Numbers for Masochists:
A Guide to Mental Factoring

Hilarie Orman and Richard Schroeppel

June 5, 2018

DRAFT

Contents

All Is Number
– Aristotle, Metaphysics, on the Pythagoreans

1 Introduction

Many people can multiply large numbers mentally, and there are numerous treatises on how to do it. However, the inverse problem, factoring, is rarely discussed. This paper will show you how to factor numbers up to 100,000 in your head. In fact, you will be able to factor some numbers much larger than that.

People who have a love for numbers will understand the delight in seeing an integer "split" into its factors or to know for a fact that it is prime. Others may come to understand the beauty in factoring by practicing the skill, but if not, there are some motivational scenarios.

Counting sheep has long been a recreation for insomniacs, but it is insufficiently absorbing to be a guaranteed soporific. Richard Schroeppel suggests that rather than counting sheep, you assume that you have a herd of more than $100,000$ and then try to arrange them in a rectangle. How many sheep on each side?

Or suppose that you have survived a shipwreck and have washed ashore on a desert island. The only piece of wreckage to survive with you is the emergency supply case, which has a six digit combination lock. There is a six digit number written on the top of the case, and a copy of this manuscript taped to the bottom. Because the safety officer was an amateur mathematician, you guess that the combination is the six digits of the two prime factors of the six digit number. Can you open the case in time to save your life? If you have mastered mental factoring, then, yes, you will survive.

We will describe all you need to master in order to take on the challenge of mental factoring. Although some of the methods rely on theorems from the field of number theory, we have tried to describe everything without relying on any theoretical mathematics other than high school algebra. Our terminology will be mathematically informal. For example, we will usually say "a divides b" rather than "a is a divisor of b" or "b is a multiple of a."

If you dare to go on, a word of warning. Although the techniques we describe are intended for mental calculation, and almost anyone can learn to conquer numbers less than $10,000$, working on larger numbers can be stressful. It may take twenty minutes of intense concentration to analyze a 6 or 7 digit number. Don't try it while driving, it is worse than texting.

2 Basic concepts

A prime is an integer that has no factors other than itself. The smallest prime is 2, and that is the only even prime.

What is factorization?

To factor an integer means to list all the prime numbers that when multiplied together are equal to the integer. The factors of 6 are 2 and 3, the factors of 24 are 2, 2, 2, and 3. There are divisors of 24, such as 8 and 12, that are not primes. It is important to know that a number has only one factorization into primes.

Although one can carry out the calculations described here without knowing any more math than simple arithmetic, our explanations use some facts from algebra and elementary number theory and terminology from that field. We will refer to these concepts:

- Quotient and remainder. For an integer a and a non-zero integer b, we say that a divided by b has a quotient q and a remainder r such that $a = q * b + r$. For any pair a and b, q and r are unique, and $0 \leq r < |b|$.
- Divisibility. We say that b divides a if the remainder of a divided by b is zero. Another way to say this is that b is a divisor of a. This is written as $b|a$.
- Prime divisors.
  - If a prime p divides a product ab, then p must divide a or b.
  - If n is a product of primes not including p, then p does not divide n.
- Modular equivalence and reduction. We can do arithmetic with remainders. We say $a \equiv c \ (mod\ b)$ if a and c have the same remainder when divided by b. We often use the remainder as a substitute for a number and call that the "reduced form" of $a \equiv r \ (mod\ b)$. This means that a divided by b has remainder r. We also say "a is congruent to r mod b." In this representation, b is called the "modulus" and r is the "residue".
- Modular arithmetic. Most of the ordinary arithmetic operations still work when we are using a fixed modulus. If

  $$a \equiv r \ (mod\ b)$$

  $$c \equiv s \ (mod\ b)$$

  then

  $$a + c \equiv r + s \ (mod\ b)$$

  Subtraction and multiplication also work. Division and square roots sometimes work, but sometimes they don't because there is no solution for the particular modulus.
- Greatest common divisor (GCD). The GCD of a and b is the largest number that divides both a and b. For example, the GCD of 12 and 15, written as, $\gcd(12, 15)$, is 3.
- Relatively prime. If there is no prime number p such that p divides a and p divides b, then it follows that the GCD of a and b is 1. We say that a and b are relatively prime.
- Least common multiple. The smallest number that is divisible by integers a and b is called the least common multiple. It is written as $lcm(a,\ b)$.
- Complex integers. Let i denote the square root of -1. For integers a and b, the number $a + bi$ is called a complex integer.

3 Overview

Mental factoring uses mathematics to reduce the amount of mental arithmetic needed to factor a number. The methods are a set of rules that can be memorized and applied to any particular number. Larger numbers use more complicated rules – there is a tradeoff between the complexity of the rules and the difficulty of multiplying and dividing mentally. We have tried to minimize the rules so that only a few arithmetic operations with 3 or 4 digit numbers are necessary, but you will find it necessary to be facile with mental arithmetic to ensure that the endeavor is enjoyable.

You will need to understand the material in the early sections, before beginning to factor 5 digit numbers, but once you have mastered those concepts, here is a guide to using this document for factoring a number m:

1. Using the techniques of section 4, remove all small prime factors from m by division. Call the result n. For numbers less than 10,000, this will probably complete the factorization.
2. If n is small, try to use Difference of Squares (section 4.1) to factor it.
3. If n larger than 10,000, then find its remainder when divided by 4; call this r.
4. If r is 1, use the method described in section 7.3.
5. If r is 3, use the method described in section 7.5.
6. If r is 1 and Step 4 did not result in a factorization, then go to section 7.7 and try one or more of the methods there. If that does not work, try one or more of the methods in section 8.
7. If r is 3 and Step 5 did not result in a factorization, then go to section 8 and try one or more of the methods there.

4 Cheap divisor tricks

The methods in this section have simple "tricks of the trade" that can be used to factor small numbers (less than 1000). They will often work for numbers up to 10,000, and in all cases they are useful preliminaries to starting to use the advanced methods in later sections.

The integer number to be factored is named n in our discussions.

You may already know of some tricks, like knowing that if the low digit is 5, the number is divisible by 5, or if the low order digit is zero, the number is a multiple of 10. You may even know about "casting out nines." We'll show you some more tricks to use for larger numbers.

In the following rules, we show how to to identify small prime factors of n. If a prime p divides n, then the quotient of n/p becomes the number we are trying to factor. We replace n by that quotient and continue applying the rules. We will sometimes call the quotient "the remaining number". Mathematicians call it the "co-factor".

In this section we describe how to to test and usually reject possible small prime divisors. We emphasize how to decide easily if p does not divide n. Importantly, we don't need the quotient nor the remainder of n divided by p: we only need to establish that p does or doesn't divide n. We can transform n in various ways that preserve the "divides" property of p into n, even though the quotient and/or remainder may be different.

Many of the following quick tricks rely on a principle of divisibility: if p divides $n \pm i * p$, then p divides n. This means that we can add or subtract multiples of p to n without changing divisibility (or non-divisibility) by p.

Another basic principle is that n can be multiplied or divided by primes that are not equal to p without changing the divisibility by p. For example, take $310/10 = 31$. Because 31 is prime, we know that 310 is not divisible by 7 or 11, etc. (of course, it is divisible by 2 and 5).

The following is a list of "tricks" to check if n is divisible by primes up to 73. We begin a factorization by removing all the small prime factors. It is important to keep repeating a rule until it no long applies to the remaining quotient. For example, 48 is even, so we know that $48 = 2 * 24$. But 24 is also even, so $48 = 2 * 2 * 12$, and 12 is even, and 6 is even, so $48 = 2 * 2 * 2 * 2 * 3$. So when we say "remove a prime factor", we mean to remove all copies of that prime.

2: if the low order digit of n is even, n is divisible by 2.
3: if the sum of the digits of n is divisible by 3, n is divisible by 3.
5: if the low order digit is zero or 5, n is divisible by 5.
7: 7 divides 98. For a three digit number n, if the hundreds digit of n is h, calculate $2h + (n \ (mod\ 100))$. If that is a multiple of 7, then so is n. If n is 4 digits, and the thousands digit is t, the two-digit number formed by th is denoted by t_h. Calculate $2t_h + (n \ (mod\ 100))$. If that is a multiple of 7, then so is n.
7, 11, and 13:
$1001 = 7 * 11 * 13$. Calculate $n \ (mod\ 1001)$ (i.e. the remainder of n divided by 1001), and determine if the result is divisible by 7, 11, or 13. If so, then n is divisible by that prime. There is a trick to computing the remainder. For example, if $n = 6223$, then $n \ (mod\ 1001)$ is $223 - 6 = 217 = 7 * 31$. That is to say, for a four digit number abcd, the remainder modulo 1001 is $bcd - a$.
11: For a 3 digit number, abc, if $b = a + c$ or $b + 11 = a + c$, then $abc = 11 * ac$ or $11zc$ where $z = a - 1$. For a 4 digit number abcd, examine $a + c$ and $b + d$. If they are equal or if the difference is 11, then 11 divides abcd.
13: just learn the small multiples of 13 and divide quickly: 13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, 156, 169, 182, 195, 208, 221, 234, 247, 299. The fact that 299 is in the list leads to a cute trick. You can divide n by 300 and take the quotient q and the remainder r. If $q + r$ is divisble by 13, then so is n.
17 and 19: these are discussed later as divisors of numbers near 1000.
31: 31 divides 992.
23 and 29: Note that $2001 = 3 * 23 * 29$. If n differs from 2001 by a multiple of 23 or 29, then that prime divides n. For some numbers n, it will be easy to see that $n - i * 2001$ is a multiple of 23 or 29. For example, $4117 - 2 * 2001 = 115$ and $115 = 5 * 23$ (note that although 23 divides n, 5 does not). The test only works for the primes that divide 2001. This trick also works for $i * 2001 - n$, for example, $6003 - 5133 = 870 = 30 * 29$.

Another way to use 2001 is to add or subtract multiples of 2001 to n to force the low order digit of $n \pm i * 2001$ to 0. Then you can divide that number by 10 and work with the quotient. For example, take $n = 9193$. Then $n - 3 * 2001 = 3190$. After dividing by 10 we have 319, which is $11 * 29$.

Similar techniques can be used with other numbers that are multiples of small primes. Numbers near 10000 can be particularly useful, and we will call the following set the "m's":

- $10001 = 73 * 137$.
- 10004 is divisible by 41 and 61.
- $10005 = 5 * 2001 = 5 * 3 * 23 * 29$
- $10010 = 10 * 1001$, and we recall that $1001 = 7 * 11 * 13$.
- 10011 is divisible by 47 and 71.
- $10013 = 17 * 19 * 31$.
- 10017 is divisible by 53.
- 10019 is divisible by 43.

To check if n is divisible by the factors of an m number, compute a multiple of 10001 that is close to n and subtract from n. If that difference is divisible by 73 or 137, then so is n. Let's call that difference a. To check n against 10004, we can use some of the information that we just computed

for 10001. Recall the small number that we used for multiplying in the previous case; let's call that number j. The difference between n and $j * 10004$ will be $a - (10004 - 10001)j = a - 3j$. If $a - 3j$ is divisible by 41 or 61, then so if n. In this way we can check each of the m's in turn with minimal mental effort.

We can work through the m's in either increasing or decreasing order. Here is an example using increasing order:
Check for factors of 160101.
$160101 - 16 * 10001 = 85$ which is not divisible by 73 or 137, so we can eliminate those numbers as factors.
$160101 - 16 * 10004 = 85 - 48 = 37$ which is not divisible by 47 or 71, so we can also eliminate those as factors.
In this way, calculate n $(mod\ m)$ for each of the m's using multiples of 16. You will find that none of the m's yield any factors of 160101.

Here is an example using the m's in decreasing order, starting at 10013 and working down (optional m's are not used):
Check for factors of 160109. Our multiplier, q, is 16.
160109 - 16 * 10013 = 160109 - 160000 - 16*13 = 109 - 208 = -99.
That is not divisible by 17, 19, or 31, so none of them are factors of 160109.
$160109 - 16 * 10011 = -99 + 2 * q = -99 + 2 * 16 = -67$
That is not divisible by 47 or 71, so they are not factors of 160109.
$160109 - 16 * 10010 = -67 + 1 * q = -67 + 16 = -51$
That is not divisible by 7, 11, or 13, so they are not factors of 160109.
$160109 - 16 * 10005 = -51 + 5 * q = -51 + 5 * 16 = 29$
That is divisible by 29, and therefore 29 is a factor of 160109.

Before trying to divide 160109 by 29, we apply the remaining tests just in case they reveal another factor.

$160109 - 16 * 10004 = 29 + 1 * q = 29 + 16 = 45$
That is not divisible by 41 or 61, so they are not factors of 160109. $160109 - 16 * 10001 = 45 + 3 * q = 45 + 48 = 93$
That is not divisible by 73 or 137, so they are not factors of 160109. $160109 - 16 * 10000 = 93 + 1 * q = 93 + 16 = 109$
The low digits of our target number are 109, so we know that we have correctly tested the m numbers.

We will need to divide 160109 by 29 mentally. It takes some practice do this, but once you've mastered it, you'll see that the quotient is 5521 with less than a minute of thinking. Remember that we have to eliminate all copies of a factor, so we need to determine if 29 divides 5521. We previously noted that 29 divides 2001. Let's subtract 2001 from 5521, yielding 3520. If 29 divides 352, then it is a factor, but it doesn't, so we can move on to checking other possible prime divisors.

Can we determine the factors of 5521? The square root is about 75, and our previous test have eliminated all lower factors except 37, 43, 53, 59, and 67. After we list a few more tricks, we will show how to factor 5521.
17, 19, 31, a cheap trick:
$17 * 19 * 31 = 10013$. Compute $n * i$ where i is small to force low order digit to be 3. This might reduce with 10013 quickly. This is not guaranteed to work, but it is a useful, cheap check. Another trick is to add 10013 if the low order digit of n is 7. If the low order digit is 1 or 9, triple n and then add or subtract 10013.

Now that you know how to use numbers near 10,000 to test for prime divisors, we'll give you a few more numbers that you can use in a similar way.

A few more useful things to know about small prime factors:
17: 17 divides 1003 and 6001 and 102.
19: 19 divides 1007 and 399 and 7999 and 1501.
31 and 43: 3999 is divisible by 31 and 43.
37: 999 is divisible by 37, and 111 is divisible by 37. If n has 3 digits, you can rotate them and preserve divisibility by 37.
43: 43 divides 301.
53: 53 divides 1007.
59: 59 divides 1003 and 20001.

If you have tried all the primes up to this point without factoring the target number, then you should switch over to using quadratic forms, as explained in the section 7.

The following tests for larger primes are useful in the Difference of Squares method in section 8.3.
67: 67 divides 201.
71: 71 divides 994 and 10011.
73: 73 divides 511 and 1022.
79: 79 divides 1501 and 3002.
83: 83 divides 996 and 20003.
89: 89 divides 801.
97 and 103: both divide 9991.
101: 101 divides 9999.
$100 \pm n$: each divides $10000 - n^2$.
107: 107 divides 9951, 20009.
109: 109 divides 981, 10028, 40003.
113: 113 divides 1017 and 20001.
127: 127 divides 8001 and 1016.
241: 241 divides 964 and 20003.

Matching multiples. You may wonder which multiple of a prime number to use when testing it for any particular n. If you are trying to factor 4567 by testing for 53, should you use $5 * 1007$ or $4 * 1007$? Probably $5 * 1007$ is easiest, because it is closest to 4567, but sometimes you might use a number that is further away because you can see that it cancels the low order digits. The "shape" of a number matters, and you will eventually come to see that some "shapes" are easier to work with than others. There's a little bit of room for creativity, even in this algorithmic kind of exercise.

Example: Completion of factorization of 160109. From the example above, we know that $160109 = 29 * 5521$, but we haven't factored 5521. If 43 were a factor, then by the trick shown above, $5521 - 3999 = 1522$ should be divisible by 43. To avoid the mental division, we can use the second trick for 43 on 1522 by multiplying 301 by 5: $1522 - 5 * 301 = 17$ which is not divisible by 43, so it is not a factor of 5521.

To check 37, we use $5 * 10 * 111 = 5550$. Then $5550 - 5521 = 29$ which is not a multiple of 37.

To check 53, use 1007 and compute $6 * 1007 - 5521 = 6042 - 5521 = 521$ which clearly is not a multiple of 53 because it is too close to 530.

To check 59, use 1003 and compute $5 * 1003 - 5521 = 5015 - 5521 = 506$. That is not a multiple of 59 because the quotient would be between 8 and 9.

To check 67, use 201 and first compute $5521 - 201 = 5320$. We can see that 67 must divide 532 if it is a factor of 5521. But 67 does not divide 532, so we have proven that 5521 is prime.

Therefore, the complete factorization of 160109 is $29 * 5521$.

For memory experts. There are 1200 primes less than 10000. If you can memorize all of them, then you can avoid the step of prime testing the 4 digit divisors that turn up after dividing out small factors or finding two quadratic forms. This will significantly increase your mental factoring speed.

Some primes are especially memorable, like 4567. You can try to find a large number of them that seem easy to recognize and build on that. If you are interested in becoming a memory expert, we recommend Josh Foer's wonderful book "Moonwalking With Einstein".

4.1 Difference of Squares

If there is an x such that $x^2 - n$ is a square, then you've got the factors! To find x, calculate the closest square larger than $\sqrt{n}$, call this x^2, try $x^2 - n$, is it a small square? Then you've got at least one divisor, because $n = x^2 - y^2 = (x + y)(x - y)$. If the difference is not a square, then advance x^2 to the square of the next higher odd number $(x + 2)^2$ by calculating $x^2 + 4x + 4$. If the difference between that and n is not a square, then advance another step.

The stepping can be speeded up by advancing from one prime to another just by knowing the difference between two primes. We use high school algebra to compute "finite differences" between squares. Suppose we have just computed the square of 41, which is 1681. What is the square of 43? It is $1681 + 4 * 41 + 4 = 1849$ (the California Gold Rush!). The next higher prime after 43 is 47. Because $(x + 4)^2 = x^2 + 8x + 16$, we know that $47^2 = 43^2 + 8 * 43 + 16 = 1849 + 344 + 16 = 2209$.

This method is fairly easy to use for small numbers. For example, 629 has no obvious small factors, but it differs from 729 by 100. Now, 729 is a wonderful number: it is 3 raised to the 6th power. That means that it is the square of 27. We have $27^2 - 10^2 = 629$, proving that $629 = (27 - 10)(27 + 10) = 17 * 37$.

As a more substantial example, factor 10001. We note that squares have a low order digit of 0, 1, 4, 5, 6, or 9. The rounded up square root of 10001 is 101. The first square larger than 10001 is $101^2 = 10201$. The difference between that and 10001 is 200. That difference is not a square, so we move to the next larger square, 102^2. Because $102^2 = 101^2 + 2 * 101 + 1$, we know that the difference between that 10001 is $2 * 101 + 1$ plus the previous difference, 200, i.e. 403. Now 403 is not a square, so we move on. The next odd number greater than 203 is 205, we add that to 403, which is 608 is still not a square. The next larger odd number after 205 is 207, and that plus 608 is 815 (not a square because the square of a multiple of 5 must have 25 as its low order digits). The next odd number after 207 is 209, and that plus 815 is 1024, which is the square of 32. So we have the fact that $11025 = 101 + 4^2$ and $11025 - 10001 = 32^2$. Therefore, $10001 = 105^2 - 32^2$. The factors of 10001 are therefore $105 + 32 = 137$ and $105 - 32 = 73$.

Later (section 8.3) we will show how factor larger numbers with a refinement of this method.

4.2 Checking for primality

Is n prime? If you've removed all the factors up to 31 and the remaining number is 3 digits, then it is prime and you've completed the factorization of n. If the remaining number is 4 digits, it is probably prime. If you have removed all factors up to 73 and the remaining number is less than 6000, then it is prime and the factorization is complete.

A useful thing to know is that there are 143 primes p such that $100 < p < 1000$. The more of these that you can memorize the easier mental factoring will be.

If you check all prime divisors up to cube the root of n, the only remaining possibility is that n is the product of two primes between $\sqrt[3]{n}$ and $\sqrt[3]{n^2}$. For $5000 < n < 10000$, if you have removed prime factors up to 73, the difference of squares method (section 4.1) will complete the factorization in fewer than 5 advances of the finite difference.

5 What you need to master in mental arithmetic

From the proceeding section, it is clear that you need to be able to mentally add and subtract numbers of 5 or 6 digits without too much effort. You also need to be able to divide two digit numbers into 4 or 5 digit numbers in less than a minute. It is also helpful to recognize the squares of primes less than 100.

The advanced material requires some agility in recognizing properties of squares. The patterns are simple, and they will greatly simplify the mental effort in factoring larger numbers.

5.1 The last two digits of a square number

Consider the possible solutions to n^2 (mod 100). For small n we are familiar with the solutions 1, 4, 9, 16, 25, 36, 49, 64, 81. It is clear that the low order digit is restricted to 0, 1, 4, 5, 6, or 9. What about the tens digit? If the units digit is 1, 4, or 9, then the tens digit is even. If the unit's digit 6, then the tens digit is odd. The remaining cases are 00 (i.e., 10^2) and 25; these are squares.

Can a square number end in the digits 39? No, because the low order digit is 9, and that implies that the tens digit is even.

The sum of the digits of a square number must be either a multiple of 9 or one more than a multiple of 3.

5.2 Testing for squares divisible by 25

The methods we use are amenable to mental factoring because they take advantage of how numbers are represented in base 10. In particular, if a number is divisible by 25, that fact is immediately obvious in base 10. It will be very important to recognize the numbers that are squares of numbers that are divisible by 5. The squares of those numbers will have the lower order two digits equal to 25 (i.e., $\equiv 25$ (mod 100)).

If $k^2 \equiv 25$ (mod 100), then the quotient of $k^2/100$ will be the product of two consecutive integers, j and $j+1$. You may have noticed this when looking at $25 * 25 = 625$ and $35 * 35 = 1225$. The pattern is still true for larger numbers, like $30625 = 175^2$ where $306 = 17 * 18$.

Note that the hundreds digit is always 0, 2, or 6. If it is 6, then the thousands digit must be 0 or 5.

In summary, the possible endings for squares ending in 25 are 025, 225, 0625, and 5625.

Another useful rule is that the sum of the digits excluding the 25 is either divisible by 3 or $\equiv 2 \ (mod\ 9)$.

5.3 Recognizing $2n^2$ when n^2 ends in '25'

The advanced factoring methods frequently involve numbers of the for $2n^2$ where n is an odd multiple of 5, and it is helpful to have rules for quickly deciding if a number that arises as an intermediate result could be represented this way.

From the discussion above, we can see that the hundreds digit of the double of the square of number ending in the digits "25" must be even. Moreover, the hundreds digit must be 0, 2, or 4. If the digit is 6 or 8, the number is not a square. Another simple fact is that the thousands and hundreds digits taken as a two digit number must be divisible by 4.

In summary, the possible low digit endings for this type of number are 050, 1250, and 450.

5.4 Recognizing $3n^2$ when n^2 ends in '25'

The possible low digit endings are 075, 675, 1875, and 6875.

5.5 Squaring numbers

The high school algebra formula $(x+y)^2 = x^2 + 2xy + y^2$ is the basis for squaring numbers without writing them down. A two digit number can be written as $10a + b$. Its square is $100a^2 + 20ab + b^2$. Each term is easy to compute.

For example, $73^2 = (70+3)^2 = 100 * 7^2 + 20(7*3) + 9$. That is, $4900 + 420 + 9 = 5329$.

You can also use differences. For example, For example, $59^2 = (60-1)^2 = 100*6^2 - 20(6*1) + 1$. That is, $3600 - 120 + 1 = 3481$.

This may seem daunting at first, but with some practice it becomes second-nature.

5.6 Multiplying two digit numbers

The formula for squaring suggests that there are shortcuts for multiplying other kinds of numbers. For example, $13*17 = (15-2)(15+2) = 15^2 - 4 = 221$. Let's consider something more complicated, like $43 * 67$. This is the same as $(55-12)(55+12) = 55^2 - 144$. By the squaring trick for multiples of 5, we can see that $55^2 = 3025$, so $43 * 67 = 3025 - 144 = 2881$.

You can invent your own tricks for multiplying, it is part of the fun of mental arithmetic.

5.7 Computing $\gcd(a, b)$

The computation of the greatest common divisor of a and b involves finding the remainder of dividing the larger number by the smaller, and then computing the gcd of the smaller number and the remainder. Eventually the computation will reach a point where the remainder is zero. If it is zero, then the smaller number in that last division is $\gcd(a, b)$.

Example: $\gcd(21, 14)$. $14 < 21$ so take the remainder of 21 divided by 14. That is 7, so now find the $\gcd(14, 7)$. Because $7 < 14$, divide 14 by 7 and notice that the remainder is zero. That mean that 7 is the $\gcd(21, 14)$.

Example: $\gcd(21, 34)$. Because $21 < 34$, divide 34 by 21 and take the remainder, 13. Now compute $\gcd(13, 21)$. The smaller number is 13, and the remainder of 21 divided by 13 is 8. Now

compute $\gcd(8, 13)$. We see that 13 divided by 8 has remainder 5. Now compute $\gcd(5, 8)$. We see that the remainder of 8 divided by 5 is 3, so the next computation is $\gcd(3, 5)$. The remainder of 5 divided by 3 is 2, so we next compute $\gcd(2, 3)$. Because 3 divided by 2 has remainder 1, we now compute $\gcd(1, 2)$. Finally we have a zero remainder when we divide 2 by 1, so 1 is $\gcd(21, 34)$, i.e. they are relatively prime.

Besides this straightforward algorithm, there are many ways to compute the gcd by inspection. For example, if you see that both a and b are even, you can divide each by 2 and proceed because $\gcd(2c, 2d) = 2\gcd(c, d)$.

If a is odd and b is even, you can divide a by 2 and continue. This is because if 2 does not b $\gcd(2c, b) = \gcd(c, b)$.

If a is prime, then if b is not divisible by a, $\gcd(a, b) = 1$. Otherwise $\gcd(a, b) = a$.

More generally a is divisible p and b is not, you can divide a by p and proceed, because if p does not divide b, then $\gcd(cp, b) = \gcd(c, b)$.

6 Theoretical foundations: quadratic forms, prime proving and factorization

This section goes into some of theory behind the mental factoring methods, which may seem arcane at first. The methods are based on quadratic forms. The number of representations of an integer as a quadratic form tells us a lot about the integer's divisors.

When one of the terms in a quadratic form is divisible by 25, which is the case for the quadratic forms used in his factoring method, then the task of searching for solutions is much easier than exhaustive search. In this section we present an informal justification for why such forms exist and which numbers they apply to.

If you are eager to get to factoring, you can jump ahead to the "method" section 7.

If you are reasonably facile with the techniques of the previous sections, you are ready to use quadratic forms to analyze numbers. This may seem orthogonal to the problem of factoring because quadratic forms are not the same as factorizations, but as we will see, they are closely related. Quadratic forms greatly extend the range of mental factoring, and numbers in the millions become accessible.

6.1 General facts about quadratic forms

For our purposes, a quadratic form for the number n is an equation

$$kn = x^2 + jy^2$$

where j and k are fixed, small integers. For a given n, j, and k, there may or may not be a solution with integers x and y. Our methods for mental solutions to quadratic forms will find solutions for about 80% of the numbers that are not addressed by previous "tricks." The others will be handled with a miscellany of ad hoc methods.

The simplest quadratic form is simply $n = x^2 + y^2$. Our first theorem shows why it is useful for factoring:

Theorem 1: If n has 2 or more representations as the sum of 2 squares, it is composite.

To understand this, we look at the implication of having two representations, a^2+b^2 and c^2+d^2. Then $\gcd((a+c)^2+(b+d)^2, n) = k$ where $k > 1$. The reason for this is slightly non-obvious and relies on looking at the factorization of each of the two representations over the complex numbers.

Over the complex numbers, $a^2+b^2 = (a+bi)(a-bi)$ and $c^2+d^2 = (c+di)(c-di)$. Now $(a+bi)+(c+di) = a+c+(b+d)i$ can be factored into complex primes, and some those will also divide n, and similarly for $(a-bi)+(c-di) = a+c-(b+d)i$. Thus, the product $(a+c-(b+d)i)(a+c-(b+d)i) = (a+c)^2+(b+d)^2$ has factors in common with n. The gcd, k, of the two representations reveals a factor of n.

