The Teacher's Circle
Number Theory, Part 1

Joshua Zucker, August 14, 2006
joshua.zucker@stanfordalumni.org

[A few words about MathCounts and its web site http://mathcounts.org at some point.]

Number theory is all about adding and multiplying integers: pretty simple stuff, good for elementary school or for PhD mathematicians. Dr. Arnold Ross says of number theory, his choice for teaching the most brilliant high school students in the country as well as his own graduate students at Ohio State, that the purpose is "to think deeply of simple things." So let's do that together today.

What are integers made of? Well, there's the two important operations, adding and multiplying. If you have adding, and you have 1, you make all the positive integers: it's just counting! (Of course, counting is another interesting subject, as David Patrick and his Art of Problem Solving book will tell us!). But things get much deeper, more interesting and more subtle, when you talk about multiplying, because now starting with 1 won't really get you very far. Think of this as problem #0: if you want to make all the positive integers, using only multiplication, what raw materials will you need?

That's right, you will need to consider all of the

Primes

as being the building blocks of the integers. It's an amazing and deep fact that, just like there's only one way to write each positive integer as a sum of 1s, there's also only one way to write each positive integer as a product of primes. That's so important it's called the Fundamental Theorem of Arithmetic. (By the way, another interesting counting problem is how many ways there are to write each integer as a sum of other positive integers.)

1. How many primes are there? [If you don't know Euclid's proof, learn it! I won't do it in the session, most likely, so you can visit one of my favorite web sites and see a very brief statement of this beautiful proof by taking a look at http://www.cut-the-knot.org/proofs/primes.shtml or you can visit another cool web site and see a different proof, along with links to ones closer to Euclid's original, at http://primes.utm.edu/notes/proofs/infinite/euclids.html]

   I think one of the most important things about this proof is what it teaches about the meaning of infinity: if you have finitely many, you can be sure there's still at least one more.

2. List all the primes from 1 through 500. Yes, this sounds very tedious, but using the back of this page, you'll discover all kinds of interesting facts about patterns in multiples of numbers, and probably some other things too!

   For students, before giving them the Sieve handout (a good time to remind them of what "geometry" really means, and also to talk about how the Greeks thought of geometry and mathematics as essentially synonymous), the following problems are often helpful as warm-ups, not to mention good for teaching patience, though if that's not your goal, feel free to use some smaller numbers; alternatively, if division practice and divisibility tests aren’t your goal, let them use calculators:

(a) Is 221 prime? If not, what are its factors?

(b) What’s the largest divisor you need to check to be sure that 397 is prime? How do you know it’s the largest?

(c) Is 8171 prime, or not? How do you know for sure?

A student version of the handout, with slightly different directions than the teacher version on the back of this page, can be found on the back of this packet.

Sieve of Eratosthenes (Teacher Version)

To use this method, start with a long list of numbers like the one on this page. Forget about 1, since it is neither prime nor composite. [The mathematical term for this kind of number is *unit*]. Now you know 2 is prime, so circle it. Then cross off all the multiples of 2 (4, 6, 8, 10, 12, …) since you know they cannot be prime. Once you finish that, go to the next number after 2 that isn't crossed out [namely 3], and circle it. Cross off its multiples. Repeat this process until you have circled all the primes and crossed out all the composite numbers. There should be convenient patterns to help with a lot of the crossing out.

Things to notice while you do this: as you're crossing out, say, all the multiples of 11, which ones are already crossed out? Where's the first one that's not crossed out? What does that tell you about when you can stop crossing out and just circling?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320
321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340
341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360
361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380
381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400
401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420
421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440
441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460
461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480
481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500

Now that you have a list of primes to work with, you can start to notice some patterns. The next few examples contain some exercises to give people some raw material that might serve as motivation or inspiration for the thought that the problems will require. I wrote them a little more with the student vocabulary in mind than with yours; it probably won't take too much work to convert this to a handout you can use with your students.

The distribution of primes (what fraction of numbers are prime? How big are the gaps?)

3. You might have noticed that the gaps between primes tend to get bigger as you go along. Fill in the blanks to get one measure of how much bigger they are getting on average.

   a) Between 1 and __________ there are 10 primes.

   b) Between 100 and ________ there are 10 primes.

   c) Between 400 and ________ there are 10 primes.

   d) The longest run of consecutive composite numbers between 1 and 100 starts with _____ ______ and ends with ____________ and is ______ long.

   e) The longest run of consecutive composite numbers between 401 and 500 starts with ___ ______ and ends with ____________ and is ______ long.

