from a paper written for the Math Fair.

Also, if you are unfamiliar with modular arithmetic, please refer to the notational note on page 22 before reading further.

Definition and Examples

The totient function, denoted by $\phi(n)$, is defined as the number of natural numbers less than or equal to n that are coprime to n.

For example, it is easy to see that $\phi(20) = 8$: 20's prime factorization is $2^2 5$ so every number that is even or divisible by 5 is not coprime to 20. Crossing these numbers out we see:

$$1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}.$$

There are 8 numbers remaining, namely $1, 3, 7, 9, 11, 13, 17, 19$, so $\phi(20) = 8$.

Note that 20 is crossed out in the list for $\phi(20)$. In general, n is not coprime to itself, so it doesn't matter whether we include it in the list or not.

We now examine some more general cases. If n is a prime number, every number listed will be coprime to n, and the only number that will be crossed out will be n itself. For example,

the list for 13 would be

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \cancel{13},$$

so $\phi(13) = 12$. Therefore, we can conclude that $\phi(n) = n - 1$ if n is prime.

What if n is the product of two prime numbers, say p and q? For example, we can set $n = 33$. First, we cross out all the multiples of three. There are 11 of them.

$$1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8, \cancel{9}, 10, 11, \cancel{12}, 13, 14, \cancel{15}, 16, 17, \cancel{18},$$

$$19, 20, \cancel{21}, 22, 23, \cancel{24}, 25, 26, \cancel{27}, 28, 29, \cancel{30}, 31, 32, \cancel{33}.$$

Similarly, there are q p's in pq. Next, we cross out the multiples of 11:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \cancel{11}, 12, 13, 14, 15, 16, 17, 18,$$

$$19, 20, 21, \cancel{22}, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, \cancel{33}.$$

Similarly, note how there are 3 multiples of 11 in 33 (p q's in pq). However, also note that the two lists share a crossed-out 33. This is because 33 is both a multiple of 3 and 11. We can also be assured that pq is the only common multiple for any prime p and q since their least common multiple is pq. The final list is:

$$1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8, \cancel{9}, 10, \cancel{11}, \cancel{12}, 13, 14, \cancel{15}, 16, 17, \cancel{18},$$

$$19, 20, \cancel{21}, \cancel{22}, 23, \cancel{24}, 25, 26, \cancel{27}, 28, 29, \cancel{30}, 31, 32, \cancel{33}.$$

We crossed out 3 numbers in the first list, and 11 in the second, but since there is an overlap at the last number, we must subtract 1. So we crossed out a total of $3 + 11 - 1 = 13$ numbers, and therefore $\phi(33) = 33 - 13 = 20$.

In general, when we directly evaluate $\phi(pq)$, we cross out $p+q-1$ elements. So there are $pq-(p+q-1)$ numbers remaining in the list. This expression for $\phi(pq)$ can be factored:

$$\begin{aligned} pq-(p+q-1) &= pq-p-q+1 \\ &= (p-1)(q-1) \end{aligned}$$

Now we examine $\phi(p^n)$, where p is prime. For example, let $p=5$ and $n=3$. Since the only factor of 125 is 5, every multiple of 5 would be crossed out on the list, getting us:

$$1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,$$

$$18,19,20,\ldots 116,117,118,119,120,121,122,123,124,125.$$

The multiples of 5 here are $1\times 5, 2\times 5, 3\times 5, 4\times 5, \ldots 24\times 5$, and 25×5. Since the final multiple of 5 is 5×25, it is the 25th multiple. Since there are 25 numbers crossed off the list, $\phi(125) =$ (number of elements in original list) $-$ (number of elements crossed out) $= 125-25 = 100$.

Generally, p^n can be rewritten as$(p^{n-1})p$. The numbers that are not coprime to p in the interval of 1 to p^n (those that are crossed off the list) are all multiples of p: $p, 2p, 3p, 4p, \ldots (p^{n-1}-1)p, (p^{n-1})p$. Note how the coefficient of the crossed out number $(1,2,3,4,\ldots)$ is the number of the term to be crossed out. This means that there are p^n numbers crossed out, so we get that $\phi(p^n)$ is the difference between the number of elements in the original list and the number of elements crossed out. Thus, $\phi(p^n) = p^n - p^{n-1} = (p^{n-1})(p-1)$. However, one can factor out p^n:

$$\phi(p^n) = p^n\left(1-\frac{p^{n-1}}{p^n}\right) = p^{n-1}\left(1-\frac{1}{p}\right)$$

The Multiplicity of $\phi(N)$

To prove the general formula, we need to prove one more thing: $\phi(ab) = \phi(a)\phi(b)$ as long as a and b are coprime. For example, consider finding $\phi(120)$, with $a = 8, b = 15$. We know $\phi(8) = \phi(2^3) = 2^3(1 - \frac{1}{2}) = 4$ and $\phi(15) = \phi(3 \cdot 5) = (3 - 1)(5 - 1) = 8$, and we would like to show that $\phi(120) = (4)(8) = 32$. As usual, we list all the numbers from 1 to 120. But this time, we'll do it using 15 rows of 8:

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & 7 & 8 \\ 9 & 10 & 11 & \cdots & 15 & 16 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 113 & 114 & 115 & \cdots & 119 & 120 \end{array}$$

If a column's first entry is even, all of the entries in its column are also even, since we add 8 as we move down a column. So we cross out those columns:

$$\begin{array}{cccccc} 1 & \cancel{2} & 3 & \cdots & 7 & \cancel{8} \\ 9 & \cancel{10} & 11 & \cdots & 15 & \cancel{16} \\ \vdots & \cancel{\vdots} & \vdots & \cdots & \vdots & \cancel{\vdots} \\ 113 & \cancel{114} & 115 & \cdots & 119 & \cancel{120} \end{array}$$

Notice that only odd numbers are left, and so every number remaining is relatively prime to 8. Now we need to cross out all the numbers that aren't relatively prime to 15. Pick an arbitrary column, with first entry r. The numbers in this column are:

$$r, r + 8, r + 16, \cdots, r + 112$$

There are 15 numbers in this column. Can any two have the same remainder when divided by 15? Suppose two of them, namely $r + 8a$ and $r + 8b$, did. Then $8a$ and $8b$ have the same

remainder when divided by 15. Then their difference, $8(b-a)$ is divisible by 15. Clearly the 8 isn't contributing any of the factors of 15, so it must be $b-a$ that is divisible by 15. Then b and a have the same remainder when divided by 15. But since b and a range from 0 to 14, this must mean $b=a$. So all of the numbers in this column have different remainders when divided by 15.

Why do we care about the remainder when divided by 15? If n is coprime to 15, then $n-15$ is coprime to 15. So the number of numbers in the rth column that are coprime to 15 is the same as the number of numbers from 0 to 14 that are coprime to 15. This, by definition, is $\phi(15)=8$. So there are $\phi(8)=4$ columns, each of which have $\phi(15)$ numbers relatively prime to 120. Therefore, the total number of numbers is $\phi(8)\phi(15)$. This example can easily be generalized to show that $\phi(ab)=\phi(a)\phi(b)$ as long as a and b are coprime:

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & a-1 & a \\ a+1 & a+2 & a+3 & \cdots & 2a-1 & 2a \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \cdots & (b-1)a+(a-1) & ab \end{array}$$

There will be $\phi(a)$ columns whose first entries are coprime to a. If x is not coprime to a, then $x+a$ can't be coprime to a; similarly, if x is coprime to a, then $x+a$ is coprime to a.[1] Therefore, we consider only the $\phi(a)$ columns whose initial elements are coprime to a. In each of those columns, there will be b numbers. Consider any column, with first element r:

$$r, r+a, r+2a, \cdots, r+(b-1)a$$

Like before, we claim[2] that no two of these numbers have the same remainder when divided by

[1] See Appendix for a proof of this claim.

[2] This claim is used frequently and should be well understood by the reader. A proof is provided in the Appendix.

b. Also, like before, x is coprime to b if and only if the remainder when x is divided by b is coprime to b. So the number of numbers coprime to b in that column is the same as the number of numbers coprime to b in the following list:

$$0, 1, 2, 3, \cdots, b-1$$

By definition, there are $\phi(b)$ numbers in that list coprime to b, so there are $\phi(b)$ this column coprime to b. Any of these $\phi(b)$ numbers is also coprime to a, as we established above. So they're all coprime to ab, too. Therefore, there are $\phi(a)$ columns with $\phi(b)$ coprime numbers in each, for a total of $\phi(a)\phi(b)$ numbers coprime to ab. Therefore, $\phi(a)\phi(b) = \phi(ab)$ if a and b are relatively prime.