Consider the two quadratic forms: $n = x^2+y^2$, $2n = x^2+y^2$. If we have two solutions to either form, or if we have one solution to each, then any pairwise sum or difference of the two solutions, (u, v), has the property that u^2+v^2 shares a factor with n. The same property holds for the two forms $n = x^2+2y^2$ and $3n = x^2+2y^2$; u^2+2v^2 shares a factor with n. Also, for the two forms $n = x^2+3y^2$ and $4n = x^2+3y^2$, we can say that u^2+3v^2 shares a factor with n.

Quadratic forms can help us determine if n is composite or prime. By using restrictions on the low order digits of the decimal representation, we can quickly determine 1 of 3 possible outcomes:

1. n is prime.
2. n is composite and we know at least one divisor
3. n is composite but we will have to use another method to find divisors.

The following theorems are due to Fermat:
For an odd prime p:
Fermat 1. $p = x^2+y^2 \iff p \equiv 1 \ (mod\ 4)$.
Fermat 2. $p = x^2+2y^2 \iff p \equiv 1, 3 \ (mod\ 8)$.
Fermat 3. $p = x^2+3y^2 \iff p \equiv 1 \ (mod\ 3)$, or $p = 3$.

The sums on the righthand side of the equations are quadratic forms. These representations of p lead to some useful ways of analyzing numbers. We will be looking for ways to represent numbers that are not necessarily prime as the sum of two squares or the sum of a square and a small multiple of a square. We need to know what we can infer from the number of representations.

The Fermat theorems are even stronger than they appear, because the representation of a prime in each of those quadratic forms is unique.

Fermat 1S: If p is a prime and $p \equiv 1 \ (mod\ 4)$, then p has unique representation as the sum of two squares.

Similar complex factorizations apply to the other Fermat representations so that it is possible to derive information about the integer factorizations from the number of representations in those quadratic forms. You might wonder about the general case where $p = x^2+ny^2$. That leads to some interesting and deep results in number theory, but we will not use them for mental factoring.

6.2 Some useful facts about squares

- A square is congruent to 0 or 1 modulo 4.
- A square is congruent to 0, 1 or 4 modulo 8. This is also true modulo 5.
- If $n \equiv 3 \ (mod\ 8)$ and $n = x^2+2y^2$, then x and y are odd.
- If $n \equiv 3 \ (mod\ 8)$ and $3n = x^2+2y^2$, then x is odd and y is even.

6.3 Quadratic forms and the number 5

There are several theorems that show why our factoring methods are correct, and we will state them here, without proof, so that we can refer to them later. They are divided into two groups: those that are true for numbers of the form $4k+1$ and those that are true for numbers of the form $4k+3$.

The theorems about divisibility by 5 of quadratic form terms are restricted to numbers that are

- not divisible by 2, 3, or 5
- not perfect squares

. We will call numbers of this sort "nTFSQ" (no trivial factors and not square). All the facts in the remainder of this section apply to nTFSQ numbers.

6.3.1 About the number 25

The number 25 is very important in our factoring method. The following theorems are what the algorithms in later sections depend on.

Thm. If $n \equiv 1 \mod 10$ or $n \equiv 9 \mod 10$ and n is the sum of two squares, then at least one of the squares is divisible by 25.

Thm. If $n \equiv 3 \mod 10$ or $n \equiv 7 \mod 10$ and $2n$ is the sum of two squares, then at least one of the squares is divisible by 25.

To see why this is true, one only needs to analyze the possibilities for the residues of $2n \mod 10$. The two possibilities are 6 and 4, which means that $2n$ is either $1 \mod 5$ or $4 \mod 5$, which, by the previous lemma, means that one of squares is divisible by 5.

We state the following lemmas without proof:
Lemma. If $x^2 + y^2 \equiv 1 \mod 5$ or $x^2 + y^2 \equiv 4 \mod 5$, then one of x or y is divisible by 5. Proof: Note that a square $\mod 5$ is congruent to either 0, 1, or 4. The only way that two squares can sum to 1 is if one is congruent to $0 \mod 5$ and the other is $1 \mod 5$. The only way that two squares can sum to $4 \mod 5$ is if one of them is congruent to $0 \mod 5$ and the other is congruent to $4 \mod 5$.
Lemma. If $n = x^2 + 2y^2$, and neither x nor y is a multiple of 5, then $3n$ also has a representation of the same form, $3n = w^2 + 2z^2$, such that either w or z is a multiple of 5.
Lemma. For each solution to $n = x^2 + 2y^2$, there are two related solutions to $3n = x^2 + 2y^2$. Of the three solutions, one will have an x or y term that is divisible by 5. We omit the proof.
Lemma. If $n = x^2 + 3y^2$, and neither x nor y is a multiple of 5, then $4n$ also has a representation of the same form, $(w^2 + 3z^2)$, such that either w or z is a multiple of 5.
Lemma. For each solution to $n = x^2 + 3y^2$, there are three related solutions to $4n = x^2 + 3y^2$. Of the four solutions, one will have an x or y term that is divisible by 5.
Corollary: If $n \equiv 1 \mod 4$ and its low order digit is 3 or 7, and if n is the sum of two squares $x^2 + y^2$, then $2n$ has a representation of a sums of squares, and one of the squares is $25 \mod 100$.

6.3.2 Theorems about $4k+1$ numbers

Thm 2. If $n \equiv 1 \mod 4$ and is the sum of 2 squares in only one way, and the squares are relatively prime, then n is prime.

This is the contrapositive of Fermat 1. Note that we have added the condition that the squares in the decomposition are relatively prime. This is necessary because a number such as 45 is equal to $3^2 + 6^2$, but it is not prime.

By Thm 1, we know that if a $4k+1$ number does not have a unique representation as the sum of two relatively prime squares, then it is a composite number. It will have either no representations or two or more.

Corr 1: If a number n is of the form $4k+1$ and is not representable as the sum of 2 squares, then n is composite and has at least 2 divisors (not necessarily unique) that are $\equiv 3 \mod 4$.

Corr 2: If n is of the form $4k+1$ and is the sum of two squares and the roots are relatively prime, then it has no $4k+3$ divisors.

Thm 3: If n is of the form $4k+1$ and is the sum of two squares x^2+y^2 where $\gcd(x,y)=1$, then any divisor d of n has a representation as the sum of two squares, $d=u^2+v^2$ where $\gcd(u,v)=1$.

6.3.3 Theorems about $4k+3$ numbers

When n is congruent to 3 modulo 8. Thm 4: If n is of the form $8k+3$ and it has a unique representation as x^2+2y^2, and x and y are relatively prime, then n is prime.

Thm 5: if n is an $8k+3$ prime, then it has unique representation as x^2+2y^2 with x and y relatively prime.

Thm 6: If n is of the form $8k+3$ and is not representable in the form x^2+2y^2, then n is composite and has at least 2 divisors (not necessarily unique) where each divisor is $\equiv 5 \mod 8$ or $\equiv 7 \mod 8$.

Thm 7: If n is of the form $8j+3$ and has a x^2+2y^2 representation, and x and y are relatively prime, then n has no $8j+5$ or $8j+7$ divisors.

There are two related quadratic forms that will be the basis for our mental factoring method:

$$n = x^2 + 2y^2$$

$$3n = x^2 + 2y^2$$

Thm 8: If n is of the form $8j+1$ or $8j+3$ and is the sum of two squares x^2+2y^2 where $\gcd(x,2y)=1$, then any divisor d of n has a representation as $d=u^2+2v^2$ where $\gcd(u,2v)=1$.

The methods that we will present in later sections rely on the facts in this section.

As shown in section 6.2, for these forms, in any solution x must be odd. In the first form, y is also odd, but in the second form, y is even.

For these forms, if there is any solution to either form, there is at least one solution in which one of x or y is a multiple of 5.

For the form $n=x^2+2y^2$, there are two cases to consider. If the low order digit of n is 1 or 9, then x is not divisible by 5. If the low order digit of n is 3 or 7, then y is not divisible by 5.

For the form $3n=x^2+2y^2$, there are also two cases to consider. If the low order digit of $3n$ is 1 or 9, then x is not divisible by 5. If the low order digit of $3n$ is 3 or 7, then y is not divisible by 5.

6.3.4 Theorems About $6j+1$ Numbers

The quadratic form x^2+3y^2 also has properties that are useful for factoring, and we will use it for numbers that are congruent to 7 modulo 8.

Thm 9: If n is of the form $6j+1$ and it has a unique representation as x^2+3y^2, and x and y are relatively prime, then n is prime.

Thm 10: if n is an $6j+1$ prime, then it has unique representation as x^2+3y^2.

Thm 11: If n is of the form $6j+1$ and is not representable in the form x^2+3y^2, then n is composite and has at least 2 divisors (not necessarily unique) $\equiv 5 \mod 6$.

Thm 12: If n is of the form $6j+1$ and has a x^2+3y^2 representation, and x and y are relatively prime, then n has no $6j+5$ divisors.

Much of this information is summarized in Table 1 so that it can be quickly referenced when analyzing a number.

7 Quadratic forms and factoring: The Practical Method

NB: Throughout this section we assume that the target number is n and that it is an TFSQ number, i.e., all trivial factors (2, 3, and 5) have been removed and it is not a perfect square.

7.1 Solving a quadratic form modulo 100

We need a mental method for solving quadratic form such as $2n = x^2 + y^2$. The key to doing this is to look at the equation modulo 100, i.e. the two low order digits of each term. This will greatly cut down on the search for possible solutions. The search is further aided by assuming that x or y is divisible by 5 (this assumption is true for the conditions listed in table 1; where two equations apply, the assumption will be true for one of them).

The next sections will show how to choose an appropriate quadratic form based on simple properties of n. In general, the equation is $kn = x^2 + by^2$ where a and b are small numbers and one of x or y is divisible by 5. We will find out how many solutions there are, and that information will either result in a factorization or guide further analysis of n.

The remainder of this section describes how to look for solutions in the case where n is congruent to 1 mod 4 and the low order digit of n is 3 or 7. This will illustrate the search method, and in subsequent sections we will show how to modify it for other modular values of n.

Assume that $2n = x^2 + y^2$. We will search for solutions by working with the related equation

$$l \equiv r^2 + 25 \mod 100$$

where $l \equiv 2n \mod 100$. We rewrite this as

$$r^2 \equiv (l - 25) \mod 100 \tag{1}$$

.

By a previous lemma in section 6.3.1, y has low order digit 5, implying $y^2 \equiv 25 \mod 100$. Then the two low order digits of x^2 are $2n - 25 \mod 100$. That means that modulo 100, there are 4 possible square roots for x. This is the basis of the method of mental factoring using quadratic forms.

7.2 Overview of The Method

The main goal of The Method is to either find two representations of n using one quadratic form or to prove that it has only one such representation. The Method is an efficient way to search for these solutions using mental arithmetic.

Quadratic forms modulo 100 provide a way to determine if a number is prime or composite using mental methods. Because one of the terms of the form must be divisible by 25, the number

residue	low digit	quadratic form	5 divides	x parity	y parity	$r^2 \mod 100$
1 mod 4	1 or 9	$n = x^2 + y^2$	either	either	1-p(x)	$n, n-25$
1 mod 4	3 or 7	$2n = x^2 + y^2$	either	odd	odd	$n-25$
3 mod 8	1 or 9	$n = x^2 + 2y^2$	y	odd	odd	$n-50$
		$3n = x^2 + 2y^2$	x	odd	even	$(3n-25)/2$
3 mod 8	3 or 7	$n = x^2 + 2y^2$	x	odd	odd	$(n-25)/2$
		$3n = x^2 + 2y^2$	y	odd	even	$3n$
7 mod 24	1 or 9	$n = x^2 + 3y^2$	y	even	odd	$n-75$
		$4n = x^2 + 3y^2$	y	odd	odd	$4n-75$
7 mod 24	3 or 7	$n = x^2 + 3y^2$	x	even	odd	$n/3$
		$4n = x^2 + 3y^2$	x	odd	odd	$(4n-25)/3$

Table 1: Properties of quadratic form terms

of possibilities for the second term is greatly limited. Moreover, the tricks for recognizing squares of numbers divisible by 25 allow one to quickly eliminate candidates for the second term.

A number's residues modulo 4 (or 8 or 24) and modulo 10 determine three parameters that are important in mental factoring. For each combination, the method uses either one two specific quadratic forms; each each combination may use a small multiplier for the target number. For each combination, one term in the quadratic form or forms is divisible by 25. The parity[1] of each term is also known. Table 1 summarizes the information.

Note that some numbers, such as 47 which is 23 modulo 24, are not in the table. These have to be tackled by the other methods of section 8.

The Method is well-suited to numbers of 6 or fewer digits, but has less chance of success for 6 digit numbers. Later we will discuss how to refine the technique (section 7.7) to get an advantage on larger numbers.

If you become adept with The Method, you might be tempted to implement it in software. That would be silly. The methods in this paper are adapted specifically to human abilities. Computers use entirely different algorithms and can factor much larger numbers in an instant.

7.2.1 The Method illustrated for $n \equiv 1 \mod 4$ with low order digit 3 or 7

Step 1. Multiply n by 2 to make the last digit 4 or 6. This doesn't cause any change in the factorization of n except for an additional factor of 2. It does guarantee that if a decomposition exists, one of the squares is a multiple of 25. Set l equal to $2n \mod 100$.
Step 2. To solve equation 1 (section 7.1), we search the odd r values in the range from 1 to 23 to find solutions to $r^2 \equiv l - 25 \mod 100$. There will be one such r (if $l - 25$ is negative, add 100 to it).
Step 3. Calculate three more numbers in the range 25 to 99 which have squares that are also congruent to $l - 25 \mod 100$. These are: $50 - r$, $50 + r$, and $100 - r$.

[1] If a number is odd, its parity is 1, otherwise the parity is 0

Each member s of the set $S_4 = \{r, 50 - r, 50 + r, 100 - r\}$ is a candidate value for x, and thus is a potential solution to our quadratic form (without the modulo 100 restriction). We can check each potential value by asking if $2n - s^2$ is a square, i.e. y^2. Because we know that y^2 is divisible by 25, it will be easily recognizable as a square (see section 6.3.1). Of the four possible s values, we will determine how many of them solve the quadratic form.
Step 4: If $2n$ is larger than 10000, the four values used in set S_4 Step 3 as candidate values for x are not the only possibilities. All other candidates are based on them, however. To complete the search for solutions to the quadratic form, we calculate all x candidates of the form $s+100$, $s+200$, ...such that $s \in S_4$ and $s + 100i < \sqrt{2n}$. We will use S to denote the set of all possible candidates for x; we will frequently denote this set by $\{50j \pm r\}$, meaning "all multiples of 50 plus or minus r".

After we have determined the number of representations, we will have one of three cases. Each one must be analyzed further to complete the factorization.
Step 5, analyzing the decompositions:

- Case of only one square sum. If n has only one representation, then it might be prime. We need to determine if the two square roots (x and y) are relatively prime. Check that x and y are relatively prime by computing their GCD. If the GCD is not equal to one, it is a divisor of n. If the GCD is 1, then n is prime.
- Case of two or more square sums. We know that n must be composite.
  Let the two sums be $(a^2 + b^2)$ and $(c^2 + d^2)$. Consider the number pairs $(a, b) \pm (c, \pm d)$ and $(a, b) \pm (d, \pm c)$; these have 8 possible values. Any one of them will result in a pair (j, k) that leads to a factor. For mental factoring, the value with the largest common factor between the members of the pair is our goal. Divide out that GCD from the pair members, then square the resulting two numbers and add them to produce t. Usually t will be a prime or a prime times small number. That prime is a divisor of n. With any luck, t will be small enough that you can recognize it as a prime or a prime multiple. If not, you will need to compute the GCD of t and n (call it g) and divide that into n. We call n/g the co-factor of g.

  To finish the factorization, we need to factor g and n/g. If they are small numbers, this will be easy, but if not, simply recurse by using The Method. By Theorem 3 in section 6.3.2, we know that g and n/g are $4k + 1$ numbers and they definitely will have decompositions as the sum of two squares.
- Case of no square sum. If our search comes up empty, then n is not prime and it has at least 2 prime factors of the form $4k+3$. If $n \equiv 1 \mod 8$, then we can switch to using the quadratic form $x^2 + 2y^2$. This is described in one of the subcases in the section for $4k + 3$. If that fails, then we use one of the methods in section 8.

7.3 Method for $n \equiv 1 \mod 4$

We will examine splitting a $4k + 1$ number n into a sum of 2 squares.

To find out how many representations there are, we branch on subcases based on the low order digit of n. That digit is either 1, 3, 7, or 9.

7.3.1 Method for n with Low Order Digit 3 or 7

We apply The Method (section 7.2) to the equation $2n = x^2 + y^2$.

A Toy Example: Find the representations of 173.
Start by doubling it to 346.
$346 - 25 = 321 \equiv 21 \mod 100$
Find r such that $r^2 \equiv 21 \mod 100$
From our knowledge of the list of small squares, recognize that $r^2 = 121$ is a candidate.
The square root of 121 is 11, thus $r = 11$.
This is the only possibility for r because anything else (e.g., $50 + 11$, $50 - 11$) would have a square much larger than 173.
$2n - r^2 = 346 - 121 = 225$
Recognize 225 as 15^2.
$2n - 11^2 = 15^2$
$2n = 11^2 + 15^2$.
There are no other representations of $2n$ because there are no other possibilities for r.
11 and 15 are relatively prime.
Ergo, 173 is prime.

Example: Find the representations of 15017. Referring to Table 1, we see that the quadratic form is $2n = x^2 + y^2$, so we begin by doubling n to 30034.
$30034 - 25 = 30009 \equiv 09 \mod 100$.
Recognize 9 as a square, implying $r = 3$ and $S_4 = \{3, 47, 53, 97\}$.
The first s value in S_4 is 3, $2n - s^2 = 30034 - 9 = 30025$
Is that a square? No, $4 * 30025 = 120100/100 = 1201$
1201 is not a square, so we move on to the next s in S_4.
$2n - 47^2 = 30034 - 2209 = 27825$ Is that a square? No, because the hundreds digit is not 0, 2, or 6.
27825 is not a square, so we move on to the next s in S_4.
$2n - 53^2 = 30034 - 2809 = 27225$
Is that a square? Yes, because $(27225 - 25)/100 = 272 = 16 * 17$
Thus, $30034 = 53^2 + 165^2$.

At this point we know that we will be able to determine whether n is prime or composite. We continue looking for s candidates. Because $\sqrt{2n} \approx 173$, we will some some s values > 100.

The next s in S_4 is 97; $2 * 50 - s = 100 - 3 = 97 = r$
$2n - r^2 = 30034 - 97^2 = 30034 - 9409 = 20625$
Is that a square? No, because 206 is not the product of two consecutive numbers.
We now add 100 to the members of S_4 to get new s values.
$2n - s^2 = 30034 - 103^2 = 30034 - 10609 = 19425$
Is that a square? No, because the hundreds digit is not 0, 2, or 6.
$3 * 50 - s = 147 = r$
$2n - s^2 = 30034 - 147^2 = 30034 - 21609 = 8425$
Is that a square? No, because the hundreds digit is not 0, 2, or 6.
$3 * 50 + s = 153 = r$
$2n - r^2 = 30034 - 153^2 = 30034 - 23409 = 6625$
Is that a square? No, because 66 is not the product of two consecutive numbers.

The next possible candidate is $4 * 50 - 3 = 197$, and 197^2 is larger than the number we are trying to represent, so we are done. We found only one representation, so we know that 15017 is prime.

Example 1457:
Referring to Table 1, we see that the recommended quadratic form is $2n = x^2 + y^2$, so we begin by doubling n to 2914. The low order digits are 14, x is odd, and we are free to choose x as the term that is divisible by 5.

We see that $14 - 25 \equiv 89 \equiv y^2 \mod 100$. The smallest r^2 that is equivalent to 89 mod 100 is 17. The set of candidates s for y is $\{50j \pm 17\}$ with the restriction that $s < \sqrt{2n} < 53$.

The first candidate is 17, leading to $2n - 17^2 = 2914 - 289 = 2625$. This cannot be a square because 26 is not the product of two consecutive numbers (see section 6.3.1).

The next candidate is 33, leading to $2n - 33^2 = 2914 - 1089 = 1825$. Because the hundreds digit is 8, this cannot be a square (see section 6.3.1).

Further candidates are larger than $\sqrt{2 * 1457}$, so we conclude that 1457 has no representation as $2n = x^2 + y^2$ that is discoverable by using The Method. It is composite, but we will have to use an alternative method in section 8 to find its factors.

Example 2357:
Twice 2357 is 4714. As in the previous example, we see that $14 - 25 \equiv 89 \equiv y^2 \mod 100$. The smallest r^2 that is equivalent to 89 mod 100 is 17. The set of candidates s for y is $\{50j \pm 17\}$ with the restriction that $s < \sqrt{2n} < 69$.

The first candidate is 17, leading to $2n - 17^2 = 4714 - 289 = 4425$. This is not a square because the hundreds digit is 4.

The next candidate is 33, leading to $2n - 33^2 = 4714 - 1089 = 3625$. This is not a square because 36 is not the product of two consecutive integers.

The next candidate is 67, leading to $2n - 67^2 = 4717 - 4489 = 225$. This is the square of 15. Because $\gcd(15, 67) = 1$, this is a solution.

Further candidates are too large. We have found exactly one solution, and thus, 2357 is prime.

Example 3577:
We begin by doubling 3577 to 7154. The low order digits are 54, and we see that $54 - 25 \equiv 29 \equiv y^2 \mod 100$. The smallest number whose square matches 29 is 23 ($23^2 = 529$). The candidate set is $\{50j \pm 23\}$ where each candidate is less than the square root of 7154, which is approximately 85.

The first candidate is 23, leading to $7154 - 529 = 6625$. This is not a square because 66 is not the product of two consecutive integers.

The next candidate is 27, leading to $7154 - 729 = 6425$. This is not a square because the hundreds digit is 4.

The next candidate is 73, leading to $7154 - 5329 = 1825$. This is not a square because the hundreds digit is 8.

The next candidate is 77, leading to $7154 - 5929 = 1225$, the square of 35. The gcd of 77 and 35 is 7, so we can conclude that 7^2 divides n. The quotient of 3577 by 49 is 73 which is prime. We have have shown that the factorization of n is $7^2 * 73$.

Example 6893:
Twice 6893 is 13786. The low order digits are 86. The modular equation is $86 - 25 \equiv 61 \mod 100$. The smallest number with a square matching on its low order digits is 19 ($19^2 = 361$). The candidate set is $\{50j \pm 19\}$ where each candidate is less than the square root of 13786 which is approximately 120.

The first candidate is 19, leading to $13786 - 361 = 13425$. This is not a square because the hundreds digit is 4.

The next candidate is 31, leading to $13786 - 961 = 12825$. This is not a square the hundreds digit is 8.

The next candidate is 69, leading to $13786 - 4761 = 9025$. Because 90 is the product of two consecutive integers $(9, 10)$, this is a square, and its square root is 95. The gcd of 69 and 95 is one, so this is a solution to the quadratic form.

The next candidate is 81, leading to $13786 - 6561 = 7225$. This is the square of 85. The gcd of 81 and 85 is one, and thus, we have a second solution. To combine the two solutions into the factors of 6893, we take the pairwise subtraction of the x and y values. We are free to order them in any way, so we choose a combination that results in small numbers: $(95, 69) - (85, 81) = (10, 12)$ (we have dropped the minus sign on 12). The gcd of 10 and 12 is 2, so we can reduce the pair to $(5, 6)$. The sum of the squares is $25 + 36 = 61$. This is one of the prime factors of 6893. The quotient of 6893/61 is fairly easy to compute mentally, and we can see that $6893 = 61 * 113$.

7.3.2 Method for n with Low Order Digit 1 or 9

We will use the quadratic form $n = x^2 + y^2$. The following lemma is important for generating possible x values:

Lemma: If $n \equiv 1 \mod 4$ is the sum of two squares, x^2 and y^2, and n has low order digit 1 or 9, then one of the squares is either $25 \mod 100$ or is a multiple of 100.

By this lemma, we know there are two cases to analyze. To find a sum of squares decomposition of n we will use The Method (section 7.2) in the same manner as the previous sections for the case that of one of x^2 or y^2 is $25 \mod 100$. For the other case, x^2 or y^2 is a multiple of 100, we will use The Method with a modification for generating candidate values for x.

Assuming that one square has residue 25 modulo 100, use The Method with $n = x^2 + y^2$. This will produce 0 to 2 decompositionss. If there are fewer than 2 decompositions, consider the second case, in which one square is $\equiv 0 \mod 100$. In The Method, instead of looking for $r^2 \equiv (n - 25) \mod 25$, we will look for r such that $r^2 \equiv n \mod 25$. Form the set S_4 based on that r.

If there were two decompositions, the number is composite and the factors can be calculated from the representations.

If there are no decompositions, then n is composite. If there is only one decomposition, and if two squares are relatively prime, then n is prime. If there are two decompositionss, use the procedure described in section 7.3.1 for n with low order digit 3 or 7.

Example: factor 4469. We branch on whether one of the squares is $0 \mod 100$ or $25 \mod 100$. Assume $0 \mod 100$. The lowest two digits, 69, form the s value. The r value is a number whose square ends in those digits, and 13 satisfies that condition. We look for decompositions based on $50j + 13$ and $50j - 13$, and we can stop when we reach the a number with a square greater than 4469 (such a number will be less than 70) The candidates are 13, 37, and 63. We check to see if 4469 minus the square of one of these values is itself a square.

$4469 - 13^2 = 4300$ which is not a square.

$4469 - 37^2 = 4469 - 1369 = 3100$ which is not a square.

$4469 - 63^2 = 4469 - 3969 = 500$ which is not a square. Therefore, this case is impossible.

Now, assume one of the squares is $25 \mod 100$. We know that $25 + s = 69$, and therefore s has low order digits 44. We need an r such that r^2 ends in 44. One such value is 12. We now look at candidates of the form $50j + 12$ and $50j - 12$. The possibilities are 12, 38, and 62.

$4469 - 12^2 = 4325$ which is not a square because the hundreds digit is odd.

$4469 - 38^2 = 4469 - 1444 = 3025$ which is 55^2. Therefore we have a representation of 4469 as the sum of 55^2 and 38^2.

$4469 - 62^2 = 4469 - 3844 = 625$ which is the square of 25.

We have found two representations of 4469 as the sum of two squares, therefore it is composite. The two representations can be combined to find the factors. List the two pairs of squares with the multiple of 5 as the first member of the pair: $((55, 38), (25, 62))$. Add the pairs to get $(80, 100)$. The greatest common factor of those numbers is 20, and we divide it out to get $(4, 5)$. The sum of their squares is 41, which is prime, and it is therefore a divisor of 4469. The other factor is 109. QED.

Example: factor 10001. We will try to represent the number as the sum of two squares, $10001 = x^2 + y^2$.

We start by applying The Method (section 7.2) to the case of $y^2 \equiv 0 \mod 100$. If y^2 is divisible by 100, then r^2 must be congruent to $1 \mod 100$. We can assume that $r = 1$. The set S_4 is $\{1, 49, 51, 99\}$. (We know that these are the only ones because the next number of this form is 101, but its square is larger than our target number). The candidates for x^2 are: 1, 2401, 2601, and 9801. These imply that $y^2 = 10000$, 7600, 7400, or 200, respectively. Not all of these are squares, as we can easily see, because $x^2/100$ would be a square iff x^2 were square. The only member y candidate that is a square is 10000, and we can see that that the only possible representation from this set is $100001 = 100^2 + 1^2$.

Because there is only one decomposition from the previous step, we proceed to analyzing the case in which y^2 has low order digits 25. We use The Method with $r = l - 25 \mod 100$, i.e. 76. The unique r in the range $1 \ldots 24$ with a square ending in 76 is the number 24 ($24^2 = 576$). The set S_4 has the values 24, 26, 74, 76. The candidate x^2 values are their squares: 576, 676, 5476, and 5776. The corresponding y^2 values are 9425, 9325, 4525, and 4225, respectively. We need to know which of those values are squares.

