MATH 313: INTRODUCTION TO NUMBER THEORY: SPRING 2017
HOMEWORK SOLUTION KEY

STEVEN J. MILLER (SJM1@WILLIAMS.EDU, STEVEN.MILLER.MC.96@AYA.YALE.EDU): MATH 313, SPRING 2017

ABSTRACT. A key part of any math course is doing the homework. This ranges from reading the material in the book so that you can do the problems to thinking about the problem statement, how you might go about solving it, and why some approaches work and others don't. Another important part, which is often forgotten, is how the problem fits into math. Is this a cookbook problem with made up numbers and functions to test whether or not you've mastered the basic material, or does it have important applications throughout math and industry? Below I'll try and provide some comments to place the problems and their solutions in context.

CONTENTS

Date: April 6, 2017.

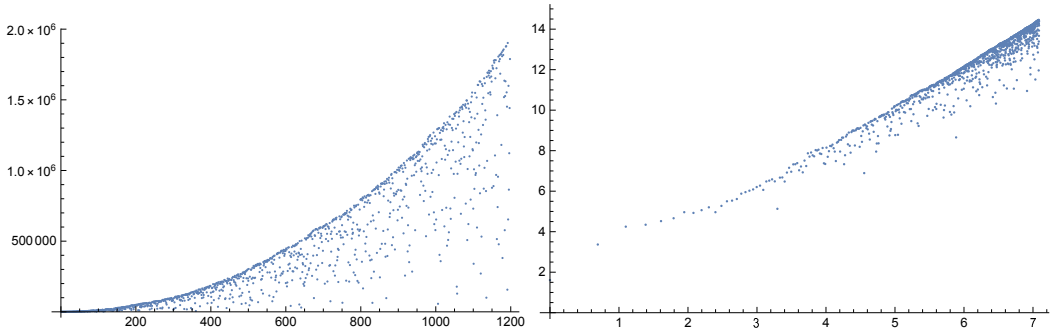

FIGURE 1. Counting the number of (n, m) yielding a perfect square. We order the points by their value of n, and plot the pair with x-coordinate equal to the count number and y-coordinate equal to the square root of the sum (the right is the log-log version of this plot).

1. HW #2: DUE FEBRUARY 10, 2017

1.1. **Problems:** (1) 1.10. Find a sequence of consecutive numbers the sum of whose squares is a square. (Must have at least three numbers.) (2) 1.15. Use induction to prove that $5|n^5 - n$ for any positive integer n. (3) 1.17. Prove that the product of 3 consecutive integers is divisible by 6.

1.2. **Solutions: (1): 1.10. Find a sequence of consecutive numbers the sum of whose squares is a square. (Must have at least three numbers.)**

Solution: Note that $\sum_{k=0}^{n} k^2 = n(n+1)(2n+1)/6$, and thus

$$(m+1)^2 + (m+2)^2 + \cdots + n^2 \;=\; \frac{n(n+1)(2n+1)}{6} - \frac{m(m+1)(2m+1)}{6}.$$

If we wish this to equal a square, say y^2, then for a fixed m we get $y^2 = f_m(n)$, where f_m is a degree three polynomial with coefficients which are a function of m. This turns out to be an elliptic curve, an extremely important object in modern number theory, with applications from cryptography to the proof of Fermat's Last Theorem.

Below is some code to numerically explore and plot the result. The first example with at least three terms is $(n, m) = (24, 1)$, with sum equal to 70^2. Note how useful a log-log plot can be in understanding the behavior.

```
f[n_, m_] :=
 n (n + 1) (2 n + 1)/6 - (m - 1) m (2 m - 1)/6 (* m^2 + ... + n^2 *)
list = {};
loglist = {};
count = 0;
For[n = 1, n <= 40000, n++,
  For[m = 1, m <= n - 1, m++,
   If[IntegerQ[Sqrt[f[n, m]]] == True,
     {
      count = count + 1;
      If[n < 10000,
       Print["(n,m) = (", n, ",", m, ") and f[n,m] = ", f[n, m],
        " " , Sqrt[f[n, m]]]];
      list = AppendTo[list, {count, Sqrt[f[n, m]]}];
      loglist = AppendTo[loglist, {Log[count], Log[Sqrt[f[n, m]]]}];
      }];
   ]];
Print[ListPlot[list]];
Print[ListPlot[loglist]];
```

(2): 1.15. Use induction to prove that $5|n^5 - n$ for any positive integer n.
Solution: Let $P(n)$ be the statement that $5|n^5 - n$. The base case clearly holds when $n = 1$, and we can check $n = 2$ or 3 as well. Let's do the inductive step: thus we assume $P(n)$ is true and must show $P(n+1)$ follows. Since $P(n)$ is true we know $5|n^5 - n$.

Consider $(n+1)^5 - (n+1)$. While we could factor out an $n+1$, we want to somehow uncover the statement $P(n)$. Thus it seems worthwhile to expand, which by the binomial theorem yields

$$(n+1)^5 - (n+1) \;=\; \left(n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1\right) - (n+1)\,.$$

Notice the two $+1$ terms cancel, and what remains is

$$n^5 - n + 5\left(n^4 + 2n^3 + 2n^2 + n\right).$$

The last part is clearly a multiple of 5, and the inductive assumption gives 5 divides $n^5 - 5$. Thus 5 divides $(n+1)^5 - (n+1)$, completing the proof.

(3): 1.17. Prove that the product of 3 consecutive integers is divisible by 6.
Solution: We sketch the proof. First one shows that every other integer is a multiple of 2, and then that every third integer is a multiple of 3. Thus in any set of three consecutive integers we must have at least one multiple of 2 and at least one multiple of 3.

For another proof, we can write any three consecutive integers as $6n + i, 6n + i + 1, 6n + i + 2$ for some $i \in \{0, 1, 2, 3, 4, 5\}$. All we need to do is show that at least one term, when we multiply the three together, is of the form $6n + j$ with j a multiple of 6.

HW #3: Due February 17, 2017: (1) 1.6: The numbers 1051, 1529, and 2246 have the same remainder r when divided by some integer d. Find d and r. (2) 1.11. For n a natural number consider $T_n = 2^{2^n}$. (a). Factor T_n for $n = 1, \ldots, 5$. (b.) Prove that T_n has at least n prime divisors. Note: what does this exercise allow you to deduce? (3) 1.25. Prove that there are infinitely many primes with remainder 3 when divided by 4. (4) Exploration problem: How many of the Fibonacci numbers $\{F_n\}$ are prime? What do you observe? What can you prove? What do you conjecture? (5) Find a formula for the sum of the first few consecutive Fibonacci numbers: $F_1 + F_2 + \cdots + F_n$. Your formula should involve the Fibonacci numbers. Here $F_0 = 0, F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$. (6) Find a formula for the sum of the first few consecutive squares of Fibonacci numbers: $F_1^2 + F_2^2 + \cdots + F_n^2$. Your formula should involve the Fibonacci numbers. (7) Prove that for any fixed integer N, there exist at least two consecutive primes differing by at least N.

2. HW #3: DUE FEBRUARY 17, 2017

2.1. **Problems.** (1) 1.6: The numbers 1051, 1529, and 2246 have the same remainder r when divided by some integer d. Find d and r. (2) 1.11. For n a natural number consider $T_n = 2^{2^n}$. (a). Factor T_n for $n = 1, \dots, 5$. (b.) Prove that T_n has at least n prime divisors. Note: what does this exercise allow you to deduce? (3) 1.25. Prove that there are infinitely many primes with remainder 3 when divided by 4. (4) Exploration problem: How many of the Fibonacci numbers $\{F_n\}$ are prime? What do you observe? What can you prove? What do you conjecture? (5) Find a formula for the sum of the first few consecutive Fibonacci numbers: $F_1 + F_2 + \cdots + F_n$. Your formula should involve the Fibonacci numbers. Here $F_0 = 0, F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$. (6) Find a formula for the sum of the first few consecutive squares of Fibonacci numbers: $F_1^2 + F_2^2 + \cdots + F_n^2$. Your formula should involve the Fibonacci numbers. (7) Prove that for any fixed integer N, there exist at least two consecutive primes differing by at least N.

