Introduction to Number Theory

KNU Math 235

Classnotes

Mark Siggers

v. November 24, 2023

These notes are for a course taught from Silverman's "A Friendly Introduction to Number Theory" International Student edition. We refer to this book as 'the text'. The point of these notes is to give students for whom English lectures are difficult a thorough outline of what parts of the text we covered. We are careful to frequently reference the text for proofs and problems so that the notes can only be used with the text. You will find that many of my problems are just examples from the book.

1 What is number theory

Number theory is the study of the properties of the integers $\mathbb{Z}$ or of the natural numbers $\mathbb{N}$.

We introduce some interesting problems that we will cover, or that motivate what we study.

Square sums of squares

When is the sum of two squares a square? In Chapter 2 we deal with Pythagoraen triples: natural numbers x, y and z such that

$$x^2 + y^2 = z^2.$$

Sums of higher powers

Are there solutions in $\mathbb{N}$ to

$$x^n + y^n = z^n?$$

This problem was is the famously difficult Fermat's last which was finally solved by Wiles in the 90s. There are no solutions for $n \geq 3$. If we get there, we will discuss the case $n = 4$ in Chapter 30.

Primes

There are lots of hard problems about primes. Some are very hard, and some we will talk about.

- Are there infinitely many of them?
- Are there infinitely many that are $1 \mod 4$? $3 \mod 4$?
- How common are they?

We know the answers to the problems above, but not to those below.

- Are there infinitely many primes of the form $n^2 + 1$?
- A pair $(n, n + 2)$ of integers are *twin primes* if they are both prime. Are there infinitely many twin primes?

Sums of Squares

Which numbers can be expressed as sums of squares?

Of course we can check for any number n if it can be expressed as $n = x^2+y^2$, but this might take a lot of calculation. Is there a quick way to decide? For primes, you quickly find experimentally that any prime p such that $p \mod 4 = 1$ is a sum of squares. We will see this in Chapter 24 and use it to decide the same thing for non-primes.

Shape Numbers

Squares are called square because we can represent them with dots arranged in a square. We can define triangle, or hexagon numbers in this way too. Gauss proved, apparently when he was 5 years old, that the n^{th} triangle number $T_n = \sum_{i=1}^{n}$ can be calculated as

$$T_n = \frac{n(n+1)}{2}.$$

Are there numbers that are both square and triangle? Some easy ones are 1 and 36. What are the others? This is your first exercise.

Speaking of which. Please do the following.

Problems from the Text

Chapter 1: 1,2,3,5,6

2 Pythagorean Triples

What are the integer solutions to the following equation?

$$x^2 + y^2 = z^2 \tag{1}$$

You know some very well: $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 + 13^2$.

Are there infinitely many? Can we find them all?

Oh, of course there are infintely many. For any integer a we have

$$(3a)^2 + (4a)^2 = (5a)^2.$$

We like to remove these cheap solutions.

Definition 2.1. A *primitive Pythagorean triple*, or a PPT, is a triple (a, b, c) of integers, having no common factors, such that

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

Note that if any two of a, b, and c have a common factor then when $a^2 + b^2 = c^2$ the third does too.

Are there infinitely may PPTs? The text lists the first 10 or so of them.

Some patterns seem to arise: only one of the numbers every seems to be odd, often $c = b + 1$. Are these observations significant?

Because we are primitive, 2 cannot divide two of the numbers, so at most one can be even. The sum of two odds is even, so exactly one of the numbers must be even. But it seems it is never c. Is this true?

Problem 2.1. Show that for a PPT (a, b, c), c cannot be even.

With this, let (a, b, c) be a PPT such that b is even. As $a^2 + b^2 = c^2$ we can write

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

Decomposing several PPTs like this, this is done in the text, we see that $(c - b)$ and $(c + b)$ always seem to be squares. Is this necessary? Their product should be a square, but why should each of them be?

Problem 2.2. Show that in the above decomposition $(c-b)$ and $(c+b)$ cannot share a divisor d.

Thus we can write

$$s^2 = (c - b) \text{ and } t^2 = (c + b)$$

where s and t are odd integers with no common factor. Solving for b and c we get

$$c = \frac{t^2 + s^2}{2} \qquad b = \frac{t^2 - s^2}{2} \qquad a = st.$$

We have proved the following.