   [By the way, there's a great opportunity to teach about fencepost errors in these last two! If boats leave every 15 minutes, how many leave from 9am to 5pm? 37, not 36! How many numbers are there from 27 through 33? 7, not 6!]

4. Do the gaps between primes get longer and longer, or is there eventually a record-size gap that never gets beaten?

   Factorials give a great clue about this problem. A factorial, like 7!, means to multiply all the integers from 7 down to 1. So, 7! is $7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$, which is the important part, or 5040, which isn't very important at all.

   a) The number $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 + 2$ is composite – not prime. How can you be sure? Well, if you can find a factor that's not 1 or the number itself, it must be prime.

   b) Is $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 + 3$ composite?

   c) Based on your answers to the previous two problems, there must be **at least** how many composite numbers in a row, starting from $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 + 2$?

   d) Name a number which you can be sure is in a string of at least 99 composite numbers in a row.

   e) Name a number which you can be sure is in a string of at least 999 composite numbers in a row.

   f) Explain how you can be sure that any record number of composites in a row eventually gets broken.

5. Primes are a lot more dense toward the beginning of the list, as we saw in the last problem. At the beginning of the list, in fact, there are three odd numbers in a row (3, 5, 7) which are all prime!

   a) Does that ever happen again in your list?

   b) Can it ever happen later on, maybe beyond 500? Why or why not?

   You can find pairs of primes in your list: two odd numbers in a row which are both prime. These are called "twin primes", like 17 and 19, or 41 and 43.

   c) List all the twin primes less than 500.

   d) In part (b) you explained why there can't be any more triple primes besides 3, 5, 7: there's only one triple prime. You also know Euclid's proof that there are infinitely many primes. How about twin primes? How many sets are there?[1]

Adding primes

Primes are made for multiplying. As long as you're multiplying and factoring, primes are the way to go. Once you start adding, things get hard. So hard, in fact, that the solution to some parts of this problem are not yet known even after hundreds of years of work by the best mathematicians. But some parts, you can do in just a few minutes!

6. Let's see what numbers we can make by adding up two primes.

   $2 + 2 = 4$ $\quad$ $2 + 3 = 5$ $\quad$ $3 + 3 = 6$ $\quad$ $2 + 5 = 7$ $\quad$ $3 + 5 = 8$ $\quad$ $2 + 7 = 9$

   and so on. It seems like every number is either prime, or we can make it by adding up two primes. For example, 39 is 37 + 2. 17 can't be made by adding two primes, but it is prime itself.

   a) Make all the composite numbers less than 20 by adding two primes.

   b) Find a number that's not prime, and is not the sum of two primes. Hint: there's one in the 20s!

   c) Is there such a number in the 30s? In the 50s?

   d) Find a pattern in these numbers. Hint: look at the size of the "gaps" between primes. Explain, based on your answer, exactly how you can tell whether an odd composite number is the sum of two primes or not.

   e) The examples in b, c, and the discussion in part d probably all led you to odd numbers. Can you find an even number which is not prime, and not the sum of two primes?

[1] Last I heard, after a couple hundred years of work, mathematicians are still not quite sure of the answer to this question, though they are gradually becoming more certain that the answer is that there are infinitely many twin primes.

Squares, Pythagoras, and Primes (with some hints of complex numbers!?)

7. A perfect square, or square number, is what you get when you multiply a whole number by itself.

   a) Just for practice, write down the first 10 perfect squares.

   b) List all the primes up to 100. For each one, determine whether it can be made by adding up two perfect squares or not. For example, 5 = 4 + 1, but 7 cannot be written as the sum of two perfect squares. For the numbers that can be written as the sum of two perfect squares, keep track of which squares you used.

   c) Find a pattern that tells you which primes can be written as the sum of two squares. Hint: look at where they land in the big sieve. How do they line up?

   d) [Some algebra required, and probably you'll want to do the problem on squares from the division section before you do this one.] Explain why all the impossible ones are impossible to write as the sum of two squares. [Hint: look for where the square numbers fall in the big sieve as well.]

   e) [Warning: really hard!] Explain why all the possible ones really are possible. That is, how do you know the pattern you've observed keeps working forever?