Because the numbers end in "25", we refer to section 6.3.1 which showed how to do this. We look at the quotient of each number divided by 100, i.e., discard the two low order digits. This yields 94, 93, 45, and 42. For a square, the low order digit must be 0, 2, or 6. This means that 42 is the only possibility, and it is the product of consecutive numbers (6 and 7), thus confirming that 4225 is the square of 65.

We now have two decompositions:
$100001 = 100^2 + 1^2$ and $10001 = 65^2 + 76^2$. Any choice of $\pm$ in the following expressions will lead to a factor :
$(100, \pm 1) \pm (76 \pm 65)$ or $(100, \pm 1) \pm (65, 76)$. To make this easy for mental calculation, choose an expression that has a multiple of five in the first component of the sum. Lets try $(100, 1) - (65, 76) = (35, -75)$. Divide out the GCD of the two numbers to get $(7, -15)$. The squares of the two components have the sum $7^2 + (-15)^2 = 49 + 225 = 274$. Dividing out the small factor of 2 leaves 137. This means that 137 divides 10001. In fact, the complete factorization is $73 * 137$, which is a very good thing for the agile factorer to remember.

Example: 7789.
We will try to represent the number as the sum of two squares, $7789 = x^2 + y^2$.

We start by applying The Method (section 7.2) to the case of $y^2 \equiv 0 \mod 100$. Then $x^2 \mod 100 = 7789 \mod 100 = 89$. In the range 1..24, the number 17 has a square that ends in 89. The set $S_4 = \{17, 33, 67, 83\}$. The x^2 candidates are squares: $\{289, 1089, 4489, 6889\}$. The corresponding y^2 candidates are {7500, 6700, 3300, 900}. Of these, only $900 = 30^2$ is a square. Its

corresponding x^2 value is $6889 = 83^2$. We note that 30 and 83 are relatively prime. We therefore know that $7789 = 83^2 + 30^2$.

We have one decomposition of our target number, and to complete the analysis we need to look for decompositions when $y^2 \equiv 25 \mod 100$. We know that $r^2 \equiv (n - y^2) \equiv (89 - 25) \mod 100$, so we want to find squares ending in 64. The r value is 8 and the set S_4 is $\{8, 42, 58, 92\}$. The set of squares is $\{64, 1764, 3364\}$ (we can eliminate 92 because its square is larger than our target number). The corresponding x^2 values are $\{7725, 6025, 4425\}$. By the rules in section 6.3.1, none of these are squares.

There is only one decomposition of 7789 into the sum of two relatively prime squares. Therefore 7789 is prime.

In section 7.7 we will show how to make the set S_4 even smaller in the special case of $y^2 \equiv 25 \mod 100$. This will be useful in factoring larger numbers.

Example: 3149.

We will try to represent the number as the sum of two squares, $3149 = x^2 + y^2$.

We start by applying The Method (section 7.2) to the case of $y^2 \equiv 0 \mod 100$. Then $x^2 \mod 100 = 3149 \mod 100 = 49$. The r value is 7, and the set S_4 is $\{7, 43, 57\}$. Their squares are $\{49, 1849, 3249\}$. We can reject 3249 because it is larger than our target number. The corresponding x^2 candidates are $\{3100, 1300\}$. Neither of these is a square, and therefore there no representations in this case.

To complete the analysis we need to look for decompositions where $y^2 \equiv 25 \mod 100$. We know that $n - y^2 \equiv (49 - 25) \mod 100$. This means that we need a candidate r^2 value that ends in 24. That is 18, and the set S_4 is $\{18, 32\}$ (the other possibilities are too large). The squares are $\{324, 1024\}$. The corresponding y^2 values are $\{2825, 2125\}$. Neither one is a square.

There are no decompositions. We can conclude that 3149 is composite and has at least two factors that are $\equiv 3 \mod 4$. We are in luck in applying the difference of squares method if we recall that we considered 57^2 as a candidate for x. That square as 3249, and we can easily see that $3149 = 57^2 - 10^2$. The factors are $(57 + 10)$ and $(57 - 10)$, and we have shown that $3149 = 47 * 67$.

7.4 Using finite differences with The Method

Finite Differences are an alternate way to calculate the sequence of squares $n - x^2$. We note that the difference between consecutive integer squares $(k + 1)^2$ and k^2 is simply $2k + 1$. Similarly, the difference between the squares of integers in an arithmetic sequence is a simple linear expression. The Second Difference, i.e. the difference between consecutive values of the linear expression, is a constant number. We can use this with The Method to cut down on the number of mental squarings.

We begin by re-ordering the candidate values for x into an arithmetic sequence. In step 3 of The Method (section 7.2) we calculate the set $S_4 = \{r, 50 - r, 50 + r, 100 - r\}$ and generate candidate values for x of the form $100j + s$ where s is a member of S_4. We need to calculate the squares of these candidate values, but we can avoid doing any complicated multiplications if we re-order the $100j + s$ so that consecutive values differ by 50.

Calculate the largest value in the set S that is less than $\sqrt{n}$ as before, and call that value x_{max}. Our arithmetic sequence is $x_{max} - 50j$, where j goes from 0 to approximately $\sqrt{n}/25$.

We'll start our quadratic progression with $n - x_{max}^2$. Then we move to $x = x_{max} - 50$, $x = x_{max} - 100$, etc. But we do not need to square these x's. The difference between x_{max}^2 and $(x_{max} - 50)^2$ is $\Delta = (x_{max} - 25) * 100$. We add this to the value of $n - x_{max}^2$ to get our next

candidate for y^2. We continue generating trial values with a sequence of additions. Because the Second Difference of the sequence of x^2 values is 5000, we can easily generate the first difference and use that to find the next square.

The algorithm begins by calculating x_{max} as the starting value for x, $\Delta = (x_{max} - 25) * 100$, and $c = n^2 - x^2$.

- Check to see if c is a square. If it is, then the values to use with The Method are $x = \Delta/100 - 25$ and $c = n - x^2$.
- Compute $\Delta \leftarrow \Delta - 5000$. Negative values are acceptable.
- Compute $c \leftarrow c + \Delta$. If c is negative, stop. Otherwise return to step 1.

The algorithm terminates early if it finds two square values for c.

Example: $n = 35209$.

The last two digits of the xs will be $\{03, 47, 53, 97\}$. The approximate square root of n is slightly less than 190, so $x_{max} = 153$.

x_{max}^2 is 23409, and $n - x_{max}^2 = c = 11800$. This is not a square because 118 isn't.

The first value for Δ is $128 * 100 = 12800$.

Add this to the running $n - x^2$ value, obtaining 24600. This is not a square.

Update Δ by subtracting 5000. The new Δ is 7800.

Add this to the running $n - x^2$ value (this is c in the algorithm), obtaining 32400. This is a square because 324 is a square.

Remember the square root, 180. We could calculate $y = \Delta/100 - 25 = 53$, but it's one more thing to put in our very limited memory. We can calculate it later from $y^2 = n - x^2$.

The next Δ is 2800. Add it to the running $n - x^2$ value, obtaining 35200, which is not a square.

The next Δ is -2200.

Add this to running $n - x^2$, obtaining 33000, which is not a square.

The next Δ is -7200, and the running $n - x^2 = 25800$ which is not a square.

The next $\Delta = -12200$, $n - x^2 = 13600$ which is not a square.

The next $\Delta = -17200$. Adding this to $n - x^2$ makes it negative, so we are done with this sequence of xs. We might check our arithmetic by subtracting the final $n - x^2$ value, 13600, from $n = 35209$, giving 21609, which should be a square. It is!

Thus far we have one solution of $n = x^2 + y^2$.

We move on to the case of y^2 ends in 25. Then x^2 will end in 84, and the potential x endings are $\{22, 28, 72, 78\}$. The square root of n is about 190, so $x_{max} = 178$.

$x_{max}^2 = 31684$, and $n - x_{max}^2 = 3525$ which is not a square because the hundreds digit is odd.

$\Delta = 15300$. The next $n - x^2$ value is 18825 which is not a square because the hundreds digit is 8, and it should be 0,2,or 6.

The next $\Delta = 10300$, $n - x^2 = 29125$ which is not a square.

The next $\Delta = 5300$, $n - x^2 = 34425$ which is not a square.

The next $\Delta = 300$, $n - x^2 = 34725$ which is not a square.

The next $\Delta = -4700$, $n - x^2 = 30025$ which is not a square. (300 is not an $n(n+1)$ number: the bracketing squares are 17^2 and 18^2, and $17 * 18$ doesn't end in 0.)

The next $\Delta = -9700$, $n - x^2 = 20325$ which is not a square.

The next $\Delta = -14700$, $n - x^2 = 5625$ which is the square of 75.

We could stop here because we have found two squares, or we could notice that the next Δ will make $n - x^2$ negative, and stop for that reason. We can calculate the matching $y = \Delta/100 - 25 = -147 - 25 = -172$.

We can ignore the minus sign; our second two-square solution is (75,172). Recall that one member of the first solution was $x = 180$. The corresponding y value is $\sqrt{n - x^2} = 35209 - 32400 = 2809 = 53^2$, so the first solution is $(180, 53)$. Swapping the second solution, subtracting from the first, and dropping signs gives $(8, 22)$. Divide out the small factor of 2, giving $(4, 11)$. Square and add the components, $16 + 121 = 137$.
Divide n by 137 to find the other factor is 257. Both 137 and 257 are prime, so the factorization is complete.

The x values in the first sequence are 153, 103, 53, 3, -47, -97, -147. If we fold the positive values in between the negatives, and drop the signs (because we are mainly interested in x^2), we have 3, 47, 53, 97, 103, 147, 153, which is same sequence we use in the regular method. In the second sequence, the trial x values are 178, 128, 78, 28, -22, -72, -122, -172. Folding over and dropping the signs gives us 22, 28, 72, 78, 122, 128, 172, 178, which is the same sequence as in the regular method. The virtue of Finite Differences is that most of our arithmetic is now additions and subtractions.

Finite Differences can also be used with $x^2 + 2y^2$ and $x^2 + 3y^2$ with minor adjustments. When examining the set of possible x values, the $n - x^2$ value must be checked for being $2y^2$ (twice a square) or $3y^2$ (three times a square). When examining the set of possible y values, the $n - x^2$ formula is replaced with $n - 2y^2$ or $n - 3y^2$; the checking step reverts to the regular test of "is this a square?". In this case, the starting value for Δ is $200 * (y - 25)$ or $300 * (y - 25)$. Also in this case, the change in Δ (i.e., the second difference) is doubled or tripled to 10000 or 15000. When a square is discovered, the square root can be calculated as $\Delta/200 - 25$ or $\Delta/300 - 25$. As in the regular method, the limit on y is $y_{max} < \sqrt{n/2}$ or $y_{max} < \sqrt{n/3}$.

7.5 Method for $n \equiv 3 \mod 4$

We will separately examine the two cases of $n \equiv 3 \mod 8$ and $n \equiv 7 \mod 8$.

7.5.1 The case of $n \equiv 3 \mod 8$

We will use The Method (section 7.2) adapted for the two equations:

$$n = x^2 + 2y^2$$
$$3n = x^2 + 2y^2$$

By the facts in 6.3.3, we know that if there are any solutions to either equation, then there is at least one solution in which one of x or y is a multiple of 5. For the first case, both x and y are odd. In the second case, we know that x is odd and y is even.

The results of The Method will tell us the following:

- If there is only one decomposition, and $\gcd(x, y) = 1$, then n is prime.
- If there is any decomposition with $\gcd(x, y) > 1$, the square of the gcd is a divisor of n.
- Two or more decompositions means n is composite (and the divisors can be easily calculated).
- No decompositions means that n is composite; of the set of factors, at least two have residues from the set $\{5, 7\}$ modulo 8.

In Table 1 we summarize the divisibility properties of the terms of the two quadratic forms. These conditions are true for representations of n if any exist, but note that for some n there will be no representation in one or the other form, and for some n there will no representation in either form.

Overview of using The Method with the form $n = x^2 + 2y^2$. At the start, we need to know which of x or y is divisible by 5. If the last digit of n is 1 or 9, then y is divisible by 5, and if the last digit is 3 or 7, then x is divisible by 5. See 6.3.3 for the proofs and table 1 (in section 7.2) for the summary.

Case of n last digit is 1 or 9. In this case, we know that y is an odd multiple of 5, and therefore, $n \equiv x^2 + 2 * 25 \mod 100$. This implies that $n + 50 \mod 100$ is the same as $x^2 \mod 100$ (note that $50 \equiv -50 \mod 100$). The smallest r value in the range $1 \ldots 24$ with a square that has low order digits matching $n + 50 \mod 100$ is the number we need to search for. The set S will be $\{50j \pm r\}$ for numbers less than $\sqrt{n}$.

For each $s \in S$, check to see if $n - s^2$ is twice a square. Section 5.3 describes how to do this by examining the hundreds and thousands digits. If those conditions are true, then look at $2(n - s^2)$ and decide if it is a square.

Case of n last digit is 3 or 7. In this case, x is an odd multiple of 5, its square will end in 25, and its hundreds digit will be even. This implies that $n \equiv 25 + 2y^2 \mod 200$. Compute $t \equiv n - 25 \mod 200$. Then find the smallest r in the range $1 \ldots 24$ such that $r^2 \equiv t/2 \mod 100$.

The set S is $\{r, 50 - r, 50 + r, 100 - r, \ldots\}$, and these are the candidate values for y. For each $s \in S$, compute $n - 2s^2$ (which will end in 25) and check to see if it is a square.

NB: the members of the set S are less than $\sqrt{n/2}$.

Once we have determined the number of representations using the first quadratic form, and assuming that there are fewer than 2 of them, we move on to solving the second quadratic form.

Using The Method with the form $3n = x^2 + 2y^2$. We know that x is odd and y is even, and we need to know which of x or y might be divisible by 5. As in the previous section, we branch on the low order digit, but this time we branch on the low order digit of $3n$.

If the low order digit of $3n$ is 1 or 9, then x is not divisible by 5, so we apply The Method with the assumption that y is an even multiple 5. Find the smallest r in the range $1 \ldots 24$ such that $r^2 \equiv 3n \mod 100$. The x candidates are $S = \{50j \pm r\}$. For each x candidate in S, check to see if $3n - x^2$ is twice a square. We can now proceed with The Method as usual, noting that the maximum value for x is $\sqrt{3n}$.

If the low order digit of $3n$ is 3 or 7, then we will look for solutions in which x is an odd multiple of 5. The Method is nearly the same as in the previous section. We have $3n - 25 \equiv 2y^2 \mod 200$. Compute $t \equiv 3n - 25 \mod 200$, and then find the smallest r in the range $1 \ldots 24$ such that $r^2 \equiv t/2 \mod 100$. The y candidates are $\{50j \pm r\}$. For each y candidate in S, check to see if $3n - 2y^2$ is a square. We can now proceed with The Method as usual, noting that the maximum value for y is $\sqrt{3n/2}$.

We provide Table 1 as a handy summary of the various cases of divisors of x and y.

Determining the factors when we have two solutions. In the previous section about $4k + 1$ numbers, we discussed how to combine two solutions to find the factors of the target number. For the current case of $4k + 3$ numbers, we can use nearly same method, although with less flexibility in rearranging the terms.

If the two solutions for x and y are (a, b) and (c, d), then $(a - c, b - d)$ gives us two numbers that can be substituted into $x^2 + 2y^2$. This number will have a common factor with the target number.

In fact, any combination of $(\pm a \pm c, \pm b \pm d)$ has this property. Sometimes it will be obvious that one combination is more tractable than another, and you can use that. However, you can choose any combination to finish the factorization. If the two components in a combination have a common factor, divide out that factor from both components.

We have found two solutions to $kn = x^2 + 2y^2$ where $k = 1$ or $k = 3$. If both solutions are for the same k, there is an optimization available. It is the case that at least one choice of $(\pm a \pm c, \pm b \pm d)$ contains a factor of five in both terms. Find that combination by trial and error, and then divide out the factor of five from each component.

As described in step 4 of section 7.2, plug the two components into $x^2 + 2y^2$ and take the gcd with n.

If any the divisors is too large to factor, then we can use theorem 8 from section 6.3.3. That tells us that any divisor d of a number representable as $x^2 + 2y^2$ where $\gcd(x, 2y) = 1$ is itself representable in the same form. Therefore, using The Method on d will result in a definitive factorization.

Example: Factor 1019.
We will look for solutions to $1019 = x^2 + 2y^2$. The low order digits are "19", and we know that if a decomposition exists, y is divisible by 5. Thus, candidates for r are of the form $19 \equiv r^2 + 50 \mod 100$. We have to go up to $r = 13$ to find a solution $19 \equiv 13^2 + 50 \mod 100$. The set S of all x candidates consists of numbers of the form $50j \pm 13$.
We see that for $j = 0$, $1019 = 13^2 + 850$, and we notice that 850 is not 2 times a square (recall section 5.3). For $j = 1$, the corresponding members of S are 37 and 63, and their squares are larger than 1019. No other candidates are feasible.
We move on to the alternate quadratic form, $3n = 3057 = x^2 + 2y^2$. In this case, x is divisible by 5. We are looking for the smallest r such that $57 \equiv 25 + 2r^2 \mod 100$. That implies that $2r^2 \equiv 32 \mod 100$, and we see that $r^2 \equiv 16 \mod 100$ or $r^2 \equiv (50 + 16) \mod 100$. The second equivalence equation is impossible because squares cannot end in 66. The set S is based on $r^2 = 16$ and thus thus consists of numbers of the form $50j \pm 4$.
It is easy to see that $3057 - 3 * 4^2 = 3025$. Further, because 30 is the product of 5 and 6, we see that 3025 is a square (55^2). It follows that $3 * 1019 = 55^2 + 2 * 4^2$.
The next candidate from the set S is $50 - 4 = -46$. Because $2 * (46)^2$ is larger than 3057, it is not a feasible solution. There are no other candidates with squares closer to 3057, so the search is complete.

We found one representation with relatively prime terms (55 and 4) and have shown that there are no others. Therefore, 1019 is prime.

Example: Factor 4003.
We will look for solutions to $4003 = x^2 + 2y^2$. The low order digits are "03" and we know that if a decomposition exists, x is divisible by 5. The reduced equation is $3 \equiv 25 + 2y^2 \mod 100$ or, equivalently, $-22 \equiv 78 \equiv 2y^2 \mod 100$. We look for the smallest solution to $39 \equiv y^2 \mod 100$. From the discussion in section 5.1, we know that there is no square ending in 39. However, there is a second solution to $78 \equiv 2y^2 \mod 100$. It is simply $(39 + 50) = 89 \equiv y^2 \mod 100$.

The smallest solution to $89 \equiv y^2 \mod 100$ is $y = 17$. The set S is based on the form $y = 50j \pm 17$. We need only examine candidates up to the square root of the quotient $4003/2 = 2001$. The square root is approximately 45.

The first candidate is $y = 17$, and we see that $4003 - 2 * 289 = 4003 - 578 = 3425$. As noted

in section 5.2, this cannot be a square because the hundreds digit is 4. We move on to the next candidate, $50 - 17 = 33$. The square of 33 is 1089, and $4003 - 2 * 1089 = 1825$. Again, we know this is not a square because the hundreds digit (8) is disallowed.

Any further candidates have squares that are too large, so we conclude that 4003 does not have a representation of the form $x^2 + 2y^2$ with 5 dividing x or y.

The second part of the analysis uses $3n = x^2 + 2y^2$. We begin by multiplying 4003 by 3 to get 12009. We know that y is divisible by 5, and we look for solutions to $12009 \equiv 9 \equiv x^2 + 2 * y^2 \mod 100$. There are two possible values for y^2 in this equation: $y^2 \equiv 0 \mod 100$ and $y^2 \equiv 50 \mod 100$. In the second case, we see by section 5.1 that 50 is not a possible square residue mod 100. We proceed to work with the equation $9 \equiv x^2 \mod 100$ or equivalently $x \equiv 3 \mod 100$. The candidates of the set S of the form $50j \pm 3$. We need only consider candidates up to the square root of 12009, or approximately 110.

The first candidate is 3, and we see that $12009 - 3^2 \mod 100 = 12000$. Because we are looking for 2 times a square, we ask if 6000 is a square, and it is not. The second candidate is $3 - 50 = -47$, the square of that is 2209, leading to $12009 - 2209 \mod 100 = 9800$. One half of 9800 is 4900, and that is the square of 70. Noting that 47 and 70 are relatively prime, we have the solution $12009 = 47^2 + 2 * 70^2$. The next feasible candidates are $3 + 50 = 53$, $3 - 2 * 50 = -97$, and $3 + 2 * 50 = 103$. None of these result in a solution.

Having found that there is only one solution to the quadratic form, we can conclude that 4003 is prime.

Example 3139:
We begin with the quadratic form $3139 = x^2 + 2y^2$. Referring to Table 1, we see that x is odd and y is an odd multiple of 5. We look for a solution to $39 \equiv x^2 + 2y^2$ where $y^2 \equiv 25 \mod 100$. This implies $39 \equiv x^2 + 50 \mod 100$, and a rearrangement gives us $39 - 50 \equiv x^2 \mod 100$, and then $89 \equiv x^2 \mod 100$. We look for the smallest x that satisfies this, and we find that it is $17^2 = 289$. The set S will consist of numbers of the form $50j \pm 17$ that are less than the square root of 3139.

We start looking for r in S such that $3139 - r^2$ is twice a square. The first candidate is 17, and we see that $(3139 - 289)/2 = 1425$ cannot be a square because the hundreds digit is disallowed per section 5.3. The next candidate is $(17 - 50) = -33$, and its square is 1089. The expression $(3130 - 1089)/2 = 1025$ cannot be a square because its thousands and hundreds digits taken together is not the product of two consecutive integers.

No other candidates are within range, and we conclude that 3139 has no representation as $x^2 + 2y^2$ that are discoverable using The Method.

We move on to $3n = x^2 + 2y^2$. From Table 1, we see that x is an odd multiple of 5 and y is even. We have $9417 \equiv 17 \equiv 25 + 2y^2 \mod 100$ which implies $92 \equiv 2y^2 \mod 100$. For this modular equation, y^2 could be equivalent to either 46 or 96. But 46 cannot be the last two digits of a square, so we proceed with $y^2 \equiv 96 \mod 100$. The smallest solution to this is $y = 14$. The set of candidates will be numbers of the form $50j \pm 14$ that are less than the square root of 9417/2 which is about 69.

The first candidate is 14, and we have the equation $9417 - 2(14)^2 = 9025$. The high order digits, 90, are the product of two consecutive integers, so we know that 9025 is the square of 95. Furthermore, 95 and 14 are relatively prime, so we have a solution to the quadratic form. Are there more?

The next candidate is $50 - 14 = 36$. Its square is 1296. Plugging that into the quadratic form, we have $9417 - 2 * 1296 = 6825$. The hundreds digit rules this out as a square.

The next candidate is $50 + 14 = 64$. Its square is 4096, and we have $9417 - 2 * 4096 = 1225$. This is the square of 35, and we have a solution to the quadratic form. Furthermore, 35 and 17 are relatively prime, so it is our second acceptable solution. From this we can conclude that 3139 is composite.

The quadratic form terms are $(95^2, 14^2)$ and $(35^2, 64^2)$. The pairwise difference of (95, 14) and (35, 64) is (60, 50). The GCD of the pair is 10. We divide out the GCD and get (6, 5). One factor of 3139 is therefore $(6^2 + 2 * 5^2)/2 = 86/2 = 43$ (which is prime). Finally, 3139 divided by 43 is 73.

This completes the factorization of 3139.

Example 7387:
Consulting Table 1 for the quadratic form $n = x^2 + 2y^2$ in the case of last digit 3 or 7, we see that x and y are both odd and x is divisible by 5. Thus we can write the form as $87 \equiv 25 + 2y^2 \mod 100$. There are two solutions to $87 - 25 = 62 \equiv 2y^2 \mod 100$, and they are $y^2 \equiv 31, y^2 \equiv 81$. Only the second solution can be the low order digits of a square (see section 5.3). We will search for solutions for y of the form $50j \pm 9$.

The first candidate for y is 9, and we see that $7387 - 2 * 81 = 7225$. Because the two high digits are the product of consecutive integers $(8 * 9)$, we see that 7225 is the square of 85. Moreover, 85 and 9 are relatively prime, and therefore we have a solution to the quadratic form with $x = 85$ and $y = 9$.

The next candidate for y is 41 and its square is 1681. The quadratic form becomes $7387 - 2 * 1681 = 4025$. Because 40 is not the product of consecutive integers, we know that 4025 is not a square.

The next candidate is 59, and this leads to $7387 - 2 * 59^2 = 7387 - 2 * 3481 = 425$. This is not a square.

Because no further candidates are less than the square root of $7387/2$, we conclude that there are no further solutions to this quadratic form.

Because we have only one representation, we now examine the quadratic form $3n = 22161 = x^2 + 2y^2$. In this case, x is odd, y is even, and y is divisible by 5. This means that y^2 is a multiple of 100, so when examine the equation modulo 100, the second term drops out leaving $61 \equiv x^2 \mod 100$.

The smallest r with square with low order digits 61 is 19. The candidates for x are the set $\{50j \pm 19\}$. The first candidate is 19. We have $22161 - 19^2 = 22161 - 361 = 21800$. By the discussion in section 5.3, we know that this is not twice a square.

The next candidate is 31. We have $22161 - 31^2 = 22161 - 961 = 21200$. By the discussion in section 5.2, we know that this is not twice a square.

The next candidate is 69. We have $22161 - 69^2 = 22161 - 4761 = 17400$. By the discussion in section 5.2, we know that this is not twice a square.

The next candidate is 81. We have $22161 - 81^2 = 22161 - 6561 = 15600$. By the discussion in section 5.2, we know that this is not twice a square.

The next candidate is 119. We have $22161 - 119^2 = 22161 - 14161 = 8000$. By the discussion in section 5.2, we know that this is not twice a square.

The next candidate is 131. We have $22161 - 131^2 = 22161 - 17161 = 5000$. This is twice 2500, and that is the square of 50. We note that 131 and 50 are relatively prime, so this is a solution.

We have now found two solutions, one for the form $n = x^2 + 2y^2$ and one for $3n = x^2 + 2y^2$. We know that that 7387 is composite.

To find its factors, we need to combine the two solutions. The x, y pairs are $(131, 50)$ and $(85, 9)$.

We begin by doing a pairwise subtraction to obtain $(46, 41)$. We evaluate this as an (x, y) solution to $x^2 + 2y^2$ and obtain $46^2 + 2(41^2) = 2116 + 3362 = 5478$. The gcd of 5478 and 7387 will reveal a factor of 7387.

To begin the gcd, we first remove small factors of 5478. It is divisible by 2 and 3, so the easily determined factors are $(2, 3, 913)$. It is possible that 913 factors into smaller numbers, so we next calculate the gcd of 7387 and 913. We notice that the quotient of 7387 divided by 913 is close to 8. This leads to the easily computed expression $8 * 913 = 7304$ and $7387 - 7304 = 83$. We can see that $913 = 11 * 83$. Because 83 divides 913, it must also divide 7387. By inspection we can see that 7387 divided by 83 is slightly less than 90, and from the low order digits of the two numbers, it is apparent that the low order digit of the quotient is 9. The factorization of 7387 is $83 * 89$.

Example 2867:
From Table 1 we see that x and y are odd and x is divisible by 5. Using the modulo 100 view of $x^2 + 2y^2$, we have $67 \equiv 25 + 2y^2 \mod 100$ or equivalently, $42 \equiv 2y^2 \mod 100$. The two possible solutions for y^2 are 21 and 71, and by section 5.1, only 21 can be the low order digits of a square. The smallest r whose square has matching low digits is 11. The set of candidates is $\{50j \pm 11\}$. The largest candidate that we need to examine is approximately $\sqrt{2867/2}$ which is about 40.

The first candidate for y is 11. We have $2867 - 2 * 11^2 = 2867 - 242 = 2625$. Because 26 is not the product of two consecutive integers, this is not twice a square.

The next candidate is 39. We have $2867 - 2 * 39^2 = 2867 - 2 * 1521$. Because this is negative, we can conclude that there are no more candidates. This quadratic form has no solutions.

We move on to the second quadratic form. In this case, x is odd, y is even and divisible by 5. We have $3 * 2867 = 8601 \equiv 1 \equiv x^2 \mod 100$. As in the previous example, the y^2 term drops out because it is divisible by 100.

