Number Theory

Tom Elliott

February 14, 2020

Contents

Part I

Fundamentals

Chapter 1

Integers

Integers

The *natural* or counting numbers which everyone learns very early in life are $1, 2, 3$ and so on.

One can get hung up on the question of whether the natural numbers would exist without the problem of counting a dozen sheep or all twenty of our fingers and toes. Leopold Kronecker famously said "God made the integers; all else is man's handiwork".

We will not worry about where they come from.

Mathematicians refer to the *set* of natural numbers and give that set a special symbol, $\mathbb{N}$. We write

$$\mathbb{N} = \{1, 2, 3 \dots\}$$

The brackets contain between them the elements or members of the set. The dots mean that this sequence continues forever.

How can we decide whether a particular n is in the set if we can't enumerate all of its members? We can tell by its form whether some n is a natural number or not.

If this seems problematic, you might call $\mathbb{N}$ a class instead (Hamming); we carry out *classification* to decide whether n is a natural number.

The notion of an unending sequence can be unnerving upon first encounter.

construction of N

To construct the set $\mathbb{N}$, start with the smallest element, 1. Then

$$1 + 1 = 2$$

$$2 + 1 = 3$$

$$3 + 1 = 4$$

$$\ldots$$

Add successive elements by forming $a_n + 1 = a_{n+1}$.

$\mathbb{N}$ is an infinite set.

We say there is no largest number in $\mathbb{N}$, no largest $n \in \mathbb{N}$. The symbol $\in$ means "in the set" or "is a member of the set".

Proof:

Suppose $\mathbb{N}$ did have a largest member, M.

Well, what about $M + 1$? By the definition we can construct it and it is clearly a member of the set, but $M + 1 > M$ so M is not the largest number in the set.

This is a proof by contradiction that $\mathbb{N}$ is infinite.

□

set membership

Sometimes people say that

$$0 \in \mathbb{N}$$

(0 is a part of the set) but most do not, and we will follow the definition given above. If you wanted to be explicit about this you could write

$$0 \notin \mathbb{N}$$

What do we mean by infinity? We mean an upper bound on the natural numbers, and later, all rational and indeed all real numbers.

All numbers $n \in \mathbb{N}$ have the property that n is contained in the interval $[1..\infty)$. However, ∞ is *not* considered part of the interval, and that is the meaning of the the right parenthesis.

∞ is not a number so it probably doesn't even make sense to write $\infty \notin \mathbb{N}$.

least element

$\mathbb{N}$ does not have a greatest number, but it does have a smallest or least one. If pairwise comparisons are carried out, a single element, the number 1, has the property that $1 \leq n$ for all numbers $n \in \mathbb{N}$. As we go on, we will find that other types of numbers (rationals and real numbers), do not have a least positive number.

well-ordered property

Since we can also find the least member of the set excluding 1, written $\mathbb{N} \setminus 1$, we can order every number in $\mathbb{N}$.

This property is called the **well-ordered** property.

the Integers

The set $\mathbb{Z}$ contains all the members of $\mathbb{N}$ plus their negatives, as well as the special number 0, often called the additive identity since $0 + n = n$ for all $n \in \mathbb{N}$.

$$\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \ldots\}$$

$\mathbb{Z}$ stands for the German word *Zahlen*, number. The set $\mathbb{Z}$ is usually referred to as the integers.

$\mathbb{Z}$ is also an infinite set and also has the well-ordered property. To show this simply order all numbers $n > 0$ with respect to zero using $<$, and all the numbers $n < 0$ using $>$.

Chapter 2

Infinity

infinity

The symbol for infinity is ∞.

In the old days, they used to write things like

$$\frac{1}{0} = \infty, \qquad \frac{1}{\infty} = 0$$

John Wallis wrote $24/0 = \infty$, in 1656, which is when the ∞ symbol was introduced with its current definition. Even Euler argued that $n/0 = \infty$ when it suited him,

It is claimed that the symbol derives from the Roman symbol for 100 million. That's interesting. I never knew any symbols larger than M, for one thousand. And I'm not sure I believe it, but that's what some people say.

According to

https://notevenpast.org/dividing-nothing/

> On 21 September 1997, the USS Yorktown battleship was testing "Smart Ship" technologies on the coast of Cape Charles,

> Virginia. At one point, a crew member entered a set of data that mistakenly included a zero in one field, causing a Windows NT computer program to divide by zero. This generated an error that crashed the computer network, causing failure of the ship's propulsion system, paralyzing the cruiser for more than a day.

no division by zero

There is a fundamental problem when we set up a division problem and 0 is in the denominator. What goes wrong when we attempt to divide by zero?

$$\frac{a}{0} = ?$$

Well, what do we mean by an expression such as

$$\frac{a}{b} = c$$

By *definition*, we mean that we will try to find c such that

$$c \cdot b = a$$

For the integers, of course, there is the problem of a possible remainder. Let us leave that aside for a minute.

Suppose we have $c \cdot b = a$ but then take b to be very small though not 0. In that case, the number c may get very large. That's OK.

We can make b as small as we wish by making c large enough or vice versa. And we can say that as $b \to 0$, then $c \to \infty$.

But we can't say $a/0 =$ some number.

If there were such a number (say $a/0 = \infty$, infinity), then what about

$$\frac{b}{0} = ??, \qquad \frac{c}{0} = ??$$

It would mean that whatever the expression $b/0$ is equal to, when multiplied by zero, we would obtain any number whatsoever. This makes no sense.

Here is another, perhaps silly, example.

$$0 \cdot 1 = 0$$

$$0 \cdot 2 = 0$$

so

$$0 \cdot 1 = 0 \cdot 2$$

but then

$$1 = 2$$

By definition, we do not allow division by zero.

infinity is not a number

And we can't answer the question what is $2 \cdot \infty$? If we allowed multiplication by ∞ then the only reasonable answer would be

$$2 \cdot \infty = \infty$$

so then also

$$n \cdot \infty = \infty$$

where n is any number. But then say

$$2 \cdot \infty = 3 \cdot \infty$$

so, cancelling

$$2 = 3$$

This would be a mess.

By definition, *infinity is not a number* and division by 0 is *undefined*.

limits

Often people say that calculus is all about limits, and they are certainly where you start in proving the theoretical basis of the field.

We will keep the discussion of limits and ϵ-δ formalism to a minimum for the reasons explained in the Introduction. But let us try to establish an intuitive idea about what we mean when we say "in the limit as $N \to \infty$".

Above we had that there is no greatest integer.

A corollary of that is the limit

$$\lim_{n\to\infty} \frac{(n+1) - n}{n} = 0$$

Why? As n increases without bound, the difference between successive numbers, as a fraction of n, tends to zero.

To get an idea about this, first simplify by multiplying by $1/n$ on top and bottom. Then we have

$$\lim_{n\to\infty} \frac{(1 + 1/n - 1)}{1} = \frac{1}{n}$$

We say that $1/n$ *tends* to zero as $n \to \infty$, and so does $[(n+1) - n]/n$.

Chapter 3

Primes

prime numbers

As you know, the positive integers larger than 1 are of two types:

- a prime number p has only two factors, p itself and 1
- a composite number has at least one additional factor. Either the number is a perfect square of a prime, or it has additional factors: $n = p_1, p_2 \ldots p_k$.

The first ten primes are:

```
2 3 5 7 11 13 17 19 23 29 ...
```

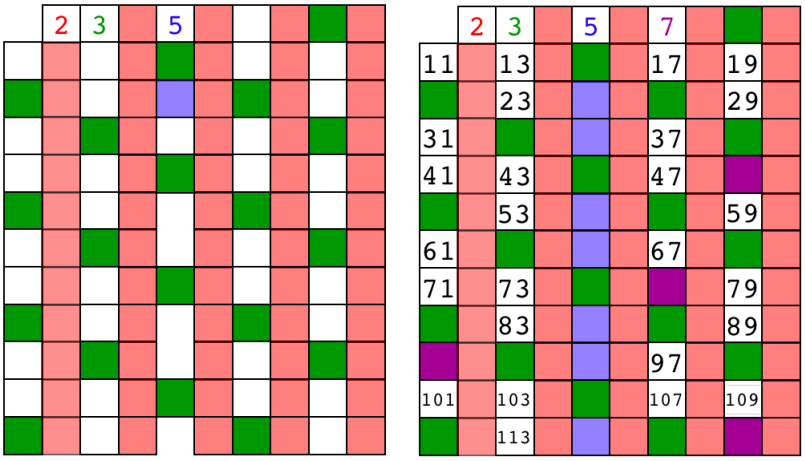
The sieve of Eratosthenes

Eratosthenes is famous in mathematics for his "sieve" which allows one to determine which numbers are prime in an economical fashion.

We will take note of him again in talking about the circumference of the earth. He was a contemporary of Archimedes and became the chief librarian at the Library of Alexandria when he was only about 35 years old.

The sieve operates by first writing down all the integers to some upper limit (here 120). To carry out the process manually it is convenient to use rows with 10 values, so there are 12 rows in all here. Most of the boxes have not yet been numbered (below, left).

Starting with the first prime number, 2, eliminate all the numbers divisible by 2 (all the red numbers, or even numbers). Here this has been done by coloring red all squares with numbers ending in $2, 4, 6, 8, 0$.



Next, do the same thing with 3 (green). 6 was already eliminated previously, but odd multiples of 3 like 9, 15 and 21 go away at this step.