Prime-generating formulas (Mersenne and Euler)

8. Mathematicians have long sought formulas that generate prime numbers, only prime numbers, and ideally every prime number. Here are two formulas that are a few centuries old, that turn out to be quite interesting prime-generating mechanisms even if they don't work quite as the mathematicians originally hoped.

   a) One famous formula involves the numbers that are one less than the powers of 2. To begin, $2^1 – 1 = 1$, a unit, not prime. Then $2^2 – 1 = 3$, which is prime. $2^3 – 1 = 7$, which is prime. But $2^4 – 1 =$ ________, which is __________.

   b) That formula has a lot better chance of working if the exponent is prime. Try $2^5 – 1$, $2^7 – 1$, and so on. Are all of those primes? How long does the pattern work?

   [Notice all the great chances to review vocabulary like exponent and power, practice some arithmetic and even long division, and for more advanced students to get into the difference of squares/cubes/nth powers formulas for factoring.]

   c) Another famous pattern, for which my favorite mathematician Euler gets the credit, is to start with any number, square it, subtract your original number, and then add 41. In other words, $n^2 – n + 41$. When $n = 1$, we get 1 squared is 1, minus the original 1 leaves 0, adding 41 gives 41. When $n = 2$, we get 2 squared is 4, minus the original 2 leaves 2, plus 41 makes 43. How long can we use this pattern to produce new prime numbers?

Sieve of Eratosthenes

A “sieve” is like a strainer. Eratosthenes is a Greek geometer who is famous for being the first to get an accurate estimate of the size of the Earth.

To use this method, start with a long list of numbers like the one on this page. Forget about 1, since it is neither prime nor composite. [The mathematical term for this kind of number is *unit*]. Now you know 2 is prime, so circle it. Then cross off all the multiples of 2 (4, 6, 8, 10, 12, …) since you know they cannot be prime. Once you finish that, go to the next number after 2 that isn’t crossed out [namely 3], and circle it. Cross off its multiples. Now circle the next number that’s not crossed out, namely 5, and then cross out all of its multiples. Repeat this process until you have circled all the primes and crossed out all the composite numbers. There should be convenient patterns to help with a lot of the crossing out.

Now you have a list of primes to use on the rest of the problems in this section! Think about your warm-ups when you do this, and you’ll be able to stop worrying about crossing out, and only circle the rest, after you reach a certain point: what is that point, and why?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280
281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320
321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340
341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360
361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380
381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400
401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420
421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440
441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460
461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480
481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500

The Teacher's Circle
Number Theory, Part 2

Joshua Zucker, August 14, 2006
joshua.zucker@stanfordalumni.org

For further reading, the Art of Problem Solving has a great *Introduction To Number Theory* that expands on a lot of the themes begun here and some other great topics as well.

Looking at how a number is built using multiplication quite naturally leads to ideas of

Divisibility

which of course also

1. How can 48 be built from primes? In what sense is there only one way? How can you organize your work in general to find the prime factors of moderately large numbers like 2006?

2. What are all the divisors of 48? Of 120? 2006? How many different ways can you find to organize those answers?

3. How many divisors does each of those numbers have? We're not talking about primes here, but all the divisors. [Some students are intimidated by notation. Others think it's cool and they feel smart to learn it. So, if you want, you can tell them about the "tau function", $\tau(n)$, like a greek letter *t*, which is commonly used to represent the number of divisors of *n*.]

4. Make a list of all the numbers from 1 through 30, their divisors, and how many divisors. What do you notice?

   Some good things to look at include when the number of divisors is odd, and when it is even (which maybe grownups like us discovered while doing the earlier problems).

   This would also be a good time to investigate the sum of the divisors, instead of just counting how many there are.

   Also look at whether the number of divisors of *m* times the number of divisors of *n* is equal to the number of divisors of *m* times *n*, which naturally leads to…

Greatest Common Divisor

5. Compute the greatest common divisor of 36 and 84.

   Compute GCD(98, 120).

   Explain how you found your answer, and explain how you are sure that the number you got is the **greatest** of all the common divisors.

   I imagine most of you described a method based on one of the methods for finding all the divisors. The prime factors are a good way of doing it, for small numbers like these. But factoring large numbers is hard! So there's a better way, which we call Euclidean algorithm [a good opportunity to explain to your students who Euclid was and what an algorithm is.] I'd explain it to students something like this.

If you want to find the greatest common divisor of 84 and 66, first you divide 84 by 66 and find the remainder of 18.