Theorem 2.2. *The PPTs (a, b, c) (with b odd) are exactly the triples*

$$\left(st, \frac{t^2 - s^2}{2}, \frac{t^2 + s^2}{2}\right)$$

where $s < t$ are odd integers with no common factors.

Oh. We didn't prove all of it. Triples like there are clearly Pythagorean, but we have not showed the are necessarily primitive. We will show that after Chapter 7.

So why is $c = b+1$ common? Why not find out by doing some fun problems.

Problems from the Text

Chapter 2: 1-8

3 Pythagorean triples and the unit circle

A point (x, y) on the unit circle $U : x^2 + y^2 = 1$ is *rational* if x and y are in $\mathbb{Q}$. Can you find any rational points other than $(0, \pm 1)$ and $(1, \pm 0)$? How many are there?

Well there are not more than there are rational numbers in the real line. Indeed consider the line L_m with slope m that goes through $(-1, 0)$, and let P_m be the other point of intersection of U and L_m. If $P_m = (a/b, c/d)$, then we can compute

$$m = \frac{c/d}{1 + a/b},$$

so if P_m is rational then m is. On the other hand.

Claim 3.1. *If $m = a/b$ is rational, then*

$$P_m = \left(\frac{b^2 - a^2}{b^2 + a^2}, \frac{2ab}{b^2 + a^2} \right),$$

which is also rational.

I think you could probably show this on your own. But there are some common techniques that we would like to recall.

Proof. To find the points of intersection of L_m and U we have to solve their two equations for (x, y):

$$U : x^2 + y^2 = 1 \text{ and } L_m : y = m(x + 1).$$

Plugging $y = m(x + 1)$ into U gives

$$1 = x^2 + (m(x + 1))^2 = (m^2 + 1)x^2 + (2m^2)x + (m^2).$$

So x can be either of the zeros of the polynomial

$$(m^2 + 1)x^2 + (2m^2)x + (m^2 - 1).$$

We could solve this, but we already know one of the zeros: $(-1, 0)$ is in the intersection of L_m and U, so $x = -1$ is a zero, and so $(x + 1)$ divides this polynomial. Doing polynomial long division:

$$\begin{array}{cccccc} & (m^2+1)x & + & (m^2-1) & & \\ \hline x_1) & (m^2+1)x^2 & + & (2m^2)x & + & (m^2-1) \\ & (m^2+1)x^2 & + & (m^2+1)x & & \\ \hline & & & (m^2-1)x & + & m^2-1 \end{array}$$

gives that the other zero is the zero of $(m^2 + 1)x + (m^2 - 1)$. Solving this for x gives

$$x = \frac{1 - m^2}{1 + m^2} \text{ and } y = m(x + 1) = m(\frac{2}{1 + m^2}).$$

Using $m = a/b$ we get

$$P_m = \frac{1}{1 + m^2} \left(1 - m^2, 2m\right) = \frac{1}{a^2 + b^2} \left(b^2 - a^2, 2ab\right),$$

as claimed. □

So we have proved the following.

Theorem 3.2. *A point (x, y) on $x^2 + y^2 = 1$ is rational if and only if it is*

$$P_m = \left(\frac{b^2 - a^2}{b^2 + a^2}, \frac{2ab}{b^2 + a^2}\right)$$

for some rational slope $m = a/b$, or if $(x, y) = (0, -1)$.

This shows that as m runs through $\mathbb{R}$, we get a rational point exactly when m is in $\mathbb{Q}$. So the rational points on U have the same 'density' as $\mathbb{Q}$ had in $\mathbb{R}$.

This has all been about rational points. What is the relation to Pythagorean triples? Well, if we have (a, b, c) such that $a^2 + b^2 = c^2$ then we get

$$(a/c)^2 + (b/c)^2 = 1$$

so we get a rational point. And for any rational point $(x, y) = \left(\frac{b^2-a^2}{b^2+a^2}, \frac{2ab}{b^2+a^2}\right)$ on U we get that

$$(b^2 - a^2, 2ab, b^2 + a^2)$$

is a Pythagorean triple. (It need not be primitive.)