The next larger number that still has a white square is 5. All the squares eliminated at this step are white ones in the fifth row, starting with 25. Continue with 7, eliminating $49, 77, 91$ and 119.

Notice that the smallest number to be eliminated with 7 is $7^2 = 49$, similarly with 5 the first was 25. The first number to be eliminated with q is q^2. This is always true.

The sieve now ends (for this upper bound of 120).

The rule is that at the beginning of a round, test the next candidate

prime q by squaring and comparing with the upper limit L. If $q^2 > L$, we terminate. So after that round using 7 , the smallest remaining integer is 11, but we terminate since $11^2 = 121 > 120$.

The graphic shows all the numbers which have yet to be eliminated after the round of 7. All of these numbers, 11, 13, 17, and so on, as well as those used as divisors for each round of the sieve $(2, 3, 5, 7)$, are prime numbers.

By testing for division by $2, 3, 5$ and 7, we have found the first 30 prime numbers.

```
 2   3   5   7  11  13  17  19  23  29
31  37  41  43  47  53  59  61  67  71
73  79  83  89  97 101 103 107 109 113
```

From a performance standpoint, it is important that we do not need to carry out division. All that is really needed is repeated addition. Coding this algorithm in, say, Python is a good challenge.

A bigger challenge is to come up with a method to *grow* the list of primes on demand. This can be done by keeping track of the first value to be tested above the limit, for each prime in the current list.

recognizing primes quickly

We did a bit of this in the previous chapter, we'll leave this here as review.

There are school problems that require you to factor numbers at least up to 100, maybe more, quickly. It can be helpful to learn to recognize the primes in this range.

- First, primes end in one of the digits: $1, 3, 7, 9$.
- Test quickly for 3 as a factor by the digit sum trick.

◦ Test 7 as a factor by trial multiplication or the 7 trick we talked about before.

For trial multiplication, let's do the first row, for an example:

```
11 21 31 41 51 61 71 81 91 101 111
```

You should recognize 11 as prime, immediately. Then remove the numbers whose digits add up to 3 or a multiple, leaving

```
31 41 61 71 91 101
```

Then, trial multiplication by 7 to get a number ending in 1.

The way I do this is by computing the difference with a number that is divisible by 7. If the difference is not divisible by 7, then neither is the candidate number.

For example, since we're in the ones column, I'm thinking $7 \cdot 3 = 21$ and so $7 \cdot (10 + 3) = 70 + 21 = 91$, so we can eliminate 91 as a possible prime.

Furthermore, by comparison with 91:

```
 91 - 71 = 20
 91 - 61 = 30
 91 - 41 = 50
101 - 91 = 30
```

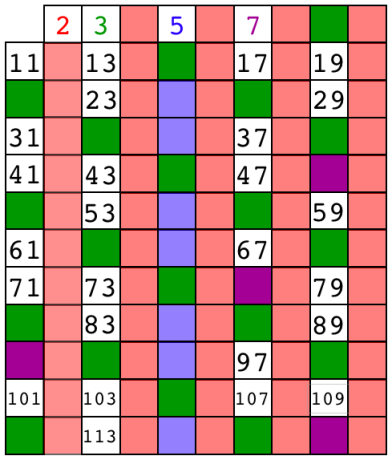
None of these differences is divisible by 7, so the numbers themselves are not, either.

I trust you recognize that 31 is 3 more than $7 \cdot 4$.

We do not need to test any primes larger than 11. All multiples of 11 are repeated double digits $(22, 33 \ldots)$, until 110.

That leaves:

```
31 41 61 71 101
```



infinite primes

Euclid has a theorem and a proof that the number of primes is infinite.

Proof:

By contradiction.

Suppose the set of primes is finite, and that p_1, $p_2 \ldots p_k$ are all of the primes. Construct the following numbers:

$$P = (p_1 \cdot p_2 \cdot \ldots p_k)$$

$$Q = P + 1$$

For a prime number p to evenly divide Q, it must divide the difference between Q and P. But that difference is 1 and so can't be divided evenly by any prime.

Therefore, none of the known primes divides Q and at least one of these is true:

- Q is a prime not in the set of known primes

- the set was originally incomplete

The assumption that the set of primes is finite leads to a contradiction.

□

Even for a relatively small number of primes, we may encounter the second situation. Start with the first prime: 2:

$$2 + 1 = 3 \text{ (prime)}$$

$$2 \cdot 3 + 1 = 7 \text{ (prime)}$$

$$2 \cdot 3 \cdot 7 + 1 = 43 \text{ (prime)}$$

$$2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$$

1807 is *not* prime. $(1807 = 13 \cdot 139)$.

testing primality

This is a pretty deep subject. However, a simple filter to apply first is to ask:

- Is the last digit one of $\{0, 2, 4, 6, 8\}$, i.e. is the number even?
- Does the number end in 5?
- Or is the number divisible by 3 or 9?
- Is the number divisible by 7.

We looked at these tricks in a previous chapter ().

A more general observation is that all primes greater than 3 are of the form $4k + 1$ or $4k + 3$, for integer k. That's because $4k$ and $4k + 2$ are even, and $4k + 4 = 4(k + 1)$.

Any composite number n has a unique prime factorization. Its smallest prime factor p has the property (easily proved):

$$p^2 \leq n$$

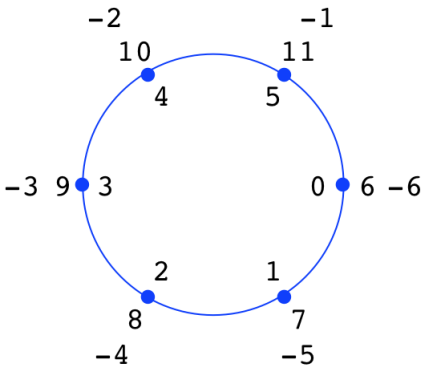
Therefore, it suffices to check whether the prime numbers less than or equal to the square root of n divide n. If the square root is not an integer, we need check only the next smallest integer, what is called the *floor* of the value. If no prime less than that divides n, then n is a prime.

This can be improved still more.

https://en.wikipedia.org/wiki/Primality_test

Chapter 4

Modular arithmetic



Modular arithmetic is sometimes called "clock" arithmetic. Modular arithmetic is all of

- addition
- multiplication
- subtraction
- division

with integers, all carried out modulo (or mod) some integer n. The rule is to keep the remainder after dividing by the modulus. This is

the "mod" operation.

We say that $5 = 17 \bmod 12$. A new term is introduced: congruence. 5 is congruent to 17 mod 12 and the symbol for that is $5 \equiv 17$.

Hardy:

> The absolute values of numbers are comparatively unimportant; we want to know what time it is, not how many minutes have passed since the creation.

Addition

Here is an addition table for $n = 7$:

```
    0  1  2  3  4  5  6
   --------------------
0 | 0  1  2  3  4  5  6
1 | 1  2  3  4  5  6  0
2 | 2  3  4  5  6  0  1
3 | 3  4  5  6  0  1  2
```

Example: $3 + 5 = 8 \equiv 1 \bmod 7$.

Since 36 mod 7 = 1 and 15 mod 7 = 1 as well, it follows that

$$36 \equiv 15 \equiv 1(\bmod 7)$$

Multiplication

7							
1	|	0	1	2	3	4	5	6
2	|	0	2	4	6	1	3	5
3	|	0	3	6	2	5	1	4
4	|	0	4	1	5	2	6	3
5	|	0	5	3	1	6	4	2
6	|	0	6	5	4	3	2	1

12												
1	|	0	1	2	3	4	5	6	7	8	9	10	11
2	|	0	2	4	6	8	10	0	2	4	6	8	10
3	|	0	3	6	9	0	3	6	9	0	3	6	9
4	|	0	4	8	0	4	8	0	4	8	0	4	8
5	|	0	5	10	3	8	1	6	11	4	9	2	7
6	|	0	6	0	6	0	6	0	6	0	6	0	6
7	|	0	7	2	9	4	11	6	1	8	3	10	5
8	|	0	8	4	0	8	4	0	8	4	0	8	4
9	|	0	9	6	3	0	9	6	3	0	9	6	3
10	|	0	10	8	6	4	2	0	10	8	6	4	2
11	|	0	11	10	9	8	7	6	5	4	3	2	1

The tables were constructed by standard multiplication, followed by the indicated mod operation.

We see certain patterns:

◦ For $n = 12$ factors which are co-prime to 12 (2, 3, 4, 6, 8, 9, 10) cycle back to 0 more than once, as a consequence they cannot generate all values $< n$ as products. The period t is such that $a \cdot t \equiv 0 \bmod n$.

◦ Also for $n = 12$, rows made by multiplication of primes generate all the integers less than 12.

◦ It's always true that 1 and $n-1$ generate all the values $< n$.

That's because

$$a \cdot b + a \cdot (n - b)$$
$$= ab + an - ab$$
$$= na \equiv 0 \text{ (mod n)}$$

So for example, with $b = 3$ we had $11 \cdot 3 = 9$ and $11 \cdot 9 = 3$, which add to zero, mod 12.

For $n = 7$, every number generated all the other ones. This always happens for n prime.

important

Since all integers smaller than n are generated from each starting integer in the special case, a *unique result must be produced for each multiplication.*

Further, if a number, multiplied by all the elements of the field generates all the elements of the field, then exactly one of those results must be equal to 1.