The smallest r such that $r^2 \equiv 1 \mod 100$ is 1. The set of candidates for x^2 is $\{50j \pm 1\}$.

The first candidate is 1. We have $8601 - 1 = 8600$, and this is not twice a square.

The next candidate is 49. We have $8601 - 49^2 = 8601 - 2401 = 6200$, and this is not twice a square.

The next candidate is 51. We have $8601 - 51^2 = 8601 - 2601 = 6000$, and this is not twice a square.

Further candidates are too large to be solutions, so we can conclude that this quadratic form has no solutions.

When a number cannot be represented in either form, we know that it is composite, but we have little information about its factors. In this case, $47 * 61 = 2867$. We will defer the discussion of how to factor these numbers to section 8.

Example 5459:
From Table 1 we see that for the quadratic form $x^2 + 2y^2$, x and y are odd and y is divisible by 5. The modulo 100 equation is $59 \equiv x^2 + 2 * 25 \mod 100$. We can conclude that $59 - 50 = 9 \equiv x^2 \mod 100$. The smallest r with a square with low order digits "09" is 3. The candidate for x are the set $\{50j \pm 3\}$.

The first candidate is 3. We have $5459 - 9 = 5450$. By the facts presented in section 5.1, we can conclude that this is not twice a square because the digits in the thousands and hundreds place (54) are not a number divisible by 4 (see section 5.3).

The next candidate is 47. The corresponding equation is $5459 - 47^2 = 5459 - 2209 = 3250$. An easy trick for seeing that this is not twice a square is to double it, and we can see that 6500 cannot

be 4 times a square.

The next candidate is 53. $5459 - 53^2 = 5459 - 2809 = 2650$. The thousands-hundreds digits (26) do not form a number divisible by 4, so it is not twice a square.

Further candidates are too large, so we conclude that 5459 has no representations as $x^2 + 2y^2$ that are discoverable using The Method.

We move on to the form $3n = x^2 + 2y^2$. We calculate $3 * 5459 = 16377$. From the table of terms, we know that x is odd and divisible by 5, and y is even. This leads to the equation $77 \equiv 25 + 2y^2 \mod 100$, and it has two possible solutions for y^2: 26 and 76. Of these, only 76 can be the low order digits of a square.

The smallest r such that the low order digits of r^2 are 76 is 24. The set of candidates for y is $\{50j \pm 24\}$.

The first candidate is 24. We have $16377 - 2 * 24^2 = 15225$. Because 152 is not the product of two consecutive integers, we know that this is not a square.

The second candidate is 26. We have $16377 - 2 * 26^2 = 15025$. This cannot be a square because 150 is not the product of two consecutive integers.

The next candidate is 74. We have $16377 - 2 * 74^2 = 5425$. This cannot be a square because the hundreds digit is not 0, 2, or 6.

The next candidate is 76. We have $16377 - 2 * 76^2 = 4825$. This cannot be a square because the hundreds digit is not 0, 2, or 6.

Further candidates are too large. There are no solutions to the quadratic forms, from which we can conclude that 5459 is composite. Its factors are 53 and 83. In section 8 we will discuss how to find them.

7.5.2 Method for the case of $n \equiv 7 \mod 24$, using the form $x^2 + 3y^2$

We previously noted that primes of the form $6j + 1$ can be represented uniquely as $x^2 + 3y^2$. This means that we can apply The Method to analyzing these numbers: a unique solution means n is prime, zero or multiple solutions mean it is composite. However, most $6j + 1$ numbers will fall into the congruence classes that we have previously covered. The ones that remain can be described by their residues modulo 24.

Although there are 3 possible residues cases corresponding to the residue of $n \mod 24$ (7, 15, and 23), only the residue 7 is both non-trivial and tractable. The case of 15 is trivial because in that case n is divisible by 3. The residue 23 case does not have unique prime decomposition in a field tractable by The Method. Therefore this section is devoted solely to the case of $n \equiv 7 \mod 24$.

We will use the form $x^2 + 3y^2$. It is the case that primes congruent to 7 modulo 24 have unique decomposition with this form. Refer back to the section on theorems about $6j + 1$ numbers (section 6.3.4).

Our mental method for working with numbers $n \equiv 7 \mod 24$ is similar to the previous ones. As before, if n is prime there is a unique decomposition, in this case, of the form $x^2 + 3y^2$. If there are 2 or more decompositions, then the previous techniques will generally find a factor. In order to apply the modulo 25 tricks, we will need to use decompositions over n and $4n$.

Method for decompositions over $n = x^2 + 3y^2$ and $4n = x^2 + 3y^2$. The method is a slight variant on the previous search methods. We describe the most common case in which n is 3 modulo 4 and also note the changes to make if n is 1 modulo 4.

Table 1 (in section 7.2) has information about x and y, depending on the last digit of n. Because n is odd, one of x and y must be odd and the other even.
Looking at the equation modulo 4, n is usually 3 modulo 4.
Squares modulo 4 are either 0 or 1.
We choose x even and y odd to make $x^2 + 3y^2 \equiv 3 \mod 4$. (If $n \equiv 1 \mod 4$, we do the opposite.)
Similar reasoning modulo 5 gives the rule in table 1:
If the last digit of n is 1 or 9, then y is the multiple of 5. If the last digit of n is 3 or 7, then x is the multiple of 5.

For decompositions of $4n = x^2 + 3y^2$, x and y must both be odd. (If x and y are both even, the solution is the double of the solution $n = (x/2)^2 + 3(y/2)^2$, but we will have already found the n solution, and the double is useless to us.) Select which of x or y is the multiple of 5 using the rule above, based on the units digit of n.

The n and $4n$ forms are handled similarly, and both depend on the low order digit of n.

For n with low order digit 3 or 7:
x is the multiple of 5.
When x is an even multiple of 5, $x^2 \equiv 0 \mod 100$.
When x is an odd multiple of 5, $x^2 \equiv 25 \mod 100$.
To solve for possible y values, note that $3y^2 \equiv n - x^2 \mod 100$ or $3y^2 \equiv 4n - x^2 \mod 100$.
We know $x^2 \mod 100$ is either 00 or 25; subtract it from n modulo 100, and then divide by 3 to get y^2 modulo 100. This must be an exact division, with no remainder. It is easiest to work out the units digit of y^2 first, and then figure out the tens digit. Choose r between 1 and 25 so that $r^2 \equiv y^2 \mod 100$. The candidates for y are $\{50j \pm r\}$. Run through the candidates, checking if $n - 3y^2$ (or $4n - 3y^2$) is a square. Stop when $3y^2$ exceeds n (or $4n$) or if the search has found two solutions (one each for n and $4n$ is fine).

For n with low order digit 1 or 9:
y is the multiple of 5.
Compute the possible x values using the equation $x^2 \equiv n - 3y^2 \mod 100$. y is usually odd, so $3y^2 \equiv 75 \mod 100$. Note that $x^2 = n - 75 \mod 100$ or $x^2 = n + 25 \mod 100$.
Choose r between 1 and 25 so that $r^2 \equiv x^2 \mod 100$.
The x candidates are $\{50j \pm r\}$. Skip any x candidate that is a multiple of 3 (because if x is a multiple of 3, then $x^2 + 3y^2$ is a multiple of 3.) For each possible x, check if $n - x^2$ (or $4n - x^2$) is the triple of a square. For the usual odd y case, $3y^2$ must end in 075, 675, 1875, or 6875 (per section 5.4). If this test is passed, then divide $n - x^2$ (or $4n - x^2$) by three and check if the quotient is a square. The quotient will end in 25. The remainder should be 0; if not, discard that x candidate. Stop when x^2 exceeds n (or $4n$) or if there are two solutions.

It is usually necessary to test both n and $4n$.

As in previous cases of quadratic form decompositions, we know that

- if there is no decomposition, then n is composite and has at least two $6j + 5$ divisors;
- if there is one decomposition, and the x and y are relatively prime, n is prime;
- if there are two (or more) decompositions, they can be combined in the same manner as the $x^2 + 2y^2$ case to find a solution. The only difference is that after the ordered pair arithmetic, the form $x^2 + 3y^2$ is used instead of $x^2 + 2y^2$.

Determining the factors when we have two solutions. If the two solutions for x and y are (a, b) and (c, d), then $(a - c, b - d)$ gives us two numbers that can be substituted into $x^2 + 3y^2$.

This number will have a common factor with the target number. In fact, any combination of $(\pm a \pm c, \pm b \pm d)$ has this property. Sometimes it will be obvious that one combination is more tractable than another, and you can use that. However, you can choose any one to finish the factorization.

The two solutions are for $kn = x^2 + 3y^2$ where $k = 1$ or $k = 4$. If both solutions are for the same k form, there is an optimization available. It is the case that at least one choice of $(\pm a \pm c, \pm b \pm d)$ contains a factor of five in both terms. Find that combination by trial and error, and then divide out the factor of five. Then proceed with the gcd algorithm.

Because the numbers in these solutions are larger than for the previous cases, we mention a simple way to use smaller numbers for the calculation: compute $m = ad \pm bc$ and take $\gcd(m, n)$. This will be a divisor of n, and we can divide it into n to find the co-factor.

If any of the divisors is too large to factor, then we can use the fact any divisor d of an odd number representable as $x^2 + 3y^2$ where $\gcd(x, 3y) = 1$, is itself representable in the same form. Therefore, using The Method on d will result in a definitive factorization.

Example 2923:
The low order digits are 23. We know that $23 - x^2 \equiv 3y^2 \mod 100$. From Table 1 we know that x is even and divisible by 5, and the modular equation is: $23 - 00 \equiv 3y^2 \mod 100$.

The smallest integer r for which $3r^2$ matches on the low digits is $r = 21$. The candidates are $\{50j \pm 21\}$.

The first candidate is 21, and $2923 - 3 * 21^2 = 2923 - 3 * 441 = 1600$. That is the square of 40, and because 40 and 21 are relatively prime, we have a solution, $2923 = 40^2 + 3 * 21^2$.

The next candidate is 29. $2923 - 3 * 29^2 = 2923 - 3 * 841 = 400$. That is, of course, the square of 20. Because 20 and 29 are relatively prime, we have a second solution, $2923 = 20^2 + 3 * 29^2$. The pairs $(40, 21)$ and $(20, 29)$ have the pairwise combination $(20, 8)$, and after eliminating the common factor of 4, we have $(5, 2)$. One factor is thus $5^2 + 3 * 2^2 = 37$. Dividing 2923 by 37 yields the second factor, 79, which is prime.

$2923 = 37 * 79$, QED.

Example: 3679
The low order digits are 79. From Table 1 we know that y is odd and divisible by 5. The modular equation is $79 - 3 * 25 = 4 \equiv x^2 \mod 100$. The smallest number r such that $r^2 \equiv 4 \mod 100$ is 2. The candidate set is $\{50j \pm 2\}$. The first candidate is 2.

$3679 - 2^2 = 3675 = 3 * 1225$. Because 12 is the product of two consecutive integers, we know that 1225 is the square of 35. We see that 2 and 35 are relatively prime, and therefore we have a solution: $3679 = 2^2 + 3 * 35^2$.

The next candidate is 52, and $3679 - 52^2 = 975 = 3 * 325$. We can see that 325 is not a square.

The next candidate is 48, $3679 - 48^2 = 1375$. Because 1375 is not divisible by 3, it cannot be a solution to quadratic form. We move on to candidate 98, which is too large.

There is only one representation for $n = x^2 + 3y^2$, so we next try to solve $4n = x^2 + 3y^2$.

$4 * 3679 = 14716 \equiv 16 \mod 100$. From Table 1 we know that y is odd and divisible by 5. The modular equation is $16 - 3 * 25 \equiv 41 \mod 100$. The smallest r such that $r^2 \equiv 41 \mod 100$ is 21. The candidate set for x is $\{50j \pm 21\}$.

The first candidate is 21. Because this is a multiple of 3, it cannot be part of a solution to this quadratic form. We move to the next candidate, 29.

$4 * 3679 = 14716 - 29^2 = 13875 = 3y^2$, implying that $y^2 = 4625$. Because 46 is not the product of two consecutive integers, 4625 is not a square.

The next candidate is 71. We have $14716 - 71^2 = 14716 - 5041 = 9675 = 3 * 3225$. We note that 3225 cannot be square because 32 is not the product of two consecutive integers.

The next candidate is 79. We have $14716 - 79^2 = 14716 - 6241 = 3 * 2825$. We see that 2825 is not a square because 28 is not the product of two consecutive integers.

The next candidate is 121. We have $4 * 3679 = 14716 - 121^2 = 14716 - 14641 = 3 * 25 = 3 * 5^2$. We note that 121 and 5 are relatively prime. We now have a second solution, $4 * 3679 = 121^2 + 3 * 5^2$.

The two solutions as ordered pairs are $(2, 35)$ and $(121, 5)$. We can choose the signs arbitrarily in their sum to achieve a useful pair in which both numbers are divisible by 3: $(123, 30)$. We remove the common factor and have $(41, 10)$. A divisor is obtained from calculating $41^2 + 3 * 10^2 = 1681 + 300 = 1981$. This will have a common factor with 3679. We can calculate $\gcd(3679, 1981)$ as $2 * 1981 - 3679 = 283$. This is a prime, and the factorization is $3679 = 13 * 283$.

Example: 5407

The low order digits are 07, and from Table 1 we see that x is even and divisible by 5. This means that x^2 is divisible by 100.

The modular equation is $5407 - 00 \equiv 3y^2 \mod 100$. The smallest number r such that $3r^2 \equiv 7 \mod 100$ is 13 ($3 * 13^2 = 507$), so the candidate set for y is $\{50j \pm 13\}$. The first candidate is 13.

We have $5407 - 3 * 13^2 = 5407 - 507 = 4900 = x^2$. This is a solution because 70 and 13 are relatively prime.

The next candidate is 37. We have $3 * 37^2 = 3 * 1369 = 4107$, leading to $5407 - 4107 = 1300 = x^2$. The hundreds digit rules out 1300 as a square.

The next candidate is 63, but $3 * 63^2 = 3 * 3969$ is larger than 5407.

We have one solution to $5407 = x^2 + 3y^2$, and we now move on to the form $4n = x^2 + 3y^2$.

$4 * 5407 = 21628 = x^2 + 3y^2$. The low order digits are 28, and from Table 1 we know that x is divisible by 5. Therefore, modulo 100, $4n - x^2 \equiv 28 - 25 = 3 * 1$. The set of candidates is given by $\{50j \pm 1\}$.

The first candidate is 1, and we have $21628 - 3 * 1 = 21625$. This does not match the patterns listed in section 5.2, and we conclude that 21625 is not a square.

The second candidate is 49, and we have $21628 - 3 * 49^2 = 14425$. Again, this does match the patterns listed in section 5.2, and we conclude it is not a square.

The third candidate is 51, and we have $21628 - 3 * 51^2 = 13825$. Again, does match the patterns listed in section 5.2, and we conclude it is not a square.

The fourth candidate is 99, and it is too large.

We have established that there is only one solution for 5407, it has relatively prime components, and therefore, 5407 is prime.

Example: 4771

(NB: This is a retry of a failed $8j + 3$ number)

We will start with the equation $x^2 = n - 3y^2$. The low order digits are 71. From Table 1 we know that y is odd and divisible by 5. Thus, y^2 ends in the digits 25 and $3y^2$ ends in 75: $x^2 \equiv 71 - 75 \mod 100 = 96$.

The smallest integer square ending in 96 is 196, so r is 14. The set of candidates for x is $\{50j \pm 14\}$. We start with $x = 14$ and substitute into the equation, resulting in $4771 - 196 = 4575 = 3y^2$. Because the hundreds digit of 4575 is odd, there is no solution to this equation.

The next candidate is $50 - 14 = 36$. Because this is a multiple of 3, we can ignore it because we have removed small prime divisors from our target number before starting the quadratic form analysis.

The next candidate is $50 + 14 = 64$. We have $4771 - 4096 = 675 = 3y^2$. If we divide by 3 we have $225 = 15^2 = y^2$, a solution to the quadratic form with x and y relatively prime. We note this pair $(64, 15)$ and move on.

The next candidate for x is $2 * 50 - 14 = 86$, but the square of 86 is larger than 4771, so it is not a possibility.

Now we analyze the equation $x^2 = 4n - 3y^2$. From Table 1 we see that x and y are both odd and y is a multiple of 5. We calculate $4n = 19084$. Because y is odd $3y^2$ will end in 75. Therefore $x^2 = 4n - 3y^2 \mod 100$ will be $84 - 75 = 9$, and we have $r = 3$ and the set of candidates is $\{50j \pm 3\}$.

The first candidate for x is 3, but as explained above, we can ignore multiples of 3.

The next candidate is 47, and we have $4n - x^2 = 19084 - 2209 = 16875$. Dividing by 3 we have $5625 = y^2$. Because 56 is the product of two consecutive integers, we know that there is a solution, and it is $y = 75$. Now we have a second solution with relatively prime x and y: $(47, 75)$.

The two pairs $(64, 15)$ and $(47, 75)$ can be combined to find a divisor. Because the two y values share the common factor 15, we can divide it out if we will be using the cross product combination method. Now the two pairs are $(64, 1)$ and $(47, 5)$. To calculate the divisors, we use the cross product of the two pairs to get $64 * 5 \pm 1 * 47$. The two results are 273 and 367. The second of these is prime and divides 4771 with a quotient of 13, so a complete factorization of 4771 is $367 * 13$. Although 273 is not prime $(3 * 7 * 13)$, it is easy to see that it shares a common factor of 13 with 4771, and so the factorization can be obtained from either result.

7.6 No decomposition, don't give up, retry!

A good fraction of difficult-to-factor numbers can be addressed by using an alternative quadratic form. The residue classes in Table 1 are not mutually exclusive, so there are opportunities for a "do over". For example, if a $4k + 1$ numbers is also a $8j + 1$ number, then it can be re-analyzed using the form $x^2 + 2y^2$. Table 2 summarizes the information to be used for retries.

Sometimes The Method will yield a piece of information that could be useful if a retry is needed. For example, suppose $n = 4921$ and we are trying the form x^2+y^2. We would encounter the equation $n = 3721 + 1200$. Although this would be rejected for the form $n = x^2 + y^2$ because 1200 is not a square, the information can be helpful in other ways, even if the form $x^2 + y^2$ doesn't resolve our number. Because 1200 is 3 times 400, we have a solution for the form $x^2 + 3y^2$. If we later decide to use the this form as a "retry", this solution gives us a head start. Furthermore, we know that we will get either a factorization or a prime proof.

7.7 More about working with quadratic forms: large numbers

The quadratic form method of factoring requires that the mental factorer try several numbers to see if they satisfy the form. Even after having mastered The Method and the shortcuts, one may find it tiresome to factor numbers of six or seven digits. Is there any way to cut down on the set of values that have to be tested? At the cost of creating more rules to memorize, the answer is "yes".

residue	last digit	quadratic form	5 divides	x parity	y parity
1 mod 8	1 or 9	$n = x^2 + 2y^2$	y	odd	even
		$3n = x^2 + 2y^2$	x	odd	odd
1 mod 8	3 or 7	$n = x^2 + 2y^2$	x	odd	even
		$3n = x^2 + 2y^2$	y	odd	odd
1 mod 12	1 or 9	$n = x^2 + 3y^2$	y	odd	even
		$4n = x^2 + 3y^2$	y	odd	odd
1 mod 12	3 or 7	$n = x^2 + 3y^2$	x	odd	even
		$4n = x^2 + 3y^2$	x	odd	odd
7 mod 12	1 or 9	$n = x^2 + 3y^2$	y	even	odd
		$4n = x^2 + 3y^2$	y	odd	odd
7 mod 12	3 or 7	$n = x^2 + 3y^2$	x	even	odd
		$4n = x^2 + 3y^2$	x	odd	odd

Table 2: Properties of other quadratic form terms

Examining candidates high-to-Low. For large n, it is likely that n is composite. When we discussed the candidate set S in The Method, we recommended using the smallest numbers in the set first. But if n is large, or if The Method has already failed and you are using a retry form, going through S from the highest possible value down to the lowest will save time (on average). The reason is that the other term in the quadratic form will then go from small to large, and small numbers are more likely to be squares or multiples of squares. If there is no representation, or only one, we must examine the full range of S to discover this. But if there is more than one representation, we can stop trying candidates in S when we find the second solution. Examining S from high-to-low will (on average) find these solutions earlier.

If either of the forms $x^2 + 2y^2$ or $x^2 + 3y^2$ is usable as a retry (because n happens to be $8j + 1$ or $12j + 1$), then they have a good chance of finding the factors, and the high-to-low order will generally be quicker than the other direction.

Another probable composite situation is when a $4k + 3$ number is being worked with The 120 Method (see section 8.1), but you can't find the needed 2, 3, 5 squares. A composite number will have only half as many squares (or fewer). When we have the incomplete results of examining S and haven't found any solutions, the odds of the number being composite are somewhat increased.

Another situation for high-to-low is if n has an obvious quadratic form solution, and we are looking for another. Euler's number, 1000009, (section 7.7.1) is in this category: The $1000^2 + 3^2$ solution for $x^2 + y^2$ is obvious. To look for another, we can evaluate S high-to-low, improving our chance of finding it early. If there's no other, all of S will be examined anyway.

Candidate filters. The hardest thing to master when working with 6 digit numbers is squaring 3 digit numbers that are candidates for x or y. The second hardest thing is finding the 3 digit co-factor of a 3 digit divisor. If you cannot do these multiplications in your head, then you will need to practice this skill so that you can get the time down to under 2 minutes. The "Trachtenberg

Speed System of Basic Mathematics" has some techniques that can be helpful, but anyone with an understanding of basic algebra can come up with ways to tackle the operations. Nonetheless, it is certainly more pleasant to accomplish a factorization without having to do more than a handful of 3x3 multiplications. This is the motivation for filters.

When working with a 6 digit or larger number, you should first work out what constraints there are for candidate solutions when viewed modulo a few small primes or prime squares. These filters cut down on the number of candidates for x and y. We will first show how to derive them for the form x^2+y^2, and then we will show how the filters can be modified for dealing with other quadratic forms.

A filter is derived from analyzing a quadratic form modulo a small number. There are only a few ways that residues of a small number can satisfy a quadratic form equation. This constrains the possibilities for x and y in The Method, and the mental factorer can just throw away the ones that don't meet the criteria. The following sections explain the method of candidate constraints.

Generally each filter requires the mental factorer to memorize a short table of information. In the following sections we explain how the tables are constructed. The advanced mental factorer should take care to understand the construction and to memorize the tables. Each one is short and the data has some symmetries and relationships that will be apparent with use.

This section uses notation such as $n/3 \mod 49$ to denote modular division. This means to find the least value $n+49i$ that is divisible by 3, compute the quotient $q = (n+49i)/3$, and compute the remainder of q divided by 49. For example, if n is 5, then i is 1, and $(5+1*49)/3 = 54/3 = 18 \equiv 18 \mod 49$.

7.7.1 Constraints for $n = x^2 + y^2$

Filter 1: last digit of n is 1 or 9 and $y^2 \equiv 25 \mod 100$. In solving $n = x^2 + y^2$ when n's last digit is 1 or 9, the set of candidates for x can be narrowed for the case of $y^2 \equiv 25 \mod 100$. This is worth knowing, because the number of possibilities for x is cut in half. When n has 5 or more digits, this eliminates a significant amount of mental strain (NB: the case of $y^2 \equiv 0 \mod 100$ must also be checked; this filter only with the first case).

We know that if a square number ends in the digits 25, then the hundreds digit is even; this means that $y^2 \equiv 25 \mod 200$. This can only happen if the hundreds digits of $n-25$ and x^2 are both even or both odd. So, we look at the hundreds digit of $n-25$ to see if it is even or odd. That forces a restriction on x^2.

We can restrict x^2 to have an odd or even hundreds digit as needed. Of the two possible x values less than 50, one will have a square with an even hundreds digit, and the other will have a square with an odd hundreds digit. We can eliminate the one that doesn't match and use the other to generate the potential x values.

The set S of candidates has members based on the set S_4 of low order digits modulo 100. We modify this set based on the parity of the hundreds digits of r^2 and $n-25$. If those hundreds digits are both even or both odd, then the set S_4 is $\{r, 100-r\}$. Otherwise, set $r' = 50-r$ and use $S_4 = \{r', 100-r'\}$.

In both cases, S_4 generates a set of candidates S that has only half as many candidates as it would without the filter.

Let's take a look at the example of 7789 in section 7.3.2. In that, we had a branch with $y^2 \equiv 25 \mod 100$. There we noted that $n - y^2 \equiv (89-25) \mod 100$, so we want to find squares ending in 64. The r value is 8 and the set S_4 is $\{8, 42, 58, 92\}$. The set of squares is $\{64, 1764, 3364\}$ (we can

eliminate 92 because its square is larger than our target number). The corresponding y^2 values are $\{7725, 6025, 4425\}$. We note that r^2 is 64, and its hundreds digit is 0, which is an even number. The hundreds digit of $7789 - 25 = 7767$ is odd. This means that we can replace r by $50 - r$ and proceed with $r = 42$. The corresponding set S_4 is simply $\{42, 58\}$. This reduction in trial candidates is very helpful when n is large, but because the filter is so easy to apply, it is worthwhile to use it even for 4 or 5 digit numbers.

When we are solving an equation that is the sum of squares, the possible values for the terms can be restricted by considering the equation modulo a small prime or prime square. Only half the residues can be the residues of squares, and the sum of the two square residues must be the same as the target number n. This analysis is simple to carry out, and it significantly cuts down on the number of possibilities for x and y. The next two filters illustrate the way to do this for $n = x^2 + y^2$. There are slight variations that work for $n = x^2 + 2y^2$ and $n = x^2 + 3y^2$ that we will discuss afterwards.

Filter 2: n modulo 3 and 9. For any $n = x^2 + y^2$ we can use information about the quadratic form modulo 3 and modulo 9 to develop restrictions on the candidates list that quickly eliminate a large fraction of them. We will concentrate on limiting the values for x because The Method for this quadratic form assumes that x is the variable for which the candidate set S is built.

The square squares modulo 3 are 0 and 1.

Because we eliminated all trivial factors, the possibilities for n are $n \equiv 1 \mod 3$ and $n \equiv 2 \mod 3$.

When n is 2 modulo 3, then it is easy to see that x^2 and y^2 must both be 1 modulo 3. This means that neither x nor y can be a multiple of 3.

When n is 1 modulo 3, we know that one of x and y is a multiple of three and the other is not. In the case that x is not divisible by 3 and y is divisible by 3, we know that $x^2 \equiv n \mod 9$. The squares modulo 9 are 1, 4, and 7, and the corresponding square roots are ± 1, ± 2, and ± 4. This constrains the possible values of $x \mod 9$.

These facts summarize how to filter candidate values for x:

- If n is equivalent to 2 modulo 3, neither x nor y is a multiple of 3. This eliminates one third of the x candidates.
- If n is equivalent to 1 modulo 3, then either x is a multiple of 3, or
  - If n is equivalent to 1 modulo 9, then x is $\pm 1 \mod 9$.
  - If n is equivalent to 4 modulo 9, then x is $\pm 2 \mod 9$.
  - If n is equivalent to 7 modulo 9, then x is $\pm 4 \mod 9$.

  This filter eliminates 4 of the possible residues modulo 9 for x.

Filter 3: n modulo 7 and 49. This filter rules out either 2 or 3 residues modulo 7.

We branch on n modulo 7. We note that the squares modulo 7 are 0, 1, 2, 4. To solve for squares $n = x^2 + y^2$, we must look for two squares that sum to n modulo 7. There are three easy cases that constrain $x \mod 7$ to one of four values:

- If n is 3 modulo 7, then $n = x^2 + y^2$ must be $3 = 1 + 2$, i.e., one of x^2 or y^2 is congruent to 1, the other is congruent to 2. This restricts the values of $x \mod 7$ to four possibilities: If $n \equiv 3$, then $x \equiv \pm 1$ or ± 3.

- If $n \equiv 5$, $5 = 1 + 4$, implying that $x \equiv \pm 1$ or ± 2.
- If $n \equiv 6$, $6 = 2 + 4$, implying that $x \equiv \pm 2$ or ± 3.