The General Formula for $\phi(n)$

We now have all the tools we need to get a general formula for $\phi(n)$ for any n. It is clear that this formula depends on the prime factorization of n. Since $\phi(p^n) = p^n(1 - \frac{1}{p})$, we have that for $N = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots + p_k^{e_k}$,

$$\begin{aligned}
\phi(N) &= \phi\left(p_1^{e_1}\right)\phi\left(p_2^{e_2}\right)\cdots\phi\left(p_k^{e_k}\right) \\
&= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_1^{e_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\
&= (p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots + p_k^{e_k})\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\
&= N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

This formula intuitively makes sense; for each prime p_i, we cross out roughly $\frac{1}{p_i}$ of the remaining numbers. For example, we calculate $\phi(5040)$:

$$5040 = 2^4 * 3^2 * 5 * 7$$

$$\phi(5040) = 5040 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 1152.$$

Uses in Modular Arithmetic

This is interesting, but it does not immediately seem useful. However, there are several extremely important and widely used theorems based on the totient function, of which the most famous is the Euler-Fermat Theorem, a generalization of Fermat's Little Theorem. Fermat's Little Theorem states that for any prime p and any natural number a, $a^{p-1} \equiv 1 \pmod{p}$. There are many beautiful proofs of this theorem, but we will not show them here.

Proof of the Euler-Fermat Theorem

We must show that if a and n are coprime integers, then:

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Proof. We consider the list of numbers from 0 to $n-1$ that are coprime to n. By definition, there must be $\phi(n)$ of them:

$$x_1, x_2, \cdots, x_{\phi(n)}$$

Now we multiply each element by a to form a new list y, with $y_i = ax_i$. Since a and n are relatively prime, $y_k = ax_k$ is also relatively prime to n. Furthermore, no two y_n have the same remainder when divided by n. So each x_i corresponds to a unique y_j, such that $x_i \equiv y_j \bmod n$. Therefore, we can rearrange the list y to get a list y':

$$y'_1, y'_2, \cdots, y'_{\phi(n)}$$

This new list is such that

$$y'_1 \equiv x_1 \bmod n, y'_2 \equiv x_2 \bmod n, \cdots, y'_{\phi(n)} \equiv x_{\phi(n)} \bmod n$$

Multiplying all of these statements together[3] gives

$$(y'_1) \cdot (y'_2) \cdot \cdots, (y'_{\phi(n)}) \equiv (x_1)(x_2) \cdots (x_{\phi(n)}) \bmod n$$

But notice that since the sequence y' is a rearrangement of the sequence y, their products are the same. Substituting $y_i = ax_i$ gives

$$(ax_1) \cdot (ax_2) \cdot \cdots, (ax_{\phi(n)}) \equiv (x_1)(x_2) \cdots (x_{\phi(n)}) \bmod n$$

Since all of the x_is are coprime to n, we can divide through by them. We are left with $\phi(n)$ a's being multiplied on the left hand side, and a 1 on the right hand side. Thus,

$$a^{\phi(n)} \equiv 1 \bmod n.$$

□

The Totient Function in RSA Cryptography

The Euler-Fermat Theorem is the center of RSA encryption, a popular system of public-key encryption. Public key means that everyone, including those trying to crack the messages being sent, know how messages are being encrypted. So the encryption process must be nearly irreversible for everyone except the intended receiver. One action that turns out to be very difficult to reverse is multiplying large primes (that is, primes with hundreds or thousands of digits). The multiplication can be done very quickly on any computer. However, even today's

[3] A review of modular multiplication and division is provided in the Appendix.

supercomputers cannot brute-force factor the result in a feasible amount of time. It is the totient function that gives us an decryption method that depends on the ability to factor products of large primes.

So how does this work? Suppose everyone wants to send message to you. You randomly pick two large, distinct primes p, q and multiply them to get $n = pq$. Now pick a relatively small odd integer e that is relatively prime to $\phi(n)$. Tell everyone what e and n are.

When people want to send a message M (a number), they send you the result of computing $M^e \bmod n$. Now, to decrypt it, we find the number d such that $ed \equiv 1 \bmod \phi(n)$. [4] Then we evaluate $C^d \bmod n$, where C is whatever they sent you. Why does this work? Since $ed \equiv 1 \bmod \phi(n)$, $ed = k\phi(n) + 1$. Then

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k\phi(n)+1} \equiv M\left(M^{\phi(n)}\right)^k \bmod n$$

Since $M^{\phi(n)} \equiv 1 \bmod n$ by Euler-Fermat, $C^d \equiv M \bmod n$; therefore, this process will yield M at the end, assuming $M < n$ (and since n is so big, M should be less than n.)

Imagine we tried to crack RSA the straightforward way; that is, given e, we tried to find a d such that $ed \equiv 1 \bmod \phi(n)$. We immediately run into the problem that $\phi(n)$ depends on the prime factorization of n. Is there an efficient way to find M given e, n, and $M^e \bmod n$? Is there an efficient way to factor large integers? Currently, the best way to find M given $M^e \bmod n$ is to find $\phi(n)$, and no efficient method is known for factoring n. This makes RSA encryption very useful and widely used today, proving the power of Euler's totient function.

[4] This number is guaranteed to exist; see the Appendix of the article about the Chicken McNugget Theorem.

Appendix

Throughout this section, the positive integers a and b are assumed to be relatively prime unless explicitly stated otherwise.

$b + a$ is coprime to a if and only if b is coprime to a.

Suppose b is not coprime to a. Then there exists a prime p that divides both b and a. So $b = pb'$ and $a = pa'$ for some integers b' and a'. Then $b + a = p(b' + a')$, so $b + a$ is divisible by p. Then $b + a$ is not coprime to a, either. So $b + a$ is coprime to a only if b is coprime to a.

Now we prove that if x and a are coprime, then $x + a$ and a are also coprime. Suppose x is coprime to a and $x + a$ is not coprime to a. Then there exists a prime p that divides both $x + a$ and a. Then $x + a = pk$ and $a = pa'$ for some integers k and a'. Then $x = (x + a) - a = p(k - a')$ is also divisible by p. So x and a are both divisible by p, contradicting our original assumption that x and a are coprime. So if x and a are coprime, then $x + a$ and a must also be coprime.

If S is the set of numbers $0 \leq x_i < a$, x_i coprime to a, and $b * x_1$, $b * x_2$, ... are elements of S', then $S = S'$

In other words, if S contains all the numbers from 0 to $a - 1$ that are coprime to a, and S' contains the result when each element from S is multiplied by b and reduced modulo 15, then S and S' contain the same elements, albeit in a different order.

To prove this, we establish that every number in S' is in S and that S' contains no repeats. By definition, S' and S have the same number of elements, so once we've established that, we conclude they must be the same set. (Think of a 6-element set containing only distinct numbers

from 1 to 6. Clearly it's $\{1, 2, 3, 4, 5, 6\}$ in some order.)

Every number in S' is of the form bx_i, where b and x_i are both relatively prime to a. Since b contains none of a's prime factors, and neither does x_i, then bx_i can't contain any of a's prime factors, either. So bx_i is coprime to a. By our earlier work above, $bx_i - ka$ is also coprime to a, if k is an integer. Therefore, $bx_i \bmod a$ is coprime to a and is between 0 and $a - 1$; therefore it is in S.

Suppose b contained a repeat; $bx_i \bmod a = bx_j \bmod a$ for some $x_i \neq x_j$. This would imply $b(x_i - x_j) \equiv 0 \bmod a$. Since b is coprime to a, we can divide by it (see below). Then $x_i - x_j \equiv 0 \bmod a$, so $x_i \equiv x_j \bmod a$. But x_i and x_j are both from 0 to $a - 1$, so they must be equal, contradicting that $x_i \neq x_j$. So there cannot be any repeated numbers; we are done.

Multiplication and Division in Modular Arithmetic

We claimed that if $x \equiv y \bmod a$ and $w \equiv z \bmod a$, then $xw \equiv yz \bmod a$. This enabled us to multiply lots of statements together. Why can we do this?

We know that $x \equiv y \bmod a$ means there's an integer k such that $x = y + ka$. Similarly, there's an integer j such that $w = z + ja$. Multiplying these equations gives

$$xw = (y + ka)(z + ja) = yz + yja + kaz + jka^2 = yz + (yj + kz + jka)a$$

so $xw = yz + Ka$, where $K = yj + kz + jka$ (so it's an integer). So $xw \equiv yz \bmod a$, as desired.

We also claimed that $bx \equiv by \bmod a$ means $x \equiv y \bmod a$ (recall that b and a are relatively prime). Recall that $bx \equiv by \bmod a$ means that $bx - by$ is a multiple of a. This means $b(x - y)$ is a multiple of a. But since b contributes none of the factors of a, the factor of $(x - y)$ must contribute all of them. So $x - y$ is divisible by a, so $x \equiv y \bmod a$, as desired.

5 On the Caccetta-Häggkvist Conjecture

by Jongyoon Lee

The History of the Problem

A *directed graph (or digraph)* $D = (V, E)$ consists of a finite set $V = V(D)$ of vertices and a finite set $E = E(D)$ of edges, where an edge is an ordered pair of vertices. The *outdegree* of a vertex $v \in V$, denoted $d_D^+(v)$ (or simply $d^+(v)$ if the underlying digraph is clear from the context), is the number of edges $e \in E$ of the form $e = (v, u)$. The *indegree* of a vertex $v \in V$, denoted $d_D^-(v)$ (or just $d^-(v)$ if D is implicit), is the number of edges $e \in E$ of the form $e = (u, v)$.