The two multiplicands with this property are called *multiplicative inverses.*

An interesting case is one where n is not prime, yet certain integers other than 1 and $n-1$ generate all the integers smaller than n. This happens when the smaller number is co-prime with n (they have no common factors other than 1).

For example, neither 10 nor 21 is prime but the row for times 10 mod 21 is:

```
10 20 9 19 8 18 7 17 6 16 5 15 4 14 3 13 2 12 1 11
```

which is itself something to think about.

Division

Consider multiplication mod n = 7 again:

7							
1	|	0	1	2	3	4	5	6
2	|	0	2	4	6	1	3	5
3	|	0	3	6	2	5	1	4
4	|	0	4	1	5	2	6	3
5	|	0	5	3	1	6	4	2
6	|	0	6	5	4	3	2	1

Since $2 \cdot 4 = 1 \pmod 7$, 4 and 2 are *multiplicative inverses.*

Similarly $(3, 5)$, $(6, 6)$ and$(1, 1)$ are as well.

We claim that division by q is the same as multiplication by the multiplicative inverse of q since, e.g.

$$\frac{5}{4} = \frac{5}{4} \cdot \frac{2}{2} = 5 \cdot 2 \equiv 3 \ (\text{ mod } 7)$$

which can be checked by

$$3 \cdot 4 \equiv 5$$

Powers

With $n = 7$, consider the powers of each $i < 7$:

	1	2	3	4	5	6
1 |	1	2	3	4	5	6
2 |	2	4	1	2	4	1
3 |	3	2	6	4	5	1

```
4 | 4  2  1  4  2  1
5 | 5  4  6  2  3  1
6 | 6  1  6  1  6  1
```

This table can be a challenge to construct. I wrote a script to help with the calculations the first time through.

We discover that the powers of 3 and 5 (but not $2, 4, 6$) give all the integers < 7.

We see another interesting pattern, that each $a < n$ raised to the $n-1$ power, is equal to one. This is explained by Fermat's little theorem, which we'll get to.

This is what wikipedia means when they talk about the "q - 1 power of unity".

Chapter 5

Congruence

Here are three equivalent statements about congruence. Two numbers a and b are congruent modulo m (or with modulus m) if

- they leave the same remainder when divided by m.

$$a = jm + r, \qquad b = km + r$$

and then we have that

$$a - b = m(j - k) = dm$$

- m divides the difference between a and b evenly

so

- $a = b + dm$

This is written as $m|a - b$ and sometimes as

$$a \equiv b \pmod{m}$$

example

$$7 \equiv 12 \pmod{5}$$

because $7 = 1 \cdot 5 + 2$ and $12 = 2 \cdot 5 + 2$. This extends to negative numbers

$$-8 = -2 \cdot 5 + 2$$

The numbers evenly divisible by $m = 5$ are

$$\cdots -10, -5, 0, 5, 10 \ldots$$

because we can find integer d such that $dm = a$ or $dm = b$.

If there is a remainder, for positive a, the difference between a and the next *smaller* multiple of m is r.

This is also true for $b < 0$, but to avoid confusion remember that the next smaller multiple is *larger* in absolute value. The multiples of 5 that "bracket" -8 are $-2 \cdot 5$ and $-1 \cdot 5$. Both these statements are true:

$$-10 < -5$$

$$|-10| > |5|$$

For $a > 0$ and $b < 0$, it is still true that m divides the difference between a and b evenly. The difference between 12 and -8 is 20, which *is* evenly divisible by 5.

Courant and Robbins:

> The usefulness of Gauss's congruence notation lies in the fact that congruence with respect to a fixed modulus has many of the formal properties of ordinary equality.

For example, congruence is transitive. If (mod m):

$$a \equiv b, \qquad b \equiv c \quad \rightarrow \quad a \equiv c$$

arithmetic

Congruences may be added, subtracted and multiplied. Simply consider the remainders modulus m. If (mod m):

$$a \equiv r_1, \qquad b \equiv r_2$$

then

$$a + b \equiv r_1 + r_2$$
$$a - b \equiv r_1 - r_2$$
$$ab \equiv r_1 \cdot r_2$$

where it is recognized that the results $r_1 \pm r_2$ and $r_1 \cdot r_2$ may need to be taken module m again.

Proofs:

We can find j and k such that

$$a = jm + r_1, \qquad b = km + r_2$$

so

$$a + b = (j + k)m + r_1 + r_2$$
$$a - b = (j - k)m + r_1 - r_2$$

and

$$a \cdot b = (jm + r_1) + (km + r_2)$$
$$a \cdot b = m \cdot (jkm + jr_2 + kr_1) + r_1 \cdot r_2$$

□

Multiplication implies the *cancellation* property. If

$$ac \equiv bc$$

then

$$a \equiv b$$

Proof: write the multiplication equality backward.

Also, if $a \equiv a'$ and $b \equiv b'$ then

$$a + b = a' + b'$$

powers of 10

Suppose we look at modulus 11 as an example.

$$10 \equiv -1$$

$$10^2 \equiv (-1)(-1) = 1$$

$$10^3 \equiv (1)(-1) = -1$$

so we obtain alternating plus and minus one.

Therefore, any integer

$$z = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + + a_n \cdot 10^n$$

leaves the same remainder on division by 11 as

$$(a_0 - a_1) + (a_2 - a_3) + \ldots$$

It follows that a number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

example

To what number between 0 and 12 inclusive is the following product congruent modulo 13?

$$3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 113$$

We have:

$$3 \cdot 7 = 21 \equiv 8$$

$$11 \cdot 17 \equiv 11 \cdot 4 = 5$$

$$19 \cdot 23 \equiv 6 \cdot 10 = 60 \equiv 8$$

$$29 \cdot 113 = 3 \cdot 9 = 27 \equiv 1$$

so

$$8 \cdot 5 \equiv 40 \equiv 1$$

And the final result is 8.

which is easily checked in Python or by using a calculator to find the product (5623656423), and then divide by 13.

Part II

Fundamental Theorem of Arithmetic

Chapter 6

Prime factorization

We will prove that every integer has a unique *prime factorization*. This is also called *the fundamental theorem of arithmetic*.

$$n = p_1 \cdot p_2 \ldots p_k$$

In the list of the prime factors of n, a factor may be repeated.

Example:

$$12 = 2 \cdot 2 \cdot 3$$

To compare two factorizations for uniqueness, we suppose they are sorted (say, from smallest to greatest).

More examples for relatively small numbers:

$$39 = 3 \cdot 13$$

$$144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$$

$$210 = 2 \cdot 3 \cdot 5 \cdot 7$$

$$2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$$

Sometimes the factors can be hard to find.

Example:

Let's try 123456789. By using the digit addition trick, we can tell that this number is divisible by 9 (I get $9 + 9 + 9 + 9 + 9$).

At first it seems easy. I found two factors of 3, leaving 13717421.

Then my luck ran out. The smallest prime factor was too large for me to find by hand. So I used Python.

https://gist.github.com/telliott99/3043a0d9ddc44f8503c83c848b2f8382

3607 and 3803 are the two prime factors of that number, which once found, are easily confirmed. Factoring is a hard problem.

background

We will prove the unique prime factorization theorem.

But before starting on that, remember that when we say that one integer *evenly divides* another one, written as $a|n$ or a is a factor of n, we mean there exists another integer k such that

$$a \cdot k = n$$

a times k is exactly equal to n with no remainder.

Take care to distinguish $a|b$ (a divides b) from a/b (a divided by b).

If there is also a number m where a evenly divides m, we write $a|m$ and mean that

$$a \cdot j = m$$

Addition or subtraction of $m + n$ gives

$$m + n = a \cdot j + a \cdot k = a(k + j)$$

$$m - n = a \cdot j - a \cdot k = a(k - j)$$

- If $a|m$ and $a|n$, a also divides their sum or difference.

We rely on this fact below.

Also, we can manually check all the numbers up to some reasonable lower limit, like 100. They all have unique prime factorizations. Therefore, if there is a number with two such factorizations, it is larger than 100, and there must be a smallest such number.

abnormal numbers

Hardy and Wright (*Theory of Numbers*, sect. 2:11) have a proof of prime factorization which I find quite elegant.

Proof.

By contradiction.

Hardy:

> Let us call numbers which can be factored into primes in more than one way, *abnormal*, and let n be the smallest abnormal number.

Start by supposing that there are two different factorizations of n:

$$n = p_1 \cdot p_2 \ldots p_k$$

and

$$n = q_1 \cdot q_2 \ldots q_j$$

where the p's and q's are all primes.

Different factorizations

As a preliminary result, consider the possibility that some factor appears in both factorizations, that some p is equal to a q.

Let us rearrange if necessary so the shared factor is listed first: let $p_1 = q_1$ and

$$n = p_1 \cdot p_2 \ldots p_k$$

$$n = p_1 \cdot q_2 \ldots q_j$$

But now, n/p_1 (n divided by p_1) is abnormal, because it has two different prime factorizations.

That is impossible, because n is the smallest abnormal number.

Therefore, no p is a q and no q is a p. If there exist abnormal numbers with two factorizations, those factorizations must be completely different.

inequality

We may take p_1 to be the least p and q_1 to be the least q. In this part, we establish that $p_1 \cdot q_1 < n$.

Since n is composite, either

- $p_1 \cdot p_1 = n$, or
- p_1 times some number larger than p_1 is equal to n.

In the second case, $p_1 \cdot p_1 < n$.

A similar result holds for q_1.