There are 3 other cases that constrain x to 5 possible values modulo 7:

- If n is 1 modulo 7, then the squares in the sum are $0 + 1$ or $4 + 4$, implying that $x \equiv 0, \pm 1, \pm 2$. Note that if $x \equiv \pm 1$, then $x^2 \equiv n \mod 49$; the values for this special case are tabulated below.
- If n is 2 modulo 7, then the squares in the sum are $0 + 2$ or $1 + 1$, implying that $x \equiv 0, \pm 1, \pm 3$. Note that if $x \equiv \pm 3$, then $x^2 \equiv n \mod 49$; the values for this special case are tabulated in the second table below.
- If n is 4 modulo 7, then the squares in the sum are $0 + 4$ or $2 + 2$, implying that $x \equiv 0, \pm 2, \pm 3$. Note that if $x \equiv \pm 2$, then $x^2 \equiv n \mod 49$; the values for this special case are tabulated in the third table below.

Optional extension of modulo 7 restriction to modulo 49. We can make use of the case $x^2 \equiv n \mod 49$ to reduce the filter's acceptance ratio from 5 out of 7 (71%) to 23 out of 49 (47%) using the tables that follow.

The formula for the allowable x values is given by the formula $u \equiv n$, and $x \equiv \pm(3u - 4) \mod 49$, shown in the table at right.

For $n \equiv 1 \mod 7$

n mod 49	x mod 49
1	±1
8	±20
15	±8
22	±13
29	±15
36	±6
43	±22

The formula for the allowable x values where $u \equiv n \mod 49$ and $x \equiv \pm(u - 12) \mod 49$, shown in the adjacent partial table.

For $n \equiv 2 \mod 7$

$n \mod 49$	$x \mod 49$
2	±10
9	±3
16	±4
...	...

In the last case, $u \equiv n \mod 49$ and $x \equiv \pm(2u-6) \mod 49$.

For $n \equiv 4 \mod 7$

$n \mod 49$	$x \mod 49$
4	±2
11	±16
18	±19
25	±5
...	...

For eliminating possible candidate values, you can use either or both modular restrictions (or neither). With practice you can work out the table values as needed instead of memorizing them.

Advantages combine if both restrictions are used. We later will show how to use the restrictions for the example of $n = 1000009$; in that case, the modulo 9 advantage is a 4/9 reduction in candidates. The modulo 7 restrictions reduce the candidates by 3/7. Together, they result in a 68% reduction.

When the low order digit of n is 3 or 7, the quadratic form that we use is $2n = x^2 + y^2$. Use the residue of $2n \mod 7$ or $2n \mod 9$ when computing restrictions.

As a rule of thumb, use modulo 9 for five digit numbers and both 9 and 7 (with 49) for six digit numbers.

A trick for mod 49. To use the tables, it is necessary to calculate n modulo 49, and this annoying subtask can be eased by viewing n as a sequence of two-digit pairs. For example, 314159 is 31, 14, 59. In general, if these digit pairs for a 6 digit number are denoted as A, B, and C, then the formula $(2 * A + B) * 2 + C \mod 49$ is equal to $n \mod 49$.

Using 314159 as an example, we can compute the terms and reduce modulo 49 as convenient:
$2 * A = 2 * 31 = 62$
$2 * A + B = 62 + 41 = 103$
103 modulo 98 is 5
$(2 * A + B) * 2 = 10$
$(2 * A + B) * 2 + C = 10 + 59 = 69$
69 modulo 49 is 20.

To check the result we can use the fact that 7 divides 1001 (see section 4). Note that $314 * 1001 = 314314$, and $314159 - 314314 = -155$. The remainder modulo 7 is -1 (which is the same as 6). We have already calculated 314159 modulo 49 as 20 (which is 6 modulo 7). Because the residues match, we have some assurance that the modulo 49 calculation was done correctly.

A famous example. Long ago, in 1778, Euler factored the number 1000009 using methods similar to those in this paper. You can see a translation of his description of how he accomplished this in "An inquiry into whether or not 1000009 is a prime number" at `https://arxiv.org/abs/math/0412062`. The original paper is "De numeris, qui sunt aggregate duorum quadratorum" and is available at EulerArchive.org. Euler relied heavily on facts about divisibility by 25 for his analysis, as does our Method. When we combine The Method with filters, we can derive the factors of 1000009 in far fewer operations than Euler used.

The number 1000009 is easily seen to be the sum of two squares ($1000^2 + 3^2$), and this constitutes one solution to the quadratic form $x^2 + y^2$. We can use The Method 7.2 to search for a second solution. Because the low order digit of n is 9, we refer to the section 7.3.2. The equation that we will work with is $1000009 - y^2 = x^2$. We can assume that y is divisible by 5. Looking at this modulo 100, we can see that if y^2 is 0 modulo 100, then $r^2 \equiv 9 \mod 100$, and thus r is congruent to $\pm 3 \mod 50$. If y^2 is 25 modulo 100, then r is congruent to ± 22 modulo 50. The set of candidate values for x is $\{50j \pm 3, 50j \pm 22\}$, where each candidate is less than the square root of 1000009 (about 1000). That results in about 80 candidate numbers, and testing them would use a lot of mental calculation.

The three filters will cut this down to about 20 candidates:

- Filter 1: Noting that $x = 50j \pm 22$ when y is an odd multiple of 5, we look at the $r = 22$ case. Because parity of the hundreds digit of r^2 does not match the parity of the hundreds digit of $n - 25 = 999984$, we can replace r by $50 - r = 28$ and use the x candidate set $\{50j \pm 3, 100j \pm 28\}$.

- Filter 2: For $n \equiv 1 \mod 9$, x is either a multiple of 3 or $\equiv \pm 1 \mod 9$.
- Filter 3: For $n \equiv 3 \mod 7$, either $x \equiv \pm 1 \mod 7$ or $x \equiv \pm 3 \mod 7$.

Finally, we work from top down for potential x's because the chances of a successful y^2 are greater for small y's. This is because we already know one solution. We can stop if we hit a second, so testing the mostly likely values earlier will pay off on average. If it should turn out that 1000009 is prime, there's no second solution, and we must check the whole range of x. This is the same amount of work in either direction.

We interleave the two sequences so that the candidates are tested largest to smallest. Our testing order for the candidate set $\{50j \pm 3, 100j \pm 28\}$ becomes 997, 972, 953, 947, 928, 903, 897, 872, ..., 47, 28, 3.

The filter for 3 and 9 tells us that 997 can be eliminated because it is not $\pm 1 \mod 9$.

972 is multiple of 3, and it is also equal to -1 modulo 7. We plug it into the equation $1000009 - x^2 = y^2$ and find that $1000009 - 972^2 = 55225$. Because $552 = 23 * 24$, we know that 55225 is a square. Thus, we have a second solution, $972^2 + 235^2$. We can combine the (x, y) pairs (1000, 3) and (972, 235) to find a factor. A pairwise subtraction results in (28, -232). We can remove the common factor of 4, yielding (7, -58). Plugging those back into $x^2 + y^2$, we get $49 + 3364 = 3413$. Does this divide 1000009? We can see that the quotient is just shy of 300. The greatest number less than 300 that would make the last digit of the product come out to be 9 is 293. Indeed, $300 * 3413 = 1023900 = 1000009 + 23891 = 1000009 + 7 * 3413$. This shows that 3413 is a divisor, and $1000009 = (300 - 7) * 3413 = 293 * 3413$.

If we had continued testing candidate values, we would have found
953 is a valid candidate
947 is not a multiple of 3 and is not $\pm 1 \mod 9$
928 is a valid candidate
903 is neither ± 1 nor $\pm 3 \mod 7$
and so on, ...
28 is neither ± 1 nor $\pm 3 \mod 7$
3 is a valid candidate.

7.7.2 Constraints for $n = x^2 + 2y^2$

As with $n = x^2 + y^2$, it is often helpful to look at the quadratic form equation with different moduli in order to find simple constraints on x and y.

Filter 1: working modulo 400. When this filter is applicable, it eliminates half of the trial x values. It applies to situations where Table 2 indicates that y is an odd multiple of 5.

We can use the fact that $2y^2 \equiv 50 \mod 400$ to get a handle on allowable values of x. Note that this implies that the thousands and hundreds digits of $2y^2$, viewed as a two digit number, is a multiple of 4. Example: if $y = 35$, then $2y^2 = 2450$, and 24 is a multiple of 4. We will call the thousands-hundreds digit combination $H(n)$. The short pattern of residues modulo 4 of $H(x^2)$ for x candidates will dictate how to eliminate half of the x candidates quickly.

We know the low two digits of x^2 from the formula $n - 2y^2$. Take $H(n - 50)$ and reduce it modulo 4. This must be equal to $H(x^2) \mod 4$. Our set of trial values for x is $\{50j \pm r\}$ with r odd. If we square the successive values of x (by incrementing j) and look at the modulo 4 residue of the H value, there are only six possible patterns, each of length 8, each with only two residue values:

$n \mod 9$	1	4	7	2	5	8
$x \mod 9$	± 1	± 2	± 4	0, 3, or 6	0, 3, or 6	0, 3, or 6
$y \mod 9$	0, 3, or 6	0, 3, or 6	0, 3, or 6	± 1	± 4	± 2

Table 3: $n = x^2 + 2y^2$ for n not divisible by 3

0022 2200
2200 0022
0202 2020
1133 3311
1313 3131
3311 1133

Given the first two values of a sequence, the rest is easily determined. Note that the first four values are reflected backwards in the second half. If the first two values are the same, then the third value is the first value plus 2 modulo 4, and the fourth value is the second value plus 2 modulo 4. If the first two values are different then the next two values are copies of the first two.

From the squares of the first two H values of $\{50j \pm r\}$, we can determine the whole sequence, and because we know the value of $H(n-2y^2)$, we can eliminate any candidate that does not match that value.

Example: suppose we have an $n = 8j + 3$ number ending in 71, such as 12371. Then y must be an odd multiple of 5, and $2y^2$ ends in 50, x^2 must end in 21, and our set of trial x values is $\{50j \pm 11\}$.
The trial x values are 11, 39, 61, 89, 111, ...
The squares are 121, 1521, 3721, 7921, 12321, ...
The H digits are 1, 15, 37, 79, 23, ...
Reduced modulo 4, these are 1, 3, 1, 3, 3, ..., matching the pattern 1313 3131.

We see that $H(12371 - 50)$ is 23, and the residue modulo 4 is 3. Therefore we can discard the x values that generate squares such that $H(x^2) \not\equiv 3 \mod 4$. This eliminates these values for x: 11, 61, 139, 189, 211, 261, 389, and admits these values: 39, 89, 111, 161, 239, 289, ...

Filter 2, modulo 3 and 9: If n is a multiple of 9, skip this filter, it is not helpful.

Assume that n is not a multiple of 9. Compute $n \mod 3$.

When n is a multiple of 3 but not of 9, then both x and y are not multiples of 3.
When n is not a multiple of 3, then one of x or y is a multiple of 3, and the other is not. If $n \equiv 1 \mod 3$, compute w such that $w^2 \equiv n \mod 9$; then y is the multiple of 3, and $x \equiv \pm w$.
If $n \equiv 2 \mod 3$, then compute $w^2 \equiv 5n \mod 9$; x is the multiple of 3 and $y \equiv \pm w \mod 9$. This information is summarized in Table 3.

While using The Method, you can reject candidates for x and y that do not satisfy the forms in the table.

In the usual case, n is not a multiple of 3, and this filter gives a strong restriction on both x and y. The method is works with one of x or y; use the appropriate filter to discard the majority of trial values.

This filter is also applicable to $3n = x^2 + 2y^2$, but it is less selective.

Filter 3, modulo 7 and 49. We examine the equation $n = x^2 + 2y^2$ modulo 7. 2 is a square mod 7, so $2y^2$ is also a square. The analysis from the form $n = x^2 + y^2$ is a guide. The x values are unchanged, but $2y^2$ must replace y^2, and the y values are different. Because the quadratic form is not symmetrical in x and y, different restrictions apply to each variable. Using the method for $x^2 + 2y^2$, determine which of x or y is being trialed. Use the appropriate restriction.

In the following cases, all values are modulo 7:
When n is a non-square:
Case $n = 3$:
The 3 splits into two squares, 1+2.
One of these is x^2 and the other is $2y^2$.
Either $x^2 = 1$ and $2y^2 = 2$, or $x^2 = 2$ and $2y^2 = 1$.
$x = \pm 1$ or ± 3, and $y = \pm 1$ or ± 2.
Case $n = 5$:
$5 = 1+4$.
Either $x^2 = 1$ and $2y^2 = 4$, or $x^2 = 4$ and $2y^2 = 1$.
$x = \pm 1$ or ± 2, $y = \pm 2$ or ± 3.
Case $n = 6$:
$6 = 2+4$.
Either $x^2 = 2$ and $2y^2 = 4$, or $x^2 = 4$ and $2y^2 = 2$.
$x = \pm 2$ or ± 3, $y = \pm 1$ or ± 3.
When n is a square:
Case $n = 1$:
The split is either 0+1 or 4+4, and $x = 0, \pm 1^*, \pm 2$, $y = 0, \pm 2^*, \pm 3$.
Case $n = 2$:
$2 = 0+2$ or $1+1$.
$x = 0, \pm 1, \pm 3^*$, $y = 0, \pm 1^*, \pm 2$.
Case $n = 4$:
$4 = 0+4$ or $2+2$.
$x = 0, \pm 2^*, \pm 3$, $y = 0, \pm 1, \pm 3^*$.

Example: let $n = 12371$. To use the modulo 7 filter, we compute $n \equiv 2 \mod 7$. Consulting the above lists, we determine that $x = 0, \pm 1, \pm 3$, and that $y = 0, \pm 1, \pm 2$.

Each restriction accepts 5 out of 7 of the possible values for x or y.

When n is a square modulo 7, we can use values modulo 49 to get tighter constraints on x and y, in a method similar to to Filter 3 for $x^2 + y^2$ in a previous section. This method applies if $x^2 = n \mod 7$ or if $2y^2 = n \mod 7$.

These values are marked with an asterisk in the lists above. In this case, the marked residue may be replaced with a mod 49 residue. The modulo 49 residue is computed as $x \equiv \pm w$, where $w^2 \equiv n \mod 49$, or $y \equiv \pm w$ where $w^2 \equiv n/2 \mod 49$ (see the note about modular division at the beginning of section 7.7).

Because n modulo 7 is 2, and that is a square modulo 7, we can use the modulo 49 filter. The formula for Filter 3 in section 7.7.2 show that the square root for n modulo 49 is $\pm(n - 12)$. Using the 'Trick for Mod 49" at the end of that section, we compute $n \equiv 23 \mod 49$ and see that its root is ± 11. We then see that $n/2 \equiv 1 \mod 7$ and $n/2 \equiv 36 \mod 49$, which shows that the square root of $n/2 \mod 49$ is 6.

Our updated restrictions are:
$x = 0, \pm 1, \pm 3$, and when $x = \pm 3$ it must also be equal to $\pm 11 \mod 49$.

$y = 0, \pm 1, \pm 2$, and when $y = \pm 1$, it must also be $\pm 6 \mod 49$.

The extra restriction reduces the filter's acceptance rate from 5 out of 7 (71%) to 23 out of 49 (47%).

See the tables in section 7.7.1 for computing square roots modulo 49.

7.7.3 Constraints for $n = x^2 + 3y^2$

The possibilities for x and y can be constrained, as before, by looking at the possibilities modulo 3 and modulo 7.

Filter 1: This filter is similar to the $x^2 + y^2$ Filter 1. It is useful only for the form $n = x^2 + 3y^2$ when the tens digit of the target n is odd. If this is true, then the filter cuts the number of candidates in half. It does this by generating the set S of candidates from the set $\{100j \pm r\}$ instead of $\{50j \pm r\}$. This may entail using a different value of r, as we explain below.

Table 1 or 2 will tell us which of x or y is the multiple of 5 (it will be an odd multiple); the other is the one for which we generate the candidate list.

We can compute the last two digits of the term x^2 or $3y^2$ using the formula $x^2 = n - 3y^2$ or $3y^2 = n - x^2 \mod 100$ respectively. The other variable must be an odd multiple of 5, so its square ends in 25, and the hundreds digit is even. If the other variable is y, then the $3y^2$ term will end in 75, and still have an even hundreds digit. In either case, we look at the hundreds digit of $n - 25$ or $n - 75$, and determine its parity. The hundreds digit of the quadratic form term (x^2 or $3y^2$) must have the same parity. The set S of candidates is $\{50j \pm r\}$, and the first trial number is r. Examine the hundreds digit of r^2 if we are working with x, or $3r^2$ if we are working with y. If it has the wrong parity, replace r with $50 - r$, which will lead to the matching parity. In either case, the trial set S is now $\{100j \pm r\}$.

Example: $n = 12391$. We consult table 1 and see that for $n \equiv 7 \mod 24$, the quadratic form $x^2 + 3y^2$ applies. The table further shows that if the last digit of n is 1, then 5 divides y and y is an odd number. We will develop a candidate list for x.

The final digits of x^2, computed from $n - 75 \mod 100$, are 16, implying that r is 4. The candidate set S is $\{50j \pm 4\}$. The tens digit of n is 9, an odd number, so we can use Filter 1 to eliminate half the values in S. The hundreds digit of $n - 75$ is 3, an odd number. We compute $r^2 = 16$ and note that the hundreds digit is 0, which is even, so we replace r with $50 - r = 46$. Our trial set S is now $\{100j \pm 46\}$.

Example: $n = 21733$. This is a $4k + 1$ number, but The Method will fail if we use the $x^2 + y^2$ form indicated in table 1. The "retry" form in table 2 for $n \equiv 1 \mod 12$ is $n = x^2 + 3y^2$. Because the last digit 3 of n is 3, we know that 5 divides x and x is odd. We will develop a list of candidates for y.

The tens digit of n is 3, an odd number, so we can apply Filter 1. The final digits of $3y^2$ are the same as the final digits of $n - x^2 \mod 100$, i.e. 08. The final digits of y^2 are 36, implying that r is 6. The trial set S is $\{50j \pm 6\}$. The hundreds digit of $n - 25$ is 7, which is odd, and $3r^2 = 108$, whose hundreds digit is 1, also an odd number. The trial set S is $\{100j \pm 6\}$.

Filter 2: modulo 3 and 9. We know that x cannot be a multiple of 3 because then $n = x^2 + 3y^2$ would also be a multiple of 3, and we have previously eliminated all small divisors.

This filter restricts x for $n \equiv 1 \mod 3$. The term $3y^2 \mod 9$ can be either 0 or 3. Because $x^2 = n - 3y^2$, we can derive the modulo 9 congruences $x^2 = n$ or $x^2 = n - 3$.

$n \mod 9$	$x \mod 9$
1	± 1 or ± 4
4	± 1 or ± 2
7	± 2 or ± 4

Table 4: Constraints modulo 9 for $n = x^2 + 3y^2$

$n \mod 7$	$x^2 + 3y^2$	$x \mod 7$	$y \mod 7$
3	$0+3, 4+6$	$x = 0, \pm 2$	$y = \pm 1^*, \pm 3$
5	$0+5, 2+3$	$x = 0, \pm 3$	$y = \pm 1, \pm 2^*$
6	0+6, 1+5	$x = 0, \pm 1$	$y = \pm 2, \pm 3^*$
1	1+0, 2+6	$x = \pm 1^*, \pm 3$	$y = 0, \pm 3$
2	2+0, 4+5	$x = \pm 2, \pm 3^*$	$y = 0, \pm 2$
4	4+0, 1+3	$x = \pm 1, \pm 2^*$	$y = 0, \pm 1$

Table 5: Modulo 7 combinations for $x^2 + 3y^2$

Table 4 shows the possible values for $x \mod 9$ based on the value of $n \mod 9$.

Filter 3: working modulo 7 and 49. This filter accepts either 3 out of 7 (43%) or 4 out of 7 (57%) candidates.

All values are reduced modulo 7, except when marked modulo 49.

The constraints on x and y modulo 7 are summarized in Table 5. To use this filter, note the remainder of n modulo 7 and lookup the possible remainders for x and y. While analyzing n with The Method, reject any x or y candidates that do not meet the constraints in the table.

As before, those residues marked with an asterisk can be further examined modulo 49.

Filtering modulo 49. Residues marked with an asterisk can be addressed through a modulo 49 restriction.

When n is a square modulo 7 (i.e., 1, 2, or 4), x can be further constrained by the condition $x \equiv \pm w \mod 49$ where $w^2 \equiv n \mod 49$. This is applicable when Table 1 indicates that 5 divides y.

When n is not a square modulo 7, y can be further constrained: $y \equiv \pm w \mod 49$ where $w^2 \equiv n/3 \mod 49$. This is applicable when Table 1 indicates that 5 divides x.

This filter removes even more candidates. If modulo 7 accepted 4 out of 7 (57%) cases, this accetps 16 out of 49 (33%).

Example: $n = 12343$.

Because the residue of n modulo 24 is 7 and the last digit is 3, we consult Table 1 and use the quadratic form is $x^2 + 3y^2$ with The Method. Table 1 notes that that x is an even multiple of 5 (i.e., a multiple of 10); thus x^2 is a multiple of 100. The low order two digits of $3y^2$ must match n, so $3y^2 \equiv 43 \mod 100$, and $y^2 \equiv 81 \mod 100$. The set of candidates for y is $\{50j \pm 9\}$, i.e., $\{9, 41, 59, 91, \dots\}$. The upper bound for y is $\sqrt{n/3} \approx 64$.

We can apply Filter 3:

$n \equiv 2 \mod 7$ and 2 is a square modulo 7.

From Table 5 we see that $y = 0, \pm 2 \mod 7$.

$y = 9$: This is 2 mod 7 which passes the filter.
$y = 41$: This is -1 mod 7 which fails the filter and can be discarded.
$y = 59$: This is 3 mod 7 which fails the filter and can be discarded.

Setting $y = 9$, in the formula $x^2 = n - 3y^2$ implies $x^2 = 12100$, a square. The pair (110,9) is the single solution to $n = x^2 + 3y^2$ using The Method.

To complete the example, we must also look at $4n = x^2 + 3y^2 = 49372$. By Table 1, both x and y are odd; x is the multiple of 5, thus x^2 will end in 25.

We examine the equation $3y^2 \equiv 4n - x^2 \mod 100$. $3y^2 \equiv 72 - 25 \equiv 47 \mod 100$, so $y^2 \equiv 49 \mod 100$. The candidates for y are $\{50j \pm 7\}$, i.e. 7, 43, 57, ...

We can now apply Filter 3.
$4n = 1 \mod 7$, and 1 is a square modulo 7.
The y constraint is $y = 0, \pm 3 \mod 7$.
The upper bound on y is $\sqrt{4n/3} \approx 128$.
$y = 7$: This is 0 modulo 7, and it passes the filter.
$y = 43$: This is 1 modulo 7 which fails the filter and can be discarded.
$y = 57$: This is 1 modulo 7 which fails the filter and can be discarded.
$y = 93$: This is 2 modulo 7 which fails the filter and can be discarded.
$y = 107$: This is 2 modulo 7 which fails the filter and can be discarded.
$y = 143$: is too big. The only possible y value is 7. Trying it, we see that $x^2 = 4n - 3y^2 = 49372 - 147 = 49225$. A quick check shows that 492 is not the product of two consecutive integers: the square root of 492 is slightly larger than 22, so the only possibility is $22 * 23$, but this product's last digit is 6, not 2.

The Method yields no solutions to $4n = x^2 + 3y^2$. The pair that we found for $n = x^2 + 3y^2$, (110,9), is the single solution. After checking that $\gcd(110, 9) = 1$, we can conclude that 12343 is prime.

8 Alternative methods

Powerful as The Method (section 7.2) is, it does not always find a representation of n as a quadratic form. For some n, there is no applicable quadratic form, and even for the n that do have one, 18% of these numbers up to one million have no representation using the quadratic forms in Table 1. There are roughly 20,000 "difficult" numbers in this range. For these, we have other methods. "The 120 Method" (section 8.1) is a heuristic method, and the second method, "Difference of Squares" (section 8.3), is deterministic. We recommend trying the heuristic method first, especially for numbers of the form $4i + 3$, because it is easier. Difference of Squares is the method of last resort.

If you have tried a quadratic form method and found no decompositions, then the number is composite, so usually when you use the methods in this section, you will be dealing with a composite number.

8.1 The 120 Method

The theoretical underpinnings of quadratic form analysis are based on the existence of square roots in a quadratic number field extension. This section describes a heuristic method for finding small squares in $Z[n]$. If 2, 3, and 5 (and sometimes -1) are squares, then we can derive a definite expression for potential divisors. As in The Method, the expression generates only a manageable number of potential divisors.

The method for searching for squares modulo n uses the form $kn = ax^2 + by^2$. We will describe how to vary k, a, and b to facilitate the search.

NB: This method is most likely to work for numbers of the form $4i + 3$. It can be applied to $4i + 1$ numbers, but the chance of success is only 1 in 8. If you have already tried The Method on a $4i + 1$ number and found no decompositions, then you know that it is composite. In that case, if the number has more than 5 digits, the best option is to proceed immediately to the Difference of Squares method in section 8.3.

This method is inspired by a theorem: If p is a $4i + 3$ prime, and c is any positive number less than p, then one of c or $-c$ is a square modulo p, and the other is not a square.

If p is a $4i+1$ prime, things are a little more complicated. If $p \equiv 1 \mod 120$ or $p \equiv 49 \mod 120$, then all six of $\pm 2, \pm 3, \pm 5$ are squares. The general case for prime p, $p = 4i + 1$, $n > 5$ is that ± 2 are squares modulo p when $p \equiv 1 \mod 8$, ± 3 are squares when $p \equiv 1 \mod 12$, and ± 5 are squares when $p \equiv 1 \mod 20$ or $p \equiv 9 \mod 20$.

For any positive n where $n \equiv 3 \mod 4$, if any of ± 2, ± 3, or ± 5 are squares modulo n, we can restrict the possible divisors of n using techniques illustrated below (for $n \equiv 1 \mod 4$, it is helpful to know if -1 is a square). We can use some clever tricks to search for squares modulo n using mental arithmetic.

The search method looks for the existence of solutions to equations of the form $kn = ax^2 + by^2$. If such a solution exists, then then one of $\pm ab$ is a square modulo n, and we remember the value ab. As we build up a set Q of these ab values, we also compute their closure (as explained below). If we can establish that all three ab values from the set $\{2, 3, 5\}$ (and sometimes -1) are in that closure, then there is a way exclude most primes as divisors of n. If we cannot establish the set of ab values, then n is probably composite and can be factored using Difference of Squares in section 8.3.

The Method redux. If you have used The Method for the target number n, then you might have already found some useful solutions for one or two particular $kn = ax^2 \pm by^2$ forms; for example, $3n = x^2 + 2y^2$. Perhaps you noticed that for $n = 2351$ and $y = 58$, $3n - 2y^2 = 325 = 13 * 5^2$. Although that relationship was not useful in The Method (because $13 * 25$ is not a square), it is useful now because it establishes that $-2 * 13$ is a square modulo n. That is why we recommend that immediately after concluding that The Method yields no decompositions for n, you go back and redo the same calculations, this time taking note of any cases in which $kn - ax^2 = by^2$ is the product of a small number times a square or is the product of small primes. For each case, put $-ab$ into the set Q and form the closure of Q as explained below. Then proceed with this new search method.

As with all methods in this paper, we assume that prime factors up to 31 have been removed from the target number. If n is greater than a million, remove any prime factors up to $\sqrt[4]{n} = \sqrt{\sqrt{n}}$.

The 120 search method. The required squares for a $4i+3$ number are 2, 3, and 5. The required squares for a $4i + 1$ number are -1, 2, 3, and 5.

1. Assign small integer values to k and a.
2. Using the form $kn = ax^2 + by^2$, vary x and look for a solution in which $kn - ax^2$ is the product of a square and a small prime. If you find such a solution, add $-ab$ to the set Q and form the closure (see below). When Q includes the required squares, proceed to step Phase IIa (step 4).

The general strategy for selecting the coefficients and looking for a solution is to select k, a, and x such that $kn \approx ax^2$. That difference is much smaller than n, and it should be easy to determine if it is a small multiple of a square. The initial value for x is an integer near $\sqrt{kn/a}$. Try varying x by small increments for a few steps to see if it yields a solution.