Euclid understood that the GCD of the original two numbers is the same as the GCD of one of the original two numbers and the remainder [how can we understand this?]. Since smaller numbers are easier to deal with, then we can say

GCD(84,66) = GCD(66,18).
And now we can repeat the process! 66 divided by 18 leaves remainder 12.
GCD(66,18) = GCD(18,12). 18 divided by 12 leaves remainder 6, so
GCD(18,12) = GCD(12,6). Now 12 divided by 6 leaves no remainder, so 6 is the GCD of the original two numbers (and indeed any pair of numbers from our collection).

Since long division is much easier than finding prime factors of big numbers, this method is really useful when you have big numbers to deal with.

6. a) Is it true that if GCD(a,b) = 1 and GCD(a,c) = 1, then GCD(b,c) must equal 1?

   b) Is it true that if GCD(a,b) = 1 and GCD(a,c) = 1, then GCD(a,$b \times c$) must equal 1?

   c) Is it true that if GCD(a,b) = 2 and GCD(a,c) = 2, then GCD(a,$b \times c$) must equal 2?

   d) Now look again at the question of whether the number of divisors of m times the number of divisors of n is equal to the number of divisors of m times n.

7. A fun GCD activity:
   Imagine a pool table with pockets in the four corners. Represent it as a rectangle drawn on graph paper. Start with a ball at the bottom left corner, moving up at a 45° angle. The ball bounces off each side of the rectangle, until finally it reaches one of the corners and falls in the pocket.

   For example, draw a 5 by 10 pool table (width 5, height 10). The ball moves up and to the right, hits the middle of the right side of the table, moves up and to the left, and falls into the top left pocket.

   a) How many times does the ball bounce on a 6 by 10 table? Which pocket does it land in?

   b) Draw tables of various sizes and make a chart listing the dimensions of the table, how many times the ball bounces in total, how many of those bounces are on the left/right sides, how many are on the top/bottom sides, and which pocket the ball lands in. Make sure to include at least the 1 by 3, 1 by 4, 1 by 6, 3 by 5, 6 by 10, 9 by 15, 1 by 12, 2 by 12, 3 by 12, 4 by 12, 5 by 12, and 6 by 12 in your list, and as many others as you have time for. [This is one of the first activities I use for teaching special cases and organization.]

   c) Think about greatest common factor (and about writing and simplifying fractions). Your drawings should help you understand why some of the rows in the table give the same answers.

d) Using the tables you have drawn, can you predict which corner the ball will end in on a 79 by 103 table? 79 by 102? 78 by 102? Explain how you made your prediction. Can you prove your answer?

e) On each of those tables, predict how many top/bottom bounces and how many left/right bounces the ball will have. Again, explain how you made your prediction, then work on proving your answer.

8. The greatest common factor of 12 and 18 is 6. Their least common multiple is 36. Take some other pairs of numbers, maybe from one of the earlier problems here, and find the GCF and LCM.

   a) Prime factorize the LCMs. Prime factorize the GCFs. Prime factorize the original numbers. What do you notice? Can you explain why the patterns you observe always work?

   b) How much is 12 times 18? How much is the GCF of 12 and 18, times the LCM of 12 and 18? Try it with some other numbers. Can you explain why this always happens? [What if you try it with sets of three numbers instead of two?]

   c) If two numbers *x* and *y* have a GCF of *d*, find a formula for the LCM. [You can also ask this question without algebra, asking them for a pattern to compute the LCM instead of an algebraic formula.]

9. You have $52 to spend, and can buy Frisbees for $8 each and soccer balls for $12 each.

   a) What choices do you have for the number of Frisbees and soccer balls to buy?

   b) What does this have to do with GCF and LCM?

   c) Can you explain a general method for solving this sort of problem, with other numbers in place of the $52, $8, and $12? [What if there are three items you can buy?]

10. Work out a formula for the number of factors of a number in terms of its prime factorization.

11. Work out a formula for the sum of the factors of a number [sometimes denoted with the greek letter *s*, sigma, for sum: for example, $\sigma(4) = 1 + 2 + 4 = 7$, for those kids who enjoy learning fancy notation].

12. If the sum of all the factors of a number, including 1 but not itself, equals the number itself, we call the number **perfect**. [Abundant numbers have a sum that's bigger, and deficient numbers have a sum that's smaller than the original number.] The smallest three perfect numbers are 6, 28, and 496.

    a) Write down their prime factorizations.

    b) Check that the numbers really are perfect.

c) Find a pattern in their prime factorizations, relate it to things that you found about prime patterns.

d) Using that pattern, see if you can guess the next perfect number, and maybe the one after that.

e) For a much much harder challenge, prove that there are no even perfect numbers except the ones contained in this pattern.

f) For a much harder challenge than that, see if you can find any odd perfect numbers.