But, since $p_1 \neq q_1$, only one of p_1 or q_1 at most, can be squared to give n. Either $p_1 \cdot p_1 < n$ or $q_1 \cdot q_1 < n$ or perhaps both are true.

From this it follows that

$$p_1 \cdot q_1 < n$$

the contradiction

Let

$$N = n - p_1 q_1$$

We known that N is not abnormal (because n is the smallest abnormal number).

We have that $N > 0$ because of the result of the last section. We also know that $N < n$, since p_1 and q_1 are non-zero and we subtracted them from n. So $0 < N < n$.

We're given that $p_1 | n$ and so, from the above equality

$$N = n - p_1 q_1$$

and our preliminary result about what factorization means, it must be that $p_1 | N$. The same is true for q_1, namely $q_1 | N$.

Hence both p_1 and q_1 appear in the unique factorization of N, so $p_1 q_1 | N$.

Certainly, $p_1 q_1$ divides itself, so it follows that $p_1 q_1 | n$, using our preliminary result about factorization.

Hence, $q_1 | (n/p_1)$.

But n/p_1 is less than n and has the unique prime factorization $p_2 \cdot p_3 \ldots p_k$.

Since q_1 is not a p, this is impossible.

Hence there cannot be any abnormal numbers.

□

As we said, this is *fundamental theorem of arithmetic*, so it's worth a bit of effort for the proof.

Chapter 7

Euclid's lemma

Since we just established the prime factorization theorem independent of Euclid's lemma, we can use it in a simple proof of the same.

Euclid's lemma

Suppose that $n = a \cdot b$. If $p|n$ then either $p|a$ or $p|b$ or both.

proof

Suppose to the contrary, $p|n$ but p does not divide either a or b.

Both a and b have a unique prime factorization and those factors multiplied together are the prime factors of n. These factors do not include p, and yet the factorization is unique.

This is a contradiction.

p must divide either a or b, or both.

□

example

Note that this is not necessarily true for non-primes. For example, $6 \cdot 10 = 60|4$ but neither $6|4$ nor $10|4$. This happens because 2 is a prime factor of both 6 and 10, generating a factor of 4 in the product.

Chapter 8

Fermat's theorem

We are concerned not with the famous "last" theorem but with Fermat's *little* theorem.

The theorem says that for any integer a and any prime p which does not divide a (a must be *co-prime* to p):

$$a^{p-1} \equiv 1 \bmod p$$

equivalently

$$a^p \equiv a \bmod p$$

Euler proved this theorem (Fermat did not) and he extended it by showing that it is true, not just for p prime, but for any n coprime to a.

examples

mod 13:

$$2^4 = 16 \equiv 3$$

$$2^{12} = 3 \cdot 3 \cdot 3 = 27 \equiv 1$$

and, mod 11

$$5^2 = 25 \equiv 3$$

$$5^4 = 9$$

$$5^8 = 81 \equiv 4$$

$$5^{10} = 3 \cdot 4 = 12 \equiv 1$$

It is a striking pattern in tables of powers, here for $p = 7$. We ensure that p does not divide a by only considering $a < p$.

```
    1  2  3  4  5  6
   --------------------
1 | 1  1  1  1  1  1
2 | 2  4  1  2  4  1
3 | 3  2  6  4  5  1
4 | 4  2  1  4  2  1
5 | 5  4  6  2  3  1
6 | 6  1  6  1  6  1
```

However, we can continue with:

```
 8 |  1   1   1   1   1   1
 9 |  2   4   1   2   4   1
10 |  3   2   6   4   5   1
```

As you can see, even for a coprime to p, one should not suppose that the powers of a generate all the integers $< p$, though some do.

Here is $p = 11$:

```
      1   2   3   4   5   6   7   8   9  10
    ----------------------------------------
 1 |  1   1   1   1   1   1   1   1   1   1
 2 |  2   4   8   5  10   9   7   3   6   1
 3 |  3   9   5   4   1   3   9   5   4   1
```

```
 4 |  4   5   9   3   1   4   5   9   3   1
 5 |  5   3   4   9   1   5   3   4   9   1
 6 |  6   3   7   9  10   5   8   4   2   1
 7 |  7   5   2   3  10   4   6   9   8   1
 8 |  8   9   6   4  10   3   2   5   7   1
 9 |  9   4   3   5   1   9   4   3   5   1
10 | 10   1  10   1  10   1  10   1  10   1
```

I found it helpful to script this:

```
def f(p):
    def x(n):
        for i in range(p):
            print i, n**i % p
    return x

g = f(11)
g(2)
```

proof

Write the multiples of a smaller than pa. Let

$$m_1 = a$$

$$m_2 = 2a$$

$$\ldots$$

$$m_{p-1} = (p-1)a$$

lemma

◦ No two of these, say m_i and m_j, can be congruent mod p.

Proof:

Suppose on the contrary that there exist m_j and m_i that *are* congruent (take $j > i$). Congruence means that their difference:

$$m_j - m_i = (j - i)a$$

is evenly divisible by p.

But by assumption, p does not divide a.

So then $j - i$ must be divisible by p (note: this is Euclid's lemma).

But

$$1 \leq i < j \leq (p - 1)$$

Thus, certainly $j - i < p$ and so p cannot divide $j - i$ either.

Therefore, no two m's are congruent.

As a result, p cannot divide the product $1 \cdot 2 \cdot \cdots \cdot p - 1$.

Another way of putting this is to say that no prime p can evenly divide any number smaller than itself, since each of those numbers has its own unique prime factorization, made up of factors smaller than p, and p does not evenly divide any of them.

Restatement: no $m \equiv 0 \bmod p$.

proof of the theorem

Since there are $p - 1$ terms m, and no two are congruent mod p, they must correspond to $1 \ldots (p - 1) \bmod p$, although they may occur in a different order after multiplication by a.

The key result is that when these terms m are multiplied out:

$$1a \cdot 2a \cdot \cdots \cdot (p - 1)a = (p - 1)!\ a^{p-1}$$

after evaluation mod p, the same terms are equal to:

$$1 \cdot 2 \cdot \cdots \cdot (p - 1) = (p - 1)!$$

So we can cancel the $(p-1)!$, equate the two, and obtain:

$$a^{p-1} = 1 \bmod p$$

$$a^p = a \bmod p$$

□

The requirement for a and p coprime arises because it ensures that each term m_i appears only once.

Part III

Euclid

Chapter 9

Quotient remainder rule

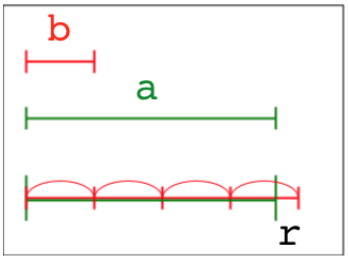
Given integer a and positive integer b, there exist unique positive integers q and r such that

$$a = b \cdot q + r$$

with $0 \leq r < b$.

This works for integer a, but it's easier to think about if we restrict things to $a > 0$.

Then, this is a version of the Archimedean property for positive integers.



We can paraphrase by saying

> given a bathtub full of water and a teaspoon, it is possible to empty the bathtub.

First, find q such that $b \cdot q \leq a$ but $(b+1) \cdot q$ produces a number larger than a.

Then either $b \cdot q = a$ and we are done or:

$$b \cdot q < a < b \cdot q + b$$

So then let $r = a - bq$ and we have found

$$0 \leq r < b$$

with $0 \leq r < b$.

second proof

A formal proof of this is surprisingly long-winded. Here is one version.

https://math.stackexchange.com/questions/724032/quotient-remainder-theorem-proving

Consider the progression:

$$a - 3b, a - 2b, a - b, a, a + b, a + 2b, a + 3b$$

This extends in both directions. By the well-ordering principle, there must exist a smallest non-negative element, r. Thus

$$r = a - qb$$

for some integer q.

r must be in the interval $[0, b)$ because otherwise $r - b$ would be smaller than r and a non-negative element in the progression.

uniqueness

We have

$$a = bq + r$$

with $0 \leq r < b$.

Suppose we have another q' and r' such that

$$a = bq' + r'$$

with $0 \leq r' < b$.

Subtracting, we see that

$$0 = bq - bq' + r - r'$$

$$r - r' = b(q' - q)$$

We conclude that $b|(r - r')$.

The largest value for $r - r'$ occurs when $r = b - 1$ and $r' = 0$ so, at most

$$r - r' < b$$

whereas at least (with $r = 0$)

$$-b < r - r'$$

so then we have that $-b < r - r' < b$.

Hence, since $b|(r - r')$, we must have that $r - r' = 0$.

So

$$r = r'$$

and thus

$$r - r' = 0 = b(q' - q)$$

so

$$q = q'$$

The original solution is unique.

□

Chapter 10

Euclidean algorithm

Consider two natural numbers a and b. Usually a is an integer (i.e., it is allowed to be negative), but to keep things simple here we will say that a and b are positive integers, with $a > b$.

We can find their *greatest common divisor*.

This is written $\gcd(a, b)$, or just (a, b).

(a, b) is the largest number which evenly divides both a and b.

To find it, simply write the unique prime factorization of a and b.

```
180 = 2.2.3.3.5
140 = 2.2.    5.7
gcd = 2.2.    5     = 20
```

Pick out the common factors and the $\gcd(a, b)$ will be their product.

problem

However, factorization is hard, and is actually impossible for the really large numbers used in cryptography. It is important that we do not need to factor a and b for the algorithm to work.

how it works

Find integers $0 \leq r < b$ and $q > 0$ such that

$$a = b \cdot q + r$$

This relies on the quotient remainder rule.