3. If Q does not have the required squares, go to Step 1 and choose different coefficient values. Advice on useful ways to do this follows in sections 8.1.1 and 8.1.2. If you have tried more than a few values without getting the required squares, go to step 5. If Q does have the required squares, then we say that we have finished Phase I.
4. Phase IIa. Having determined that the set Q has the required squares we know that the set S of potential divisors is described by
   - For a $4i + 3$ number: $120j + \{1, 49, d, e\}$ where $d = n \mod 120$, $e = 60 - 11d \mod 120$ and j goes from 0 to $\sqrt{n}/120$.
   - For a $4i + 1$ number: $120j + \{1, 49\}$ where j goes from 0 to $\sqrt{n}/120$.

   For each prime number in the set, check to see if it divides n. This is not easy – it's why we've gone to so much work to make the set small. In the worst case, this will require testing as many as 20 numbers (a good workout!).

   If you find a divisor, then the only task remaining is to factor the co-factor n/p. We have a headstart on that because the potential divisors of n/p are the same as the potential divisors of n. So, we continue testing members of S, starting with the prime that we just found, p to see if they divide the co-factor.

   If none of the primes in the potential divisor set divides n, then n is prime.
5. If Q has only 2 values from the required set (and -1 if n is 1 modulo 4), each less than or equal to 10, then that might be enough information to test all potential divisors less than $\sqrt{n}$. This is Phase IIb, and section 8.2 describes the formulas that determine the divisor set. Using that, you might either find a divisor or rule out all divisors. This is not an especially efficient approach, and we only recommend doing it for numbers of 5 digits or fewer. If n is 6 digits, or if you do not complete the full Phase IIb search, proceed to Difference of Squares (section 8.3).
6. If Q has fewer than 2 values that are less or equal to 10, then proceed to the method of last resort: Difference of Squares (section 8.3).

Closure of the set Q. For the set Q, when $n \equiv 3 \mod 4$, we don't need to keep track of the signs of ab, so we only include positive numbers. Each entry represents both itself and its negative. The set Q automatically includes all the actual squares 1, 4, 9,.... We ignore them, and usually won't bother mentioning them. Q is also closed under multiplication: If f and g are in Q, so is fg. Q is also closed under division when the division is exact: If f and g are in Q, and f divides g exactly, then g/f is in Q. We call the last rule FGH: if f and g have a common factor h, then fg/h^2 is in Q. The steps below will show how to search for more squares modulo n. The closure rules will let us combine squares into new squares.

Example: Assume $Q = \{6, 14\}$. If we have a new element, 42, to add to this set, we first use the closure rule for division of an element in Q and a new element: if f is in Q and m is a new element, then if $f|m$, f/m is in Q. We can divide 42 by an existing element of Q, namely 14, and add 3 to $Q = \{3, 6, 14, 42\}$. We can also divide 42 by 6 and then include the quotient, 7, in $Q = \{3, 6, 7, 14, 42\}$. Because 3 divides 6, we can include 6/3 in $Q = \{2, 3, 6, 7, 14, 42\}$. We can

remove any number if all its prime factors are members of Q. That means that we can take out 6, 14 and 42, $Q = \{2, 3, 7\}$.

Any number that is the product of numbers already in Q does not need to be added to the set.

If 27 were a new member to add to Q, we would divide out its square factor, 9, and only consider $27/9 = 3$ as a new member of Q.

Another example illustrates ways to keep Q to a minimal, easily memorized size. Suppose that we have these factor groups for creating Q:
3 * 5
5 * 7
3 * 17
7 * 13
5 * 13
As a memory aid, it's best to choose 3 times each of the other primes as primary, and regard the other pairs as implicit. So we'd retain 15, 21, 39, and 51 as a "generating set" and move the other pair products into the background. The background numbers like 65 are still members of Q; if needed, we can recreate them with the FGH rule applied to $15 = 3 * 5$ and $39 = 3 * 13$. Another way to think of this is that $\{3, 5, 7, 13, 17\}$ is a "subset-in-waiting" for Q. If we ever get one of these primes alone in a factorization, such as $5 * k^2$, we can merge the entire set into Q. (If we already have one of these primes alone in Q, then the whole subset can be merged into Q.) In any factorization, we can delete pairs of these factors because all the pair products are implicit members of Q. If we learn additional products which are the product of a subset member and another prime, such as $7 * 11$, we can add the other prime into the subset.

Negatives for $n \equiv 1 \mod 4$. If $n \equiv 1 \mod 4$, we will need to be aware of signs of the squares. The closure rules still apply as written, but we have to keep track of signs. If we know that 2 and -3 are squares modulo n, then so is -6. Much depends on whether the set Q contains -1. This is automatic when we have a solution to $n = x^2 + y^2$ with x and y relatively prime, or if any multiple of n has a solution. We might also discover -1 as part of building the set Q: If we find that both f and $-f$ are in Q, then the closure rules give us -1 as the quotient $(-f)/f$. If and when we discover that -1 is in Q, we can now forget about the signs, just as in the $4i + 3$ case. Keep the -1 in Q as a reminder, but make everything else positive.

This first example describes a search method that makes guesses for x and a where a is a small prime. If $kn - ax^2$ is a multiple of square number, by^2, then we know that ab is a square modulo n. Later sections discuss slightly different search methods that use a fixed a or other constraints on a or functions of a and b.

Example 1: $n = 56843$
We will find that one of ± 2 is a square modulo 56843, and similarly for ± 3 and ± 5. This restricts the set of potential divisors to $120j + \{1, 49, 83, 107\}$. We try primes in this set as potential divisors, up to $\sqrt{n} \approx 238$. The primes to be tested are 83, 107, and 227. None turns out to be a divisor, and we conclude that 56843 is prime.

For analyzing $n = 56843$ to illustrate the algorithm, we start by setting $k = 3$ and noting that $3n = 170529$. Because n is a $4ki + 3$ number, we can ignore signs in Q.

Begin the search by guessing that x is 1. Then $170529 - 1 = 2 * 85264 = 2 * 292^2$. We can rewrite this as $2 * 292^2 + 1 * 1^2 = 3n$. The product of the coefficients of the squares is $2 * 1$, implying that one of ± 2 is a square modulo n. We do not need to know the sign, and we do not need to

calculate the square root.

Next, observe that $3n + 40 = 170569 = 413^2$. This yields $1 * 413^2 - 10 * 2^2 = 3n$. The product of the coefficients is $1 * 10$, so we know that ± 10 is a square modulo n. Because ± 2 is also a square, we can divide it into ± 10 and establish that ± 5 is a square modulo n.

Thirdly, note that $n - 3 * 8281 = n - 3 * 91^2 = 32000 = 5 * 80^2$. Rearranging this, we see that $n = 3 * 91^2 + 5 * 80^2$. The product of the coefficients is 15, implying that ± 15 is a square modulo n. Because we already showed that ± 5 is a square modulo n, we can divide it out and show that ± 3 is also a square modulo n.

Having shown the required three squares, we now analyze $n \equiv 83 \mod 120$ in order to find trial divisors of n. We need to have a set of four residues modulo n. One of the residues is $n \mod 120$, two others, 1 and 49, are always in the set. The fourth can come from table lookup or a short calculation based on small multiples of 24: we add or subtract a small multiple of 24 to n modulo 120 in order to find the tens complement of the last digit.

Consider $83 - 3 * 24 = 83 - 72 = 11$
$83 - 2 * 24 = 83 - 48 = 35$
$83 - 1 * 24 = 83 - 24 = 59$
$83 + 1 * 24 = 83 + 24 = 107$

Because the low order digit of 107 is 7, and $7 + 3 = 10$, we have found a number whose low order digit is the tens complement of 3.

Alternatively, we can find the fourth residue by calculating $n + 60 - (12 * U)$ where U is the units digit of n. If this is not in the range $0 \ldots 120$, then add or subtract 120 to bring it into range.

The trial divisors will be of the form $120j + \{1, 49, 83, 107\}$.

A table of trial divisors of 56843:

divisor form	value	analysis
1	1	not useful
49	49	already excluded 7
83	83	possible divisor, mental division, fails
107	107	possible divisor, mental division, fails
$120 + 1$	121	divisible by 11, already excluded
$120 + 49$	169	divisible by 13, already excluded
$120 + 83$	203	divisible by 7, already excluded
$120 + 107$	227	possible, mental division, fails
$2 * 120 + 1$	241	greater than $\sqrt{n}$, ends search

Trial divisors of the example 56843

Because we found three squares modulo n in $\{\pm 2, \pm 3, \pm 5\}$, and we did not find a divisor, we know that $n = 56843$ is prime.

For reference we provide this useful table for calculating the tens complement of the non-trivial $4i + 3$ relatively prime residues of 120. The residue of $n \mod 120$ will occur in one of the pairs. The tens complement match is the other element of the pair:
{7, 103}
{11, 59}
{19, 91}

{23, 47}
{31, 79}
{43, 67}
{71, 119}
{83, 107}

Example 2: $n = 16147$

Note that $n \equiv 3 \mod 4$

Using the methods below for choosing k and a, we can find three representations of n. By looking at squares near n with $k = 1$ and $a = 1$ we see that

$n = 16129 + 18 = 127^2 + 2 * 3^2$.

Therefore, we can add the ab value $1 * 2$ to $Q = \{2\}$

Another square value near n

$n = 17161 - 1014 = 131^2 - 6 * 13^2$

from which we see $a = 1$, $b = 6$, $ab = 6$, and $Q = \{2, 6\}$. From the closure rules, we can include $6/2 = 3$ in Q, so $Q = \{2, 3, 6\}$

Using $k = 1$, and having a good memory for multiples of small squares, we come across

$n = 16000 + 147 = 10 * 40^2 + 3 * 7^2$

giving us $a = 10$, $b = 3$, $ab = 30$, and $Q = \{2, 3, 6, 30\}$.

Using the closure rules, we can include $30/6 = 5$ in Q, so now $Q = \{2, 3, 5, 6, 30\}$.

We can stop here because 2, 3, and 5 are in Q. Following step 4, our list of candidate factors is $120i + \{1, 49, d, e\}$.

$d = n \equiv 67 \mod 120$

$e = 60 - 11 * 67 = -677 \equiv 43 \mod 120$. The candidate list becomes $120i + \{1, 43, 49, 67\}$. We try x candidates starting with $i = 0$ up to $\sqrt{n} \approx 127$.

1 useless

43 trial division, fails

49 not prime, skip it

67 bingo!

$n = 67 * 241$.

We need to check that 241 is prime. But we've already checked for divisors up to 31, and $\sqrt{241} \approx 15$ is less than 31, so 241 must be prime.

8.1.1 Choosing k and a.

We have shown some examples of analyzing divisibility using equations of the form $kn = ax^2 \pm by^2$, but we have not discussed how to choose the coefficient k or what the consequences of the choice might be. This is a heuristic process with no single order of investigation dominating the algorithms. We present a few "tricks of the trade" that can be useful.

In each case, we examine $|kn - ax^2|$ and divide out prime factors less than 20. We are looking for cases where the result is either 1 or a square. If it is, the result will be added to the set Q using the closure rules.

- **Try to find a square that is close to the target number.** Set $k = 1$ and $a = 1$ so that $n = x^2 + by^2$. Investigate possible solutions to $n - x^2 = by^2$ by choosing x^2 values that are close to n. Try dividing the difference by small primes, looking for a result that is a square.

  If n has 4 digits, try primes less than 20; if n has 5 digits, try primes less than 35; if n has 6 digits, then try primes less than 50. Dividing a 6 digit number by, say, 43, is a challenging

mental task, but it can be mastered with practice.

Example 6667:

$\sqrt{n} \approx 81.6$. Try $x = 78 \ldots 84$.

x	x^2	$n - x^2$	factors	Q candidate?
78	6084	583	11*53	
79	6241	426	6*71	
80	6400	267	3*89	
81	6561	106	2*53	
82	6724	-57	3*19	yes
83	6889	-222	6*37	
84	7056	-389	prime	

We have one solution, with $k = 1$, $k * n = 6667$, $a = 1$, $b = -57$, $-ab = 57$, $x = 82$, and $y = 1$. We would add 57 into $Q = \{57\}$.

- **Use $a = 1$ with a small k value.**

  In the equation $kn = ax^2 + by^2$, set $a = 1$, and try k values from 2 through 7.

  E.g. $2n = x^2 + by^2$. Test 7 values, $w[0-6]$ for x, centered on $\sqrt{2n}$. Compute $kn - \{w[i]\}^2 = v$. If all the prime divisors of v are small, or if v has a large square factor, then $2n - v^2 = by^2$. We are free to choose b and y, so we set y^2 equal to the largest square divisor of v and $b = v/y^2$. The absolute value of b is added to the set Q of known squares modulo n using the closure rules.

  Example 6667:

  $k = 2$, $k * n = 13334$, $\sqrt{kn} \approx 115.5$

x	x^2	$n - x^2$	factors	Q candidate?
112	12544	790	10*79	
113	12769	565	5*113	
114	12996	338	2*13*13	yes
115	13225	109	prime	
116	13456	-122	2*61	
117	13689	-355	5*71	
118	13924	-590	10*59	

  We have one solution, with $k = 2$, $k * n = 13334$, $a = 1$, $b = 2$, $-ab = -2$, $x = 114$, and $y = 13$. We add 2 to $Q = \{2, 57\}$.

  $k = 3$, $k * n = 20001$, $\sqrt{kn} \approx 141.4$.

x	x^2	$n - x^2$	factors	Q candidate?
138	19044	957	3*11*29	
139	19321	680	10*4*17	yes
140	19600	401	prime	
141	19881	120	3*10*4	yes
142	20164	-163	prime	
143	20449	-448	7*64	yes
144	20736	-735	15*49	yes

  We have four solutions, with $|ab|$ values $10 * 17 = 170$, $3 * 10 = 30$, 7, and 15.
  We add 170, 30, 7, and 15 into Q.
  We notice that $30 = 2 * 15$, and 15 is in Q.
  Because $30/15 = 2$ is already in Q from the $k = 2$ run above, there's nothing further to add.

We notice that 170 and 30 have a common factor of 10.

We use the FGH closure rule. For $f = 170$, $g = 30$, $h = 10$,
$fg/h^2 = 170 * 30/10^2 = 5100/100 = 51$, so we can include 51 in $Q = \{2, 7, 15, 30, 51, 57, 170\}$.
We can divide 170 by 2 to get 85, and then include 85 in $Q = \{2, 7, 15, 30, 51, 57, 85, 170\}$.

$k = 4$, $k * n = 26668$, $\sqrt{kn} \approx 163.3$

x	x^2	$n - x^2$	factors	Q candidate?
160	25600	1068	4*3*89	
161	25921	747	9*83	
162	skip			
163	26569	99	9*11	yes
164	skip			
165	27225	-557	prime	
166	skip			

We skip the even x's because they duplicate the work with $k = 1$ above. We show the $x = 160$ line; compare with the $k = 1, x = 80$ line, and notice that the entries in the $k = 4, x = 160$ line, after the first column, are all 4 times the $k = 1, x = 80$ line. Because the factors in the $k = 4$ line have an extra 4, which we remove, this leads to the same ab value as the $k = 1$ line. Adding it to Q does nothing. This duplication happens whenever k has a square factor and x shares a common factor with the square.

The $x = 163$ line is new information; we add 11 to
$Q = \{2, 7, 11, 15, 30, 51, 57, 85, 170\}$.

$k = 5$ has two new potential additions to Q:
$x = 180$ yields 935, which is $5 * 11 * 17$. We divide out the existing Q element 11, getting 85. Because 85 is already in Q, we don't add it again.
$x = 183$ yields -154 which is $2 * 7 * 11$. We've already got 2, 7, and 11 in Q, so there's nothing to add.

$k = 6$ yields three good x values: 198, 200, and 201. But they each reproduce existing Q values or products of Q values, so these elements are not useful.

$k = 7$ with $x = 213$ produces 13, which we add to Q.

With $x = 217$, we get a potential Q addition of $105 = 3 * 5 * 7$. But, we've already got 7 and 15, so we don't include 105.

With $x = 218$, we get $95 = 5 * 19$. We add this to Q. Using the FGH rule with 57 produces 15, which we already know.
$Q = \{2, 7, 11, 13, 15, 30, 51, 57, 85, 95, 170\}$

$x = 219$ gives us $323 = 17 * 19$. We add this to Q. Using the FGH rule with 323 and any of 51, 57, 85, or 95, produces numbers we already know.
$Q = \{2, 7, 11, 13, 15, 30, 51, 57, 85, 95, 170, 323\}$

- **Set $k = 1$ and vary a.** Choose $a > 1$ and a is square-free.
  Choose x near $\sqrt{n/a}$. Proceed as in the previous bullet item with $v = n - ax^2$.
  Example: n=6667, $a = 2$, $\sqrt{n/a} \approx 57.7$

x	ax^2	$n - ax^2$	factors	Q candidate?
54	5832	835	5*167	
55	6050	617	prime	
56	6272	395	5*79	
57	6498	169	13*13	yes
58	6728	-61	prime	
59	6962	-295	5*59	
60	7200	-533	13*41	

The solution $k = 1$, $a = 2$, $x = 57$, gives $kn - ax^2 = 169 = 13^2$. We choose $b = 1$, $y = 13$, $-ab$ is -2. We already have 2 in Q, so nothing is added.

Trying $a = 3$, $\sqrt{n/a} \approx 47.1$

x	ax^2	$n - ax^2$	factors	Q candidate?
44	5808	859	prime	
45	6075	592	16*37	
46	6348	319	11*29	
47	6627	40	8*5	yes
48	6912	245	5*49	yes
49	7203	536	8*67	
50	7500	833	7*139	

$x = 47$ and $x = 48$ are solutions. However, after multiplying the factors column by the $a = 3$ value, and deleting squares and known Q elements, nothing new remains.

At this point, we might well conclude that we aren't going to get 3 and 5 to put into Q. Either would do because we could divide it into 15 to get the other. But we've put quite a bit of work into developing Q, and aren't getting any new results.

We are getting new solutions, with different combinations of k, a, b, x, and y. But each time, the ab value doesn't lead to anything new after we divide out square factors and existing Q elements. Our list of primes to try goes up to 20, and we've accounted for all of them in Q: 2, 7, 11, and 13 are in Q; 3, 5, 17, and 19 seem to only occur together in pairs like $15 = 3 * 5$ and $85 = 5 * 17$. This is a typical outcome for a composite number.

If n were larger, we might continue for a while longer: We would have more primes to try in our Keep list, and we could still find new values. It's time to guess that n is composite and try to break it open with Difference of Squares.

- **When n is near a multiple of a square**, it is helpful to learn to recognize numbers that are small multiples of squares, especially if they are nearly equal to other squares. It is even better if these numbers are grouped. In the list below, see if you can split the numbers into kx^2 where k is small or has only small factors. Some squares are also included, e.g. $k = 1$.

  One way to use the square: If you are trying the form $n - x^2$ or $n - ax^2$, these numbers are automatic successes for the by^2 part.

  As you do more mental factoring, these numbers will begin to stand out. This list is only a sample; experience is the best guide.

  98 147
  243 245 252 288 294
  343 360 375 405 432 486
  507 539 567
  605 675

720 722 726
845 847 867 875
1008 1024 1029 1083
1331
1440 1444
1681 1682
2400 2401 2420
3125 3136
4050 4096 4107 4205 4232 4225 4356 4375 4418
5000 5040 5041 5043 5046 5070 5120 5184
6000 6050 6075 6084
6241 6250
9408 9409
9800 9801 9900
10000 10080 10082 10086 10092 10108 10201

There is another way to use a group of these numbers: If the target number is in or near one of these groups, try subtracting the different group members, and factoring the difference.

Example: $n = 5059$ is in the 5000-5120 group.
We try subtracting group elements to see if the difference factors into small primes:
5059 - $\{5000, 5040, 5041, 5043, 5046, 5070, 5120, 5184\}$
$\rightarrow \{59, 19, 18, 16, 13, -11, -61, -125\}$
Of these, 59 and -61 are not helpful because they are primes > 20 (any number with a prime divisor > 20 is excluded)
19, 18, 16, 13, -11, and -125 are good.
We get 6 solutions:
$n = 5040 + 19 = 2 * 2500 + 19 * 1$, ab value is $38 = 2 * 19$
$n = 5041 + 18 = 1 * 5041 + 2 * 9$, ab value is 2
$n = 5043 + 16 = 3 * 1681 + 1 * 16$, ab value is 3
$n = 5046 + 13 = 6 * 841 + 13 * 1$, ab value is $78 = 2 * 3 * 13$
$n = 5070 - 11 = 30 * 169 - 11 * 1$, ab value is $330 = 2 * 3 * 5 * 11$
$n = 5184 - 125 = 1 * 5184 - 5 * 25$, ab value is 5.
We can immediately add 2, 3, and 5 to the set Q. This is enough to finish phase I and continue on to the divisor tests in Phase IIa. If we were to continue adding to Q, we could add the additional numbers $38/2 = 19$, $(78/2)/3 = 13$, and $((330/2)/3)/5 = 11$.

Even if this method fails, we can use some of the ab values that we have discovered to limit the ranges for x and y candidates in the Difference of Squares method (see section 8.3, 8.3.3).

- **When n is midway between two squares.** If squares close to n do not produce the necessary three results, then one can continuing searching by using the two nearest squares that bound n. Assume that $x^2 < n < (x+1)^2$. Denote $x(x+1)$ by j. The quantity $4(j-n)+1$ can be used as ab in the previous method.

  Example for $n = 2557$:
  $50^2 < 2557 < 51^2$. We have $j = 50 * 51 = 2550$ and $4(j - n) + 1 = -27$. We divide out the square factor 9 and have $ab = -3$. This establishes ± 3 as a square modulo n.

  This method can be extended to utilize squares that bound n but are further away. Suppose that $S^2 < n < (S + 1)^2$. Consider that ratio $\frac{(n-S^2)}{(S+1)^2-n}$. If this ratio can be approximated

by a fraction $\frac{c}{d}$ with small integers c and d (numbers less than 6), then we can conclude that $\sqrt{n} \approx S + \frac{c}{(c+d)}$.

The search method then uses the equation $kn = ax^2+by^2$ with $k = (c+d)^2$, $a = 1$, $x = S(c+d)$, and $y = 1$. This implies $b = kn - ax^2$. If b is a negative square $-f^2$, then the factors of kn are $(x - f)(x + f)$, and the divisors of those terms are divisors of n.

Example for $n = 2567$:

The bracketing squares are 50^2 and 51^2, thus $S = 50$. The ratio is $\frac{67}{34} \approx \frac{2}{1} = \frac{c}{d}$. Then $k = 2 + 1 = 3$ The square root of n is approximately 502/3. We have $k = 9$, $a = 1$, $x = (c * S) + d = 3 * 50 + 2 = 152$.

$b = kn - ax^2 = 9 * 2567 - 1 * 152^2$

$b = 23103 - 23104 = -1 = f^2 \rightarrow f = 1$. From this we know that $x \pm f$ are 153 and 151.

Trying $n = 2537$ and $S = 50$, we obtain a ratio of about $\frac{1}{2}$. $c = 1$, $d = 2$, $c + d = 3$, $k = 9$, $a = 1$, $x = 50 * 3 + 1 = 151$.

$b = kn - ax^2 = 9 * 2537 - 1 * 151^2 = 22833 - 22801 = 32$.

We can remove the square factor 16 from b and conclude that $ab = 2$. Therefore 2 is a square modulo 2537.

8.1.2 A different way to Search for x: tricks about divisibility by 100

Instead of making $kn - ax^2$ small, we can make it divisible by 100 (or 25 or 10, as we will see later). Then we can develop a candidate set for x in the same way that we did in The Method.

This method can be used along with the previous methods to build the set Q. The order of the methods is not significant. We will start with an example and then describe the general algorithm.

Example: $n = 17111$

We need to add to, or subtract a square from n, to make the result a multiple of 100. For this n, we will add squares ending in 89. The smallest square ending in 89 is 289, and its square root is 17. We'll try x values in the set $\{50j \pm 17\}$, up to $2\sqrt{n}$, which is about 260.

Because n is a 5-digit number, we'll call primes up to 35 "small". We've deliberately selected an example with a lot of Q candidates; that's atypical.

x	x^2	$n + x^2$	factors	Q candidate?
17	289	17400	$100 * 6 * 29$	yes
33	1089	18200	$100 * 2 * 7 * 13$	yes
67	4489	21600	$100 * 6 * 36$	yes
83	6889	24000	$100 * 15 * 16$	yes
117	13689	30800	$100 * 4 * 7 * 11$	yes
133	17689	34800	$100 * 12 * 29$	yes
167	27889	45000	$100 * 2 * 225$	yes
183	33489	50600	$100 * 2 * 11 * 23$	yes
217	47089	64200	$100 * 6 * 107$	no
233	54289	71400	$100 * 6 * 7 * 17$	yes

We list the Q candidates, removing square factors. Every Q candidate has a factor of 100 removed; some have additional square factors to remove.

The Q candidates are 174, 182, 6, 15, 77, 87, 2, 506, and 714. Adding these to Q using the smallest values first, we add 2, then 6, then 15. With the closure rules, we also get $6/2 = 3$, and

$15/3 = 5$. This is enough to end phase I, and we can go to phase IIa, checking for divisors.

The set of possible divisors is $120j + \{1, 49, d, e\}$. We use the formulas for d and e given at the beginning of section 8.1.

$n \equiv 71 \mod 120$, so $d = 71$.

e is $60 - 11d = -721 \equiv -1 \equiv 119 \mod 120$.

Our set of trial divisors will be $120j + \{1, 49, 71, 119\}$. 49 is excluded, because we've already checked divisors ≤ 31, and 7 is less than 31. 71 is the first possible divisor, and we find $n = 71 * 241$.

Algorithm for making $kn - ax^2$ divisible by 100. We first determine k based on $n \mod 10$:

- If the last digit of n is 3 or 7, we use $k = 3$ and then $k = 7$.
- If the last digit of n is 1 or 9, we use $k = 1$.

We next branch on $kn \mod 4$. When $kn \equiv 3 \mod 4$ we will arrange to add squares to kn to make the sum a multiple of 100. When $kn \equiv 1 \mod 4$ we will make the difference between kn and selected squares a multiple of 100.

- If $kn \equiv 1 \mod 4$, set $a = 1$ and look for an r value in the range 1 to 24 such that r^2 has the same last two digits as n. The candidate set for x is then $\{50j \pm r\}$.

  The starting value for x is the nearest candidate less than $\sqrt{kn}$. The value $kn - x^2$ will be divisible by 100, so it is easy to divide out 100 and see if the result is a square or a small number times a square. If it is, then we have a solution for y. If not, use the next smaller number in the candidate set, and so on, for about 7 values of x. If there is no solution, then try using candidates larger than $\sqrt{kn}$, and work upwards for about 7 values.

  If there is a solution, then we have a value for by^2, and $ab = -b$ is added to the set of known squares Q and the closure of Q is computed.

  Remember, when $n \equiv 1 \mod 4$, we need to retain the signs for numbers in Q until we get a -1. If and when we get a -1 in Q, we can drop the signs and make everything positive.

  Example: $n = 15401$

  $n = x^2 + by^2$, $a = 1$, $r^2 = 1 \mod 100$, therefore $r = 1$. The candidate set for x is $\{50j \pm 1\}$.

  $\sqrt{n} \approx 124$. We start at $x = 101$ and work down. After hitting bottom at $x = 1$, we reset to $x = 149$ and work up. n is a 5-digit number, so we accept primes ≤ 35 in Q candidates, and n is $4i + 1$, so we keep the signs for Q candidates until a -1 appears.

x	x^2	$n - x^2$	factors	Q candidate?	-ab value
101	10201	5200	100*4*13	yes	-13
99	9801	5600	100*4*14	yes	-14
51	2601	12800	100*64*2	yes	-2
49	2401	13000	100*2*5*13	yes	-130
1	1	15400	100*2*7*11	yes	-154
149	22201	-6800	100*4*17	yes	17
151	22801	-7400	100*2*37	no	
199	39601	-24200	100*2*121	yes	2
201	40401	-25000	100*10*25	yes	10
249	62001	-46600	100*2*233	no	
251	63001	-47600	100*4*7*17	yes	119
299	89401	-74000	100*20*37	no	

We have both 2 and -2 for Q values, so we have the quotient $-2/2 = -1$. Therefore, we can drop the signs from the Q values. We retain a -1 in Q as a reminder.
Begin with $Q = \{-1, 2\}$.
Next up, in order of absolute value, smallest first, is 10. We add $10/2 = 5$ (10 will be implicit, as the product of 2 and 5.) $Q = \{-1, 2, 5\}$.
We add 13, $Q = \{-1, 2, 5, 13\}$.
We add $14/2 = 7$, $Q = \{-1, 2, 5, 7, 13\}$.
We add 17, $Q = \{-1, 2, 5, 7, 13, 17\}$.