2.2. **Solutions. (1) 1.6: The numbers 1051, 1529, and 2246 have the same remainder r when divided by some integer d. Find d and r.**
Solution: We write

$$1051 \ = \ ad + r, \quad 1529 \ = \ bd + r, \quad 2246 \ = \ cd + r.$$

While this is three equations in four unknowns, our quantities must be integers, and that helps. If we subtract the first from the second and the second from the third we get

$$478 \ = \ (b-a)d, \quad 717 \ = \ (c-b)d.$$

We know d must divide 478 and 717. If we factor these we find $478 = 2 \cdot 239$ and $717 = 3 \cdot 239$. Thus the only options are $d = 1$ or $d = 239$.

Note $d = 1$ works, giving $r = 0$. If we try $d = 239$ then we have

$$1051 \ = \ 4 \cdot 239 + 95, \quad 1529 \ = \ 6 \cdot 239 + 95, \quad 2246 \ = \ 9 \cdot 239 + 95.$$

Thus $d = 239, r = 95$ also works.

(2) 1.11. For n a natural number consider $T_n = 2^{2^n} - 1$. (a). Factor T_n for $n = 1, \dots, 5$. (b.) Prove that T_n has at least n prime divisors. Note: what does this exercise allow you to deduce?
Solution: As $a^2 - b^2 = (a-b)(a+b)$, we have

$$T_n \ = \ 2^{2^n} - 1 \ = \ \left(2^{2^{n-1}}\right)^2 - 1^2 \ = \ \left(2^{2^{n-1}} - 1\right)\left(2^{2^{n-1}} + 1\right) \ = \ T_{n-1} \cdot (T_{n-1} + 2).$$

We proceed by induction, and factor T_{n-1} as $T_{n-2} \cdot (T_{n-2} + 2)$, and thus find

$$T_n \ = \ T_0(T_0 + 2)(T_1 + 2) \cdots (T_{n-1} + 2)$$

(as $T_0 = 1$ we can drop that if we wish).

```
T[n_] := 2^(2^n) - 1;
factorT[n_] := FactorInteger[T[n]];
theoryfactorT[n_] := FactorInteger[Product[T[i] + 2, {i, 0, n - 1}]];
For[n = 1, n <= 5, n++, Print["direct: ", factorT[n], "; theory: ", theoryfactorT[n]]]
```

The theoretical approach matches the brute force approach for $n \le 5$; the results are

- 3: 3.
- 15: $3 \cdot 5$.
- 255: $3 \cdot 5 \cdot 17$.
- 65535: $3 \cdot 5 \cdot 17 \cdot 257$.
- 4294967295: $3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$.

We see that T_n equals $T_{n-1} \cdot (T_{n-1} + 2)$. As T_n is odd for $n \ge 1$, $T_{n-1} + 2$ is relatively prime to T_{n-1} (if d divided both it divides their difference; as that difference is 2 the only options for d are 1 or 2). Thus every time we increase n we add a new factor which is at least 2 and cannot share a factor with earlier numbers. Thus T_n has at least n prime factors, and *we have proved there are infinitely many primes!* Not bad for a homework assignment!

Note: These numbers are closely related to the Fermat numbers, $F_n = 2^{2^n} + 1$. In particular, $T_n = T_{n-1} \cdot F_n$. The factorizations above suggest the conjecture that all Fermat numbers are prime; interestingly these five are the *only* ones known to be prime (and it is believed there are no others). If there is interest I can give a heuristic proof that there are about 3 Fermat numbers which are prime (yes, I know there are five!).

(3) 1.25. Prove that there are infinitely many primes with remainder 3 when divided by 4.
Solution: We can tweak Euclid's proof. Assume there are only finitely many such primes, which we denote $p_1 = 3, p_2 = 7, \dots, p_n$. Consider $x_n = 4p_2p_3 \cdots p_n + 3$. Note $x_n \ge 12$, and no prime in our list divides it. Further 3 does not divide x_n (it is important that

3 is not included in the product, else that could be the prime). If x_n is prime we found a new prime not on our list of the correct form. If it is composite we see it cannot only be divisible by primes with remainder 1 when divided by 4, which other than 2 are all the remaining prime candidates (and note our number is clearly odd and thus not a multiple of 2). The reason is two numbers that have a remainder of 1 when divided by 4 have a product that also has a remainder of 1 when divided by 4. Thus at least one factor of x_n must have a remainder of 3 when divided by 4.

Interestingly this argument only works for some remainders. We will probably talk about what happens in general. Sadly elementary proofs don't work for all cases. For more see R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University, (1988), 161–169.

(4) Exploration problem: How many of the Fibonacci numbers $\{F_n\}$ are prime? What do you observe? What can you prove? What do you conjecture?
Solution: Let's write some code. Mathematica fortunately has good functions for primality testing.

```
fibprime[n_] := PrimeQ[Fibonacci[n]]
fibprimeexplore[num_] := Module[{},
   count = 0;
   For[n = 1, n <= num, n++, If[fibprime[n] == True,
      {
       If[n <= 100, Print[n, " ", Fibonacci[n]]];
       count = count + 1;
       }];
    ];
   Print["Number F[n] prime for n up to ", num, " is ", count];
   Print["Percentage of n up to ", num, " giving prime is ",
    100. count/num];
   ];
```

For $n \le 5000$ there are 23 n giving rise to Fibonacci numbers that are prime; that increases to 26 if we let n go up to 10000. It is conjectured that there are infinitely many Fibonacci numbers that are prime, but this is not known. If there is interest I can give a heuristic on how many Fibonacci numbers should be prime. *One can also ask similar questions about the intersection of Fibonacci numbers and other special sequences, such as the perfect squares. In other words, how often is a Fibonacci number a square? See* https://math.la.asu.edu/~checkman/SquareFibonacci.html *for the answer.*

(5) Find a formula for the sum of the first few consecutive Fibonacci numbers: $F_1 + F_2 + \cdots + F_n$. Your formula should involve the Fibonacci numbers. Here $F_0 = 0, F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$.
Solution: If we look at the Fibonacci numbers 1, 1, 2, 3, 5, 8, 13, 21, we see the first few sums are 1, 2, 4, 7, 12, 20, 33. We see that these sums are 1 less than a Fibonacci number, and conjecture $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$. We can now prove this by induction. The base case has been done, and for the inductive step we assume it holds for the sum of the first n and examine the sum of the first $n+1$. We find

$$\begin{aligned} F_1 + F_2 + \cdots + F_{n+1} &= (F_1 + F_2 + \cdots + F_n) + F_{n+1} \\ &= F_{n+2} - 1 + F_{n+1} \ = \ F_{n+3} - 1, \end{aligned}$$

as claimed.

(6) Find a formula for the sum of the first few consecutive squares of Fibonacci numbers: $F_1^2 + F_2^2 + \cdots + F_n^2$. Your formula should involve the Fibonacci numbers.
Solution: It is $F_n F_{n+1}$. There are several ways to prove this. Now that you know the answer, try to do it by induction. For another proof, one can show that the Fibonaccis tile the plane in a spiral that gives us a rectangle at each stage; we do this by having squares of side length F_i. Draw the picture. Thus we have a rectangle that is F_n by $F_n + F_{n-1} = F_{n+1}$, and hence its area is the product of the two; however, the rectangle is just a union of disjoint squares with side lengths F_i, and thus the area is also the sum of the squares.

For more on this, see my blog post https://math.williams.edu/to-bead-or-not-to-bead/ (which has some great additional readings). Figure **??** gives a (fun) depiction.