◦ If $r = 0$ we are done: b divides a equally. Otherwise

◦ switch $a = b$ and $b = r$ and repeat. Then b is the gcd of the original a and b.

In our example

```
180 = 140.1 + 40
140 =  40.3 + 20
 40 =  20.2 + 0
gcd =  20
```

why it works

Now let u be the largest integer that divides both a and b (the greatest common divisor)

$$a = su$$

$$b = tu$$

Then

$$a = b \cdot q + r$$

$$su = q \cdot tu + r$$

$$r = su - q \cdot tu$$

We conclude that u divides r.

Every common divisor of a and b is also a divisor of b and r.

Python code

Here are two examples of programs in different styles that implement the algorithm (with no error checking):

```
def gcd(a,b):
    r = a % b
    if r == 0:
        return b
    return gcd(b,r)
```

```
def gcd(a,b):
    r = a % b
    while r != 0:
        a,b = b,r
        r = a % b
    return b
```

The first version is *recursive*, it may call itself. The second uses a **while** loop to accomplish the same thing.

Chapter 11

Bezout's identity sketch

Bezout's identity relies on the fact that Euclid's algorithm works, and it provides information that can be used to write a linear combination:

$$sa + tb = g$$

where s and t are integers and g is the $\gcd(a, b)$.

extended Euclid's algorithm

If the algorithm is carried out sequentially:

$$\begin{aligned} a &= b \cdot q_1 + r_1 \qquad (0 < r_1 < b) \\ b &= r_1 \cdot q_2 + r_2 \qquad (0 < r_2 < r_1) \\ r_1 &= r_2 \cdot q_3 + r_3 \qquad (0 < r_3 < r_2) \\ &\cdots \\ r_n &= r_{n+1} \cdot q_{n+2} + 0 = g \end{aligned}$$

The successive remainders form a steadily decreasing sequence of positive numbers:

$$b > r_1 > r_2 > r_3 \cdots > r_n > r_{n+1} > 0$$

After *at most* b steps, and usually much faster, the algorithm must terminate, when say, r_{n+2} is 0. Then $r_n = (a, b) = g$.

consequence

We claim that we can find integers s and t such that

$$r_n = sa + tb$$

Start with r_1. We have that

$$r_1 = a - b \cdot q_1$$

Change the notation from q, r to s, t with $s_1 = 1$ and $t_1 = -q_1$ so

$$r_1 = s_1 \cdot a + t_1 \cdot b$$

The next equation is $r_2 = b - q_2 \cdot r_1$ so we can write

$$r_2 = b - q_2(s_1 \cdot a + t_1 \cdot b)$$

$$= -q_2 \cdot s_1 \cdot a + (1 - t_1)b$$

Relabel $s_2 = -q_2 \cdot s_1$ and $t_2 = 1 - t_1$ so

$$r_2 = s_2 \cdot a + t_2 \cdot b$$

and then just work our way down the (finite) series of equations.

$$\ldots$$

$$r_n = s_n \cdot a + t_n \cdot b$$

This continues until $r_n = g$, i.e. when $r_{n+1} = 0$.

$$g = r_n = s_n a + t_n b$$

$$g = sa + tb$$

□

The proof can be done more rigorously, but we can see why the claim is correct.

Part IV

Classical approach to FTA

Chapter 12

Bezout's identity

This proof is a bit challenging at the critical step.

We follow Aitken

https://public.csusm.edu/aitken_html/m422/Handout1.pdf

Another source is Hefferon

http://joshua.smcvt.edu/numbertheory/book.pdf

theorem

- let a and b be integers, not both zero
- form a linear combination: $sa + tb$
- there is a least positive such combination with value d
- there is also a greatest common divisor or $\gcd(ab) = g$
- the theorem says that $g = d$

proof of the theorem

Def 1. A common divisor of a and b is an integer that divides both a and b.

Def 2. A linear combination is $sa + tb$, for integer s and t

P3. Let d be a common divisor of (a, b), then $d \mid sa + tb$.

Proof:

We have $a = dk$ and $b = dl$ for some integer k and l so

$$sa + tb = s(dk) + t(dl) = d(sk + tl)$$

P4. If a and b are both non-zero, then the GCD exists.

Proof:

Suppose $a \neq 0$ and S is the set of common divisors. $1 \in S$.

- S is not empty since $1 \in S$
- the maximum element of S is $|a|$
- Therefore S has a maximum d and $d \geq 1$

P5. There is a *least* positive integer combination $sa + tb$.

Proof: For convenience suppose $a \neq 0$. Let S be the set of positive linear combinations.

- clearly, $|a| \in S$
- S is not empty
- S has a minimum

Here is the tricky part.

lemma

If $a \neq 0$ and $b \neq 0$, then the least positive linear combination of a and b is a common divisor of a and b.

Proof:

Let $m = sa + tb$ be the least positive linear combination of a and b.

Using the Quotient Remainder Rule write $a = qm + r$. So

$$\begin{aligned} r &= a - qm \\ &= a - q(sa + tb) \\ &= a(1 - qs) - qtb \end{aligned}$$

The quotient rule defines $0 \leq r < m$.

- r is non-negative
- r is a linear combination (above)
- but m is the smallest positive linear combination

Therefore $r = 0$.

Since $r = 0$, $a = qm$ and therefore $m|a$.

Similarly, $m|b$. m is a common divisor of a and b.

theorem

T7. (Bezout's Identity). If a and b are not both zero, then the least positive linear combination of a and b is equal to their greatest common divisor.

Proof:

Let m be the least positive linear combination, and let g be the GCD.

- $g|m$ by Proposition 3, which means that $g \leq m$
- by the lemma, m is a common divisor
- the greatest common divisor is g, so $g < m$ cannot be true

Therefore, $g = m$.

Chapter 13

Euclid's lemma again

Euclid's lemma

Every natural number $n > 1$, i.e. every positive integer greater than 1, is either prime, or it is the product of two smaller natural numbers a and b.

Suppose a given prime p divides $n = ab$, i.e. $p|n$.

We claim that either $p|a$ or $p|b$ (or both).

Given the theorem on prime factorization, proved by a method independent of Euclid's lemma, there is a very simple proof of Euclid's lemma.

Here is a more standard approach.

Bezout's identity

We rely on Bezout's identity, which says that there exist integers r and s such that

$$ra + sp = d$$

where d is the greatest common divisor of a and p.

Of course, if p is prime, then

$$ra + sp = 1$$

proof

Suppose that $p|n = ab$ but $\gcd(p, a) = 1$.

Then, we can find a linear combination of a and p in the integers such that:

$$ra + sp = 1$$

But then,

$$b(ra + sp) = b$$

$$rab + spb = b$$

Since $p|p$ and $p|ab$ (by hypothesis), $p|b$, as desired.

converse

On the other hand, if p is not prime, it must be composite, i.e. $p = ab$.

In that case, p divides neither a nor b (since they are smaller than p).

https://artofproblemsolving.com/wiki/index.php/Euclid%27s_Lemma

Chapter 14

FTA standard proof

We will prove that every integer has a unique prime factorization.

$$n = p_1 \cdot p_2 \ldots p_i$$

In this list of prime factors, a factor may be repeated. For example $12 = 2 \cdot 2 \cdot 3$.

This is our second proof of the theorem. A preliminary result that is needed for this version is called Euclid's lemma.

Euclid's lemma

Every positive integer greater than 1 is either prime, or it is the product of two smaller natural numbers a and b.

But the same is true of a and b in turn. So every $n = ab$ is the product of the prime factors of a times the prime factors of b.

Suppose a given prime p divides $n = ab$, i.e. $p|n$.

Then $p|a$ or $p|b$, or both.

quick proof of FTA

The proof is by contradiction.

Now, suppose p is prime and and $p|ab$ but p divides neither a nor b.

Because a and p are co-prime, Bezout says that there exist integers x and y such that:

$$ax + py = 1$$

similarly (because b and p are co-prime) there exist X and Y such that:

$$bX + pY = 1$$

so

$$1 = (ax + py)(bX + pY)$$
$$1 = axbX + axpY + pybX + p^2yY$$
$$1 = ab(xX) + p(axY + ybX + pyY)$$

Since $p|ab$, p divides the right hand side, so p divides the left-hand side, that is, $p|1$. But this is absurd.

Therefore, p divides at least one of a and b.

proof of FTA

The proof is by induction.

Assume the lemma is true for all numbers between 1 and n. It is certainly true for $n < 31$, because we can check each case.

If n is prime there is nothing to prove and we move to $n + 1$.

If n is not prime, then there exist integers a and b (with $1 < a \leq b < n$) such that $n = a \cdot b$.

By the induction hypothesis, since $a < n$ and $b < n$, a has prime factors $p_1 \cdot p_2 \ldots$ and b has prime factors $q_1 \cdot q_2 \ldots$ so

$$n = ab = p_1 \cdot p_2 \ldots q_1 \cdot q_2 \ldots$$

This shows there exists a prime factorization of n.

uniqueness

To show that the prime factorization is unique, suppose that n is the smallest integer for which there exist two different factorizations:

$$n = p_1 \cdot p_2 \ldots p_i$$

and

$$n = q_1 \cdot q_2 \ldots q_j$$

Pick the first factor p_1. Since p_1 divides $n = q_1 q_2 \ldots$, by Euclid's lemma, it must divide some particular q_j. Rearrange the q's to make that q the first one.