Problems from the Text

Chapter 3: 2, 3, 4

4 Fermat's Last Theorem

This chapter is just history. We skip it.

5 Divisibility and the GCD

In this section we give some basic definitions and results that we use everywhere.

For integers m and n, if there is an integer z such that $zm = n$ then we write $m|n$ and say

- m *divides* n, or
- m is a *divisor* of n, or
- n is a *multiple* of m.

If there is no such z we write $m \nmid n$.

If d divides m and n, then it is a *common divisor* of m and n. The *greatest common divisor* of m and n is denoted $\gcd(m, n)$. If $\gcd(m, n) = 1$ then m and n are *relatively prime*.

Example 5.1.

$$\gcd(15, 25) = 5 \qquad \gcd(15, 21) = 3 \qquad \gcd(21, 25) = 1$$

Problem 5.1. What is $\gcd(4477, 1073)$? Use the Euclicean Algorithm. I taught it to you in high school.

Oh, for the Euclidean algorithm we need the following.

Claim 5.2. *If $d \mid a$ and $d \mid b$ then $d \mid a \pm b$.*

Proof. As $d \mid a, b$ we have, by definition, z_a and z_b such that

$$a = dz_a \qquad \text{and} \qquad b = dz_b$$

so $a \pm b = d(z_a \pm z_b)$ showing that $d \mid a \pm b$. □

Theorem 5.3. *The value* $\gcd(a, b)$ *can be computed as follows for* $b \leq a$*:*

i). Set $r_{-1} = a$ and $r_0 = b$, and $i = 0$.

ii). While $r_i > 0$ do: *Increase i by 1. Let r_i be the value r with $0 \leq r < r_{i-1}$ such that*

$$r_{i-2} = qr_{i-1} + r_i.$$

iii). Now $r_i = 0$, return $\gcd(a, b) = r_{i-1}$.

As r_i always decreases and never goes below 0 this algorithm terminates. Indeed it is easy to see that it terminates in at most b steps. In the exercises you will see that in fact it terminates in at most $2 \log_2 b$. Speaking of which.

Problems from the Text

Chapter 5: 1,3,4,5

6 Linear equations and the GCD

An integer n is a *linear combination* of integers a and b if we can write it as

$$n = ax + yb$$

for integers x and y.

What numbers are linear combinations of a and b? What is the smallest positive number you can write as a linear combination of 10 and 25?

Right! It is 5, which is $\gcd(10, 25)$! We can always write $\gcd(a, b)$ as a linear combination of a and b. We do so using the Extended Euclidean Algorithm. We ran the Euclidean Algorithm for $\gcd(4477, 1073)$.

Step	a	$=$	b	$\cdot$	q	$+$	r
1	4477	=	1073	·	4	+	185
2	1073	=	185	·	5	+	148
3	185	=	148	·	1	+	37
4	148	=	37	·	4	+	0

Now we extend this. The columns on the right keep track of the numbers x and y such that $r = x(4477) + y(1073)$. Figure it out!

Step	a	$=$	b	$\cdot$	q	$+$	r	x	y
1	4477	=	1073	·	4	+	185	1	-4
2	1073	=	185	·	5	+	148	-5	$1 - 5(-4) = 21$
3	185	=	148	·	1	+	37	$1 + 5 = 6$	$-4 - 21 = -25$
4	148	=	37	·	4	+	0		

On the other hand if $n = ax + by$ then $\gcd(a, b)$ divides ax and by, so it divides n. Thus we have the following.

Fact 6.1. *An integer n is a linear combination of a and b if and only if $\gcd(a, b) | n$.*

Using the EEA we find x_1 and y_1 such that

$$\gcd(a, b) = x_1 a + y_1 b.$$

Can we find another expression of $\gcd(a, b)$ as a linear combination of a and b?

Problem 6.1. Show that if $g = x_1a + y_1b$ then $g = (x_1 + b)a + (y_1 - a)b$. Conclude that $g = (x_1 + kb)a + (y_1 - ka)b$ for all $k \in \mathbb{Z}$.

For example, we would find that

$$5 = (1)25 + (-2)10,$$

and so get

$$5 = (1 + 10)25 + (-2 - 25)10,$$

by moving 250 from the second summand to the first. Can we move less?