(7) Prove that for any fixed integer N, there exist at least two consecutive primes differing by at least N.
Solution: For any N, let $x_N = N! + 2$. Note that x_N is not prime as it is a multiple of 2. Further, $x_N + j$ is composite for $0 \le j \le N - 2$ as it is divisible by $j + 2$. Thus the largest prime at most x_N is $N! + 1$ or smaller, while the smallest prime at least $x_N + 1$ is $N! + N$ or larger. Thus we have found two primes that differ by at least N.

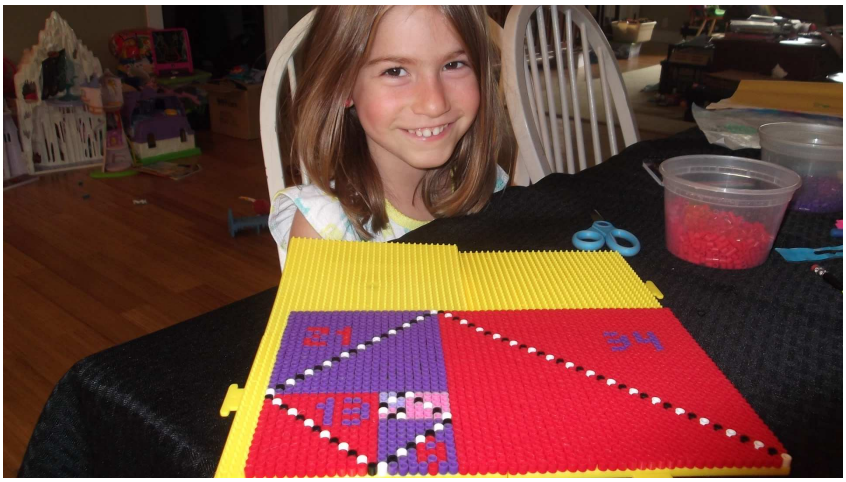

FIGURE 2. Fibonacci spiral, made with Kayla and Cameron Miller.

Note: instead of setting $x_N = N! + 2$ we could study $y_P = P\# + 2$, where $\#$ denotes the *primorial*. The primorial is similar to the factorial, except we only multiply by the primes from P down to 2. For extra credit, investigate how fast the primorial grows relative to the factorial. Is this a big savings? Is this worth doing? This method, while it works, appears quite wasteful. Compare the ratio N/x_N or P/y_P; is it possible to get a larger value so the numerators and denominators are of comparable size?

Homework #4: Due Friday, Feb 24, 2017: (1) Prove Wilson's theorem: n > 1 is prime if and only if (n-1)! = -1 mod n. Discuss how this can be used for a primality test. (2, 3, 4, 5: yes, counts as 4 problems!) Write a computer program to investigate Fermat's little Theorem for all n from 3 to 10000. For each n use ALL a relatively prime to n (take 1 < a < n), and record what fraction of these a have $a^(n-1) = 1 \bmod n$. Gather data, list all the Carmichael numbers you find, and formulate conjectures. YOU get to choose what data to gather, what you want to study, what you want to conjecture. One of the purposes is to give you a feel of what research is like; you have freedom here! Do not look up answers online.... (6, 7, 8, 9: yes, counts as four problems): Investigate the number of solutions to $x^d = a \bmod n$ for $d = 1$ to 10, $n = 2$ to 100, and for each n let a range over all numbers relatively prime to n AND also include $a = 0$. What is true about the average number of solutions to $x^d = a \bmod n$ as we range over all these values of a for a fixed n and d? Make a conjecture.... Now look at $x^2 - ax - b = 0 \bmod n$ where a and b are either 0 or relatively prime to n; note as they range we cover all possible quadratic polynomials. Investigate the average number of solutions for $1 < n < 42$. Make a conjecture....

3. HW #4: DUE FEBRUARY 24, 2017

3.1. **Problems.** Homework #4: Due Friday, Feb 24, 2017: (1) Prove Wilson's theorem: $n > 1$ is prime if and only if $(n-1)! = -1 \bmod n$. Discuss how this can be used for a primality test. (2, 3, 4, 5: yes, counts as 4 problems!) Write a computer program to investigate Fermat's little Theorem for all n from 3 to 10000. For each n use ALL a relatively prime to n (take 1 < a < n), and record what fraction of these a have $a^(n-1) = 1 \bmod n$. Gather data, list all the Carmichael numbers you find, and formulate conjectures. YOU get to choose what data to gather, what you want to study, what you want to conjecture. One of the purposes is to give you a feel of what research is like; you have freedom here! Do not look up answers online.... (6, 7, 8, 9: yes, counts as four problems): Investigate the number of solutions to $x^d = a \bmod n$ for $d = 1$ to 10, $n = 2$ to 100, and for each n let a range over all numbers relatively prime to n AND also include $a = 0$. What is true about the average number of solutions to $x^d = a \bmod n$ as we range over all these values of a for a fixed n and d? Make a conjecture.... Now look at $x^2 - ax - b = 0 \bmod n$ where a and b are either 0 or relatively prime to n; note as they range we cover all possible quadratic polynomials. Investigate the average number of solutions for $1 < n < 42$. Make a conjecture....

3.2. **Solutions. (1) Prove Wilson's theorem: $n > 1$ is prime if and only if $(n-1)! = -1 \bmod n$. Discuss how this can be used for a primality test. Solution:** If n is composite, say $n = ab$, then $2 \le a, b \le n-1$ and thus $n|(n-1)!$; hence $(n-1)! = 0 \bmod n$.

Assume now n is prime; to emphasize this let's write p. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative group, each number has an inverse and the inverses are distinct (i.e., no element is the inverse to two elements). Two elements are their own inverse: 1, -1. Can any other number be its own inverse? In other words, what are the solutions to $x^2 = 1 \bmod p$? Well, for this to hold there must be some m such that $x^2 = 1 + mp$. Thus

$$x^2 - 1 \;=\; mp, \quad \text{or} \quad (x-1)(x+1) \;=\; mp$$

with $1 \le x \le p-1$. Since p is prime, p must divide either $x-1$ or $x+1$. For our range of x the first factor is a multiple of p only for $x = 1$, while the second only for $x = p-1$ (which is the same as $-1 \bmod p$). Thus no other elements are their own inverses, and when we look at the product

$$1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) \bmod p$$

we can pair off all the terms by putting a and a^{-1} together (which gives a product of 1 modulo p) except for 1 and $p-1$. Thus the product is $p-1 \bmod p$, or $-1 \bmod p$.

This provides a simple primality test. If we compute $(n-1)! \bmod n$, if it is zero our number is composite while if it is -1 our number is prime. Unfortunately it is painful to compute this for large n!

(2, 3, 4, 5: yes, counts as 4 problems!) Write a computer program to investigate Fermat's little Theorem for all n from 3 to 10000. For each n use ALL a relatively prime to n (take 1 < a < n), and record what fraction of these a have $a^(n-1) = 1 \bmod n$. Gather data, list all the Carmichael numbers you find, and formulate conjectures. YOU get to choose what data to gather, what you want to study, what you want to conjecture. One of the purposes is to give you a feel of what research is like; you have freedom here! Do not look up answers online....