Next up is 119. Because $119 = 7 * 17$, and both 7 and 17 are in Q, we (implicitly) have 119 already.

Next up is 130. $130 = 2 * 5 * 13$, and 2,5,13 are already present in Q, so no action is needed.

Next up is 154. We remove factors of 2 and 7, leaving 11 to add to $Q = \{-1, 2, 5, 7, 11, 13, 17\}$. It looks like 3 not going to show up in Q. But we can take advantage of divisor restrictions in tables 7 and 8 to limit possible divisors of n.

Looking at the "2 and 5" entry in table 8, we find divisors must be $40j \pm \{1, 9\}$. Intersecting this with the -1 entry $(4j+1)$, our divisor list is trimmed to $40j+\{1, 9\}$. Note that $\sqrt{n} \approx 124$, so the trial set is not too big.

Because 7 (and implicitly -7) are in Q, we could enforce the restriction for the form $x^2 + 7y^2$, and require divisors to be $7j + \{1, 2, 4\}$. The combination with $40k + \{1, 9\}$ would have the form $280j+\{\text{six elements}\}$. Or, we could simply filter divisors generated from $40j + \{1, 9\}$.

Opting for simplicity, we ignore the mod 7 divisor restriction.

We assume tests for divisors ≤ 31 have already been carried out, with no factor found.

Our first divisor candidate is 41. It fails to divide n.
49 is a multiple of 7, so it's out.
81 is a multiple of 3, so it's out.
89 is possible, but it does not divide n. It fails.
121 is a multiple of 11, so it's out.
The next candidate is 129, exceeding $\sqrt{n}$. With no divisors found, we know n is a prime.
If we had included the modulo 7 filter, both 41 and 89 would have been excluded, because $41 \equiv 6 \mod 7$ and $89 \equiv 5 \mod 7$.

- For $kn \equiv 3 \mod 4$. Set $a = -1$ and find r such that r^2 has the same last two digits as $100 - kn$. The candidate set for x is $\{50j \pm r\}$. In this case we are examining $(kn + x^2)/100$, looking for a result that is a small multiple of a square. If we find it, we have a solution for y.

  The search begins with $x = r$ and works upwards, again for about 7 values.

  If there is a solution, then we have a value for by^2, and $ab = b$ is added to the set of known squares Q and the closure of Q is computed.

  Example: $n = 15271$, $k = 1$. The last two digits of $100 - n$ are 29. The smallest square ending in 29 is $529 = 23^2$. We set $r = 23$. The set of candidates for x is $\{50j \pm 23\}$. We start with 23 and work up. Our target is a five-digit number, so we accept primes < 35 in the factorizations of $n + x^2$ as Q candidates.

x	x^2	$n + x^2$	factors	Q candidate?
23	529	15800	$100 * 2 * 79$	
27	729	16000	$100 * 16 * 10$	yes
73	5329	20600	$100 * 2 * 103$	
77	5929	21200	$100 * 4 * 53$	
123	15129	30400	$100 * 16 * 19$	yes
127	16129	31400	$100 * 2 * 157$	
173	29929	45200	$100 * 4 * 113$	

We can add 10 and 19 to Q.

Example $n = 4567$. We work with $k = 3$, $3n = 13701$, $\sqrt{3n} \approx 117$. $r^2 \equiv 3n \equiv 1 \mod 100$, so $r = 1$ and the x candidate set is $\{50j \pm 1\}$. We will compute $3n - x^2$ and factor it. We start with x near the square root and work down first, and then up from the square root. Because n has four digits, we limit the factorizations for Q candidates to primes < 20.

x	x^2	$3n - x^2$	factors	Q candidate?
101	10201	3500	$100 * 5 * 7$	yes
99	9801	3900	$100 * 3 * 13$	yes
51	2601	11100	$100 * 3 * 37$	
49	2401	11300	$100 * 113$	
1	1	13700	$100 * 137$	
149	22201	-8500	$100 * 5 * 17$	yes
151	22801	-9100	$100 * 7 * 13$	yes
199	39601	-25900	$100 * 7 * 37$	
201	40401	-26700	$100 * 3 * 89$	
249	62001	-48300	$100 * 3 * 7 * 23$	
251	63001	-49300	$100 * 17 * 29$	
299	89401	-75700	$100 * 757$	

We can add 35, 39, 85, and 91 to Q, and we can use the FGH closure rule to add all the pair products of the primes 3, 5, 7, 13, and 17 to Q.

We started this section about "a different way to search for x" by arranging to have $kn - ax^2$ be divisible by 100. To get more Q candidates, we can arrange to have it be divisible by 25. The set of candidates for x is $\{25j \pm r\}$ where j is odd (1, 3, 5, ...).

NB: We recommend using the divisibility by 100 method first because it is more likely to yield results and because the numbers in column 4 of the tables will be smaller. Although we show how to use divisibility by 25 or 10, we only weakly recommend using these variants. If you like the arithmetic, use them, otherwise, go on to "When n is midway between two squares", then Difference of Squares in section 8.3

The process of checking for Q candidates is the same as before because where we used x candidates of $\{50j \pm r\}$, with r^2 or $100 - r^2$ matching the low order two digits of n (or $3n$), we instead can use x candidates adjusted by ± 25, and the expression $kn - ax^2$ will still be a multiple of 25.

Example: $n = 13579$. We compute $r = 11$ and use $a = -1$, $k = 1$. Our new set of trial x values is $\{25k \pm 11\}$ with k odd. As usual with the form $n + x^2$, we start with small x values and work up.

x	x^2	$n + x^2$	factors	Q candidate?
14	196	13775	$25 * 19 * 29$	yes
36	1296	14875	$25 * 5 * 7 * 17$	yes
64	4096	17675	$25 * 7 * 101$	
86	7396	20975	$25 * 839$	
114	12996	26575	$25 * 1063$	
136	18496	32075	$25 * 1283$	
164	26896	40475	$25 * 1619$	

We can add $551 = 19 * 29$ and $595 = 5 * 7 * 17$ to Q.

To work modulo 10, use candidate set $\{10k \pm d\}$ where d is the low digit of r. This produces more candidates with less likelihood of success.

8.2 Divisor constraints

8.2.1 Failed quadratic forms

Even if none of the quadratic form attempts, even the retries, find decompositions, the effort that goes into searching with The Method is not in vain. There is information available about the form of the prime divisors. The fact that a number does not have a particular quadratic form representation gives us some insight into its possible factors. We discuss each possibility below, and Table 6 summarizes the information.

Caution: We will illustrate combining multiple divisor constraints in section 8.3.3. Normally, multiple constraints can be combined without any concerns, but there's a special case for divisor constraints from Table 6: If the target number could have more than two prime factors (i.e., the smallest untested prime divisor is less than or equal to the cube root of n), then at most one constraint from the table may be used in a combination. If the target is known to have at most two prime divisors, then you can use all the Table 6 constraints that apply. In the most restrictive case, if the target was tried for all three quadratic forms ($x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$) and no solutions exist, then all three restrictions can be combined, along with any other Q set information or information from Tables 7 and 8.

We will give an example of how to utilize this in the calculation of search limits in the Difference of Squares algorithm (section 8.3).

- Case of $n \equiv 1 \mod 4$. Referring to the information in Table 1, if there are no representations in which x or y is divisible by 5, then we know that n is composite and it has at least two prime factors that are equivalent to $3 \mod 4$. The multiplicity of these factors is even (every instance of a factor counts towards the multiplicity; p^d is d factors). There might be other prime factors.

  There is another quadratic form decomposition that can be tested. If $n \equiv 1 \mod 8$, then the forms $n = x^2 + 2y^2$ and $3n = x^2 + 2y^2$ can be tested. That will result in a factorization about half the time.

  There is yet another quadratic form decomposition that can be tested. If $n \equiv 1 \mod 6$, then the forms $n = x^2 + 3y^2$ and $4n = x^2 + 3y^2$ can be tested. That will result in a factorization about one time in six.

- Case of $n \equiv 3 \mod 8$. Referring to the information in Table 1, if there are no representations in which x or y is divisible by 5, then we know that n is composite and it has at least two

residue	quadratic forms	prime divisors
1 mod 4	$n = x^2 + y^2$ $n = x^2 + 2y^2$	even number of $4k + 3$ primes
3 mod 8	$n = x^2 + 2y^2$ $3n = x^2 + 2y^2$	at least two $8j + 5$, $8j + 7$
7 mod 24	$n = x^2 + 3y^2$ $4n = x^2 + 3y^2$	at least two $6j + 5$

Table 6: Prime divisors in the zero representation case; there are always at least two prime divisors of the form shown in column 3, and the multiplicity of the divisors is even.

prime factors that are equivalent to 5 or 7 modulo 4. The multiplicity of these factors is even (every instance of a factor counts towards the multiplicity; p^d has d factors). There might be other prime factors.

If we have tested all possible divisors of n that are less than or equal to the cube root of n, then n must be the product of two primes p and q where $p \equiv 5 \mod 8$ and $q \equiv 7 \mod 8$.

There is yet another quadratic form decomposition that can be tested. If $n \equiv 1 \mod 6$, then the forms $n = x^2 + 3y^2$ and $4n = x^2 + 3y^2$ can be tested. That will result in a factorization about one time in six.

- Case of $n \equiv 7 \mod 24$. There are at least two prime divisors that are congruent to 5 modulo 6. These primes occur in pairs (i.e., the multiplicity of the primes is even).

8.2.2 Divisor set formulas

Somehow or other, after you've done The Method (and The Method again), and The 120 Method, you will have a bunch of ab values in Q. Each of these values has an associated linear expression that is a superset of the divisors of n.

In general, it is useful to combine the individual linear forms into a single linear form. The combined form is an efficient and sparse representation of possible divisors of n. There are two uses for the combined form: working with a set Q from The 120 Method that has only 2 of the required values, and for minimizing the testing of potential divisors in Difference of Squares. Those divisors have to be tested using mental division, so the fewer things that need testing, the less stress on the mental arithmetic unit.

In Table 7, we have examples of quadratic forms, the negative of the product of the a and b coefficients, and the divisor forms allowed. If we are fortunate enough to have two different values for ab, then we can combine them as shown in the second table. With some experience, you should be able to generate these expressions yourself.

We will revisit these tables when we discuss the upper limit variable in the Difference of Squares method.

form	-ab value	allowed divisor values
$x^2 + y^2$	-1	4j + 1
$x^2 + 2y^2$	-2	8j + {1,3}
$x^2 + 3y^2$	-3	6j + 1
$x^2 + 5y^2$	-5	20j + {1,3,7,9}, tens digit is even
$x^2 + 6y^2$	-6	24j + {1,5,7,11}
$x^2 + 7y^2$	-7	7j + 1,2,4 (or 14j+1,4,9)
$x^2 + 10y^2$	-10	40n + 1,7,9,11,13,19,23,37
$x^2 + 15y^2$	-15	30j + 1,17,19,23
$x^2 + 30y^2$	-30	120j + 1,11,13,17,23,29,31,37,43,47,49,59,67,79,101,113
the forms with negative coefficients can be negated: $x^2 - 2y^2$ is equivalent to $2x^2 - y^2$, etc.		
$x^2 - 2y^2$	2	8j ± 1
$x^2 - 3y^2$	3	12j ± 1
$x^2 - 5y^2$	5	10j ± 1
$x^2 - 6y^2$	6	24j ± {1,5}
$x^2 - 7y^2$	7	28j ± {1,3,9}
$x^2 - 10y^2$	10	40j ± {1,3,9,13}
$x^2 - 15y^2$	15	15j ± {1,4} or 30k ± {1,11}
$x^2 - 30y^2$	30	120j ± {1,7,13,17,19,29,37,49}
Forms $ax^2 + by^2$ are equivalent to $x^2 + aby^2$.		

Table 7: Coefficients and implied divisor constraints.

-ab values	allowed divisor values
-1 and 2	8j + 1
-1 and 3	12j + 1
-1 and 5	20j + {1,9}
-1 and 6	24j + {1,5}
-1 and 7	28j + {1,9,25}
-1 and 10	40j + {1,9,13,37}
-1 and 15	60j + {1,29,41,49}
-1 and 30	120j + {1,13,17,29,37,49,101,113}
2 and 3	24j ± 1
2 and 5	40j ± 1,9
3 and 5	60j ± 1,11
-2 and 3	24j + 1,11
2 and -3	24j + 1,7
-2 and -3	24j + 1,19
-2 and 5	40j + 1,9,11,19
2 and -5	40j + 1,7,9,23
-2 and -5	40j + 1,3,9,27
-3 and 5	30j + 1,19
3 and -5	60j + 1,23,47,49
-3 and -5	60j + 1,7,43,49
-1 and +-2 and +-3	24j+1
-1 and +-2 and +-5	40j+1,9
-1 and +-3 and +-5	60j+1,49

Table 8: Combinations of *ab* constraints

Combining values for two relatively prime moduli. Suppose the moduli are m and n, $\gcd(m, n) = 1$. We consider all choices of a residue $r \mod m$ and a residue $s \mod n$. For each combination of an r and an s: Look at s, $s + n$, $s + 2n$, ... and check if the value is $\equiv r \mod m$. There will be one solution; you can stop when you find it. If you reach $s + mn$, you've gone too far. This method gives one combination residue (modulo mn) for each combination of an r with an s. The total number of combinations is the number of possible r's times the number of possible s's.

You can speed up the calculations in two ways. First, you can combine all of the r's with one s. As before, look at s, $s + n$, $s + 2n$, ..., up-to-but-not-including $s + mn$. Reduce each $s + kn$ value modulo m, and see if the result is in the list of acceptable r's. If so, keep $s + kn$.

The second speedup applies when both the r values and s values come in $\pm$pairs. (For this speedup, a 0 residue can be viewed as ± 0, and the 2 in $4j + 2$ can be viewed as $4j \pm 2$.) Consider only the non-negative r values in combination with the $\pm s$ values. For each of the combination residue, include both the positive and negative value.

If the moduli are not relatively prime, the formulas can still be combined, and we leave that method as an exercise for the reader.

How to compute restrictions on divisors. Here is a method. The exact steps are a matter of experience.

- Picking a divisor generating formula.

  Recall the members of the set Q in the 120 Method. Although we previously said that the signs did not matter, you need to know them now. You need to either remember the signs of the small integers in Q (those less than 10) or else you need to carry out the 120 Method again. Using the single digit, signed members of Q and Table 7, make note of the formula for each one. For example, -1 has the simple formula $4j + 1$.

  In Table 8, we see that the formulas for -1, 2, 3, and 5 can be combined in pairs to create a formula that describes, for example, the combination of the formula for $x^2 + 2y^2$ and the formula for $x^2 - 3y^2$ into the single formula $24j + \{1, 11\}$. For the Q values that you've calculated, combine any two in the manner of Table 8. You might have four Q values and combine two pairs into two formulas, or you might combine two and have a single formula from Table 7, etc.

  If you have a combination form, that will be the main generator for prime divisors of n. If you do not have a combination, then the formula with smallest multiplier of j will be the main generator. Any other formulas will be secondary generators.

  Calculate j such that the main generator yields a value L or larger (L is initially 31 in our method). Do the same for the secondary generators.

- Using the information in Table 1, make note of the information about divisors. For example, if $n \equiv 1 \mod 4$, then n has an even number of $4i + 3$ divisors. This information will be useful if we need to test potential divisors that are larger than the cube root of n.

For example, if you know $n = x^2 - 2y^2$ (always with x and y relatively prime) and $n = x^2 - 5y^2$, (of course, with a different x and y), then it follows that 2 and 5 are squares modulo n. Using 2, we get the divisor restriction $8j \pm 1$, and 5 gives the restriction $10k \pm 1$. These restrictions can be combined to get $40k \pm \{1, 9\}$. So you can zip through potential prime divisors: 1 is useless, 9 isn't prime, so 31 is the first candidate to try. 39 is composite, 41 is a possibility, 49 is composite, 71 and 79 are possibilities, etc. (If you've done the m tests, 31, 41, and 71 are already checked, so 79 is the first untried prime divisor.)

If you have more divisor constraints with combinations not covered in table 8, they can be applied as well: suppose you also know that $n = x^2 + 7y^2$; that restricts divisors to the residues 1, 2, or 4 modulo 7. In the $40k \pm \{1, 9\}$ case above, you can go two ways: You can work out the residues modulo 280 which satisfy both constraints, giving
$280k + \{1, 9, 39, 71, 79, 81, 121, 151, 169, 191, 249, 239\}$.
Alternatively, you can just apply the modulo 7 residues to any primes in the $40k \pm \{1, 9\}$ set:
$31 \equiv 3 \mod 7$, so we can skip testing it.
$41 \equiv 6 \mod 7$, also skippable.
$71 \equiv 1 \mod 7$, which is acceptable for testing.
$79 \equiv 2 \mod 7$, also a potentially a divisor.
$89 \equiv 5 \mod 7$, skip it. Etc.

The divisor constraints shown in table 6 can be used if n has no solutions of a certain shape, such as $x^2 + y^2$. If n is 1 modulo 4, this tells us that n is composite, and it must have an even number of $4j + 3$ prime factors. If we've checked n for divisors up to its cube root, then n must have exactly two prime factors, so both of them must be $4j + 3$ numbers. Otherwise, n might have more prime factors of the form $4j + 1$ in addition to the minimum of two $4j + 3$ primes.

We might choose to temporarily ignore possible $4j + 1$ divisors and focus on the $4j + 3$ divisors. At least one must be less than or equal to the square root of n. We can skip over any $4j + 1$ divisors in our testing work. When we find the factors of n, we'll need to check if they are prime. Any ignored $4j + 1$ divisors will be exposed at this point.

Working with a small Q set. Next we present an example using a two member Q set from the 120 Method. NB: Normally we don't have to remember the quadratic forms that we discovered, we just need the ab values, and for $4j + 3$ numbers we don't need to know the signs. Unfortunately, working with the small Q sets requires that we know the signs of the members of Q, and in order to know that, we have to remember the equations. With any luck, they stuck in your mind or you can recompute them quickly.
Example: $n = 10579$.
Assume that The 120 Method turned up 3 usable quadratic form solutions:
$n = 10609 - 30 = 1 * 103^2 - 30 * 1^2$ has ab value 30
$n = 10404 + 175 = 1 * 102^2 + 7 * 5^2$ has ab value 7
$n = 2 * 5290 - 1$, with $5290 = 10 * 529 = 10 * 23^2$.
We notice that 5290 is a small number 10 times the square 529. Substituting in $10 * 529$ for 5290, we have $n = 20 * 529 - 1 = 20 * 23^2 - 1 * 1^2$ with ab value of 20. Dividing out the square divisor 4, we reduce 20 to 5. We note that $5|30$, so we reduce 30 to 6. Additional searching fails to locate 2 and/or 3, so we have $Q = \{5, 6, 7\}$.

We consider using divisor constraints, testing primes that are less than the square root of n which is approximately 103.
Effort estimation:
First, we estimate the number of primes $< \sqrt{n}$.
There are 25 primes < 100.
We're estimating, so use a linear extrapolation to estimate $25 * 103/100 \approx 26$ primes $< \sqrt{n}$.
We assume that we have eliminated prime divisor through 31 by using the methods in section 4.
This leaves about 13 primes to try.
Each divisor constraint reduces the set of eligible trial prime by about half. A single constraint should leave us with about 6 primes to try. Two constraints should leave about 3 primes to try,

and using all three constraints will leave about 2. These are estimates, but that's good enough for deciding how to proceed.
We decide to use all three constraints.

We can combine two of them with reasonable effort, and use the third as a separate checking method.
We need to know the signs of the Q values to select the rows to use from Table 7.
Unlike the Modulo 120 Method, we need to know the signs of the members of Q, even though n is 3 modulo 4. In order to do this, we need to know the equations that gave rise to them, which is why we presented them at the start of this example. We use the Q completion rules as before to get 5, 6, and 7, but now we keep track of the signs:
$n = 1 * 103^2 - 30 * 1^2$ has a $-ab$ value of $-1 * 1 * -30 = +30$.
$n = 1 * 102^2 + 7 * 5^2$ has a $-ab$ value of $-1 * 1 * 7 = -7$.
$n = 20 * 23^2 - 1 * 1^2$ has a $-ab$ value of $-1 * 20 * -1 = +20$.
Using the closure rules for +20, we divide out the square 4, giving +5 for the first Q value.
-7 is the second Q value, with no closure processing needed.
$+30/+5 = +6$ for the third Q value. Consulting Table 7, we find +5 in the $-ab$ column, with the corresponding form $x^2 - 5y^2$, and divisor constraint $10j \pm 1$.
We find +6 in the $-ab$ column, and divisor constraint $24j \pm \{1, 5\}$.
We find -7 in the $-ab$ column, and divisor constraint $7j + \{1, 2, 4\}$.
We decide to combine the constraints for +5 and -7 because that will produce the minimum size set of residues (6).
The LCM of the moduli 10 and 7 is their product $10 * 7 = 70$.
This will be the modulus for the combined constraint. Begin with $10j+1$: List the values, stopping when we hit 70:
1, 11, 21, 31, 41, 51, 61.
Compute the remainders modulo 7:
1, 4, 0, 3, 6, 2, 5.
Based on the constraint $7j + \{1, 2, 4\}$, the remainders 1, 2, and 4 are accepted. So we select 1, 11, and 51 from this group. Next, we look at $10j - 1$:
9, 19, 29, 39, 49, 59, 69.
2, 5, 1, 4, 0, 3, 6.
We could stop after finding 4 because all the residues $\{1, 2, 4\}$ are covered. We select 9, 29, and 39 here. Our intersection set of the +5 and -7 constraints is
$70j + \{1, 9, 11, 29, 39, 51\}$.
We hold the third constraint, for +6, in reserve. (To combine it in would create a large set: $840j+$ {24 residues}. This is a lot of work, for not much value.) Now we're ready to start testing divisors: We need to cover primes < 103. We've already checked up through 31. We look at our constraint set, and see that the first eligible number from the set exceeding 31 is 39. Because 39 is composite it already has been implicitly tested. ($39 = 3 * 13$, and we've already checked 3 and 13.)
Next is 51,which we reject for the same reason.

We wrap around the set and bump j up to 1. Now we have to consider $70 * 1 + 1 = 71$. This is prime. We invoke the remaining constraint for Q member +6, which is $24j + -\{1, 5\}$; 71 mod 24 is $3 * 24 - 1$, so 71 is accepted, and we check to see if 10579 is a multiple of 71. In the section 4 we noted that 10011 is a multiple of 71. Subtracting $10579 - 10011 = 568$, which is clearly $8 * 71$. We've found a factor; we need the other one. $10579/71 = 149$. Both 71 and 149 are prime, so we're done: $10579 = 71 * 149$.

To get an idea of the effectiveness of combined divisor restrictions, let's pretend we have to continue testing primes. Next up is $1 * 70 + 9 = 79$, which is prime, but it is 72+7, so the third set, $24j \pm \{1, 5\}$, eliminates it, and we do not need to do that trial division.
Next is 81, a composite.
Next is 99, a composite.
Next is 109, which exceeds $\sqrt{n}$.
We note, for the record, that the second factor 149 is a member of our testing set $70j+\{\text{stuff}\}$, and that it is a member of the third set, $24j \pm \{1, 5\}$ because $149 = 144 + 5 \equiv 5 \mod 24$.

8.3 The Difference of Squares Method

In section 4.1 we discussed the difference of squares method for small numbers. This section discusses approaches that make larger numbers tractable.

All of the previous methods have had the possibility of ending with an ambiguity as to whether n is prime or if its factors are unknowable with the given method. Difference of squares, if carried through completely, gives a definite answer. We use it as the method of last resort because although it is guaranteed to find the answer, it is not the method of least computation. Some of the information from the previous methods can help cut down on that computation. We describe how to do this, mostly through examples.

The fundamental equation for this method is $n = x^2 - y^2$. A naive approach to solving it would be to try all x values between $\sqrt{n}$ and n and determine if $n - y^2$ is a square. The methods in this section do that, but they utilize two ways to narrow that range: dividing out small primes using the techniques of section 4 and divisor restrictions described previously.

Another naive approach to solving $n = x^2 - y^2$ would be to test all prime divisors between 1 and $\sqrt{n}$. If a prime p divides n, then we have $p * (n/p) = n$. There must be some x and y such that $n = (x + y)(x - y)$ where $x - y = p$ and $x + y = n/p$. In fact, $x = (p + n/p)/2$ and $y = (n/p - p)/2$. As we raise p, y decreases rapidly. This gives us a second way to narrow the range of x: test small primes in the range 2 to some p (usually less than 500) as potential divisors of n.

These two range-narrowing methods work in concert for the Difference of Squares algorithm. Assume that we have some efficient way to test candidates for x and y where x and y grow monotonically (see the Modulo 25 method below) or a method for testing just x as x grows monotonically (see the Modulo 60 method in section 8.3.2). Also assume that we know that n has no prime divisors less than p (as explained later, we can start with $p = 37$. Then do the following (if using the Modulo 60 method, ignore the instructions about advancing and comparing y):

1. Remove all prime factors up to 31 from n (all methods in this paper assume that this has been done). Set $L = 37$.
2. Compute the formula for sets of candidates for x and y using either of the two methods below (Multiple of 25 or x Modulo 60).
3. Start with a candidate for x that is the least integer larger than $\sqrt{x}$. The y value begins at 0.
4. Test a candidate for x or y . If $n - x^2$ or $n - y^2$ is a square then this is a solution, and the algorithm can stop.
5. Try the next larger candidate for x or y (if using the Modulo 25 Method) and check for a solution. If x is larger than $(L + n/L)/2$ and, if using the Modulo 25 Method, $y > (n/L - L)/2$, then the algorithm terminates with the result that n is prime.

6. After trying a block of a few candidates for x and y, increase L by testing some of the next primes p larger than L as a divisor of n. Section 4 shows mental tricks to use for primes up to 127; if p becomes larger than this, you may have to carry out some of the trial divisions mentally (see section 8.3.3 for how to avoid most of them). If p does not divide n, then set $L = p$ and return to step 4 above. If $L + n/L < 2x$, and if using the Modulo 25 Method, $n - L/n < 2y$, then the algorithm terminates with the result that n is prime.
7. As with most factorization methods, it is possible that the factors we have found may be composite and will need further factoring effort.

8.3.1 Modulo 25 Method

The equation $n = x^2 - y^2$ where $\gcd(x, y) = 1$ is interesting because a solution to it immediately yields two divisors of n: $(x + y)$ and $(x - y)$. We describe a search method that will either find a solution of that form or result in the conclusion that n is prime.

We first apply this method n values with low digit 1 or 9, and then explain the minor modifications for n with low digit 3 or 7.

We state without proof that any solution to $n = x^2 - y^2$ with $n \equiv \pm 1 \mod 5$ will have either x or y divisible by 5. Similar to our previous analyses of modular equations, this result follows from noting the squares modulo 5 and the set of differences achievable with them.

The algorithm for n with low order digit 1 or 9. We analyze the difference of squares equation modulo 25. As with The Method, the two low order digits of the variables is the key to cutting down on the number of trials in the search for x and y.

Therefore, one of the two squares will end in 00 or 25. We can solve for the other square modulo 100 using the following equations.
For $n \equiv 1 \mod 4$:
$x \equiv 5 \mod 10$, $y^2 \equiv 25 - n \mod 100$
$y \equiv 0 \mod 10$, $x^2 \equiv n + 0 \mod 100$
For $n \equiv 3 \mod 4$:
$x \equiv 0 \mod 10$, $y^2 \equiv 0 - n \mod 100$
$y \equiv 5 \mod 10$, $x^2 \equiv n + 25 \mod 100$

Of the two solutions, one is based on x, the other on y. Use the solutions to build candidate sets the form $\{50j \pm r\}$ as in The Method; one is for x candidates, the other is for y candidates.