A *directed cycle of length* l in D is a sequence of l edges (v_0, v_1), $(v_1, v_2), \ldots$ (v_{l-1}, v_l) such that $v_i \neq v_j$ for all $0 \leq i < j \leq l-1$ and $v_0 = v_l$. A cycle of length 1 is an edge of the form (v, v); cycles of length 1 are also called *loops*. A cycle of length 2 consists of two edges (u, v) and (v, u) where $v \neq u$; cycles of length 2 are called *digons*. A *directed triangle* is a cycle of length 3 with edges (u, v), (v, w) and (w, u), where vertices u, v and w are distinct. The *girth* of a digraph is the length of the shortest directed cycle in the digraph.

It is reasonable to expect that a directed graph with many edges should have directed cycles and in particular, small girth. However, this intuition is contradicted by *transitive tournaments*, digraphs T with $V(T) := \{v_1, v_2, \ldots, v_n\}$ and $E(T) := \{(v_i, v_j) \,|\, 1 \leq i < j \leq n\}$. It is clear that $|E(T)| = \binom{n}{2}$ but T has no directed cycles. Notice that vertex v_n in T is a *sink*, that is, a vertex of outdegree 0. This observation suggests the following

Conjecture 1.1 *(Caccetta and Häggkvist, [3]) Let D be a digraph on n vertices. If every vertex*

of D has outdegree at least d then the digraph contains a directed cycle of length at most $\lceil n/d \rceil$.

The following construction shows that the upper bound on the outdegree is the best possible.

Theorem 1.2 *(Behzad, Chartrand and Wall, [1]) Let d be a positive integer. For every integer $n \geq d$ there exists a digraph $D = (V, E)$ with $|V| = n$ vertices such that $d_D^+(v) \geq d$ for all $v \in V$ and the girth of D is exactly $\lceil n/d \rceil$.*

Proof. Let $n \geq d$ and let $R = \{1, 2, \ldots, d\}$. Consider the additive group $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, where $\overline{x} = x + n\mathbb{Z}$. Consider the digraph $D(V, E)$ with $V = \mathbb{Z}_n$ and whose edges are the ordered pairs of the form $\{(\overline{x}, \overline{x} + \overline{r})$, where $\overline{x} \in \mathbb{Z}_n$ and $r \in R$. Obviously, D thus constructed satisfies the required hypotheses.

Let now (v_0, v_1), $(v_1, v_2), \ldots,$ (v_{l-1}, v_l) be a cycle of length l where $v_0 = v_l$ and $v_i = v_{i-1} + r_i$ for $r_i \in R$. Then $\overline{r_1} + \overline{r_2} + \ldots + \overline{r_l} = \overline{0}$ in $\mathbb{Z}_n$ and so

$$r_1 + r_2 + \ldots r_l \equiv 0 \pmod{n}.$$

Since $0 < r_1 + r_2 + \ldots r_l \leq d\,l$ it follows that $d\,l \geq n$ which implies that $l \geq n/d$. Thus the girth of D is at least $\lceil n/d \rceil$.

It remains to show there exists a directed cycle of length exactly $\lceil n/d \rceil$. Let $n = d\,l - r$ where l and r are integers and $0 \leq r \leq n - 1$. It then follows that $l = \lceil n/d \rceil$. If $r = 0$ then let $r_i = d$ for all $i = 1, 2, \ldots, l$. If $1 \leq r \leq n - 1$ then let $r_i = r$ for $i = 1, 2, \ldots, l - 1$ and $r_l = d - r$. This choice gives that $r_i \in R$ and $r_1 + r_2 + \ldots + r_l = n$. Let $v_i = \overline{r_1} + \overline{r_2} + \ldots + \overline{r_i}$, for $i = 1, 2, \ldots, l$. Then (v_0, v_1), $(v_1, v_2), \ldots,$ (v_{l-1}, v_l) is a cycle of length $l = \lceil n/d \rceil$. This completes the proof. □

Despite its elementary statement and intuitive appeal Conjecture 1.1 is far from being solved. The case $d = 1$ is elementary. The case $d = 2$ has been proved by Caccetta and Häggkvist themselves in [3]. The case $d = 3$ was proved by Hamidoune in [6], and the cases $d = 4$ and $d = 5$ were settled by Hoáng and Reed [8]. Shen [13] proved that the conjecture holds for all $d \geq 2$ and $n \geq 2d^2 - 3d + 1$.

To this date, these are the only cases in which Conjecture 1.1 has been proved in its full strength. Short of settling the original statement, several researchers attempted to prove some weaker results.

For instance, one approach is to show that under the conditions stated in the hypothesis, there is a directed cycle of length at most $\lceil n/d \rceil + k$ where k is some small constant. This has been shown for some values of k, as follows: Chvátal and Szemerédi proved in [4] that $k = 2500$ is a valid choice; Nishimura [10] showed that it suffices to take $k = 304$; finally, the current record is held by Shen, who showed in [14] that $k = 73$ is good enough. Hence, Caccetta-Häggkvist conjecture is true up to an additive constant.

As mentioned in the second last paragraph, the problem is solved when d is small. The much more interesting cases are when $d = \Omega(n)$. For instance, the case $d = \lceil n/2 \rceil$ is an elementary exercise, but the case $d = \lceil n/3 \rceil$ is still unsolved despite a lot of attention.

Researchers have looked for a minimum constant c such that the condition that every vertex has outdegree at least cn forces a directed cycle of length 3. The conjecture is that $c = 1/3$. We give below a brief history of the progress made in this particular case.

- $c = (3 - \sqrt{5})/2 = 0.38196\ldots$ by Caccetta and Häggkvist via an induction approach [3].
- $c = (2\sqrt{6} - 3)/5 = 0.379795\ldots$ by Bondy with a nice subgraph counting argument [2].

- $c = 3 - \sqrt{7} = 0.35424\ldots$ by Shen with another inductive proof [12].
- $c = 0.3465\ldots$ by Hladký, Král and Norin [7] using Razborov's flag-algebra method.
- $c = 0.34354\ldots$ by Lichiardopol [9] with a refinement of the technique in [7].

While it is obvious from the above enumeration that a lot of effort was focused on the directed triangle case, it is quite surprising that the literature lacks any bounds on the very next unsolved case. More precisely, we are raising the following

Problem 1.3 *Let D be a digraph such that the outdegree of each vertex is at least cn. What value of c guarantees the existence of a directed cycle of length at most 4?*

Of course, $c = 0.34354\ldots$ is already a sufficiently high value as per Lichiardopol's result cited earlier. Fortunately, we can do a little bit better.

Theorem 1.4 *Let D be a digraph on $n \geq 3$ vertices such that the outdegree of each vertex is greater than $(n-2)/3$. Then D contains a directed cycle of length at most 4.*

Admittedly, the result is rather weak if regarded from the point of view of the Caccetta-Häggkvist conjecture. A "good" value for c would be in the neighborhood of $1/4$ rather than $1/3$. However, we believe the result is new and moreover, the proof is entirely elementary (which is not the case with the results proved in [7] and [9]).

Second, we use a combination of Shen's and Bondy's techniques to achieve a slightly better bound than Shen's $c = 3 - \sqrt{7}$ bound mentioned above.

Theorem 1.5 *Let D be a digraph on n vertices such that the outdegree of each vertex is at least αn, where $\alpha = 0.354222103\ldots$ is the smallest real root of the cubic equation $39x^3 - 105x^2 + 69x - 13 = 0$. Then D contains a directed cycle of length at most 3.*

While this represents only a tiny improvement on Shen's $3-\sqrt{7} = 0.35424868\ldots$ bound, we feel that a more inspired use of both inductive and counting arguments might lead to a substantially better result.

The rest of the paper is organized as follows. In section 2 we follow the presentation from [2] and introduce a useful counting technique. The section ends with a proof of Theorem 1.4. Section 3 presents Shen's inductive argument needed for the $c = 3 - \sqrt{7}$ bound; the section concludes with a proof of Theorem 1.5. The paper ends with a section dedicated to conclusions and directions of future research.

Counting Subgraphs

Let D be a digraph on n vertices with no cycle of length ≤ 3. Hence, D contains no loops, no digons and no directed triangles. Assume that each vertex of D has out-degree d (the same for all vertices in $V(D)$) and we denote by d_i the in-degree of vertex v_i, for $i = 1, 2, \ldots, n$. As Bondy noticed in [2], there are 32 types of 4-vertex sub-digraphs of D, shown in figure 3.