Solution: From running our program we find the Carmichael numbers up to 10000 are: $\{561, 1105, 1729, 2465, 2821, 6601, 8911\}$. Further,

```
Carmichael number 561 has factorization {{3,1},{11,1},{17,1}}.
Carmichael number 1105 has factorization {{5,1},{13,1},{17,1}}.
Carmichael number 1729 has factorization {{7,1},{13,1},{19,1}}.
Carmichael number 2465 has factorization {{5,1},{17,1},{29,1}}.
Carmichael number 2821 has factorization {{7,1},{13,1},{31,1}}.
Carmichael number 6601 has factorization {{7,1},{23,1},{41,1}}.
Carmichael number 8911 has factorization {{7,1},{19,1},{67,1}}.
```

Here is the code; see Figures 3 and 4 for results of the exploration.

```
FlTtester[numdo_] := Module[{},
  (* store results here *)
  (* storing two ways: both as a list of n and value to plot, and just the values *)
  results = {}; (*stores n and percent of a that led to a failed test for n composite *)
  histogramresults = {}; (* same as above but stores not a pair,
  just percent of a failing *)
  lowestresults = {}; (* stores pair of n and first a that failed *)
  histogramlowestresults = {}; (* same as above but stores not a pair, just first a that failed *)
  carmichael = {}; (* stores our carmichael numbers here *)
  For[n = 3, n <= numdo, n++, (* look at the numbers from 3 to numdo *)
   {
```

```
  numpass = 0; (* for each n initialize number of a that pass fail test to 0 *)
  numfail = 0;
  foundlowest = 0; (* use this to record first a that failed *)
  For[a = 2, a <= n - 1, a++, (* tests a relatively prime to n *)
   {
    If[GCD[a, n] == 1, (* only need to test a that are relatively prime to n,
     hence this test *)
     If[Mod[a^(n - 1), n] == 1, numpass = numpass + 1,
       numfail = numfail + 1];
     (* above:
     if equals 1 then pass test and increment numpass by 1,
     else fail and increment numfail by 1 *)
     ]; (* end of gcd test and increment *)
    If[foundlowest == 0 && numfail == 1, (* enter here if FIRST time failed a test *)
     {
      foundlowest = 1; (*
      increment foundlowest so that won't enter again for this n *)
      lowestresults = AppendTo[lowestresults, {n, a}]; (*save results to file *)
      histogramlowestresults = AppendTo[histogramlowestresults, a];
      }
     ]; (* end of IF loop *)
    }]; (* end of a loop *)
  (* now that a loop is done we will save results *)
  (* first bits are to make output nice *)
  If[numfail == 0, printclaim = {PASSED ALL}, {}];
  If[PrimeQ[n] == True, primestatus = {PRIME},
   primestatus = {COMPOSITE}];
  (* prints out a lot of info on first 20 numbers *)
  If[n <= 20,
   Print[n, ", numpass = ", numpass, ", numfail = ", numfail,
    ", ", printclaim, ", ", primestatus]];
  If[Mod[n, numdo/10] == 0,
   Print["We have done ", 100.0 n/numdo, "%."]]; (*update every 10% on where we are *)
  If[numfail == 0 && PrimeQ[n] == False, (*this prints out carmichael numbers and
                                          adds to our carmichael list *)
   {
    Print["       ", n, " is CARMICHAEL."];
    carmichael = AppendTo[carmichael, n];
    }
   ];
  If[PrimeQ[n] == False, (* saves info on composite numbers *)
   {
    results =
     AppendTo[results, {n, 1.0 numfail / (EulerPhi[n] - 1)}];
    histogramresults =
     AppendTo[histogramresults, 1.0 numfail / (EulerPhi[n] - 1)];
    }]; (* end of composite loop *)
  }]; (* end of n loop *)
Print[ " "]; (* blank line followed by outputting results *)
Print["Carmichael numbers up to ", numdo, " are: ", carmichael];
For[c = 1, c <= Length[carmichael], c++,
 Print["Carmichael number ", carmichael[[c]],
  " has factorization ", FactorInteger[carmichael[[c]]], "."]];
Print["Plots of how often tests fail for composite numbers."];
Print[ListPlot[results, PlotRange -> Full]];
Print[Histogram[histogramresults, Automatic, "Probability"]];
Print["Plots of location of first failure for composite numbers."];
Print["Largest value of the first a to fail is ",
 Max[histogramlowestresults]];
Print[ListPlot[lowestresults, PlotRange -> Full]];
```

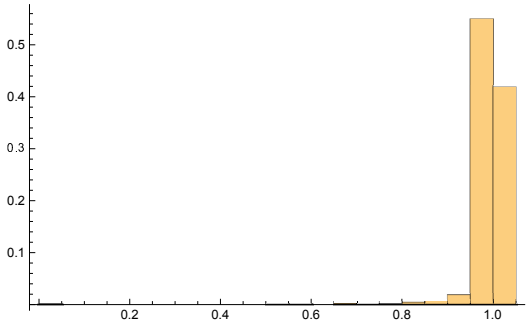

FIGURE 3. Plot of what percent of a relatively prime to a composite n fail $a^{n-1} = 1 \bmod n$.

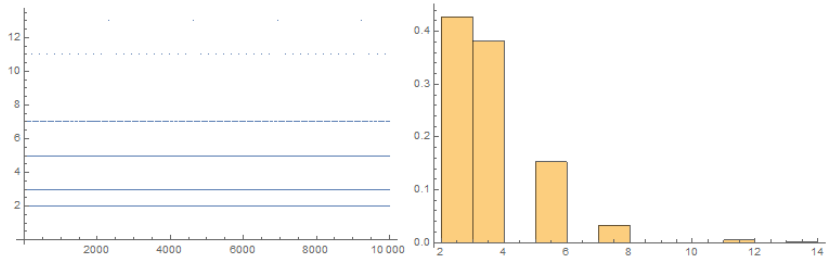

FIGURE 4. Location of first a relatively prime to a composite n that fails $a^{n-1} = 1 \bmod n$.

```
Print[Histogram[histogramlowestresults, Automatic, "Probability"]]
] (* end of module *)
```

Some possible conjectures on Carmichael numbers: (1) Square-free. (2) At least three factors. (3) Probably having a 3, 5 or 7 is due to small set and not worth conjecturing, but.... (4) Most numbers if fail, fail quickly and often (around 50% of a witness the failure, but maybe should look at prime a and not just a relatively prime to n).

(6, 7, 8, 9: yes, counts as four problems): Investigate the number of solutions to $x^d = a \bmod n$ for $d = 1$ to 10, $n = 2$ to 100, and for each n let a range over all numbers relatively prime to n AND also include $a = 0$. What is true about the average number of solutions to $x^d = a \bmod n$ as we range over all these values of a for a fixed n and d? Make a conjecture.... Now look at $x^2 - ax - b = 0 \bmod n$ where a and b are either 0 or relatively prime to n; note as they range we cover all possible quadratic polynomials. Investigate the average number of solutions for $1 < n < 42$. Make a conjecture....
Solution: Below is the code to investigate. Interestingly the average number of solutions is always exactly 1! Natural to conjecture this is always the case.

```
quadratictester[numdo_, deg_, printall_] := Module[{},
   results = {}; (* store results here *)
   Print[" "]; (* blank line to separate outputs *)
   Print[
    "If printall == 1 print all; else just print when the average
        number of solns to x^d == a mod n is not exactly 1."];
   Print["d = ", d, " and n ranges from 2 to ", numdo];
   For[n = 2, n <= numdo, n++,
    {
     templist = {}; (* place to store data for given a, temp spot *)
     numsolnsalla = 0; (* keeps track of number of solns as vary a,
     fixed n *)
     For[a = 0, a <= n - 1, a++, (* our a counting loop *)
      {
       If[GCD[a, n] == 1 || GCD[a, n] == n, (* only look at a=0 or a rel prime to n *)
```

```
        {
         numsolns = 0; (* for given a, set number of solns to zero *)
         For[x = 0, x <= n - 1, x++, (* brute force:
          see how many solns to x^deg = a mod n *)
          {
           (*simple check: if a given x works then increment by 1, make sure x rel prime to n or is 0*)
           If[Mod[x^deg - a , n] == 0 && (GCD[x, n] == 1 || GCD[x, n] == n), numsolns = numsolns + 1];
           }]; (* end of x loop *)
         templist = AppendTo[templist, {n, a, numsolns}]; (* store temp results to results *)
         numsolnsalla = numsolnsalla + numsolns; (* compute total number of solns for fixed a *)
         }]; (* end of IF statement from a rel prime to n *OR* a is zero *)
       }]; (* end of a loop *)
     If[printall == 1,
      Print["n = ", n, " and average number of solutions: ", numsolnsalla / (EulerPhi[n] + 1)]];
     (* prints average numb solns if told to print all *)
     If[ numsolnsalla / (EulerPhi[n] + 1) != 1,
      Print["n = ", n, " and average number solns is ", numsolnsalla / (EulerPhi[n] + 1)]];
     results = AppendTo[results, templist];
     }]; (* end of n loop *)
   ]; (* end of module *)
```