But since p_1 divides q_1 and both are prime, it follows that $p_1 = q_1$.

As wikipedia says now:

> This can be done for each of the m p_i's, showing that $m \leq n$ and every p_i is some q_j. Applying the same argument with the p's and q's reversed shows $n \leq m$ (hence $m = n$) and every q_j is a p_i.

□

Part V

The inverse

Chapter 15

Euler's totient

Euler's totient function is symbolized by $\phi(n)$.

ϕ gives a count of how many numbers in the set $\{1, 2, 3 \ldots, n-1\}$, that is, $a \in \mathbb{N} \mid a < n$

share no common factors with n other than 1, i.e. that have a gcd with n equal to 1. We include 1 in the count.

If n is prime, this is easy.

For a prime p, the only number that evenly divides p is 1 (and 1 always has a gcd of 1 with another integer), so the count of numbers less than p that have gcd $= 1$ is $p - 1$.

non-primes

Otherwise, it gets more difficult.

The fundamental theorem of arithmetic says that any number n has a *unique* prime factorization.

There is another theorem that says that if we have the prime factors

of n:

$$n = p_1 \cdot p_2 \cdot p_3 \ldots$$

then

$$\phi(n) = \phi(p_1) \cdot \phi(p_2) \cdot \phi(p_3) \ldots$$

This is true not just for primes, but for any two coprime factors of n.

This will explain why we are able to write (in deriving an RSA key), that since $n = p \cdot q$:

$$\phi(n) = (p-1)(q-1)$$

So if

$$\phi(n) = \phi(p_1)\ \phi(p_2)\ \phi(p_3) \ldots$$

We can multiply and divide by the product of the prime factors of n and obtain

$$\phi(n) = \frac{p_1\ p_2 \ldots}{p_1\ p_2 \ldots}(p_1 - 1)\ (p_2 - 1)\ \ldots$$
$$\phi(n) = n(p_1 - 1/p_1)(p_2 - 1/p_2)\ \ldots$$

I found a nice write-up of this here:

http://www.claysturner.com/dsp/totient.pdf

In the write-up there is a sketch of a proof of the last line above, and you can follow it backward to what we were given:

$$\phi(n) = \phi(p_1) \cdot \phi(p_2) \cdot \phi(p_3) \ldots$$

example

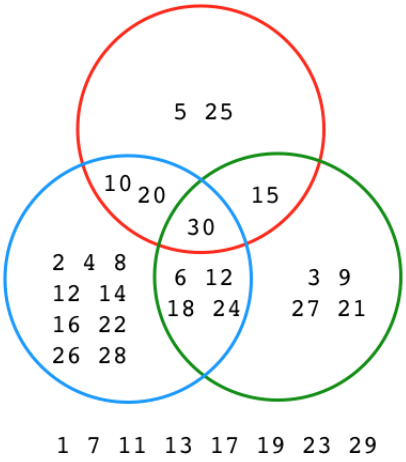
Consider $n = 30$. If we run Euclid's algorithm on $1 < m < n$, we can find numbers that are coprime to (do not share any factor with) 30:

```
7 11 13 17 19 23 29
```

These are the primes smaller than n, excluding those that divide n.

The set we seek includes 1, hence $\{1, 7, 11, 13, 17, 19, 23, 29\}$.

These are the numbers that are not included in the Venn circles:



The prime factors of 30 are 2, 3 and 5.

We can divide $1 \leq m \leq n$ into several sets:

- n itself
- prime factors of n: 2, 3 or 5

plus

- gcd equal to a single prime factor
- gcd equal to a product of prime factors

and last

- 1
- prime, not a factor of n

We are trying to count the last group.

Let

- A be the set of integers that 2 divides into evenly, including n
- B be the set .. 3
- C be the set .. 5

We want to find the count or size of the set of all the numbers that are not in A, B or C (the numbers listed along the bottom of the figure).

This is sizeof $\neg(A \cup B \cup C)$

where $\neg$ symbolizes the complement of the set, those elements not in the given set, and $\cup$ is set union.

There is a famous theorem in set theory that says:

$$\neg(A \cup B \cup C) = (\neg A) \cap (\neg B) \cap (\neg C)$$

$\cap$ is set intersection.

so we want the size of the right-hand side.

using probability

It is somewhat surprising, but we can easily calculate the probability that a number is in the set $\neg A$.

Consider the set including 2 and all its multiples. The probability that a number ≤ 30 is contained in the complement of that set is $1 - 1/2$, the fraction of all numbers that are even, times 30.

Similarly, for B, the probability is $1 - 1/3$ times 30 and so on.

The total probability is the product of the individual probabilities.

And that total probability, times n, is equal to the count.

Thus

$$\begin{aligned}\phi(30) = &\text{ sizeof } (\neg A) \cap (\neg B) \cap (\neg C) \\ &= 30 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5)\end{aligned}$$

And generalizing

$$\phi(n) = n \cdot (1 - 1/p_1) \cdot (1 - 1/p_2) \ldots$$

which is what we needed to prove.

□

This can be rewritten as

$$\phi(n) = (p_1 - 1) \cdot (p_2 - 1) \ldots$$

goal

For cryptography, what we're looking for is a function that has an inverse, where

$$(m^e)^d = (m^d)^e = m$$

Always, mod n.

So with Euler's extension of Fermat's little theorem (substituting m for a):

$$m^{\phi(n)} = 1$$

In this case, raising to the power k doesn't change the result:

$$m^{k \cdot \phi(n)} = 1$$

$$m^{k \cdot \phi(n)+1} = m$$

So, we see that it will work to find

$$e \cdot d := k \cdot \phi(n) + 1$$

And thus

$$e \cdot d := 1 \ mod \ \phi(n)$$

And that's why it works.

Chapter 16

Chinese remainder

The Chinese remainder theorem is sometimes abbreviated as the CRT.

> There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number? – Sun Tsu Suan-Ching

https://www.cut-the-knot.org/blue/chinese.shtml

Consider n and its prime factors (or even combinations of prime factors, as long as each value is coprime), then

> the tuple of remainders from the modulus operation on n with its coprime factors is unique

Not only is the tuple unique, but

> it can be used to reconstruct the result of the modulus operation on n

Therefore, that operation can be replaced by easier operations on each of the smaller factors. This result is used to simplify some operations with RSA keys, as we'll see.

examples

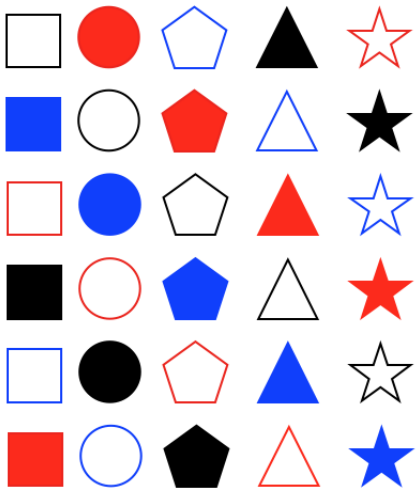
Let $n = 20$ and consider the coprime factors 4 and 5:

```
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
      |       |       |       |       |
1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0   mod 4
        |           |           |           |
1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0   mod 5
```

For each number in the range $[1..n]$ write the result mod 4 or 5 as a tuple:

```
(1,1),(2,2),(3,3),(0,4),(1,0)
(2,1),(3,2),(0,3),(1,4),(2,0)
(3,1),(0,2),(1,3),(2,4),(3,0)
(0,1),(1,2),(2,3),(3,4),(0,0)
```

Each one is unique.



In the picture above, we have

- 5 distinct shapes

- 3 different colors
- 2 states, either filled or empty

As you can see, there are precisely 30 possible types.

For example, each shape can be one of three colors, filled or empty, so there are 6 possibilities for each of the five shapes. This is simply a consequence of the fact that

$$5 \cdot 3 \cdot 2 = 30$$

Since there are 30 numbers in [1..30], there is exactly one type for each number.

theorem

If N is composed of coprime factors

$$N = p \cdot q \cdot r \ldots$$

and n is in the range $[1..N]$.

Suppose n has the set of remainders with those factors:

- $n = a \bmod p$
- $n = b \bmod q$
- $n = c \bmod r$

Then this tuple (a, b, c) uniquely identifies n.

example

Suppose $N = 60$, so

$$30 = 2 \cdot 3 \cdot 5$$

Make a table of remainders:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2:	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3:	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
5:	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2:	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
3:	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
5:	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Any particular triplet of remainders is unique, say: $(1, 1, 3) \to 13$.

This is also true if the factors are not prime but simply co-prime:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
5:	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
6:	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
5:	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
6:	4	5	0	1	2	3	4	5	0	1	2	3	4	5	0

solving the system

I picked a column at random from above.

Consider the following table of remainders (congruences):

$$x \equiv 1 \pmod 2$$

$$x \equiv 1 \pmod 3$$

$$x \equiv 3 \pmod 5$$

The CRT says that this tuple uniquely determines x. We can actually solve the system for x.

It's kind of spammy, but I found out how to do this here

https://brilliant.org/wiki/chinese-remainder-theorem

Start with the largest modulus $x \equiv 3 \pmod 5$. Re-write this as:

$$x = 5j + 3$$

For some integer j. Substitute into $x \equiv 1 \pmod 3$:

$$5j + 3 = 1 \pmod 3$$

Solve for j:

$$5j = 1 \pmod 3$$
$$2j = 1 \pmod 3$$
$$j = 2 \pmod 3$$

A multiplication table can help with the last step above.