Sure

$$5 = (1 + 2)25 + (-2 - 5)10.$$

What are these 2 and 5.

Problem 6.2. Show that $g = \gcd(a, b)$ and $g = x_1a + y_1b$ then $g = (x_1 + b/g)a + (y_1 - a/g)b$. Conclude that $g = (x_1 + kb/g)a + (y_1 - ka/g)b$ for all $k \in \mathbb{Z}$.

Theorem 6.2. *Let a and b be integers with $g = \gcd(a, b)$. The equation*

$$g = ax + by$$

has an integer solution (x_1, y_1) that we get with the EEA. The full set of integer solutions is

$$\{(x_1 + \frac{b}{g}k, y_1 - \frac{a}{g}k) \mid k \in \mathbb{Z}\}.$$

Proof. We have seen that all of the claimed solutions are solutions. We show that all solutions are of this form. Indeed, let (x_2, y_2) be some solution. We show that $(x_1 - x_2) = \frac{b}{g}k$ for some integer k.

As it is a solution, we have $ax_2 + by_2 = g = ax_1 + by_1$, which yields

$$a(x_1 - x_2) = b(y_2 - y_1) \text{ and so } (x_1 - x_2) = b(y_2 - y_1)/a.$$

Setting $k = (y_2 - y_1)g/a$ gives that $(x_1 - x_2) = \frac{b}{g}k$ so it is enough to show that this k is an integer. Well

$$ak = y_2g - y_2g = y_2(x_1a + y_1b) - y_1(x_2a + y_2b) = a(x_1y_1 + y_1x_2).$$

Dividing both sides by a shows that k is an integer, as needed. □

Problems from the Text

Chapter 6: 1, 2, 4, 5, 6

7 Factorisation and the Fundamental Theorem of Arithmetic

Recall that an integer $p > 1$ is prime if its only postive divisors are 1 and p. Positive non prime integers are *composite*.

We take for granted that a integer has a unique factorisation into primes:

$$60 = 2^3 \cdot 3 \cdot 5$$

but really we should prove this.

Number systems without unique factorisation

Attaching a root of 5 to the integers $\mathbb{Z}$ we get a number system (a ring!) $\mathbb{Z}[\sqrt{-5}]$. It contains all numbers that we can get from $\mathbb{Z}$ and $\sqrt{-5}$ via addition and multiplication. We can show that as sets

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

In $\mathbb{Z}[\sqrt{-5}]$ the number $\sqrt{-5}$ is prime; as is $a + b\sqrt{-5}$ if $\gcd(a, b) = 1$. But

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5});$$

so 6 does not have a unique factorisation into primes.

Problem 7.1. Show that in the number system $\mathbb{E}$ of even integers, with usual addition and multiplication, the number 180 does not have unique factorisation.

Unique Factorisation

We start with some preliminary results.

Lemma 7.1. *If a prime p divides ab then it divides a or b.*

Proof. Let $p|ab$. If $p|a$ we are done, so we may assume that $p \nmid a$. So $\gcd(a, p)$ which must divide p so must be 1 or p, is 1. But then we can write $1 = xp + ya$, for integers x and y. And so multiplying both sides by b get

$$b = xpb + yab.$$

As p divides xpb and yab it divides b. □

With this we get the following.

Theorem 7.2. *(Prime Divisibility Property) Let p be prime. If $p|a_1a_2 \dots a_r$ then p divides at least one of the a_i.*

Proof. By the lemma, $p|a_1$ or $p|a_2a_3\dots a_r$. In the former case we are done so assume the latter. By the lemma, $p|a_2$ or $p|a_3\dots,a_r$. Continuing in this way we get that $p|a_i$ for some i. □

Now!

Theorem 7.3. *(Fundamental Theorem of Arithmetic) Every integer $n \geq 2$ can be factored uniquely into primes*

$$n = p_1p_2\dots p_n.$$

(Uniqueness is upto order.)

Proof. We first show that n can be factored, then that the factorisation is unique.

The proof that n can be factored is by induction on n. The statement is clear if $n = 2$, as 2 is prime. Assume that we have proved the statement for all $n \leq N$; we use this to prove it for $n = N + 1$. The principle of induction then says that the statement is true for all $n \geq 2$.