For the second part, we just need to tweak the middle code.

```
numsolnsallab = 0; (* keeps track of number of solns as vary a, fixed n *)
For[b = 0, b <= n - 1, b++,
 {
  If[GCD[b, n] == 1 || GCD[b, n] == n, (* only look at b=0 or n rel prime to n *)
   For[a = 0, a <= n - 1, a++, (* our a counting loop *)
    {
     If[GCD[a, n] == 1 || GCD[a, n] == n, (* only look at a=0 or a rel prime to n *)
      {
       numsolns = 0; (* for given a, set number of solns to zero *)
       For[x = 0, x <= n - 1, x++, (* brute force:
        see how many solns to x^deg = a mod n *)
        {
         (*simple check: if a given x works then increment by 1,make sure x rel prime to n or is 0*)
         If[
           Mod[x^2 - a x - b , n] == 0 && (GCD[x, n] == 1 || GCD[x, n] == n),
           numsolns = numsolns + 1];
         }]; (* end of x loop *)
       templist = AppendTo[templist, {n, a, numsolns}]; (* store temp results to results *)
       numsolnsallab = numsolnsallab + numsolns; (*compute total number of solns for fixed a *)
       }]; (* end of IF statement from a rel prime to n *OR* a is zero *)
     }]; (* end of a loop *)
   ]; (* end of if statement for b gcd test *)
  }]; (* end of b loop *)
```

See the average number of solutions is exactly 1 if n prime, fluctuates otherwise. Conjecture: range over all a, b that are 0 or relatively prime to a prime p, the average number of solutions to $x^2 - ax - b = 0 \bmod p$ is 1 (divide by p^2, as $\varphi(p) + 1 = p$).

Proof: As $n = p$ is prime, the condition that the gcd of a and b with p is 1 *or* they are zero means a and b freely range over $\{0, 1, \ldots, p-1\}$. Thus consider the triples (x, a, b), where x runs over the same range. There are p^3 such triples. Given a pair (x, a) there is a unique b such that $x^2 - ax - b = 0 \bmod p$; we just take $b = x^2 - ax$! Thus there are p^2 solutions to the p^2 equations, so on average there is one solution! There is nothing special about a quadratic; the same argument and the same average holds for any finite degree polynomial.

If n were composite, however, this would break down as sometimes we would have the constant term equal to an element outside of $(\mathbb{Z}/n\mathbb{Z})^* \cup \{0\}$, though if we studied this in $(\mathbb{Z}/n\mathbb{Z})$ we would again have on average 1 solution. For example, if we have $x^2 - 7x - b = 0 \bmod 12$ then $b = x(x-7) \bmod 12$, and if $x = 11$ (which is invertible modulo 12, as is 7, then we would have $b = 8 \bmod 12$ and 8 is not invertible modulo 12 and thus not accessible. If we look at *all* polynomials, however, then on average we do regain exactly one solution; if we have $x^d - a_{d-1}x^{d-1} - \cdots - a_0$ then given any tuple $(x, a_{d-1}, \ldots, a_1) \in (\mathbb{Z}/n\mathbb{Z})^d$ there is a unique choice for a_0 that gives a solution. *Moral: we should be investigating these polynomials with coefficients and values in $\mathbb{Z}/n\mathbb{Z}$, not $(\mathbb{Z}/n\mathbb{Z})^*$.*

Due Friday, March 3: Might be easier to do in a different order.... Some problems might be very easy, others might require work, and p always refers to a prime number. (1) Do Exercise 3.1 from Hutz' book. (2) Do Exercise 3.2 from Hutz' book. (3) Do Exercise 3.11 from Hutz' book. (4) Show that if a is a root of $f(x)$ modulo a prime p then $f(x) = (x-a)g(x) \bmod p$ for some polynomial $g(x)$ of degree less than f. (5) Prove a polynomial of degree d has at most d roots modulo p. (6) Prove the polynomial $x^(p-1) = 1 \bmod p$ has exactly $p-1$ roots modulo p. (7) The order of an a in $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$ is the smallest d such that $a^d = 1 \bmod p$. Prove that the order of any a in $(\mathbb{Z}/p\mathbb{Z})^*$ divides $p-1$. (8) Prove if a and b are two relatively prime roots to $x^(p-1) = 1 \bmod p$ with orders d_a and d_b that if d_a and d_b are relatively prime then ab has order $d_a d_b$. (9) Let q be a prime dividing $p-1$. Prove there is an element x in $(\mathbb{Z}/p\mathbb{Z})^*$ that has order exactly q. (10) Assume $p-1$ is a square-free number; thus if n^2 divides $p-1$ then $n = 1$. Prove for such primes that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic; this means there is some g such that the group equals $\{1, g, g^2, \ldots, g^(p-2)\}$. This result actually holds for all primes (done in the book); this is meant to be a guided set of exercises to this important result in a special case; you can look and see where we use the prime has special properties, and can that be removed.

4. HW #5: DUE MARCH 3, 2017

4.1. **Problems. Due Friday, March 3: Might be easier to do in a different order.... Some problems might be very easy, others might require work, and p always refers to a prime number. (1) Do Exercise 3.1 from Hutz' book. (2) Do Exercise 3.2 from Hutz' book. (3) Do Exercise 3.11 from Hutz' book. (4) Show that if a is a root of $f(x)$ modulo a prime p then $f(x) = (x-a)g(x) \bmod p$ for some polynomial $g(x)$ of degree less than f. (5) Prove a polynomial of degree d has at most d roots modulo p. (6) Prove the polynomial $x^(p-1) = 1 \bmod p$ has exactly $p-1$ roots modulo p. (7) The order of an a in $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$ is the smallest d such that $a^d = 1 \bmod p$. Prove that the order of any a in $(\mathbb{Z}/p\mathbb{Z})^*$ divides $p-1$. (8) Prove if a and b are two relatively prime roots to $x^(p-1) = 1 \bmod p$ with orders d_a and d_b that if d_a and d_b are relatively prime then ab has order $d_a d_b$. (9) Let q be a prime dividing $p-1$. Prove there is an element x in $(\mathbb{Z}/p\mathbb{Z})^*$ that has order exactly q. (10) Assume $p-1$ is a square-free number; thus if n^2 divides $p-1$ then $n = 1$. Prove for such primes that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic; this means there is some g such that the group equals $\{1, g, g^2, \ldots, g^(p-2)\}$. This result actually holds for all primes (done in the book); this is meant to be a guided set of exercises to this important result in a special case; you can look and see where we use the prime has special properties, and can that be removed.**

4.2. **Solutions.**

(1) Do Exercise 3.1 from Hutz' book.
Solution: For (a): We have

$$\left(\frac{324}{31}\right) = \left(\frac{14}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{7}{31}\right).$$

As $8^2 = 2 \bmod 31$ and $10^2 = 7 \bmod 31$ both symbols above are 1, and thus 324 is a square modulo 31 (it is $80 \bmod 31$, or 18).

For (b): We have

$$\left(\frac{34538}{1237}\right) = \left(\frac{1139}{1237}\right) = \left(\frac{17}{1237}\right)\left(\frac{67}{1237}\right).$$

As 1237, 17 and 67 are primes we can use quadratic reciprocity. As $1237 \bmod 4 = 1$ the power of -1 is even, and thus we do not need to worry about it. We find

$$\left(\frac{34538}{1237}\right) = \left(\frac{1237}{17}\right)\left(\frac{1237}{67}\right) = \left(\frac{13}{17}\right)\left(\frac{31}{67}\right).$$

We use quadratic reciprocity again; the first factor has -1 to an even power as both primes are 1 mod 4, while the second has -1 to an odd power as both primes are 3 mod 4, giving

$$\left(\frac{34538}{1237}\right) = -\left(\frac{17}{13}\right)\left(\frac{67}{31}\right) = -\left(\frac{4}{13}\right)\left(\frac{5}{31}\right).$$

As $6^2 = 5 \bmod 31$ we see both symbols above are 1, and thus the answer here is -1, so 34538 is not a square modulo 1237.