Rewrite this as a congruence relation for some integer k.

$$j = 3k + 2$$

Back-substitute:

$$x = 5j + 3$$
$$x = 5(3k + 2)$$
$$x = 15k + 13$$

Now we have x in terms of k. We are done with equation 2.

Repeat the cycle by substituting into $x \equiv 1 \pmod 2$ and solve for k.

$$15k + 13 = 1 \pmod 5$$

$$k + 3 = 1 \pmod 5$$

$$k = -2 = 0 \pmod 2$$

which means that

$$k = 2m$$

for some m. And then

$$x = 15k + 13$$

$$x = 15(2m) + 13$$

$$x = 13 \pmod{30}$$

riddle

The answer is

```
>>> for i in range(106):
...     t = (i,i%3,i%5,i%7)
...     print(t)
...     if t[1:] == (2,3,2):
...         break
...
..
(23, 2, 3, 2)
```

Chapter 17

Multiplicative inverse

statement

a is the multiplicative inverse of $b \pmod{n}$ if

$$ab = 1 \bmod n$$

That is,

$$n = kab + 1$$

Obviously, a and b must be co-prime to n. n cannot divide either a or b because then it must be that $n|1$.

theorem

If p is prime, then $\pmod{p}$

every $1 < a < p$ has a multiplicative inverse

Furthermore, we claim that *every* product has two unique factors mod p.

The statement

$$ab \equiv r \bmod p$$

is equivalent to

$$ab = qp + r$$

Suppose that

$$ab' = q'p + r$$

then

$$a(b - b') = (q - q')p$$

$$a(b - b') \equiv 0$$

Since $a \neq 0$, it must be true that $b = b'$.

examples

Suppose $a = 6$ and $b = 10$. Then, $g = 2$ and so we write Bezout's identity:

$$6s + 10t = 2$$

Obviously, one of s or t must be negative.

One solution is $s = 2, t = -1$. Another is $s = -3, t = 2$.

More generally, the integers of the form $sa+tb$ are exactly the multiples of d.

Corollary: a and b are co-prime with gcd $(a, b) = 1$, if and only if there exist integers s and t such that

$$sa + tb = 1.$$

For example, if $a = 6$ and $b = 5$ then we can find

$$6s + 5t = 1$$

A simple solution is $s = 1, t = -1$.

An application is that if

$$6s + 5t = 1$$

$$6s = 1 - 5t$$

then (mod t):

$$6s = 1$$

6 is the multiplicative inverse of s mod t.

As an example, construct a table for $p = 17$. In addition to $1 \cdot 17$, there are seven pairs and one square:

```
2.9 =    18 = 1
3.6 =    18 = 1
5.7 =    35 = 1
4.13 =   52 = 1
8.15 =  120 = 1
10.12 = 120 = 1
11.14 = 154 = 1
16.16 = 256 = 1
```

Notice that 16 is its own inverse *and* $16 \equiv -1 \mod 17$. See Wilson's theorem.

uniqueness

Bezout's lemma says that for every a with $\gcd(a, p) = 1$ (and this is true of every $a < p$, there exists

$$sa + tp = 1$$

That is

$$sa \equiv 1 \mod p$$

So, there exists an s which is the multiplicative inverse for a.

Why is there only one such s smaller than p?

Suppose that a has two inverses mod p. That is

$$as \equiv as' \equiv 1$$

By the cancellation property

$$s \equiv s'$$

Chapter 18

Wilson's theorem

theorem

Let p be prime. Then

$$(p-1)! = -1 \bmod p$$

proof

If p is prime, then $x < p$ may be its own multiplicative inverse.

$$x^2 = 1 \bmod p$$

However, this (must) happen only if

$$x^2 - 1 = 0 \bmod p$$

$$(x-1)(x+1) = 0 \bmod p$$

That is, $x - 1 = 0 \bmod p$ or $x + 1 = 0$, mod p.

But the only numbers in $[1 \ldots p]$ which satisfy this are 1 and $p - 1$.

Therefore, no other number can be its own multiplicative inverse.

Consider the product

$$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$$

For nearly all the factors in the factorial the multiplicative inverse is also present, and that pair then contribute only 1 to the product (mod p).

The exceptions 1 and $(p-1)$ are their own inverses. The result follows.

Part VI

Squares

Chapter 19

Pythagorean triples

Pythagorean triples

The simplest right triangle with integer sides is $3, 4, 5$:

$$3^2 + 4^2 = 5^2$$

any multiple n will work

$$(3n)^2 + (4n)^2 = (5n)^2$$

but that's not so interesting.

The triples which are not multiples of another triple are called *primitive*.

There is a small table of triples in this discussion of Euclid X:29 by Joyce:

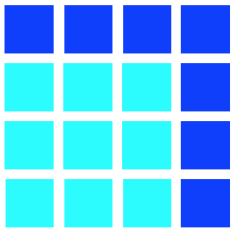
https://mathcs.clarku.edu/~djoyce/elements/bookX/propX29.html

	1	3	5	7	9	11	13
3	3 : 4 : 5						
5	5 : 12 : 13	15 : 8 : 17					
7	7 : 24 : 25	21 : 20 : 29	35 : 12 : 37				
9	9 : 40 : 41	27 : 36 : 45	45 : 28 : 53	63 : 16 : 65			
11	11 : 60 : 61	33 : 56 : 65	55 : 48 : 73	77 : 36 : 85	99 : 20 : 101		
13	13 : 84 : 85	39 : 80 : 89	65 : 72 : 97	91 : 60 : 109	117 : 44 : 125	143 : 24 : 145	
15	15 : 112 : 113	45 : 108 : 117	75 : 100 : 125	105 : 88 : 137	135 : 72 : 153	165 : 52 : 173	195 : 28 : 197

We can explain the first column

$$(3, 4, 5) \quad (5, 12, 13) \quad (7, 24, 25) \quad (9, 40, 41)$$

using this graphic



$$n^2 + (2n + 1) = (n + 1)^2$$

where $2n + 1$ is the count of dark blue squares in the top column plus the rightmost row.

Of course, this is just basic algebra. However, if that odd number is also a perfect square we have that

$$2n + 1 = a^2$$

so

$$(n + 1)^2 = n^2 + a^2$$

Every odd number, when squared, gives an odd perfect square:

$$3^2 = 9$$
$$5^2 = 25$$
$$7^2 = 49$$

So every odd number (≥ 3) is the basis for one of the entries. Its two paired values in the triple can be computed as

$$b = \frac{a^2 - 1}{2}, \qquad c = b + 1$$

We can also explain the first diagonal

$$(8, 15, 17) \quad (12, 35, 37) \quad (16, 63, 65) \quad (20, 99, 101)$$

The first value is $4n$ for $n = 2, 3, 4 \ldots$.

The other two values are $4n^2 \pm 1$. This works because

$$(4n^2 + 1)^2 = (4n^2 - 1)^2 + (4n)^2$$

The fourth powers cancel and the ones cancel and we have

$$8n^2 = -8n^2 + 16n^2$$

which is correct.

Euclid's formula

To go further, we can use Euclid's formula. For every integer m, n, with $m > n$, a Pythagorean triple is given by

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

This works because

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)$$

Canceling the fourth powers, we have

$$-2m^2n^2 + 4m^2n^2 = 2m^2n^2$$

So c is a sum of squares and a the difference. For the first column c is:

$$2^2 + 3^2, \quad 3^2 + 4^2, \quad 4^2 + 5^2$$

and for the second c is

$$1^2 + 4^2, \quad 1^2 + 6^2, \quad 1^2 + 8^2, \quad 1^2 + 10^2$$

Clearly a number of patterns will be found.

It is possible to show that Euclid's formula gives *every* Pythagorean triple.

https://en.wikipedia.org/wiki/Pythagorean_triple#Enumeration_of_primitive_Pythagorean_triples

A thousand years before Pythagoras, the Babylonians knew the triple $4601, 4800, 6649$. It seems unlikely that they found this by random search.

all primitive triples

Maor gives a proof that *all primitive triples* can be found using Euclid's formula.

Consider

$$a^2 + b^2 = c^2$$

For a primitive triple, a and b should be of opposite parity, with one even and one odd. For if not:

Suppose a and b both even. Then $a = 2m$ and $b = 2n$ and

$$a^2 + b^2 = 4(m^2 + n^2) = c^2$$

Thus c is even and the triple is not primitive.

Otherwise, suppose a and b both odd. Then $a = 2j + 1$ and $b = 2k + 1$ and

$$a^2 + b^2 = 4j^2 + 4j + 1 + 4k^2 + 4k + 1 = c^2$$

Hence c^2 is even but not divisible by 4.

On the other hand, if a and b are odd, so are a^2 and b^2, thus their sum is even. But if c^2 is even, then so is c, thus

$$(c)^2 = (2i)^2$$

and c^2 must be divisible by 4. We have reached a contradiction.

Therefore only one of a and b is even. Let $a = 2t$.

$$(2t)^2 + b^2 = c^2$$

$$(2t)^2 = c^2 - b^2$$

$$(2t)^2 = (c + b) \cdot (c - b)$$

$$t^2 = \frac{c + b}{2} \cdot \frac{c - b}{2}$$

Since a^2 is even and b^2 is odd, c^2 is odd, so c is also odd.