If n is prime then we are done, so suppose it factors as $n = n_1n_2$ for $1 \leq n_1, n_2 \leq N$. As the statement holds for n_1 and n_2 we get by the induction hypothesis that

$$n_1 = p_1\dots p_r \text{ and } n_2 = q_1\dots q_s$$

for primes p_i and q_j, so

$$n = n_1n_2 = p_1\dots p_rq_1\dots q_s$$

as needed.

Uniqueness.

Assume that

$$p_1\dots p_r = n = q_1\dots q_s$$

are two factorisations of n. As p_1 divides $n = q_1\dots q_s$ it divides q_i for some i. As q_i is prime $p_1 = q_1$. Reordering the q_i we may assume that $p_1 = q_1$ and so get that

$$p_2\dots p_r = q_2\dots q_s.$$

Continuing as above we get that $r = s$ and $p_i = q_i$ for all i. □

Problem 7.2. Show that the number $\sqrt{-5}$ is prime in $\mathbb{Z}[\sqrt{-5}]$.

Problems from the Text

Chapter 7: 1, 2, 3, 5, 6

8 Congruences

The integer a is *congruent to* b *module* m, written

$$a \equiv b \mod m \qquad \text{or} \qquad a \equiv_m b,$$

if $m|a-b$.

Example 8.1. We have $27 \equiv_4 3$ and

$$-19 \equiv_{10} -9 \equiv_{10} 1 \equiv_{10} 11 \equiv_{10} 21.$$

If division by m gives that

$$a = mb + r$$

then $a \equiv_m r$.

The relation $\equiv_m$ is an *equivalence relation* or a *congruence*. The m is called the *modulus*.

Our common arithmetic operations 'commute' with congruence.

If $a_1 \equiv_m b_1$ and $a_2 \equiv_m b_2$ then

- $a_1 + a_2 \equiv_m b_1 + b_2$.
- $a_1 - a_2 \equiv_m b_1 - b_2$.
- $a_1 a_2 \equiv_m b_1 b_2$.

Oh. Did I leave out division? It doesn't always work for division. Even if we stay in the integers, there is another problem. We have $6 \equiv_6 12$, but if we try to divide both sides by 3 we get $2 \equiv_6 = 4$, which is false. We cannot 'cancel'. And we can have two non-zero integers, like 2 and 3 modulo 6, whose product is 0.

We have to be careful with division. But in the exercises, you will show that if $\gcd(c, m) = 1$, then you can cancel c.

Solving modular congruences

Knowing these operations, let's try to solve some modular equations, or congruences. It is easy to solve

$$x + 12 \equiv_8 5.$$

Indeed, $x \equiv_8 5 - 12 = -7 \equiv_8 1$. Either 1 or -7 are acceptable answers. Actually, 9 is as well. We call these solutions *congruent*, and generally prefer to give the solution in $[0, m-1]$, or occasionally in $[-m+1, 0]$. If there are

more solutions to a congruence module m in $[0, m-1]$, as can happen wiht a non-linear congruence, the solutions are called *incongruent*.

If we cannot divide, how do we solve

$$4x \equiv_{19} 3?$$

Well, we can just plug in all values of x from 0 to 18. We would find that $4 \cdot 5 \equiv_{19} 1$, and so get $x \equiv_{19} 5$. But this isn't satisfying.

Observe that $ax \equiv_m c$ if and only if there is some y such that

$$ax + my = c.$$

We saw that this equation has a solution (x, y) if and only if $\gcd(a, m)|c$, and in this case we can find solutions (x_0, y_0) by the EEA. When we find this we also have solutions $(x_0 + k(m/g), y_0 + k(a/g))$ for any integer k.

Theorem 8.2. *Let a, c and m be integers with $m \geq 1$, and let $g = \gcd(a, m)$. The modular equation*

$$ax \equiv_m c$$

has no solutions if $g \nmid c$, but if $g|c$, then it has g incongruent solutions modulo m. Where (x_0, y_0) is a solution to

$$ax + my = c,$$

the solutions are $x_0 + k(m/g) \mod m$ for $k = 0, \ldots, g-1$.