(2) Do Exercise 3.2 from Hutz' book. *Find all the residue classes which are quadratic residues modulo 61.*
Solution: We could compute x^2 for each $x \in (\mathbb{Z}/61\mathbb{Z})^*$ and see which 30 values emerge.

```
list = {};
For[n = 1, n <= 60, n++,
 If[MemberQ[list, Mod[n^2, 61]] == False,
  list = AppendTo[list, Mod[n^2, 61]]]]
Print[Sort[list]]
{1,3,4,5,9,12,13,14,15,16,19,20,22,25,27,34,36,39,41,42,45,46,47,48,49,52,56,57,58,60}
```

We could also use Euler's criterion to encode the Legendre symbol.

```
list = {};
For[n = 1, n <= 60, n++,
  If[Mod[n^30, 61] == 1, list = AppendTo[list, n]]];
Print[list]

{1,3,4,5,9,12,13,14,15,16,19,20,22,25,27,34,36,39,41,42,45,46,47,48,49,52,56,57,58,60}
```

(3) Do Exercise 3.11 from Hutz' book. *Let $p > 2$ be a prime. Prove that $\left(\frac{-1}{p}\right) = 1$ if and only if $p = 1 \bmod 4$.*
Solution: For this problem we use the results of the rest of the homework, namely that since p is prime, the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic and generated by some element g of order $p-1$. Thus there is an m such that $-1 = g^m \bmod p$.

Assume $p = 1 \bmod 4$ Then there is a k such that $p - 1 = 4k$, and the order of g is $4k$. In particular, this means that g^{2k} is not 1 modulo p; however, since g^{2k} squares to 1 it must be 1 or -1. As it is not 1 the only option left is it is -1, and hence -1 is a square (it is congruent to g^{2k}, which is $(g^k)^2$).

Assume now $p \neq 1 \bmod 4$. If $p = 2$ then $-1 = 1 \bmod p$ and -1 would thus be a square, however, the problem states that $p > 2$ so there is no need to look at this case. Thus $p = 3 \bmod 4$, and we may write $p - 1$ as $4k + 2$ for some k. Thus g^{2k+1} squares to 1 modulo p, and must be 1 or -1. It can't be 1 as then the order of g would be too small, and must be -1. Thus $-1 = g^{2k+1} \bmod p$, and -1 is not a square as it is an odd power of the generator. We could also use Euler's criterion:

$$(-1)^{(p-1)/2} \;=\; (g^{2k+1})^{(p-1)/2} \;=\; (g^{(p-1)/2})^{2k+1} \;=\; (-1)^{2k+1} \;=\; -1 \bmod p.$$

(4) Show that if a is a root of $f(x)$ modulo a prime p then $f(x) = (x - a)g(x) \bmod p$ for some polynomial $g(x)$ of degree less than f.

As every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is invertible, we can perform polynomial long division and write $f(x)$ as $(x - a)g(x) + r(x)$, where the degree of $r(x)$ is less than that of $x - a$, and hence $r(x)$ is constant. To see this, say $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$. We find g term by term. To get the leading term we see we must multiply $x - a$ by $c_n x^{n-1}$ to get the leading term of f. We then have

$$f(x) - c_n x^{n-1}(x - a) \;=\; (c_{n-1} - ac_n)\, x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0 \bmod p.$$

We then proceed by induction. If $c_{n-1} = ac_n \bmod p$ we can skip the next term, if not the next term of g is $(c_{n-1} - ac_n)x^{n-2}$.

All that remains is showing that $r(x) = 0$. We know r is a constant, say c. Thus $f(x) = (x - a)g(x) + c \bmod p$; however, as $f(a) = 0$ we see c must be zero, completing the proof.

Remark: the result above holds in much greater generality. What greatly aids us is that $x - a$ is a monic coefficient and we have a field (non-zero elements have multiplicative inverses. If instead we had a composite moduli and tried to write $3x^2 - 9x$ as $(4x-4)g(x)$ with a remainder, we would be in trouble. The method above would generalize and we would want to start by multiplying $4x - 4$ by $3 \cdot 4^{-1}x$, but 4 is not invertible. The trouble is when there are divisors of zeros, two non-zero elements multiplying to zero. Think about how far you can generalize this result.

(5) Prove a polynomial of degree d has at most d roots modulo p.

Solution: From the previous problem we can pull the roots out one at a time. If there are fewer than d roots the problem is trivial. If there are d roots we may label them $r_1, \ldots, r_d$ and we have

$$f(x) \;=\; (x - r_1) \cdots (x - r_d)g_r(x) \bmod p$$

for some $g_r(x)$; we must show that g_r is constant. This follows from the previous problem, as this g_r is of degree 0 and hence constant (remember each time we pull out a root the degree of the g polynomial is at most one less than that of the polynomial whose root we are taking). If $g_r(x)$ is identically zero then f is identically zero, contradicting the fact that it is a polynomial of degree d. Thus $g_r(x)$ is some non-zero constant, say c. Because p is a prime, if we evaluate $f(x)$ for any x not one of our d roots then we have a product of non-zero numbers modulo p, which must be non-zero; note this step would fail if p were composite (if we were working modulo 12, for example, we could have a product that is $2 \cdot 2 \cdot 3$ which vanishes, even though no term vanishes).

Remark: The proof here illustrates a common technique: do it once and then lather, rinse, repeat; this is often called the shampoo method. We'll see this method again later.

(6) Prove the polynomial $x^(p - 1) = 1 \bmod p$ has exactly $p - 1$ roots modulo p.

Solution: By Fermat's little Theorem we know if $\gcd(a, p) = 1$ then $a^{p-1} = 1 \bmod p$. Thus each of the $p - 1$ elements of $(Z/p\mathbb{Z})^*$ is a root, and hence there are exactly $p - 1$ roots modulo p as 0 is not a root.

(7) The order of an a in $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p - 1\}$ is the smallest d such that $a^d = 1 \bmod p$. Prove that the order of any a in $(\mathbb{Z}/p\mathbb{Z})^*$ divides $p - 1$.

Solution: We know $a^{p-1} = 1 \bmod p$. If d divides $p - 1$ we're done, if not assume $1 < \gcd(d, p - 1) = k < d$. By the Euclidean algorithm there are α, β such that $\alpha d + \beta(p - 1) = k$. Thus

$$a^k \;=\; a^{\alpha d + \beta(p-1)} \;=\; a^{\alpha d} a^{\beta(p-1)} \;=\; \left(a^d\right)^{\alpha} \left(a^{p-1}\right) \beta \;=\; 1 \bmod p.$$

Thus $a^k = 1 \bmod p$, contradicting the fact that d is the order.

Remark: This won't be the first time on the homework that knowing some abstract algebra, specifically Lagrange's theorem, would help! What we're doing is independently deriving these results just in the special cases we need!

(8) Prove if a and b are two relatively prime roots to $x^(p - 1) = 1 \bmod p$ with orders d_a and d_b that if d_a and d_b are relatively prime then ab has order $d_a d_b$.

Solution: Clearly the order of ab divides $d_a d_b$ as

$$(ab)^{d_a d_b} \ = \ (a^{d_a})^{d_b}(b^{d_b})^{d_a} \ = \ 1 \cdot 1 \ = \ 1 \bmod p.$$

Could the order be smaller?