Therefore the sum $c+b$ and difference $c-b$ are both even. This means that the terms on the right-hand side in the last expression above are integers.

b and c are also both relatively prime. If they were not, then the sum and difference would share this factor and the same factor would also be shared by a, contrary to the assumption that this is a primitive triple.

The left-hand side

$$t^2 = \frac{c + b}{2} \cdot \frac{c - b}{2}$$

is a perfect square, so the right-hand side is also.

On the right, since the two terms are relatively prime, each term must itself be a perfect square, otherwise their product would not be a perfect square.

So we can write:

$$u^2 = \frac{c+b}{2}$$

$$v^2 = \frac{c-b}{2}$$

Adding the two equations we obtain

$$u^2 + v^2 = c^2$$

Since c and c^2 are both odd, this shows that u and v have *opposite* parity. Subtracting

$$u^2 - v^2 = b^2$$

Finally

$$t^2 = u^2 v^2$$

$$t = uv$$

$$a = 2t = 2uv$$

There is a small table of triples in this discussion of Euclid X:29 by Joyce:

https://mathcs.clarku.edu/~djoyce/elements/bookX/propX29.html

	1	3	5	7	9	11	13
3	3 : 4 : 5						
5	5 : 12 : 13	15 : 8 : 17					
7	7 : 24 : 25	21 : 20 : 29	35 : 12 : 37				
9	9 : 40 : 41	27 : 36 : 45	45 : 28 : 53	63 : 16 : 65			
11	11 : 60 : 61	33 : 56 : 65	55 : 48 : 73	77 : 36 : 85	99 : 20 : 101		
13	13 : 84 : 85	39 : 80 : 89	65 : 72 : 97	91 : 60 : 109	117 : 44 : 125	143 : 24 : 145	
15	15 : 112 : 113	45 : 108 : 117	75 : 100 : 125	105 : 88 : 137	135 : 72 : 153	165 : 52 : 173	195 : 28 : 197

code

Here is a Python script to generate triples by exhaustive search:

https://gist.github.com/telliott99/b543f41d84155bc9171df68b6350e256

And here is one that implements Euclid's formula:

https://gist.github.com/telliott99/144c1a7e90740eb1614ca8ceb5bdeed9

Here is some output (m, n, a, b, c) from the second script, sorted on m and n:

```
> python triples2.py
  1   2   3   4   5
  1   4   8  15  17
  1   6  12  35  37
  1   8  16  63  65
  1  10  20  99 101
  1  12  24 143 145
  1  14  28 195 197
  2   3   5  12  13
  2   5  20  21  29
  2   7  28  45  53
  2   9  36  77  85
```

```
  2  11  44 117 125
  2  13  52 165 173
  3   4   7  24  25
  3   8  48  55  73
  3  10  60  91 109
  3  14  84 187 205
  4   5   9  40  41
  4   7  33  56  65
  4   9  65  72  97
  4  11  88 105 137
  4  13 104 153 185  not in list
...
```

To test triples for being primitive, we look for a greatest common divisor of a and b equal to 1. All such triples have m and n of opposite parity.

The last entry says "not in list" because the limit set for the exhaustive search was exceeded. With a larger search, this triple would be found (or it can just be confirmed by direct computation).

When sorted on a, b, c all triples found by exhaustive search appear to also be found by Euclid's formula, but this wasn't tested explicitly. That could be done easily, as an exercise.

There are some interesting patterns in lists of triples. Here are two:

```
  3   4   5
  5  12  13
  7  24  25
  9  40  41
 11  60  61
 13  84  85
 15 112 113
```

```
17  144  145
19  180  181
21  220  221
23  264  265
25  312  313
27  364  365
```

The first entry doesn't fit the pattern. But starting with $5, 12, 13$, for every step $\Delta a = 2$, we get Δb increasing in steps of 4, with $c = b + 1$.

Below, starting with $8, 15, 17$, for every step $\Delta a = 4$, we get Δb increasing in steps of 8, with $c = b + 2$.

```
 8   15   17
12   35   37
16   63   65
20   99  101
24  143  145
28  195  197
```

Chapter 20

Pell equation

Silverman, 1.1

> The first two numbers that are both squares and triangles are 1 and 36. Find the next one and, if possible, the one after that. Can you figure out an efficient way to find triangular square numbers? Do you think there are infinitely many?

A "triangle" or triangular number is constructed from positive integer n as

$$\frac{n(n+1)}{2}$$

The sequence is

```
  1    3    6   10   15   21   28   36   45   55
 66   78   91  105  120  136  153  171  190  210
```

No more squares yet. Obviously, it will be much easier to use the computer to find more. We continue:

```
231  253  276  300  325  351  378  406  435  465
496  528  361  595  630  666  703  741  780  820
861  903  946  990 1035 1081 1128 1176 1225
```

The first three triangular numbers that are also perfect squares

```
1  36 1225
```

$$49 \cdot 50 = 2450 = 2 \cdot 35^2$$

Rather than pre-compute squares, I came up with a routine to test for that:

```
def is_square(x):
    s = int(x**0.5)
    return s**2 == x
```

The Python int function returns the floor of a decimal number. So then:

```
def f(r):
    for i in range(r):
        t = i*(i+1)/2
        if is_square(t):
            s = int(t**0.5)
            print i, t, s, s**2
```

which gives

```
>>> f(10000)
0 0 0 0
1 1 1 1
8 36 6 36
49 1225 35 1225
288 41616 204 41616
1681 1413721 1189 1413721
9800 48024900 6930 48024900
```

So we have two sequences, the squares

```
1    6    35    204    1189    6930
1   36 1225 41616   ..
```

and the n for the triangular numbers.

```
1    8    49    288    1681    9800
```

I'm looking for a pattern, and I found two. Here are the good triangular numbers:

$$1 = 1^2, \qquad 8 = 3^2 - 1, \qquad 49 = 7^2$$
$$288 = 17^2 - 1, \qquad 1681 = 41^2, \qquad 9800 = 99^2 - 1$$

They are odd squares

```
1 3 7 17 41 99
```

with alternating -1...

pattern with differences

The difference between each root is

```
2 4 10 24 58
```

Each successive difference is

$$d_n = 2 \cdot d_{n-1} + d_{n-2}$$

which predicts that the next two differences are 140 and 338

```
2 4 10 24 58 140 338
```

- the next root would be $99 + 140 = 239$ with $239^2 = 57121$.
- the root following that would be 577 with $577^2 - 1 = 332928$.

pattern with roots

This can also be seen as a pattern with the roots themselves:

```
2 .  3 +   1 =    7
2 .  7 +   3 =   17
2 . 17 +   7 =   41
2 . 41 +  17 =   99
2 . 99 +  41 =  239
2 .239 +  99 =  577
2 .577 + 239 = 1393
```

Let's check:

```
>>> f(1000000)
0 0 0 0
1 1 1 1
8 36 6 36
49 1225 35 1225
288 41616 204 41616
1681 1413721 1189 1413721
9800 48024900 6930 48024900
57121 1631432881 40391 1631432881
332928 55420693056 235416 55420693056
```

So now, what remains is to figure out *why* this happens.

Pell equation

If we look again at the basic equation:

$$n^2 + n - 2q^2 = 0$$

We can solve for n in terms of a given q:

$$n = (1/2) \cdot \ [\ -1 + \sqrt{1 + 8q^2)}\ ]$$

which can only be integer if the discriminant ($D = 1 + 8q^2$) is a perfect square *and also* the numerator is evenly divisible by -2.

The solutions are:

- $q = 1, D = 9, \sqrt{D} = 3, n = 1$
- $q = 6, D = 289, \sqrt{D} = 17, n = 8$
- $q = 35, D = 9801, \sqrt{D} = 99, n = 49$
- $q = 204, D = 332929, \sqrt{D} = 577, n = 288$

http://precollegiate.stanford.edu/circle/math/Pell.pdf

According to the link, a slightly different approach is to first multiply by 4

$$4n^2 + 4n = 8q^2$$

$$(2n + 1)^2 - 1 = 8q^2$$

which suggests the substitutions $x = 2n + 1$ and $y = 2q$ giving

$$x^2 - 2y^2 = 1$$

which is a Diophantine equation whose particular type is a Pell equation. Remember to reverse the substitution at the end.

We can find one solution by inspection: $x = 3, y = 2$. So $n = 1, q = 1$.

Factor

$$(x + \sqrt{2}y)(x - \sqrt{2}y) = 1$$

Plug in the first solution:

$$(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$$

Square both sides

$$(3 + 2\sqrt{2})(3 + 2\sqrt{2})\ (3 - 2\sqrt{2})(3 - 2\sqrt{2}) = 1$$

$$(17 + 12\sqrt{2})(17 - 12\sqrt{2}) = 1$$

We have produced a new solution by squaring the old one. We have $x = 17, y = 12$, which we can check and it works. Then $n = 8, q = 6$.

$$(3 + 2\sqrt{2})(17 + 12\sqrt{2})\ (3 - 2\sqrt{2})(17 - 12\sqrt{2}) = 1$$
$$(99 + 70\sqrt{2})(99 - 70\sqrt{2}) = 1$$

We have produced a new solution by squaring the old one. We have $x = 99, y = 70$, which we can check and it works. Then $n = 49, q = 35$.

That's our third solution.

Finally,

$$(x + \sqrt{2}y)(x - \sqrt{2}y) = 1$$

if $y = \sqrt{2}$ then

$$(x + 2)(x - 2) = 1$$
$$x^2 = 5$$
$$x = \sqrt{5}$$