Just in case we have more time, review some

Divisibility Rules

at least for 2, 3, 4, 5, 9, and 11. [Here's an example that works up from hard-ish exercises toward problems, once you know the divisibility rules and why they work. And if you don't, you can find it in the Ask Dr Math web site frequently asked questions, in the divisibility rules section: http://www.mathforum.org/dr.math/faq .]

13. a) Is 7391 divisible by 11? If not, can you change one digit to make it divisible by 11? [A good example of multiple possible answers.]
b) Is 349602 divisible by 3? If not, what is the nearest number that is?
c) What choice(s) for the last digit * will make 37493 divisible by 4?

d) Knowing the divisibility tests you have learned, how would you check if a number is divisible by 6?[2]
e) Is 73645362 divisible by 6?

f) Knowing the divisibility tests you have learned, how would you check if a number is divisible by 8?[3]
g) Prove that your test for divisibility by 8 really works: that is, that numbers divisible by 8 pass the test, and numbers not divisible by 8 do not pass the test.
h) What other numbers have divisibility tests of this type?

i) Can you make a divisibility test for 27 based on the same idea as the tests for 3 and 9? Hint: 999 is divisible by 27.
j) By looking at the factors of 999, what other number will have the same divisibility test

[2] Some students may need the hint that 6 is 2 times 3. They might even need to do some special cases: make a list of multiples of 6, and observe what they have in common (they're all even … and maybe they also notice they're all multiples of 3). And if they understand prime factorization, they can see that it works both ways (all even multiples of 3 are multiples of 6).

[3] Good students will check if it's divisible by 2 and 4. Really good students will realize that it doesn't work. Really really good students will be able explain clearly why it doesn't work (because the divisibility by 4 automatically guarantees divisibility by 2, so checking it provides no new information). Really really really good students will see the pattern in 2 and 4 and realize that since 8 is 2^3 that the pattern continues, so you look at the last 3 digits. Or they'll understand the reason that the divisibility tests work, perhaps because you explained them really successfully, so the hint that 1000 is divisible by 8 will help them (because they'll see it as the same as the facts that 10 is divisible by 2 and 100 is divisible by 4).

as 27?
k) Think about factors of 99, 9999, and 99999. Do they lead to any other useful divisibility tests?

l) Combining the divisibility tests you know so far (for 2, 3, 4, 5, 9, and 11), along with the techniques used to establish divisibility tests for 6 and 8 and 27, what numbers less than 100 can you make divisibility tests for?

m) Using the fact that $7\times 11 \times 13 = 1001$, invent divisibility tests for 7 and 13 that have a similar spirit to the divisibility test for 11.
n) Test 1390312 for divisibility by 7 and 13. Is the test you invented worth the trouble?

o) [From George Polya's *How To Solve It*] You find a very old book which records purchases made at a farm. Someone has bought 72 turkeys, for $*.** each, and the total cost was $*67.9*, where each * represents a digit that was too smudged to read. How much did each turkey cost?

p) What is the probability that 5*383*8*2*936*5*8*203*9*3*76 is divisible by 396? Each * stands for an unknown digit 0 through 9, and each of the ten digits is used exactly once, placed at random. Hint: 396 is 4 times 9 times 11.

Another fundamental idea in number theory is what happens when things aren't necessarily evenly divisible, and you spend your energy focused on the remainder. The problem about the primes being a sum of two squares is one such example, but in general the study of remainders is called

Modular Arithmetic

Or sometimes "modulo" instead.
The fundamental idea is to classify numbers according to the remainder when you divide by some fixed number called the "modulus". For example, if you are interested in the last digit of a number only, you can look at the number "mod 10". If you want the last two digits, that's "mod 100". If you want to know whether it's even or odd, that's the same as saying it's 0 or 1 "mod 2". If you want to know what time it will be in 83 hours, that's "mod 12" (or maybe 24 if you care about AM/PM).