First note that $\{1, a, a^2, \ldots, a^{d_a-1}\}$ and $\{1, b, b^2, \ldots, b^{d_b-1}\}$ only have one element in common, 1. The reason is these are cyclic groups and the order of anything in the first set must non-trivially divide d_a (if it isn't 1), while similarly the order of anything in the second set must non-trivially divide d_b (if it isn't 1). To see our claim about orders we could use Lagrange's theorem from group theory, but as abstract algebra is *not* a pre-requisite for this course we'll also give a direct proof. Imagine for example that a^i, which we assume is not 1, has order d not dividing d_a. Since d_a is the smallest power of a that is 1 modulo p, we *must* have $id \geq d_a$. If they are equal we are done, if not assume $id > d_a$. By the division algorithm we can write $id = \alpha d_a + r$ for some $r \in \{0, 1, \ldots, d_a - 1\}$. But now

$$1 \ = \ a^{id} \ = \ a^{\alpha d_a + r} \ = \ a^{\alpha d_a} a^r \ = \ (a^{d_a})^{\alpha} a^r \ = \ a^r \bmod p;$$

thus $a^r = 1 \bmod p$, contradicting d being the minimal order.

We now return to the main proof, using the cyclicity of the two sets and showing the only element in common is 1. If $a^i = b_j$ then the order of this element must divide both d_a and d_b; as these two numbers are relatively prime the only possibility is that the order of this element is 1, and hence $a^i = b^j = 1 \bmod p$.

Thus the only way $(ab)^d$ can be 1 is if a^d and b^d are both 1 modulo p (as otherwise a^d is the inverse of b^d, which is $b^{d_b - d} \bmod p$). Thus d must be a multiple of d_a and a multiple of d_b; the smallest multiple it can be is $d_a d_b$, which we have shown works, completing the proof. *Note we never needed to use a and b are relatively prime, only that their orders are!*

Remark: while sometimes we may think we need or want certain conditions, oftentimes they turn out to be unnecessary. We don't need the two elements to be relatively prime. What we need is their `orders` *to be relatively prime. The key idea is getting a sense of the structure of the sub-group generated by a (or by b). The proof that the order of a^i divides the order of a could be deduced from Lagrange's theorem, but again our goal is to do things elementarily. We obtain a nice contradiction by the concept of* `minimality`*; the order is the smallest integer with a given problem, and we show that if the order of a^i is not a divisor of that then we can find a smaller power of a that is 1. This is an extremely important property, and one of the biggest uses of the division algorithm.*

(9) Let q be a prime dividing $p-1$. Prove there is an element x in $(\mathbb{Z}/p\mathbb{Z})^*$ that has order exactly q.

Solution: We know every element has order dividing $p-1$, and $x^d = 1 \bmod p$ has at most d roots. Assume there are no solutions to $x^q = 1 \bmod p$ for some q dividing $p-1$. Note there cannot be an element of order q^2 or q^3 et cetera; if say $x^{q^2} = 1 \bmod p$ then x^q would have order q. More generally, if some x had order bq for some $b > 0$ then $x^{bq} = 1 \bmod p$ implies (x^b) has order q, violating our assumption. Thus *all* elements have order relatively prime to q.

By Fermat's little Theorem we know $x^{p-1} = 1 \bmod p$ for all $x \in (\mathbb{Z}/p\mathbb{Z})^*$; thus there are exactly $p-1$ roots to this equation. Since each element has order dividing $p-1$ and by assumption each order is relatively prime to q, we see each element also has order dividing $(p-1)/q$. But by Exercise (5) the polynomial $x^{(p-1)/q} = 1 \bmod p$ can have at most $(p-1)/q$ roots, but it must have $p-1$ roots (as all elements satisfy it); contradiction.

Remark: What if q^ℓ divides $p-1$? What can you say?

(10) Assume $p-1$ is a square-free number; thus if n^2 divides $p-1$ then $n = 1$. Prove for such primes that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic; this means there is some g such that the group equals $\{1, g, g^2, \ldots, g^(p-2)\}$. This result actually holds for all primes (done in the book); this is meant to be a guided set of exercises to this important result in a special case; you can look and see where we use the prime has special properties, and can that be removed.

Solution: The problem follows by showing there is an element of order $p-1$. By the previous result, for each prime q dividing $p-1$ there is an element x_q of order q. Let $p-1 = q_1 \cdots q_r$; note the primes are distinct as $p-1$ is assumed square-free. Consider $x_1 \cdots x_r$. This element has order $q_1 \cdots q_r = p-1$ by repeated applications of Exercise (8) (i.e., grouping). To see this, we first note x_1 and x_2 have relatively prime orders (our proof never used the elements being relatively prime, only their orders). Thus the order of $x_1 x_2$ is $q_1 q_2$. We now apply Exercise (8) again, this time to $x_1 x_2$ and x_3, with relatively prime orders $q_1 q_2$ and q_3, and find $x_1 x_2 x_3$ has order $q_1 q_2 q_3$. We continue marching down....

As a nice exercise, can you prove $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic for all primes? All that you need to change is that if ℓ is the highest power of q dividing $p-1$ then there is an element of order q^ℓ.

NO WRITTEN HW DUE NEXT WEEK BECAUSE OF MIDTERM.

5. HW #7: DUE MARCH 17, 2017

#1: Problem 4.4: Find the inverse cipher to the affine cipher $3x + 7 \bmod 26$.
Solution: If $y = 3x + 7 \bmod 26$ then $x = (y - 7)3^{-1} \bmod 26$, where $3^{-1} = 9 \bmod 26$. Thus $x = 9y - 63 = 9y + 15 \bmod 26$, so the inverse is the map $9y + 15 \bmod 26$.

#2: Devise a system so that three people can share a secret in a crowded room, but no one else will know it.
Solution: We can extend the method from class. Let p be a prime and g a generator for $(\mathbb{Z}/p\mathbb{Z})^*$. Let Alice choose an a, Bob a b, and Charlie a c, which they keep private. They compute g^a, g^b, g^c and share. They now publicly share g^{ab}, g^{ac}, g^{bc}. Each can now compute g^{abc}. This is the the simplest method I can think of, and is essentially what is on Wikipedia (see https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#Operation_with_more_than_two_parties). The natural question, of course, is how secure is all of this. See also http://ijns.jalaxy.com.tw/contents/ijns-v15-n4/ijns-2013-v15-n4-p256-264.pdf.

#3: Generalize the previous problem so that N people can share a secret in a crowded room, but no one else will know.
Solution: Let each person choose a number a_i and, with g as in the previous problem, compute g^{a_i}. We want the most efficient way to get to $g^{a_1 \cdots a_n}$. One way is to start with the first person (Alice), who sends g^{a_1} to the second person (Bob), who sends $g^{a_1 a_2}$ to the third person (Charlie), and so on. This chain will end with the n^{th} person (Nancy) receiving $g^{a_1 \cdots a_{n-1}}$. She raises this to the ${a_n}^{\text{th}}$ power to get the secret. At this point only the last person knows the secret.

We now help the first find the secret. Bob starts another of these chains, sending g^{a_2} to Charlie. Charlie sends $g^{a_2 a_3}$ to Denise, and so on. Eventually Nancy sends $g^{a_2 \cdots a_n}$ to Alice, who raises this to the ${a_1}^{\text{th}}$ power, and now she too has the secret.

Thus we have n chains, and afterwards all have the secret. How many computations would there be if we used the method from the previous problem, with everyone talking to everyone? Note in this method you only communicate with the person immediately before or after.