Let us denote by y_i, the number of subgraphs of D of type i and let x_i denote the number of *induced* subgraphs of D of type i, for $i = 1, 2, \ldots, 32$. Of course, every y_i can be expressed in terms of the x_j-s; it is enough to count how many different subgraphs of type i are contained in every subgraph of type j and then sum up over j from 1 to 32. For instance, we have

$$\begin{aligned} y_2 = x_2 + 2(x_3 + x_4 + x_5 + x_6) + 3(x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15}) + \\ + 4(x_{16} + x_{17} + x_{18} + x_{19} + x_{20} + x_{21} + x_{22} + x_{23} + x_{24} + x_{25}) + \\ + 5(x_{26} + x_{27} + x_{28} + x_{29} + x_{30} + x_{31}) + 6x_{32}, \end{aligned}$$

as the graph of type 1 contains no edge, the graph of type 2 contains exactly one edge, the

graphs of type i with $3 \leq i \leq 6$ contain three edges each etc. Similarly, we have

$$y_4 = x_4 + 2x_7 + 2x_8 + 2x_9 + x_{12} + x_{14} + x_{15} + 3x_{16} + 2x_{17} + x_{18} + 3x_{19} + x_{20} + 2x_{21} +$$

$$+ 2x_{22} + 2x_{24} + 4x_{25} + 2x_{26} + 3x_{27} + 4x_{28} + 2x_{29} + 2x_{30} + 3x_{31} + 4x_{32},$$

as the graph of type 4 has one directed path of length 2, the graph of type 7 contains two such paths and so on. In general, if $\mathbf{y} = (y_1, y_2, \ldots y_{32})$ and $\mathbf{x} = (x_1, x_2, \ldots, x_{32})$, then we can write

$$\mathbf{y} = \mathbf{x}\,\mathbf{A}^T,$$

where A is a 32×32 matrix.

It follows that for every $1 \leq i \leq 32$, y_i can be written as a linear combination of x_j's,

$$y_i = \sum_{j=1}^{32} a_{i,j} x_j, \tag{1}$$

where the coefficients $a_{i,j}$ are the entries of matrix $\mathbf{A}$ – see table 1. We corrected an error which appeared in [2] - the seventh and eighth row were basically switched. The error was inconsequential since Bondy did not use y_7 and y_8 in establishing his result. However, we are going to use these quantities later, so it is essential to have the correct expressions.

At this point let us introduce two quantities which are going to be needed later. Let t denote the number of transitive triangles in D; a *transitive triangle* is isomorphic to a digraph with edge set $\{(u,v),(u,w),(v,w)\}$ as shown in figure 1 (a). We say that w is the "sink-vertex" of the triangle and that u is the "source-vertex" of the triangle.

Also, let $s = \sum_{i=1}^{n} \binom{d_i}{2}$, the number of 2-in claws in D. A 2-*in claw* is isomorphic to a digraph with edge set $\{(u,w),(v,w)\}$ as shown in figure 1 (b). A 2-*out claw* is isomorphic to a digraph with edge set $\{(u,v),(u,w)\}$. We prove the following inequality which is going to be needed later.

$$t \leq n\binom{d}{2} \leq s. \tag{2}$$

The left inequality is a consequence of the fact that the number of transitive triangles cannot exceed the number of 2-out claws. But this latter one equals $\sum_{i=1}^{n} \binom{d}{2} = n\binom{d}{2}$ as desired. The right inequality follows from the equality

$$\sum_{i=1}^{n} d = \sum_{i=1}^{n} d_i$$

and from the fact that $f(x) = x^2$ is concave up. Applying Jensen's inequality we obtain that

$$\sum_{i=1}^{n} \binom{d}{2} \leq \sum_{i=1}^{n} \binom{d_i}{2},$$

which completes the argument.

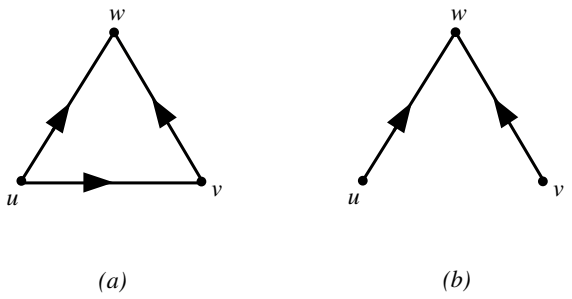


Figure 1: (a) A transitive triangle. (b) A 2-in claw.

We saw in (1) that *every* y_i can be written as a linear combination of x_j's. It turns out that *some* of the y_i's can be expressed in terms of n, d, s and t. The results are contained in the following

Theorem 2.1 *(Bondy [2]) With the notations above we have*

$$
\begin{aligned}
y_1 &= \binom{n}{4}, \quad y_2 = nd\binom{n-2}{2}, \quad y_3 = \frac{n(n-3)d^2}{2} - s, \quad y_4 = n(n-3)d^2, \\
y_5 &= n(n-3)\binom{d}{2}, \quad y_6 = (n-3)s, \quad y_7 = nd\binom{d}{2}, \quad y_8 = ds, \\
y_9 &= nd^3, \quad y_{10} = n\binom{d}{3}, \quad y_{12} = 2nd\binom{d}{2} - t, \quad y_{13} = 2ds - t, \\
y_{15} &= (n-3)t, \quad y_{16} = dt, \quad y_{17} = (d-1)t, \quad y_{18} = (d-2)t.
\end{aligned}
$$

Proof. Most of these equalities are quite obvious - actually, none of them is proved in [2] The formulae for y_1, y_2, y_5, y_6, y_8, y_{10} and y_{12} are trivial. On the other hand, it is easy to evaluate y_{15}, y_{16}, y_{17} and y_{18} since the corresponding digraphs consist of a transitive triangle plus (eventually) an extra out-edge from either one of the three vertices. To save space, we skip these simple proofs. We will prove the equalities for y_3, y_4, y_7, y_9, y_{12} and y_{13} only.

Start with y_3. There are nd edges in D. We have to find the number of disjoint pairs. This means that from $\binom{nd}{2}$ we have to subtract the number of 2-out claws, the number of 2-in claws and the number of directed paths of length 2. It follows that

$$
y_3 = \binom{nd}{2} - n\binom{d}{2} - \sum_{i=1}^{n}\binom{d_i}{2} - \sum_{i=1}^{n} d_i d = \frac{nd}{2}\left(nd - 1 - (d-1) - 2d\right) - s = \frac{n(n-3)d^2}{2} - s.
$$

Notice that Bondy got the formula for y_3 slightly wrong in his paper: $y_3 = \frac{n(n-1)d^2}{2} - s$ instead of the correct one proved above. In the end, this did not matter since the leading term was the same in both expressions. The other equalities follow along similar lines.

$$
\begin{aligned}
y_4 &= (n-3)\sum_{i=1}^{n} d\, d_i = (n-3)d\sum_{i=1}^{n} d_i = (n-3)d\sum_{i=1}^{n} d = n(n-3)d^2. \\
y_7 &= \sum_{i=1}^{n} d_i\binom{d}{2} = \binom{d}{2}\sum_{i=1}^{n} d_i = \binom{d}{2}\sum_{i=1}^{n} d = nd\binom{d}{2}. \\
y_9 &= \sum_{(v_i,v_j)\in E} d^+(v_j)d^-(v_i) = d\sum_{(v_i,v_j)\in E} d_i = d\sum_{i=1}^{n} d\, d_i = d^2\sum_{i=1}^{n} d_i = d^2\sum_{i=1}^{n} d = nd^3. \\
y_{13} &= \sum_{i=1}^{n}\left(\binom{d_i}{2}2d - \text{number of triangles having } v_i \text{ as a sink vertex}\right) = 2ds - t.
\end{aligned}
$$

□

We are now in position to prove the main result of our paper.

Theorem 2.2 *Let D be a digraph on n vertices such that the outdegree of each vertex is greater than $(n-2)/3$. Then D has a directed cycle of length at most four.*

Proof. . Let $d > (n-2)/3$ denote the minimum outdegree over all vertices of D. Suppose that D does not contain any directed cycle of length less than or equal to 4. We seek to obtain a contradiction. Without loss of generality, we may assume that every vertex of D has outdegree *exactly* d. Indeed, if a vertex v has initial outdegree $d' > d$, remove from D exactly $d' - d$ edges of the form (v, w). Obviously, this procedure cannot create any new cycles.

Consider the quantity $y_3 - y_9 - y_{12} + y_{16}$. From (1) we obtain that

$$y_3 - y_9 - y_{12} + y_{16} = x_3 + x_{13} + x_{14} + x_{20} + x_{21} + 2x_{23} - 2x_{25} + 2x_{29}. \tag{3}$$

Recall that we assumed D does not contain any cycles of length 4 ; this translates to $x_{25} = 0$. Combining this information with (3) it follows that

$$y_3 - y_9 - y_{12} + y_{16} \geq 0. \tag{4}$$

On the other hand, from Theorem 2.1 we have that

$$y_3 - y_9 - y_{12} + y_{16} = \frac{n(n-3)d^2}{2} - s - nd^3 - 2nd\binom{d}{2} + t + dt. \tag{5}$$

From (4) and (5) it follows that

$$\frac{n(n-3)d^2}{2} - nd^3 - 2nd\binom{d}{2} + dt \geq s - t.$$

Using now (2) and the last inequality we get that

$$\frac{n(n-3)d^2}{2} - nd^3 - 2nd\binom{d}{2} + dn\binom{d}{2} \geq 0.$$

This is equivalent to $d \leq (n-2)/3$, contradiction. □

An Inductive Argument

Let c be a positive number such that the condition that every vertex of a n vertex digraph has outdegree at least cn forces a directed cycle of length at most 3. As mentioned in the introductory section Shen [12] proved that $c = 3 - \sqrt{7} = 0.354248689\ldots$ is one such value. We present his argument below.