Example 8.3. Find the solutions to

i). $6x \equiv_{22} 15$

ii). $6x \equiv_{22} 16$

For i). there are no solutions, as $\gcd(6, 22) = 2 \nmid 15$. For ii). we have $\gcd(6, 22) = 2 \mid 16$ so using the EEA we find

$$6 \cdot 4 - 22 \cdot 1 = 2,$$

which gives $6 \cdot 4 \equiv_{22} 2$. Multiplying by 8 to get 16 gives our first solution $x = 4 \cdot 8 \equiv_{22} 10$:

$$6 \cdot 10 \equiv_{22} 16.$$

Adding 11 gives another solution, so our solutions are $x = 10, 21$.

When $\gcd(a, m) = 1$ there is only the one incongruent solution x to $ax \equiv_m = 1$, and in this case we write $x \equiv_m 1/a$ or $x \equiv_m a^{-1}$.

Example 8.4. Module 10 we have that $3 \cdot 7 \equiv_{10} 1$ so we can write $1/3$ for 7.

Beyond linear equations

We might also like to solve non-linear equations. Congruences such as

$$x^2 \equiv_m 1 \qquad \text{or} \qquad z^2 \equiv_m -1$$

have solutions or not depending on what m is. And quadratic equations can have more than two incongruent solutions:

$$x^2 + x \equiv_6 0$$

has solutions $x = 0, 2, 3, 5$. Modulo primes p though, things tend to work more as expected.

Theorem 8.5 (Polynomial Roots mod p Theorem)**.** *Let p be prime and let*

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$$

be an polynomial of degree d with integer co-efficients (and $p \nmid a_0$). There are at most d incongruent solutions, modulo p, to $f(x) \equiv_p 0$.

Proof. Call a solution of $f(x) \equiv_p 0$ in $\{0, 1, \ldots, p-1\}$ a *root* of $f(x)$. The strategy is to assume that $f(x)$ has too many roots. For a root r_i, if we can write $f(x) = (x - r_i)g(x)$ for some polynomial $g(x)$ smaller degree, and then show all the other roots are roots of $g(x)$, then $g(x)$ also has too many roots. Let's do it.

The theorem is clearly true for polynomials of degree 1, so if there theorem is not true, there is a minimum degree polynomial $f(x)$, of degree $d \geq 2$, which has more than d distinct roots $\{r_0, \ldots, r_d\}$. Consider the polynomial

$$f(x) - f(y) = a_0(x^d - y^d) + \cdots + a_{d-1}(x - y).$$

As $x^i - y^i = (x-y)(x^{i-1} + x^{i-2}y^1 + \ldots x^1 y^{i-2} + y^{i-1})$, we can pull $(x - y)$ out of each term, and get

$$f(x) - f(y) = (x - y)g(x, y)$$

for some polynomial $g(x, y)$ of degree less than d.

Plugging a root r_0 in for y gives

$$f(x) \equiv_p (x - r_0)g(x, r_0)$$

so $g_0(x) = g(x, r_0)$ is smaller polynomial we were looking for.

Observe that for any other root r_i

$$0 \equiv_p f(r_i) = (r_i - r_0)g_0(r_i).$$

As r_i and r_0 are distinct, $g_0(r_i) = 0$. So $g_0(x)$ has degree less than d but at least d roots, contradicting our choice of $f(x)$. □

Problems from the Text

Chapter 8: 1,2,3,4,5,6,10

9 Congruences, Powers, and Fermat's little theorem

Consider the powers of the different numbers mod 5. The powers of 2 are

$$2, 4, 3, 1, 2, 4, 3, 1, 2...$$

Whatever you start with, except 0 eventually hits 1 and then repeats. In fact, the same is true modulo any prime p.

For any prime p and integer a not divisible by p we have $\gcd(a, p) = 1$, and so we can write 1 as a linear combination of a and p:

$$aa' + cp = 1.$$

This means that $aa' \equiv_p 1$. Writing a' as a^{-1} we get the following.

Fact 9.1. *Any a such that $a \not\equiv_p 0$ has an inverse a^{-1} mod p.*

Theorem 9.2 (Fermat's Little Theorem)**.** *For any prime p and any number $a \not\equiv_p 0$, we have*

$$a^{p-1} \equiv_p 1.$$

Proof. As p is a prime, and $a \not\equiv_p 0$, a has an inverse a^{-1} modulo p, so the sets

$$\{1, 2 \ldots, p-1\} \qquad \text{and} \qquad \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$$

are the same set of non-zero images modulo p. Thus the products of these sets are the same:

$$(p-1)! \equiv_p a^{p-1}(p-1)!.$$

As $p \nmid (p-1)!$, we can divide by it to get $1 \equiv_p a^{p-1}$, as needed.