The search strategy alternates between trying x's and trying y's until there is a solution or they both exceed their current upper limit. The upper limit is a function of L, as described the six-step algorithm above.

Next choose a block size B. A good choice is the nearest multiple of 25 greater than $\sqrt{n}$. First test candidate x values, starting from $\sqrt{n}$ up to $2B$. Then test candidate y values, starting from 0, up to $2B$.

If there is not solution after these tests, then it is necessary to update the upper limit as described in section 8.3.3. The next test range for x and y is $2B$ to $3B$. Note that because of the upper limit adjustment, one or both of x or y may exceed the new upper limit. If both exceed their limits, then the algorithm terminates and n is prime. Otherwise, continue to the next block of values, and repeat the tests, the upper limit update, etc.

Example: $n = 13579$

We want to search for solutions to $x^2 - y^2 \equiv 79 \mod 100$ where x or y is divisible by 5. The four possibilities are:
$00 - 21 \equiv 79$ is possible for $y \equiv 11$
$25 - 46 \equiv 79$ is impossible because no square ends in 46
$79 - 00 \equiv 79$ is impossible because no square ends in 79
$04 - 25 \equiv 79$ is possible for $x \equiv 2$.
This implies that either $y^2 \equiv 21 \rightarrow y = 11, 39, 61, 89, \ldots$
or
$x^2 \equiv 04 \rightarrow x = 02, 48, 52, 98, \ldots, 148, \ldots\ldots$

Choose the blocksize B to be 125.

The starting value for x will be 148 because that is the first member of the candidate set for x that is larger than the square root of n ($\sqrt{13579} \approx 117$).
$x = 148$, $21904 - 13579 = 8325$ is not a square by the hundreds digit rule (section 5.3).
$x = 152$, $23104 - 13579 = 9525$ is not a square by the hundreds digit rule.
$x = 198$, $39204 - 13579 = 25625$ is not a square (it is too close to $25600 = 160^2$).
$x = 202$, $40804 - 13579 = 27225$ is a square because $272 = 16 * 17$.

We have shown that $13579 = 202^2 - 165^2 = (202 + 165) * (202 - 165) = 37 * 367$. The two factors are primes, and the factorization is complete.
If we hadn't found the $x = 202$ solution, we would continue with $x = 248$, and then switch to trying y's. The first few y trials are
$y = 11$, $13579 + 121 = 13700$ is not a square
$y = 39$, $13579 + 1521 = 15100$ is not a square
$y = 61$, $13579 + 3721 = 17300$ is not a square
$y = 89$, $13579 + 7921 = 21500$ is not a square
$y = 111$, $13579 + 12321 = 25900$ is not a square.

The algorithm for n with low digit 3 or 7: We state without proof that any solution to $3n = x^2 - y^2$ with $n = \pm 3 \mod 10$ will have either x or y divisible by 5. The adapted method for $10k \pm 3$ numbers uses the form $3n = x^2 - y^2$. Follow the $10k \pm 1$ method, using $3n$ in place of n throughout. In computing the limit prime L, we pretend that the prime 3 has already been checked.

If the method fails to find a solution, then n is prime. If the method succeeds in finding a solution $3n = x^2 - y^2 = (x - y)(x + y)$, one of the factors $x \pm y$ will have a factor of 3. This factor of 3 must be divided out to get a factorization of n.

Example: $n = 16543$. $3n = 49629$, $\sqrt{3n} \approx 222.8$
. The two-digit square differences are
$3n = x^2 - y^2 = 29 - 00 \equiv 25 - 96 \mod 100$.
Because $23 * 23 = 529$, we set $r = 23$. The x candidates are the set $\{50j \pm 23\}$.

Similarly, we use 96 as the digits for finding r for the set of y candidates. Because $14 * 14 = 196$ we set $r = 14$ and the candidate set is $\{50j \pm 14\}$.

Begin with x candidates, starting at $\sqrt{3n}$. The first x is 223.
$x^2 = 49729$, and $n - x^2 = 100$, a square.
The two factors are $(223 - 10)(223 + 10) = 213 * 233$.
We remove the factor of 3 from 213, getting 71.

Both 71 and 233 are prime.
The final factorization is $n = 16543 = 71 * 233$.
This example terminates quickly, because the factors 213 and 233 are roughly equal.

Example: $n = 21253$, $3n = 63759$, $\sqrt{3n} \approx 252.5$.
The two-digit square differences are
$3n = x^2 - y^2 = 84 - 25$ or $00 - 41 \mod 100$.
For 84, r is 22, the x candidates are the set $\{50j \pm 22\}$
For last two digits 41, r is 21, and the y candidates are $\{50j \pm 21\}$.
Begin with $x = 272$ and use 250 for the block size B.

x	x^2	$x^2 - 3n$	square?
272	73984	10225	no, 102 is too close to the square 100
278	77284	13525	no, hundreds digit is odd
322	103684	39925	no, hundreds digit is odd
328	107584	43825	no, hundreds digit is impossible
372	138384	74625	no, thousands.hundreds digits are impossible
378	142884	79125	no, hundreds digit is odd
422	178084	114325	no, hundreds digit is odd
428	183184	119425	no, hundreds digit is impossible
472	222784	159025	no, 1590 is too close to the square 1600
478	228484	164725	no, hundreds digit is odd

Having found no acceptable x in the first block B, we switch over to trying y candidates.

y	y^2	$3n + y^2$	/100	square?
21	441	64200	642	no, bad units digit
29	841	64600	646	no, tens.units not a multiple of 4
71	5041	68800	688	no, bad units digit
79	6241	70000	700	no, 7 is not a square
121	14641	78400	784	yes, 28^2

Using 280 for y, we compute $3n = 63759 = 280^2 - 121^2 = (280 - 121) * (280 + 121) = 159 * 401$.
Removing the factor of 3 from 159 gives $n = 21253 = 53 * 401$, with both factors prime.

8.3.2 The x Modulo 60 Method

This method scans through a list of x candidates, calculating $x^2 - n$ and checking if it's a square. If it is, we have a solution $y^2 = x^2 - n$, which we rearrange as $n = x^2 - y^2 = (x - y)(x + y)$, which is a factorization of n. (Remember to check if these factors can be further factored.)

Before doing the x scan, we look at n modulo some small primes and prime powers. Each possible remainder will define a (usually severe) restriction on x. We combine these restrictions. The result is a small set of possible values for x, modulo the product of the individual restriction moduli. The minimum moduli product is 60, and it is usually 120 or larger.

The restrictions on x can also be used with the mod 25 method, although they are often redundant. Because the modulo 25 method can also scan y candidates, we also include restrictions on y.

The limits on x and y are discussed in section 8.3.3.

x and y restrictions based on $n \mod 32$. We recall some information about squares:
The square of an odd number is $8j + 1$.
The squares mod 16 are 0, 1, 4, 9.
The square of an even number is a multiple of 4.
The square of a multiple of 4 is a multiple of 16.
The square of a $4i + 2$ number is $32j + 4$ because a $4i + 2$ number is twice an odd number.

For $n = x^2 - y^2$:
If $n = 4i + 1$, x must be odd and y must be even.
If $n = 4i + 3$, x must be even and y must be odd.

x and y restrictions based on $n \mod 32$		
$n \mod 32$	x	y
1	$\pm 1 \mod 8$	$0 \mod 4$
9	$\pm 3 \mod 8$	$0 \mod 4$
17	$\pm 1 \mod 8$	$0 \mod 4$
25	$\pm 3 \mod 8$	$0 \mod 4$
5	$\pm 3 \mod 16$	$2 \mod 4$
13	$\pm 7 \mod 16$	$2 \mod 4$
21	$\pm 5 \mod 16$	$2 \mod 4$
29	$\pm 1 \mod 16$	$2 \mod 4$
7	$0 \mod 4$	$\pm 3 \mod 8$
15	$0 \mod 4$	$\pm 1 \mod 8$
23	$0 \mod 4$	$\pm 3 \mod 8$
31	$0 \mod 4$	$\pm 1 \mod 8$
3	$2 \mod 4$	$\pm 1 \mod 16$
11	$2 \mod 4$	$\pm 5 \mod 16$
19	$2 \mod 4$	$\pm 7 \mod 16$
27	$2 \mod 4$	$\pm 3 \mod 16$

x and y restrictions based on $n \mod 9$		
$n \mod 9$	x	y
1	$\pm 1 \mod 9$	$0 \mod 3$
4	$\pm 2 \mod 9$	$0 \mod 3$
7	$\pm 4 \mod 9$	$0 \mod 3$
2	$0 \mod 3$	$\pm 4 \mod 9$
5	$0 \mod 3$	$\pm 2 \mod 9$
8	$0 \mod 3$	$\pm 1 \mod 9$

$n = 1 \mod 3$ implies y is a multiple of 3, and $x = \pm\sqrt{n} \mod 9$. If n is a multiple of 3 but not of 9, both x and y are not divisible by 3.
If n is a multiple of 9, x and y are not restricted mod 3 or 9.

x and y restrictions based on n mod 5		
n mod 5	x mod 5	y mod 5
1	0, ±1	0, ±2
2	±1	±2
3	±2	±1
4	0, ±2	0, ±1

Combining x restrictions for different moduli. The best restrictions (most stringent) leave only a few x values to test in each modular range. We get these by combining the restrictions in the tables above by using the method described in 8.2.2.

The combination of two (or more) restrictions will have a modulus that is the least common multiple (LCM) of the ingredient moduli. We will be combining restrictions for a power of 2, a power of 3, and a power of 5, so the LCM is simply the product of these moduli. The smallest modulus we can get is $4*3*5 = 60$, and the largest is $16*9*5 = 720$. Usually we'll get something in between. The number of possible residues is also the product of the possibilities for each ingredient modulus. This could be as small as $1*1*2 = 2$ or as big as $2*2*3 = 12$. One simplification is that the residue set can always be written as a bunch of ± values, so the maximum number of these ± pairs is 6.

8.3.3 Upper Limits

The Difference of Squares algorithm uses the value L to determine an upper limit on the search space for x and y. When all small divisors up to the limit L have been tried, then the upper limit for x is the average of L and n/L; the upper limit for y is the semi-difference $((n/L) - L)/2$. However, we can generally improve on that as the algorithm progresses by testing for more prime divisors of n, increasing L, and thus lowering the upper limits. Improving the upper limit is critical to using difference of squares for larger numbers because the x and y candidates can be large enough to bog down the mental arithmetic computing unit.

The main algorithm for difference of squares mentions that after trying a few x and y candidates, you should increase L. This section describes how to do that by analyzing divisor restrictions. This often will result in a formula for possible prime divisors of n that has about half as many possibilities as there would be without restrictions. The Difference of Squares algorithm recommends alternating two calculations: testing x and y candidates a few at time and increasing L by a few steps. This rest of this section describes how to develop the formula for possible prime divisors of n.

Usually, L is the smallest prime that has not been tested as a divisor of n. We always assume that small prime factors have been eliminated from the target number, so $L = 37$ is a good value to start with. If you have done divisor tests for larger primes, then you can start Difference of Squares with a larger L. However, before diving into the tests in section 4 for larger prime divisors, use divisor constraints as described in this section.

In general, we will be trying to get L to be a prime in the low hundreds; in some cases we will be able to show that L is near 500. If we do find a prime divisor, we can divide it out, and this may result in a residual target number that is easily tackled with another go-round with quadratic forms.

When L becomes so large that mental division is stressful, it is time to pull together the information about divisors. We can use divisor constraints as shown in tables 6, 7, and 8. If n was

previously analyzed with The Method, then there is a divisor restriction for it in table 6. Information for other constraints might have been derived while using The 120 Method (section 8.1). You can apply these formulas one at a time to each divisor candidate, or you can combine them into a single linear form and only test the primes that satisfy the form.

For example, if you find a solution to $n = x^2 + y^2$, with x and y relatively prime, then any odd divisor of n must be of the form $4j + 1$ (this fact is reflected in the first line of table 7. This rule also applies to multiples of n: if you solve $x^2 + y^2 = 2n$ or $3n$ or $4n$ or $13n$ etc, and x and y are relatively prime, then the odd divisors of n must be 1 modulo 4.

Section 8.2 has information on how to combine restrictions and derive a "main generator" that encompasses potential prime divisors of n, and use that to refine L.

Test sequential primes to see if they divide n. Start with 37 and work upwards. For each prime, see if it is in the set generated by the main generator formula (or, run the formula forward a step and see if it generates a prime). Also check to see if the number satisfies any of the secondary formulas. If it passes all checks, the then use any applicable tests from section 4. After a few steps, continue with the main algorithm in Difference of Squares.

If L is greater than the cube root of n, then its divisors must be primes greater than that value, and there are at most 2 of them. That's when the information from table 1 becomes valuable.

The simple divisor tests eliminate divisors less than 37, but if you've done the "m" prime divisor tests from section 4 and a few of the optional tests following that, and have checked 37, then the smallest untried prime divisors are 59, 67, 79, 83, and 89. If we are working with a number that has the $4j + 1$ divisor constraint, the smallest possible divisor is 89, because $59 \ldots 83$ are all $4j + 3$ primes. The $4j + 1$ primes in this range are 61 and 73, which are covered in the m tests. Table 7 lists some divisor restrictions. If you know several restrictions, they can all be applied.

Examples of x restrictions with Difference of Squares Modulo 60. These examples use information in the tables in section 8.3.2.

Example: $n = 13579$,
$\sqrt{n} \approx 116.5$
$n \equiv 11 \mod 32$ has $x \equiv 2 \mod 4$
$n \equiv 7 \mod 9$ has $x \equiv \pm 4 \mod 9$
$n \equiv 4 \mod 5$ has $x \equiv \pm 0 \mod 5$ or $x \equiv \pm 2 \mod 5$
The combined x formula can be calculated using the method described in "Combining values for two relatively prime moduli". The result is $180j \pm \{22, 50, 58\}$.
$x^2 - n = 27225$, which is a square. This is a solution, and we compute $y = 165$, and the factors $x - y = 37$, and $x + y = 367$.

Example: $n = 16543$
$\sqrt{n} < 128$
$n \equiv 31 \mod 32$ has $x \equiv 0 \mod 4$
$n \equiv 1 \mod 9$ has $x \equiv \pm 1 \mod 9$
$n \equiv 3 \mod 5$ has $x \equiv \pm 2 \mod 5$
Combining these gives the formula $x = 180j \pm \{8, 28\}$
Trials would start at $180 - 28$, which is larger than $\sqrt{n}$, yielding
$x = 152$. $x^2 - n = 6561$, which is the square of 81. This is a solution, and we compute $y = 81$ and the factors $x - y = 71$, and $x + y = 233$.

Example: $n = 21253$
$\sqrt{n} < 145$
$n \equiv 5 \mod 32$ has $x \equiv \pm 3 \mod 16$
$n \equiv 4 \mod 9$ has $x \equiv \pm 2 \mod 9$
$n \equiv 3 \mod 5$ has $x \equiv \pm 2 \mod 5$
The combined form is $720j \pm \{83, 173, 227, 317\}$
Starting from the first value larger than the square root of n, we try 173, then 227. $x^2 - n = 30276$, which is a square. We compute its square root and have the solution $x = 227$, $y = 174$, and the factors $(x - y) = 53$, $(x + y) = 401$.

This is an example of using divisor restrictions to increase L.
Example: $n = 121987$,
$\sqrt{n} \approx 349$, $\sqrt[3]{n} \approx 49$. Because $n \equiv 3 \mod 8$, we tried The Method with the form $x^2 + 2y^2$. This finds no solutions, and therefore we have a divisor restriction from table 6.
n is composite, and must have at least two factors from the set $8j + \{5, 7\}$. A little dabbling with The 120 Method turns up the solution $n - 3 * 201^2 = 784 = 28^2$, and thus $n = 28^2 + 3 * 201^2$ with $-ab$ value -3. Table 7 tells us that any divisor of n must be in the set $\{6j + 1\}$.
We compute the combined restrictions, intersecting $\{6j+1\}$ with $\{8j+5, 7\}$. The combined modulus will be $lcm(6,\ 8) = 24$.
The sequence of $6j + 1$ values is 1, 7, 13, 19. We stop at the lcm, 24.
Testing each value modulo 8, the remainders are 1, 7, 5, 3.
We accept 7 and 13, and discard 1 and 19.
Our combined restriction on possible divisors of n is $24k + \{7, 13\}$.
We assume as always that primes up to 31 have been checked; set $L = 37$.
The lower limit for x is $\sqrt{(n)} \approx 349$
. The upper limit for x is $(L + n/L)/2 \approx 1666$.
Using the modulo 60 method, we find: $n \equiv 3\ (mod\ 32)$, $n \equiv 1\ (mod\ 9)$,
and $n \equiv 2\ (mod\ 5)$.
These have three linear expressions for x:
$x = 4j + 2$, $x = 9j \pm 1$, $x = 5j \pm 1$.
Using the method of 8.2.2, combining the x restrictions gives $x = 180j \pm \{26, 46\}$.
The range for x is $350 \leq x \leq 1666$.
We increase L so as to reduce the upper limit on x.
If we can raise L to 100, the upper limit for x will drop to $(100 + 1219.87)/ \approx 660$.
Our possible divisors for n are $24j + \{7, 13\}$. The first untested prime is 37, and the sequence continues 55, 61, 79, 85, 103, ...
We must check the divisors 37, 61, and 79; 55 and 85 are composites and don't need to be checked.
Each of $\{37, 61, 79\}$ fails. We set $L = 103$. The upper limit for x is 643.
Because the new L exceeds cube root of n, n has at most two factors.
The first element of $180j \pm \{26, 46\}$ that is bigger than 349 is $360 + 26 = 386$.
Trying out $x = 386$: $386^2 - n = 27009$. The nearest square is $164^2 = 26896$, which is not a solution.
Trying out $x = 406$: $406^2 - n = 42809$. The nearest square is $207^2 = 42809$, a solution!
The factors are 406 ± 207; $n = 199 * 613$.
Because n has at most two factors, both divisors must be prime.

9 If you got this far ...

In writing this guide, we came to realize that mental factoring requires a very good memory and a dedicated love of arithmetic. These skills are not important in the modern world where you can ask your smart watch to lookup number factorizations. Then why try to master mental factoring?

Mathematical discovery propels scientific progress, and mental arithmetic is one pathway to that goal. Numbers and their patterns have inspired mathematicians of the past, and numbers remain at the heart of mathematics and computing. Mental factoring is a skill that can be personally satisfying, but it is also a way to discover other relationships among numbers and to understand deeper theorems.

Whether you use mental factoring as a parlor trick or an excursion into number theory, we hope you have found some pleasing nuggets of arithmetical techniques and feel the enchantment of numbers.

Appendix A Bibliography

"The Great Mental Calculators", Steven B. Smith, Columbia University Press, 1983, ISBN 0-231-05640-0.

"The Art of Mental Factoring", Willem Bouman, 2012, unpublished document.

"The Trachtenberg Speed System of Basic Mathematics", translated and adapted by Ann Cutler and Rudolph McShane, Doubleday and Company, New York, 1960, LCCN 60-13513.

Appendix B A Mental Factoring Cheat Sheet

Quick divisibility tests
2: low order digit of n is even. **3**: sum of the digits of n is divisible by 3.
5: low order digit is zero or 5. **7**: if $n = abc$, then n modulo 7 is $2 * a + bc$.
7, 11, and 13: $abcd$ modulo 1001 is $bcd - a$.
11: For abc, if $b = a + c$ or $b + 11 = a + c$, then $abc = 11 * ac$ or $11 * zc$ where $z = a - 1$. $11|abcd$ iff $a + c$ and $b + d$ are equal or if the difference is 11. **13**: $n/300 = \{q, r\}$, $13|(q + r)$ iff $13|n$.
37: If n has 3 digits, rotation preserves divisibility by 37.
97, 101, 103, ...: each $100 \pm n$ divides $10000 - n^2$.
The Method for Factoring n: Using Table 2, select the quadratic form(s) and the term that is divisible by 5 (NB: if

Table 9: Useful and Memorable Multiples of Small Primes

	Column - high order digits, Row - units digit			
	1	3	7	9
1	1001	299, 1001	102, 1003, 6001, 10013	399, 1007, 1501, 7999, 10013
2		2001		2001
3	992, 3999, 10013		111, 999	
4	10004	301, 3999, 10019	10011	
5		1007, 10017		1003, 20001
6	10004		201	
7	994, 10011	511, 1022, 10001		1501, 3002
8		996, 20003		801
9			9991	
10	9999	9991	9951, 20009	981, 10028, 40003
11		1017, 20001		
12			1016, 8001	
13			10001	
24	964, 20003			

there is no entry for n, use the 120 Method and/or Difference of Squares). Solve each form modulo 100 using the fact that one of the squares is a multiple of 25. For each form, there will be one or two solutions < 25, call them r (and s). The candidates for the non-multiple-of-5 term are the set $\{50i \pm r, 50i \pm s\}$ such that the square is less than n (or $n/2$ or $n/3$).

For each candidate value, plug in its square into the quadratic form and solve for the square of the other variable. If that solution is, indeed, a square, and if $\gcd(x, y) = 1$, then the x and y values are a solution to the quadratic form.

If you find **two solutions**, the number is composite. Calculate the factors using vector addition/subtraction on the two solutions to minimize the result vector (u, v) and/or to have both terms divisible by 5. Divide both terms by $\gcd(u, v)$. Substitute u and v for x and y in the QF; the result will have a factor of n.

If all potential candidates less than the square root of n have been tried, and there is only **one solution**, then n is prime. If there are **no solutions**, n is composite; the factorization must be done with another method.

Example: 4469. Per table 2, we use the QF $x^2 + y^2$. Either $x^2 \equiv 0 \mod 100$ or $x^2 \equiv 25 \mod 100$. First assume 0 mod 100; then $r = 13$ because $13 * 13 \equiv 69 \mod 100$. The y candidates are $50j \pm 13$, and $y < 70$. Possibilities are 13, 37, and 63.

$4469 - 13^2 = 4300$ which is not a square.

$4469 - 37^2 = 4469 - 1369 = 3100$ which is not a square.

Table 10: Properties of quadratic form terms

residue	low digit	quadratic form	5 divides	x parity	y parity	$r^2 \mod 100$
1 mod 4	1 or 9	$n = x^2 + y^2$	either	either	1-p(x)	n, $n-25$
1 mod 4	3 or 7	$2n = x^2 + y^2$	either	odd	odd	$n-25$
3 mod 8	1 or 9	$n = x^2 + 2y^2$	y	odd	odd	$n-50$
		$3n = x^2 + 2y^2$	x	odd	even	$(3n-25)/2$
3 mod 8	3 or 7	$n = x^2 + 2y^2$	x	odd	odd	$(n-25)/2$
		$3n = x^2 + 2y^2$	y	odd	even	$3n$
7 mod 24	1 or 9	$n = x^2 + 3y^2$	y	even	odd	$n-75$
		$4n = x^2 + 3y^2$	y	odd	odd	$4n-75$
7 mod 24	3 or 7	$n = x^2 + 3y^2$	x	even	odd	$n/3$
		$4n = x^2 + 3y^2$	x	odd	odd	$(4n-25)/3$

$4469 - 63^2 = 4469 - 3969 = 500$ which is not a square. Therefore, $x^2 \equiv 0 \mod 100$ is impossible.

Now assume $x^2 \equiv 25 \mod 100$; find r such that $r^2 \equiv 69 - 25 \mod 100 = 44$. That would be 12. The y candidates are $50j \pm 12$, $y < 70$: 12, 38, and 62.

$4469 - 12^2 = 4325$ which is not a square because the hundreds digit is odd.

$4469 - 38^2 = 4469 - 1444 = 3025 = 55^2$. This is a representation of 4469 as $55^2 + 38^2$.

$4469 - 62^2 = 4469 - 3844 = 625 = 25^2$.

Add the two representations $(55, 38)$ and $(25, 62)$ to get $(80, 100)$. The gcd is 20, dividing it out yields $(4, 5)$, $4^2 + 5^2 = 41$. By mental arithmetic, $4469/41 = 109$.

Filters. $n \equiv x^2 + y^2 \mod 3$. The squares modulo 3 are 0 and 1, the corresponding square roots are 0, ± 1. Let m be the residue of n modulo 3. List all solutions to $m \equiv u^2 + v^2 \mod 3$ using 0 and 1 for u^2 and v^2. When trying an x or y candidate, check that it is consistent with the solution set modulo 3. If it isn't, discard it. You can do the same thing modulo 9 (squares are 0, 1, 4, and 7), modulo 7 (squares are 0, 1, 2, and 4), or modulo 49 (squares are 0, $7j + \{1, 2, 4\}$).

Modulo 100 filters. Match the parity of the hundreds digits in n and the square of a candidate value. If y is an odd multiple of 5 and the QF is $x^2 + 2y^2$, use the pattern of thousands-hundreds digits. If the QF is $x^2 + 3y^2$ and the tens digit of n is odd, match the parity of the hundreds digit of $n - 25$ or $n - 75$ to the parity of the hundreds digit of the candidate.

Example: $1000009 = 1000^2 + 3^2$. From Table 2, $y^2 \mod 100$ is either 00 or 25.
$09 - 00 = 9 = x^2 \mod 100 \rightarrow r = 3$, and $09 - 25 = 84 = x^2 \mod 100 \rightarrow r = 22$, so the x candidates are 3, 22, $50 + 3$, $50 - 3$, $50 - 22$, $50 + 22$, ...; $50k \pm 22$ is modified to $100k \pm 28$ to match hundred's digit parity. Squares modulo 9 eliminate 997; squares modulo 7 and modulo 9 accept 972. $1000009 - 972^2 = 55225 = 235^2$. Combine $(1000, 3)$ with $(235, 972)$ to get factors 293 and 3413.

The 120 Method. Find solutions to $kn = ax^2 + by^2$ where k, a, and b are small. For each solution, add $-ab$ to the set Q and compute the closure of Q under multiplication, exact division, and division by a square.
For a $4i + 3$ number, if 2, 3, and 5 (irrespective of sign) are in Q, n can be factored or proved prime. For a $4i + 1$ number, if -1, 2, 3, and 5 are in Q, n can be factored or proved prime.
The trial divisors of n for a $4i + 3$ number: $120j + \{1, 49, d, e\}$ where $d = n \mod 120$, $e = 60 - 11d \mod 120$ and j goes from 0 to $\sqrt{n}/120$; for a $4i + 1$ number: $120j + \{1, 49\}$ where j goes from 0 to $\sqrt{n}/120$. Only prime divisors need be tested.

Example 2503: $n = 50^2 + 3 = 51^2 - 98 = 15 * 13^2 - 32$. The corresponding $-ab$ values are -3, 2, 30. By closure, $Q = \{2, 3, 30, 15, 5\}$. Then $d = 103$, $e = 7$; trial divisors are $120j + \{1, 7, 49, 103\}$. Testing 7 fails, 49 is composite, $103 > \sqrt{n}$. Therefore n is prime.

The Difference of Squares Method. Find x and y such that $n = x^2 - y^2$. One of the two squares will end in 00 or 25. Solve for the other square modulo 100 using the following equations (if the final digit of n is 3 or 7, use $3n$ throughout).

For $n \equiv 1 \mod 4$:
$x \equiv 5 \mod 10$, $y^2 \equiv 25 - n \mod 100$
$y \equiv 0 \mod 10$, $x^2 \equiv n + 0 \mod 100$

For $n \equiv 3 \mod 4$:
$x \equiv 0 \mod 10$, $y^2 \equiv 0 - n \mod 100$
$y \equiv 5 \mod 10$, $x^2 \equiv n + 25 \mod 100$

Of the two solutions, one is based on x, the other on y. Use the solutions to build candidate sets of the form $\{50j \pm r\}$ as in The Method; one is for x candidates, the other is for y candidates. Alternate trying x candidates and y candidates, then change the limits for x and y as described next. If x and y both exceed their limits, then n is prime.

Limits for x and y. Use divisibility tricks to eliminate possible divisors up to $L = 37$. Call the upper limit for x L_x. $L_x = (L + n/L)/2$; the upper limit for y is $L_x - L$. To change the limits, use mental arithmetic to test more primes in sequence, set L to the smallest untested prime, and recompute the limits. Divisor restrictions (see full paper) can eliminate some primes without testing.