Theorem 3.1 *(Shen [12]) Any digraph on n vertices with minimum outdegree at least cn with $c = 3 - \sqrt{7}$ contains a directed cycle of length at most 3.*

Proof. We proceed by induction on n. It is easily seen that the statement is valid for $n = 3$. Let now suppose that the result holds for all digraphs with fewer that n vertices and let D be a counterexample with n vertices. As in the proof of Theorem 2.2 it may be supposed that $d^+(v) = d = \lceil cn \rceil$ for all $v \in V$, that is, all vertices of D have the same outdegree. Let $N^+(u) = \{v \in V \,|\, (u,v) \in E\}$, the out-neighborhood of u and $N^-(u) = \{v \in V \,|\, (v,u) \in E\}$, the in-neighborhood of u.

For any edge $(u,v) \in E$ define

$p(u,v) := |N^+(v) \setminus N^+(u)|$, the number of *induced* 2-paths whose first edge is (u,v).

$q(u,v) := |N^-(u) \setminus N^-(v)|$, the number of *induced* 2-paths whose second edge is (u,v).

$t(u,v) := |N^+(u) \cap N^+(v)|$, the number of transitive triangles whose "base" is (u,v).

We claim that

$$n > 2d + d^-(v) - ct(u,v) + q(u,v) - p(u,v). \tag{6}$$

Indeed, if $t(u,v) = 0$ then $N^+(v)$, $N^-(v)$ and $N^-(u) \setminus N^-(v)$ are pairwise disjoint sets of cardinalities d, $d^-(v)$ and $q(u,v)$, respectively. Since in this case $p(u,v) = d$, inequality (6) follows. If $t(u,v) > 0$, some vertex $w \in N^+(u) \cap N^+(v)$ has outdegree less than $ct(u,v)$ in the sub-digraph induced by $N^+(u) \cap N^+(v)$ otherwise this sub-digraph would contain a

cycle of length at most 3, from the minimality of D. It follows that w is joined to at least $d^+(w) - p(u,v) - c\,t(u,v)$ vertices which are not in $N^+(v)$ - see Figure 2, the red bubble.

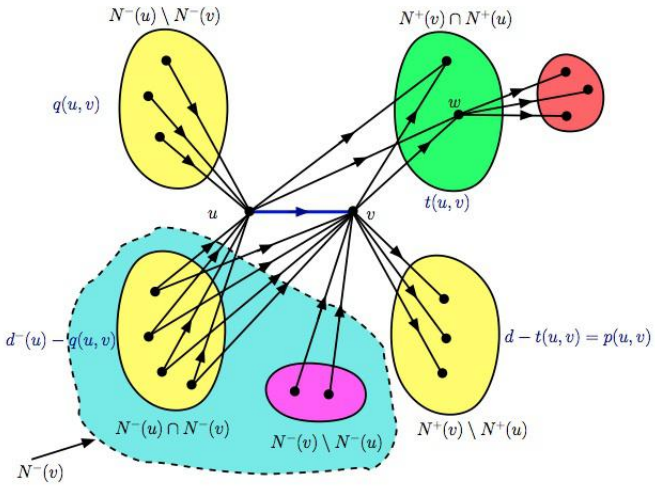


Figure 2: The sets in Theorem 3.1; the sizes of the sets are in blue

Since D has no directed triangle, these vertices are neither in $N^-(v)$ nor in $N^-(u) \setminus N^-(v)$. It follows that we have four pairwise disjoint subsets: $N^-(v)$ (the blue bubble), $N^-(u) \setminus N^-(v)$ (the top left yellow bubble), $N^+(v)$ (the two right bubbles) and the set of out-neighbors of w which are not in $N^+(v)$ (the red bubble). It follows that

$$n-2 \geq \big(d^+(w) - p(u,v) - c\,t(u,v)\big) + d^-(v) + d + q(u,v) = 2d + d^-(v) - c\,t(u,v) + q(u,v) - p(u,v).$$

This proves (6). Notice also the following equalities:

$$\sum_{(u,v)\in E} t(u,v) = t, \quad \text{the number of transitive triangles in } D.$$

$$\sum_{(u,v)\in E} d^-(v) = \sum_{v\in V} (d^-(v))^2 = 2\sum_{v\in V} \binom{d^-(v)}{2} + \sum_{v\in V} d^-(v) = 2s + nd.$$

$$\sum_{(u,v)\in E} p(u,v) = \sum_{(u,v)\in E} q(u,v), \quad \text{the number of induced } 2-\text{paths in } D.$$

Sum now inequality (6) over all $(u,v) \in E$. Using the three equalities above we obtain that

$$n^2 d > 2nd^2 + 2s + nd - c\,t, \tag{7}$$

which after using (2) gives

$$n^2 d > 2nd^2 + nd + (2-c)n\binom{d}{2} > 2nd^2 + \frac{2-c}{2} nd^2.$$

Using now that $d = \lceil cn \rceil$ this readily implies that

$$1 > \left(3 - \frac{c}{2}\right) c \qquad \text{from which } c > 3 - \sqrt{7}.$$

The proof of Theorem 3.1 is complete. □

We can marginally improve this bound by combining Shen's argument with Bondy's counting technique.

Theorem 3.2 *Let D be a digraph on n vertices such that the outdegree of each vertex is at least αn, where $\alpha = 0.354222103\ldots$ is the smallest real root of the cubic equation $39x^3 - 105x^2 + 69x - 13 = 0$. Then D contains a directed cycle of length at most 3.*

Proof. The proof is identical to the proof of Theorem 3.1 until we obtain inequality (7). Notice that in this case $d = \lceil \alpha n \rceil$. With the new notation this becomes

$$n^2 d > 2nd^2 + 2s + nd - \alpha t, \tag{8}$$

Refer to quantities y_i introduced in section 2. Consider the following expression:

$$P := 8y_1 - 6y_2 + 4y_3 + 4y_4 + 6y_5 + 4y_6 - 4y_7 - 2y_8 - 2y_9 - 6y_{10} - 4y_{12} - 3y_{13} - 4y_{15} + 2y_{16} + 3y_{17} + 3y_{18}.$$

Using the entries of $\mathbf{A}$ – see table 1 we obtain that

$$P = 8x_1 + 2x_2 + 2x_5 + 2x_{10} + 2x_{11} + x_{13} + 2x_{14} + 3x_{20} + x_{21} + x_{22} + 2x_{24} + x_{27} + 2x_{30} \geq 0.$$

On the other hand, using Theorem 2.1 we obtain that

$$P = -\frac{1}{3}n(3d - n)^3 + 2(2n - 4d - 5)(s - t) - 2n(3d - n)^2 - \frac{11}{3}n(3d - n) - 2n - 6s,$$

from which, taking into account that $n/3 \leq d$ and $s \geq t$ (see (2)) gives that

$$P < \frac{1}{3}n(n - 3d)^3 + 2(2n - 4d)(s - t).$$

If we now combine the last two relations we obtain that

$$\frac{1}{3}n(n-3d)^3 + 4(n-2d)(s-t) \geq 0. \tag{9}$$

From (8) and (9) we obtain that

$$s - \frac{n(3d-n)^3}{12(n-2d)} \geq t > \frac{2s + 2nd^2 - n^2 d}{\alpha}$$

which after using (2) leads to

$$n^2 d - 2nd^2 - \frac{\alpha(3d-n)^3}{12(n-2d)} > (2-\alpha)s \geq (2-\alpha)n\binom{d}{2}.$$

Replacing now d by αn and ignoring the lower order terms the inequality above can be written as

$$1 - 2\alpha - \frac{(3\alpha-1)^3}{12(1-2\alpha)} > \frac{\alpha(2-\alpha)}{2}.$$

which eventually reduces to

$$39\alpha^3 - 105\alpha^2 + 69\alpha - 13 < 0.$$

This is the same cubic from the hypothesis of Theorem 3.2. This completes the proof. □

Conclusions

We proved that every digraph on n vertices with minimum outdegree $d > (n-2)/3$ contains a directed cycle of length at most 4. We also showed that every digraph on n vertices with minimum outdegree $d > 0.3542221\ldots n$ contains a directed cycle of length at most 3. Solving the Caccetta-Häggkvist conjecture in its strongest form seems to be out of reach at this particular moment.

It is reasonable to expect that better results may be obtained by a more inspired use of Bondy's counting arguments. One possible line of attack would be to consider the digraphs on 5 vertices. There are 317 different 5-vertex digraphs which contain no directed cycle of length

less than or equal to 3. Of these, 302 are acyclic, 16 have girth 4 and one has girth 5. Obviously, given this amount of data, the use of a computer becomes indispensable.

A different idea would be to employ Razborov's flag algebra technique. There have been quite a few instances lately where this method proved to be successful. As we already mentioned in the introduction the currently best bounds for the triangle case were obtained via this technique - see [7, 9]. Razborov himself showed in [11] that Caccetta-Häggkvist conjecture holds digraphs which do not contain any (induced) sub-digraphs of types 17, 21 or 22 - see Figure 3.