□

This little theorem is useful in computing powers.

Example 9.3. Evaluate 2^{39} modulo 7.

$$\begin{aligned} 2^{39} \equiv_7 2^{6(6)+3} &\equiv_7 2^6 \cdot \ldots \cdot 2^6 \cdot 2^3 \\ &\equiv_7 1 \cdot \ldots \cdot 1 \cdot 2^3 \equiv_7 1 \end{aligned}$$

Problem 9.1. Solve $x^{103} \equiv_{11} 4$.

You probably found that you had to solve $x^3 \equiv_{11} 4$ to solve this. How did you do it? Did you just evaluate a^3 mod 11 until you found something that gave a 4? A little unsatisfying, eh? Well, taking roots is a hard problem. We will see a cryptography system based on this fact. You can do better than 'checking every solution' but not a lot better.

We will also see how Euler's theorem can be used to help us decide if a big number such as $b = 340829383947293772093482 73$ is prime.

Problem 9.2. Compute $(p-1)!$ modulo p for a couple values of p. Is there a pattern? Why?

Problems from the Text

Chapter 9: 1,2,3,4

10 Euler's Formula

Fermat's little theorem said for prime p that

$$a^{p-1} \equiv_p 1$$

for all $a \neq 0$.

What if m is composite? Is there some power $d > 0$ such that

$$a^d \equiv_m 1$$

for all $a \neq 0$. No, taking $m = 6$ we see that $4^d \equiv_6 4$ for all d.

Our proof for Fermats little theorem breaks because there are elements mod m that do not have inverses. So lets just look at the elements that have inverses.

Let $\Phi(m) = \{a \in \{1, \ldots, m-1\} \mid gcd(a, m) = 1\}$, and let $\phi(m) = |\phi(m)|$

We see that $\phi(p) = p - 1$ for primes p, and we can compute, say:

$$\Phi(10) = \{1, 3, 7, 9\} \qquad \text{and} \qquad \phi(10) = 4.$$

Hey, look! Modulo 10 we have

$$1^4 \equiv_{10} 1 \qquad 3^4 \equiv_{10} 1 \qquad 7^4 \equiv_{10} 1 \qquad 9^4 \equiv_{10} 1.$$

Recalling the proof of Fermats little theorem, the lists

$$\Phi(m) \qquad \text{and} \qquad b\Phi(m) := \{ba \mid a \in \Phi(m)\}$$

are the same for any $b \in \Phi(m)$ because b is invertible.

So their products are

$$\Pi_{a\in\Phi(m)} a \equiv_m b^{\phi(m)} \Pi_{a\in\Phi(m)} a.$$

Now Φa is invertible, as it is the product of invertible elements, so we can cancel it, giving $b^{\phi(m)} \equiv_m 1$.

This proved the following.

Theorem 10.1 (Euler's Theorem)**.** *For all a in $\Phi(m)$, we have $a^{\phi(m)} \equiv_m 1$.*

Problems from the Text

Chapter 10: 1, 2, 3

11 Euler ϕ function and the Chinese Remainder Theorem

This useful function $\phi(m) = |\Phi(m)|$ that counts the number of integers modulo m that are relatively prime to m is called the Euler ϕ function, or the Euler totient function.

We know that $\phi(p) = p - 1$ if p is prime, what is if for composite numbers? There are two steps to figuring this out.

Problem 11.1. What is $\phi(p^d)$ for prime p ?

If we can now find $\phi(mn)$ when $\gcd(m, n) = 1$ we have a formula. Let's start with an example.

Problem 11.2. What is $\phi(15)$?

Hopefully from this question you have conjectured, and maybe even proved the following with a counting argument.

Lemma 11.1. *If* $\gcd(m, n) = 1$ *then* $\phi(mn) = \phi(m) \cdot \phi(n)$.