14. Let's focus on perfect squares first to see if we can understand why at least half of the prime fact must be true.

Look at things mod 2. If you square an even number, the answer is even. If you square an odd number, the square is odd. The amazing thing is that to prove that, you only need to consider $0^2 = 0$ and $1^2 = 1$ and you're done, because every even number can be written like $(2n + 0)$, and squaring it, all the $2n$ parts are still even, so on dividing by 2 they leave no remainder. Similarly the odd numbers are $(2n + 1)$, and squaring it, again all the $2n$ parts are still even, so only the 1 matters when you divide by 2 and take the remainder. This is because adding multiples of 2, or multiplying multiples of 2, always gives multiples of 2 (and in fact that works if you replace the 2 with 37 or any other number).

a) Now try mod 3: your starting number leaves remainder 0, 1, or 2 [or perhaps it's cleverer to choose 0, 1, and –1 as the remainders instead.] So what must be true when you square a number? What are the possible remainders of n^2 mod 3?

b) Repeat with mod 4.

c) Explain why any prime that is equal to 3 mod 4 (that is, leaves remainder 3 when you divide by 4) cannot be made by adding two squares.

d) What about mod 5? 7? 8? 10? [The fact about the last digits of squares is pretty cool, and explaining why only the numbers 0 through 5 need to be checked is a good exercise in symmetry and in multiplication: only the last digits can affect the last digits, which is another way of saying the $2n$ and $2n + 1$ comments above.] [There's a beautiful, but somewhat difficult, theory of figuring out which numbers can be perfect squares mod other numbers, and the crowning discovery there is called "quadratic reciprocity". It's a rather similar time-saver to the Euclidean algorithm for greatest common factor, but it's a lot harder to understand why it works.]

15. Now let's try division. But watch out! We're going to stick to integers. So normally, you'd say to divide 6 by 2, that's the same as 6 times 1/2, which is 3. But 1/2 doesn't exist necessarily! To illustrate what this means, let's think about the clock, so instead of saying 5 times 5 is 25, on the clock we'll see it pointing at a time just one hour later, so we'll say 5 times 5 is 1. That is, we'll work mod 12, only looking at the remainder because that's the only thing that affects where the clock hands will be pointing.

a) Normally, in division, because $2 \times 3 = 6$, we can also say that $6 \div 3$ is 2, and $6 \div 2$ is 3, and there's no trouble. There's only one solution to each division problem. But on the clock, in addition to $2 \times 3 = 6$, there's another solution: $2 \times ? = 6$. What is the other solution?

b) Because there are two solutions, $6 \div 2$ doesn't make sense, and 1/2 doesn't exist on the clock. To be more specific, there is no solution to the equation $2 \times ? = 1$; that's another clear way to see . But some relationships, like multiplying by 5, do give only one solution, and so 1/5 does exist. In fact, because 5 times 5 is 1, 1/5 = 5! To check that this really works, take a number like 10. What is $10 \times 1/5$? It's the same as 10×5. Explain.

c) Make a multiplication table for mod 5, remembering to only write the answer when you divide by 5. Which numbers can be multiplied to make 1?

d) Make a multiplication table for mod 6, and answer the same question.

e) Look for patterns: which numbers can be multiplied to make 1 in which mods? For example, is there an easy way to tell whether 87 will have an inverse mod 99? What about 91, mod 137?[4]

16. Another classic type of mod problem is called the Chinese Remainder Theorem. This is where you know something about the remainder of a number in several different mods, and you have to combine them into one answer. For example:

A miserly old man in the desert is considering giving away all his camels. "I could

[4] Try some special cases of other small mods like 5 and 6, and look for patterns. If you're still stuck, think about greatest common factors carefully, and it will lead you not only to the answer but also to a proof of the answer.

divide them among my two sons, but there would be one left over. If I divided them among all my five children, but there would be two left over. Maybe I should divide them among all my seventeen children and grandchildren ... but no, then there would be three left over. I suppose I might as well keep them all."

a) How many camels does he have?

b) Are there other possible numbers of camels?

c) Generalize! [For a student, I'd give lots of easier examples with just two mods, and pretty small numbers, and then ask if they can give a general rule for solving all of those problems.]

17. To follow up on the squares from a few problems ago:
Instead of always having the exponent 2, and different bases, it's also very interesting to start with a certain base, and look at different exponents.

    a) What are the powers of 2, mod 5?

    b) What are the powers of 2, mod 10?

    c) What are the powers of 2, mod 6? How many do you have to list before you get bored?

    d) Experiment and explore with the patterns you notice!

18. If we have time, which I'm quite sure we won't – in fact I suspect that nobody will even get this far in reading the handout – this would be a great time to start exploring the Euler phi function, which unifies the "greatest common factor 1" ideas with the ideas of some of the previous problems here.