We can easily prove the following similar

Theorem 4.1 *Let D be a digraph on n vertices which contains no induced subgraphs of types* 16 *or* 28 *as described in Figure 3. Further assume that every vertex has outdegree $d > (n-2)/3$. Then D contains a directed cycle of length at most* 3.

Proof. Suppose by contradiction that D contains no loop, no digon and no directed triangle. The condition in the theorem translates to $x_{16} = x_{28} = 0$. Using matrix $\mathbf{A}$ - see table 1 - it turns out that

$$y_{15} - 2y_{16} - y_{17} = x_{15} - x_{16} + x_{18} + x_{19} + x_{20} + x_{21} + x_{27} - x_{28} + 2x_{29} + 2x_{30}.$$

On the other hand from Theorem 2.1 it immediately follows that

$$y_{15} - 2y_{16} - y_{17} = (n-3)\,t - 2d\,t - (d-1)\,t = (n-2-3d)\,t.$$

Combining the last two equations and using that $x_{16} = x_{28} = 0$ it follows that

$$(n-2-3d)\,t \geq 0 \longrightarrow d \leq (n-2)/3.$$

But this contradicts the assumption in the theorem. The proof is complete. □

Most likely, other results similar to the ones mentioned above are possible. These are useful as they help us better understand the structure of the extremal digraphs. Conceivably, this may shed some light on the nature of difficulties surrounding the problem.

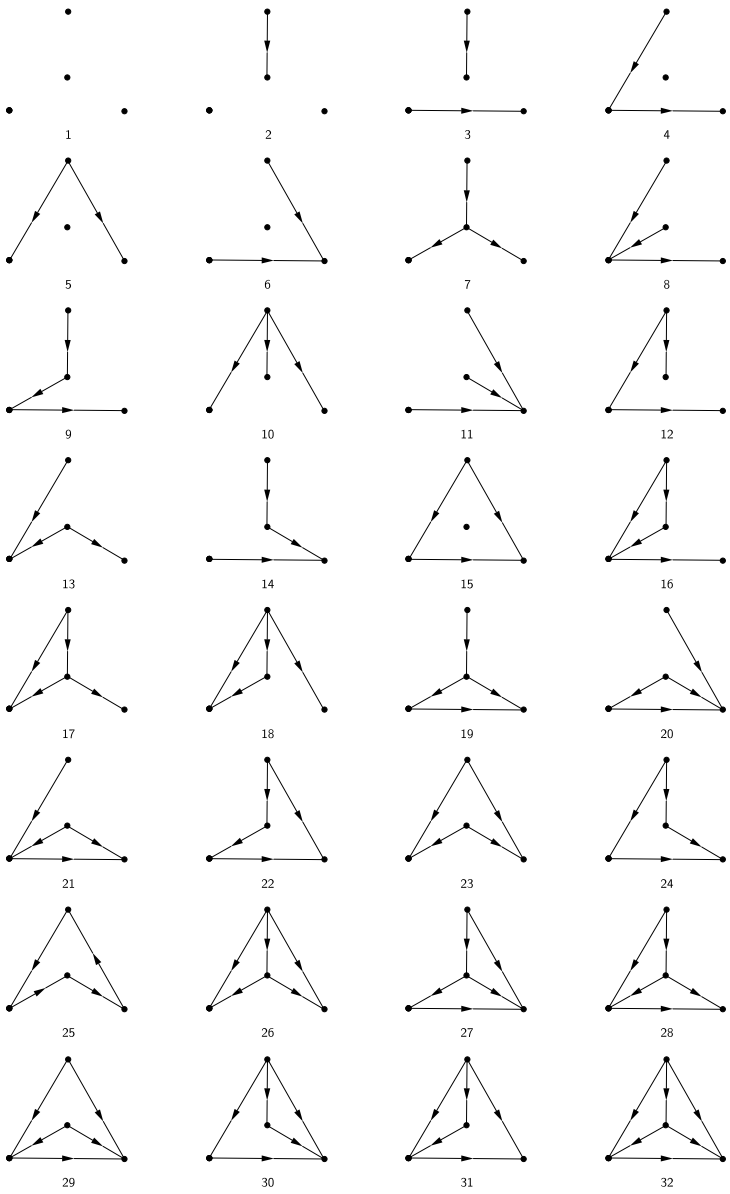


Figure 3: The 4-vertex digraphs3

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 5 & 5 & 5 & 5 & 5 & 5 & 6 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 3 \\
0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 1 & 3 & 2 & 1 & 3 & 1 & 2 & 2 & 0 & 2 & 4 & 2 & 3 & 4 & 2 & 2 & 3 & 4 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 3 & 0 & 1 & 1 & 0 & 1 & 1 & 2 & 3 & 1 & 1 & 1 & 1 & 2 & 1 & 0 & 4 & 2 & 2 & 2 & 3 & 3 & 4 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 3 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 3 & 2 & 1 & 2 & 1 & 0 & 2 & 3 & 2 & 4 & 3 & 2 & 4 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 4 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 2 & 1 & 2 & 0 & 2 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 4 & 0 & 0 & 4 & 2 & 1 & 4 & 2 & 2 & 5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 2 & 1 & 3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 1 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}$$

Table 1: Matrix $\mathbf{A}$ with $\mathbf{y} = \mathbf{x}\,\mathbf{A}^T$.

References

[1] M. Behzad, G. Chartrand and C. E. Wall, On minimal regular digraphs with given girth, Fundamenta Mathematica **69** (1970), 227–231.

[2] J. A. Bondy, Counting subgraphs: a new approach to the Caccetta-Häggkvist conjecture, *Discrete Mathematics* **165/166** (1997), 71–80, Graphs and combinatorics (Marseille, 1995).

[3] L. Caccetta and R. Häggkvist, On minimal digraphs with given girth, Proceedings of the Ninth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1978) (Winnipeg, Man.), *Congressus Numerantium, XXI, Utilitas Mathematica*, 1978, pp. 181–187.

[4] V. Chvátal and E. Szemerédi, Short cycles in directed graphs, *Journal of Combinatorial Theory, Series B* **35** (1983), no. 3, 323–327.

[5] Y. O. Hamidoune, An application of connectivity theory in graphs to factorizations of elements in groups, *European Journal of Combinatorics* **2** (1981), no. 4, 349–355.

[6] Y. O. Hamidoune, A note on minimal directed graphs with given girth, *Journal of Combinatorial Theory, Series B* **43** (1987), no. 3, 343–348.

[7] J. Hladký, D. Král and S. Norin, Counting flags in triangle-free digraphs. European Conference on Combinatorics, Graph Theory and Applications (EuroComb 2009), 621?625, *Electronic Notes in Discrete Math.*,**34**, Elsevier Sci. B. V., Amsterdam, 2009.

[8] C. T. Hoàng and B. Reed, A note on short cycles in digraphs, *Discrete Mathematics* **66** (1987), no. 1-2, 103–107.

[9] N. Lichiardopol, A new bound for a particular case of the Caccetta-Häggkvist conjecture. *Discrete Mathematics* **310** (2010), no. 23, 3368?3372.

[10] T. Nishimura, Short cycles in digraphs, *Proceedings of the First Japan Conference on Graph Theory and Applications* (Hakone, 1986), vol. 72, 1988, pp. 295–298.

[11] A. A. Razborov, On the Caccetta-Haggkvist conjecture with forbidden graphs, preprint, arXiv:1107.2247, August 2012.

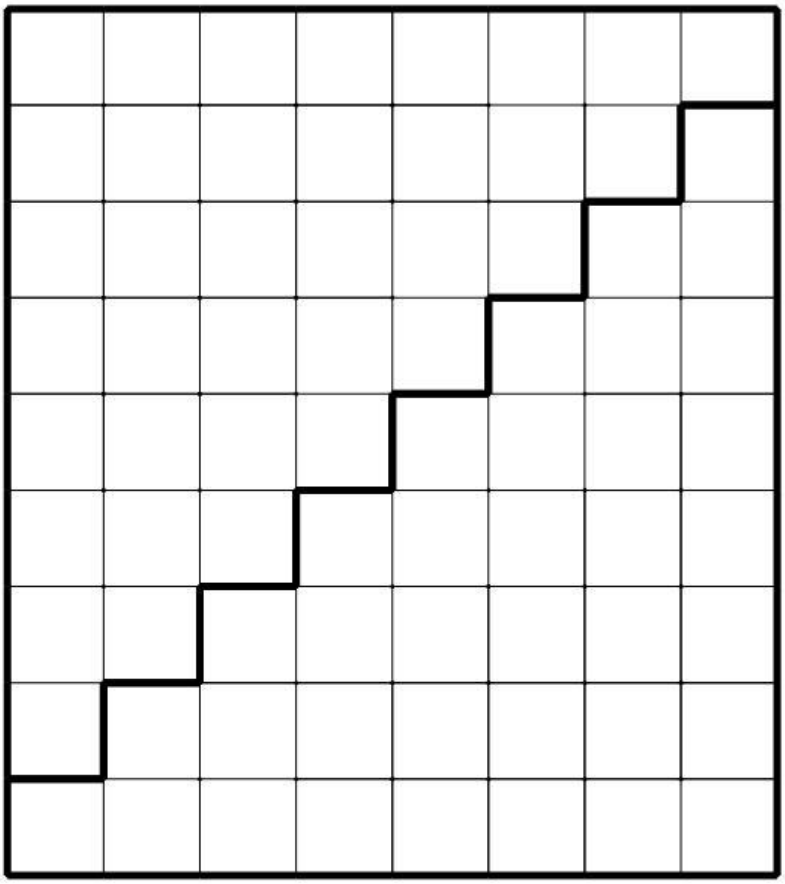
[12] J. Shen, Directed triangles in digraphs, *Journal of Combinatorial Theory, Series B* **74** (1998), no. 2, 405–407.