Chapter 5: #4: Calculate the average order of ϕ in various ranges: this means find $\frac{1}{x}\sum_{n \le x} \phi(n)$ for various x. Make a conjecture about the rate of growth.
Solution: Below is the code and we give some plots in Figure 5; it sure does look like the average order is linearly increasing! It's often worth doing a log-log plot, as that can illuminate relationships. For example, it may be hard to see a curve looks like $y = Cx^r$ (especially if r is some number like $11\sqrt{2}/3$), but if we do a log-log plot we get $\mathcal{Y} = r\mathcal{X} + \mathcal{C}$, where $\mathcal{Y} = \log(y)$, $\mathcal{X} = \log(x)$ and $\mathcal{C} = \log(C)$. We can thus use the method of least squares to figure out the exponent r and the constant $C = \exp(\mathcal{C})$.

```
phiplot[num_] := Module[{},
   (* will do up to num, saving results in lists *)
   list = {};
   loglist = {};
   sum = 0; (* initializes sum to 0 *)
   For[n = 1, n <= num, n++,
    {
     sum = sum + EulerPhi[n]; (* increases sum by phi(n) *)
     If[Mod[n, num/1000] == 0, (*
      only print every 1000 to keep size manageable *)
     { (* stores results in list, for plot and log-log plot *)
      list = AppendTo[list, {n, 1.0 sum/n}];
      loglist = AppendTo[loglist, {Log[n], Log[1.0 sum/n]}];
      }];
     }];
   Print[ListPlot[list]]; (* prints output *)
   Print[ListPlot[loglist]];
   (* Best Fit Line Parts: Will do for log-log plot *)
   (* x_n = log(n), y_n = log(sum at n divided by n, N =
   Length(loglist) *)
   Print[
    "Using Method of Least Squares: analysis online available at"];
   Print[
    Hyperlink[
     "https://web.williams.edu/Mathematics/sjmiller/public_html/BrownClasses/
     54/handouts/MethodLeastSquares.pdf"]];
   bigN = Length[loglist];
```

```
   xsum = Sum[loglist[[n, 1]], {n, 1, bigN}];
   xxsum = Sum[loglist[[n, 1]]^2, {n, 1, bigN}];
   ysum =  Sum[loglist[[n, 2]], {n, 1, bigN}];
   xysum =  Sum[loglist[[n, 1]] loglist[[n, 2]], {n, 1, bigN}];
   matM = {{xxsum, xsum}, {xsum, bigN}};
   outputvec = {{xysum}, {ysum}};
   bestfit = Inverse[matM].outputvec;
   Print[
    "Looks like of the form Const x^power + smaller; trying to get Const, power."];
   Print["Best guess for power from log-log plot: ", bestfit[[1, 1]]];
   Print["Best guess for Const from log-log plot: ",
    Exp[bestfit[[2, 1]]]];
   Print["Note 1/(2 zeta(2)) = 3/pi^2 = ", 3. / Pi^2];
   ];

Looks like of the form Const x^power + smaller; trying to get Const, power.
Best guess for power from log-log plot: 0.999999
Best guess for Const from log-log plot: 0.303969
Note 1/(2 zeta(2)) = 3/pi^2 = 0.303964
```

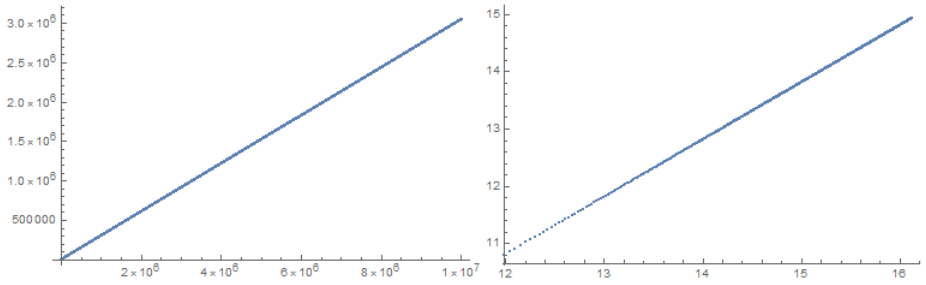

FIGURE 5. Left: average order of the Euler totient function. Right: log-log plot of average order of the Euler totient function.

Figure 6 is a proof from a former student of mine: http://mathoverflow.net/questions/84571/averages-of-euler-phi-function-and-similar.

Here is the standard, but very enlightening, elementary computation. Using $\phi(n) = n\sum_{d|n}\frac{\mu(d)}{d} = \sum_{md=n} m\mu(d)$, we manipulate finite sums:

$$\sum_{n<X}\phi(n) = \sum_{dm<X} m\mu(d) = \sum_{d<X}\mu(d)\sum_{m<X/d} m$$

$$= \sum_{d<X}\mu(d)(\tfrac{1}{2}X^2/d^2 + O(X/d)) = \tfrac{1}{2}X^2\sum_{d<X} d^{-2}\mu(d) + O(X\log X)$$

$$= \frac{1}{2\zeta(2)}X^2 + O(X\log X).$$

A similar calculation gives $\sum_{n<X}\theta(n) = \frac{1}{3\zeta(3)}X^3 + O(X^2)$. (Why is the error log-free?)

share cite improve this answer

answered Dec 30 '11 at 6:17

David Hansen
7,474 • 5 • 37 • 67

FIGURE 6. Post proving the growth rate of the average order of the Euler totient function.

No written HW over spring break.

6. HW #8: DUE APRIL 7, 2017

6.1. **Problems. Homework #8: Due Friday April 7, 2017: #1: Prove $\sqrt{p}$ is irrational if p is prime. #2: Use Roth's theorem to prove that there are only finitely many solutions in the integers to $x^3 - 2y^3 = 2017$. #3: (Exercise 6.12a) Prove that for any two rational numbers a and b with a < b, there is an irrational number x with a < x < b. #4: (Exercise 6.14): Prove or find a counter example for each of the following statements. a. The product of two rational numbers is rational. b. The product of two nonzero irrational numbers is irrational. c. The product of a nonzero irrational number and a nonzero rational number is irrational.**

6.2. **Solutions. Solution:** #1: If $\sqrt{p} = a/b$ with a, b relatively prime then $b^2p = a^2$ so $p|a^2$ and since p is prime we have $p|a$ (if a prime divides a product it divides at least one term). Thus we may write $a = p\alpha$, then find $b^2p = \alpha^2p^2$ so $b^2 = \alpha^2p$, and thus $p|b^2$ so $p|b$, contradicting a, b relatively prime.

Solution: #2: There are only finitely many integer solutions $(x, y) \in \mathbb{Z}^2$ to

$$x^3 - 2y^3 \;=\; a$$

(we do the more general case, not just $a = 2017$). In order to see this, we proceed as follows. Let $\rho = e^{2\pi i/3} = (-1)^{1/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Then

$$x^3 - 2y^3 \;=\; (x - 2^{1/3}y)(x - \rho 2^{1/3}y)(x - \rho^2 2^{1/3}y),$$

and therefore

$$\begin{aligned}
\left|\frac{a}{y^3}\right| &= \left|\frac{x}{y} - 2^{1/3}\right| \left|\frac{x}{y} - \rho 2^{1/3}\right| \left|\frac{x}{y} - \rho^2 2^{1/3}\right| \\
&\geq \left|\frac{x}{y} - 2^{1/3}\right| \left|\mathfrak{Im}(\rho 2^{1/3})\right| \left|\mathfrak{Im}(\rho^2 2^{1/3})\right| \\
&= \frac{3}{2^{4/3}} \left|\frac{x}{y} - 2^{1/3}\right|.
\end{aligned}$$

Hence every integer solution (x, y) to $x^3 - 2y^3 = a$ is a solution to

$$\left|2^{1/3} - \frac{x}{y}\right| \;\leq\; \frac{3 \cdot 2^{-4/3}}{|y|^3}.$$

By Roth's Theorem there are only finitely many such solutions.

Solution: #3: We want to find an irrational between two rational numbers a and b. Let $D = (b-a)/2^{2017}$. Note $a + \sqrt{2}L$ is irrational, and as $\sqrt{2}L < b - a$ we have $a < a + \sqrt{2}L < b$. (If our number were rational, say equal to p/q, then $\sqrt{2} = (p/q - a)/L$ and thus $\sqrt{2}$ would be rational.

Solution: #4: (a) True: if $r_1 = p_1/q_1$ and $r_2 = p_2/q_2$ then $r_1r_2 = (p_1p_2)/(q_1q_2)$. (b) False: As $\sqrt{2}$ is irrational, then $\sqrt{2}\sqrt{2} = 2$ is rational. (c) True: if $r = p/q$ and x is irrational, assume rx is rational; then $rx = a/b$ for some integers a, b, which implies $x = a/br = aq/bp$ is rational, contradicting x irrational.