[13] J. Shen, On the girth of digraphs, *Discrete Mathematics* **211** (2000), no. 1-3, 167–181.

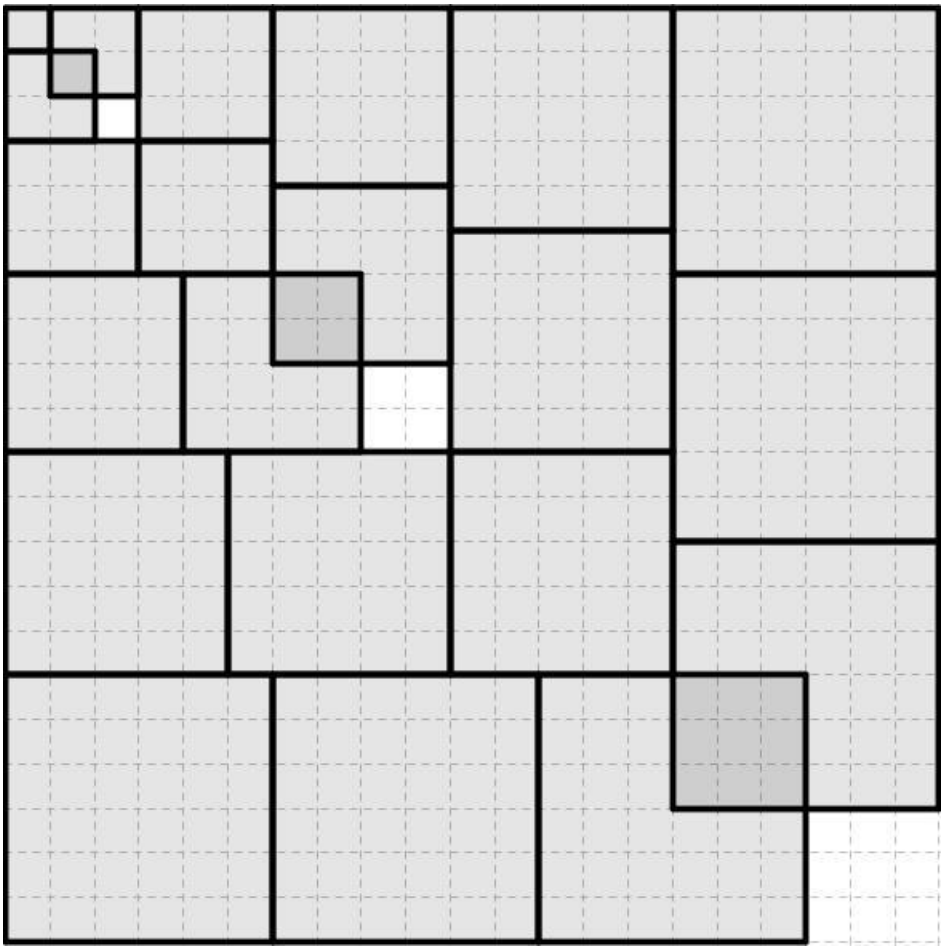
[14] J. Shen, On the Caccetta-Häggkvist conjecture, *Graphs and Combinatorics* **18** (2002), no. 3, 645–654.

6 Proofs Without Words

Sum of Natural Numbers

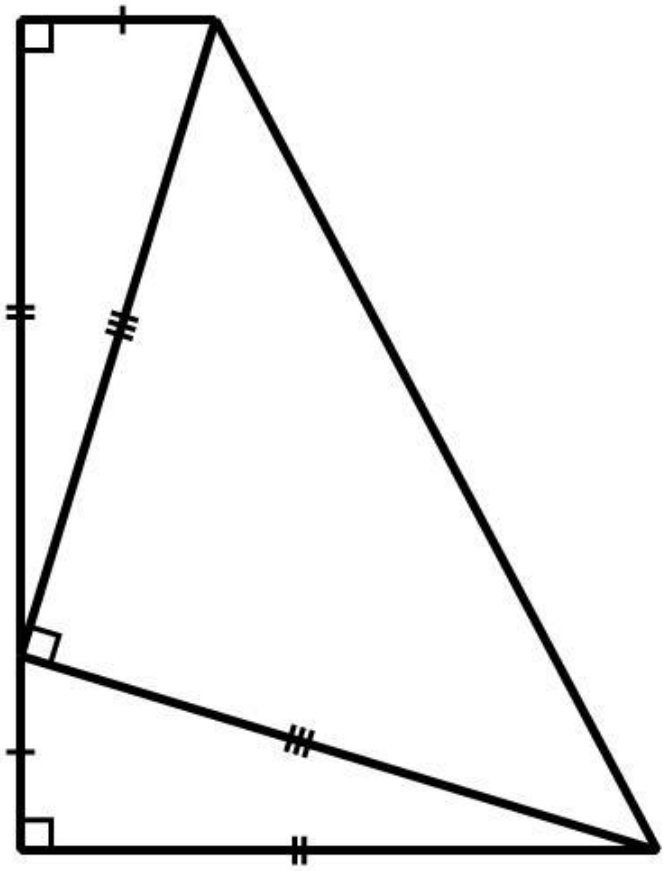


Sum of Cubes of Natural Numbers



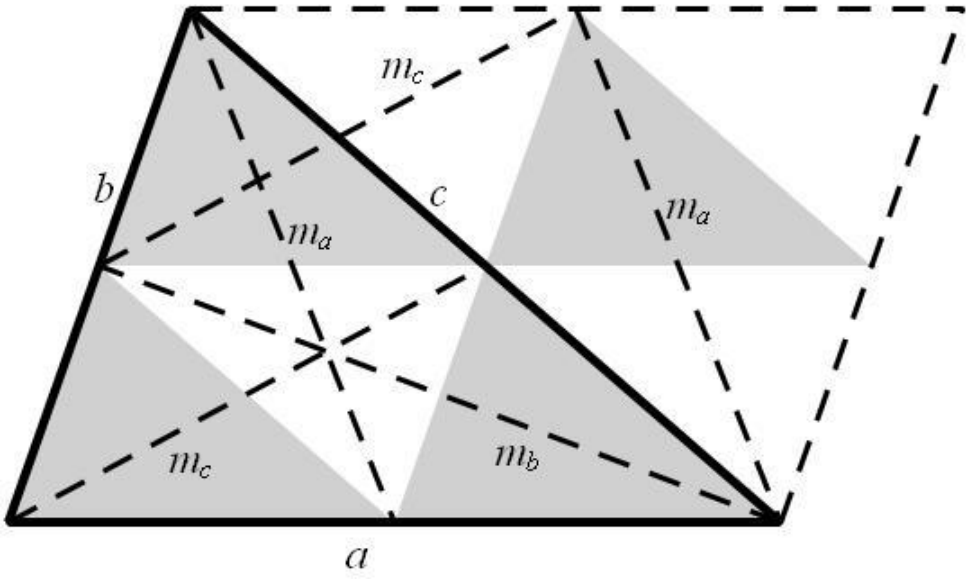
The sum of the first n cubes is the square of the sum of the first n natural numbers.

Pythagorean Theorem



A proof of the Pythagorean Theorem by James A. Garfield, the 20^{th} United States President.

A Triangle of Medians



A triangle of medians has three-fourths the area of the original triangle. (Norbert Hungerbühler)

7 Problems

1. Find the number of ways to tile a 2×8 board with 1×2 dominoes.

2. Find the number of non-negative ordered triples (a, b, c) such that $a^2 + b^2 + c^2 = 136$.

3. How many ordered triples (A, B, C) of three positive integers are there such that $A+B+C = 30$?

4. The real root of the equation $8x^3 - 3x^2 - 3x - 1 = 0$ has the form $\frac{\sqrt[3]{a}+\sqrt[3]{b}+1}{c}$, where a, b, and c are positive integers. Find $a + b + c$. [AIME]

5. The expression $\frac{1}{2013} + \frac{2}{2013^2} + \frac{3}{2013^3} + \frac{4}{2013^4} + ...$ has a value of the form $\frac{a}{b^2}$. Find the value of the expression in the form $\frac{a}{b^2}$. [NYSML]

6. Values $a_1, ..., a_{2013}$ are chosen independently and at random from the set $\{1, ..., 2013\}$. What is the expected number of distinct values in the set $\{a_1, ..., a_{2013}\}$? [HMMT]

7. Let N_x equal 66...6, where the digit 6 appears x times. How many N_x, where x is an integer between 1 and 2013 inclusive, will be divisible by 1673? (Hint: $1111111 = 239 * 4649$)

8. Find the prime factorization of $6^7 + 6^2 + 1$.

9. $x^4 + ax^3 + bx^2 + cx + 1296 = 0$ crosses the x-axis only at two distinct lattice points to the

right of the origin and contains no imaginary roots. Find the absolute value of the sum of all possible values of a.

10. 11 is raised to the power 20122012. Find the remainder upon dividing this integer by 1000.

8 Solutions

1. Define $f(n)$ to be the number of ways to tile a $2 \times n$ board with 1×2 dominoes. We notice that $f(1) = 2$ and $f(2) = 2$. For any integer value of $n > 2$, consider the rightmost tile(s) placed on a $2 \times n$ board. If the last tile was placed vertically, there are $f(n-1)$ ways to tile the remaining $2 \times (n-1)$ board. If it was placed horizontally, then the piece on top of it must also be a horizontal 1×2 domino. There are then $f(n-2)$ ways to tile the remaining $2 \times (n-2)$ board. Thus, we obtain the recursive relation $f(n) = f(n-1) + f(n-2)$. Using our base cases of $n = 1$ and $n = 2$, we can build upwards to compute the value of $f(8)$.

2. Notice that 136 is a multiple of 4. By testing residues (mod 4) , we see that all perfect squares must be either a multiple of four or one more than a multiple of four. As a result, for three perfect squares to sum to a multiple of four, they must all be multiples of four. Thus, we can rewrite a^2 as $4A^2$, b^2 as $4B^2$, and c^2 as $4C^2$ for non-negative integers A, B, C so that our original equation becomes $4A^4 + 4B^2 + 4C^2 = 136$ or $A^2 + B^2 + C^2 = 34$. Without loss of generality, we can assume $A \leq B \leq C$ and then consider different permutations of A, B, and C. Since C is the largest of the three, C^2 must be at least 12 and C must be at least 4, and since A^2 and B^2 are non-negative, C^2 must be at most 34 and C must be at most 5. Thus, C is either 4 or 5, and we can list out cases to see that the only possibilities for (A, B, C) are $(3, 3, 4)$ and $(0, 3, 5)$. There are 3 ways to permute the first and 6 ways to permute the second, and each of these gives a distinct solution for (a, b, c), so there are a total of 9 solutions.

3. Consider the following method of picking A, B, and C: arrange 30 identical balls and two dividers so that the number of balls to the left of the first divider is A, the number of balls

in between the first and the second is B, and the number of balls to the right of the second is C. This ensures that $A + B + C = 30$. To deal with the restriction that A, B, and C are positive, we can take three of the balls and add one to each of the three regions formed by the two dividers. Now we have a bijection between an arrangement 27 balls and two dividers with no restrictions and the number of positive integer ordered triples (A, B, C) which have $A + B + C = 30$. There are $\binom{29}{2} = \frac{29!}{27!\cdot 2!}$ ways to arrange the balls and the dividers.

4. $9x^3 = (x+1)^3$, so $\sqrt[3]{9}x = x + 1$. Solving for x yields $\frac{1}{\sqrt[3]{9}-1} = \frac{\sqrt[3]{81}+\sqrt[3]{9}+1}{8}$.

5. Let $S = \frac{1}{2013} + \frac{2}{2013^2} + \frac{3}{2013^3} + \frac{4}{2013^4} + ...$ Then $2013S = 1 + \frac{2}{2013} + \frac{3}{2013^2} + \frac{4}{2013^3} + ... \Rightarrow$ $2013S - S = 1 + \frac{1}{2013} + \frac{1}{2013^2} + \frac{1}{2013^3} + ... = \frac{1}{1-\frac{1}{2013}}$. Thus, $2012S = \frac{1}{\frac{2012}{2013}}$, so $S = \frac{2013}{2012^2}$.

Alternate Solution: Consider the function $f(x) = 1 + x + x^2 + ... = \frac{1}{1-x}, |x| < 1$. $f'(x) = 1 + 2x + 3x^2 + 4x^3 + ... = \frac{1}{(1-x)^2}$. Let $g(x) = x \cdot f'(x) = x + 2x^2 + 3x^3 + 4x^4 + ... = \frac{x}{(1-x)^2}$. Notice that our expression is equal to $g(\frac{1}{2013}) = \frac{\frac{1}{2013}}{(\frac{2012}{2013})^2} = \frac{2013}{2012^2}$.

6. For each $n \in \{1, ..., 2013\}$, n contributes 1 to the number of distinct values if it appears and 0 if it does not. Since the expected contribution of each value of n to the total number of distinct values is independent of the contributions of the other values of n, the expected number of distinct terms is $2013E$, where E is the expected contribution of any value of n from 1 to 2013. By the definition of expected value, $E = 1 \cdot P(1) + 0 \cdot P(0)$, where $P(k)$ is the probability n contributes k to the number of distinct values. Since $P(1) = 1 - P(0) = 1 - (\frac{2012}{2013})^{2013}$, the expected number of distinct values that appear in the set $\{a_1, ..., a_{2013}\}$ is $2013(1-(\frac{2012}{2013})^{2013}) =$

$\frac{2013^{2013}-2012^{2013}}{2013^{2012}}$.

7. $1673 = 239 * 7$. The number N_x must be divisible by 6666666 and 666666. So therefore it must contain a repetition of the number 6 $42k$ times, where k is a positive integer. $\lfloor 2013/42 \rfloor$ is 47.

8. Note that $x^7 + x^2 + 1 = (x^2 + x + 1)(x^5 - x^4 + x^2 - x + 1)$. Therefore, $6^7 + 6^2 + 1 = (36 + 6 + 1)(7776 - 1296 + 36 - 6 + 1) = 43 * 6511$. We can check exhaustively to show that $6511 = 17 * 383$. Therefore, the answer is $17 * 43 * 383$.

9. There can either be two double roots, or a triple root and a single root. The roots can be 1 and 36, 2 and 18, 3 and 12, or 4 and 9 for two double roots, or 1 and 1296, 2 and 162, and 3 and 48 for a triple and a single root. The sum of all possible sums of roots is 1696.

10. Write the number as $(10 + 1)^{20122012}$. The last term of the binomial expansion will be 1. The term before will be $10 * 20122012$. 2012 is congruent to 0 mod 4, so 20122012 will end in a 6. The number $10 * 20122012$ will have the last 2 digits of 60. The third to last term will be $100 * \binom{20122012}{2}$.. This is the same as $100 * (20122012)(20122012 - 1)/2$. Since 20122012 ends in a 6, $20122012 - 1$ ends in a 5. Their product will end in a zero, and so will this number divided by 2, since it contains 4023 powers of 2 and at least one power of 5. Multiplying this number by 100 means this term ends in three zeroes, so the last three digits of the number are 061. Each term before has more than three terminal zeroes, so they do not affect the last three digits.

9 Some Useful Formulas and Results in Problem Solving

- Ptolemy's Theorem: For any cyclic quadrilateral $ABCD$, $(AB)(CD) + (BC)(AD) = (AC)(BD)$.
- For any triangle with side length a, b, c, area K, and circumradius R, $K = \frac{abc}{4R}$.
- For any triangle with inradius r, semiperimeter S, and area K, $K = rS$.
- Power of a Point Theorem: Consider point P, circle O, and two lines M and N passing through both P and circle O. If A and B are the intersections of M with circle O and C and D are the intersections of N with circle O, then $(PA)(PB) = (PC)(PD)$
- Two Pole Problem: Segment AC and segment BD are perpendicular to segment AB with C and D on the same side of AB. Let P be the intersection of BC and AD. The perpendicular distance from P to AB is $\frac{1}{\frac{1}{AC}+\frac{1}{BD}}$
- British Flag Theorem: For any rectangle $ABCD$ and point P, $PA^2+PC^2 = PB^2+PD^2$.
- Menelaus' Theorem: For any triangle ABC with point D on line BC, point E on segment AC, and point F on segment AB, points D, E, and F are collinear if and only if $(\frac{AF}{FB})(\frac{BD}{DC})(\frac{CE}{EA}) = 1$.
- If $a + b + c = \pi$, then $\tan a + \tan b + \tan c = \tan a \tan b \tan c$
- $\sin^2 a - \sin^2 b = \sin(a - b)\sin(a + b)$
- $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$

- $a^2 + b^2 + c^2 - ab - bc - ca = \frac{(a-b)^2+(b-c)^2+(c-a)^2}{2}$
- $(a + \frac{1}{b})(b + \frac{1}{c})(c + \frac{1}{a}) = abc + \frac{1}{abc} + (a + \frac{1}{b}) + (b + \frac{1}{c}) + (c + \frac{1}{a})$
- $(a - b)(b - c)(c - a) = a^2(b - c) + b^2(c - a) + c^2(a - b)$