Proof. We show that the function

$$f : \Phi(mn) \to \Phi(m) \times \Phi(n) : x \mapsto (x \mod m, x \mod n)$$

is a bijection.

To see that it really maps to $\Phi(m) \times \Phi(n)$ observe that if $x \mod m$ is not in $\Phi(m)$, then $1 < \gcd(x, m) \mid \gcd(x, mn)$ so x is not in $\Phi(mn)$. Similarily if $x \mod n$ is not in $\Phi(n)$ then x is not in $\Phi(mn)$.

To show that f is a bijection we show that it has an inverse: we show for every pair (a, b) in $\Phi(m) \times \Phi(n)$ there is some x in $\Phi(mn)$ such that

$$x \equiv_m a \qquad \text{and} \qquad x \equiv_n b.$$

We do this with the next theorem. □

Theorem 11.2 (Chinese Remainder Theorem)**.** *Let m and n be integers with $\gcd(m, n) = 1$. For integers a and b there is a unique $x \in [mn]$ such that*

$$x \equiv_m a \qquad \textit{and} \qquad x \equiv_n b.$$

Proof. We have already shown uniqueness above, so we need only show existence. The congruence $x \equiv_m a$ means that $x = a + cm$ for some c. Plugging this into $x \equiv_n b$ gives

$$a + cm \equiv_n b \qquad \text{or equivalently} \qquad a - b \equiv_n cm.$$

Now as $\gcd(m, n) = 1$ we have that m is invertible modulo n and so

$$c \equiv_n (a - b)/m.$$

So $x = a + cm$ is the required solution. □

With this we have completed the proof of Lemma 11.1. Use it to show the following.

Problem 11.3. Where m has prime decomposition $m = p_1^{d_1} p_2^{d_2} \dots p_n^{d_n}$ show that

$$\phi(m) = m \cdot \Pi_{i=1}^{n}(1 - 1/p_i).$$

The Chinese Remainder Theorem is quite useful on its own right. Let's practice using it.

Example 11.3. Let's find a number x such that $x \equiv_5 4$ and $x \equiv_7 3$. We follow our proof.

As $x \equiv_5 4$ there is some c such that

$$x = 5c + 4.$$

Now using that $x \equiv_7 3$ we get that

$$4 + 5c \equiv_7 3.$$

To solve for c we need the inverse of 5 mod 7. We would use the EEA to find this, but as 7 is small, we quickly see that $5^{-1} \equiv_7 3$. Solving then

$$\begin{aligned} 4 + 5c \equiv_7 3 \quad &\iff \quad 5c \equiv_7 6 \\ &\iff \quad c \equiv_7 3 \cdot 6 \equiv_7 4. \end{aligned}$$

Thus $x = 5c + 4 = 5(4) + 4 = 24$.

Problem 11.4. Find a number x satisfying $x \equiv_3 2$, $x \equiv_5 1$ and $x \equiv_7 4$.

Problems from the Text

Chapter 11: 1, 2, 3, 5, 6, 9, 11, 12, 13

12 Prime Numbers

Recall Euler's proof of the infinity of primes.

Theorem 12.1 (Infinity of Primes)**.** *There are infinitely many prime numbers.*

Proof. Assume that there are finitely many: $p_1, \ldots, p_n$. Let $A = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. As each p_i divides $A - 1$, but not 1, it does not divide A. So A is another prime, bigger than all the p_i. □

There are infinitely many primes, but there is only one that is congruent to 2 mod 4: 2. Clearly there are no primes congruent to 0 mod 4. Are there infinitely many primes that are 1 mod 4? Or 3 mod 4? The answer to both questions is 'Yes' but it is much easier to prove for 3.

Theorem 12.2. *There are infinitely many primes congruent to* 3 *mod* 4*.*

Proof. We mimic the proof above. Assume that there are finitely many primes that are congruent to 3 mod 4: $3, p_1, \ldots, p_n$, and let $A = 4p_1p_2 \ldots p_n + 3$. We have that $A \equiv_4 3$, and none of the p_1 divide A, as they divide $A - 3$ but not 3. Also $3 \nmid A$ as it does not divide $A - 3$: if it did, then it would have to divide 4 or one of the p_i. So if A is not prime, all of its prime factors are congruent to 1 or 2 mod 4. But the product of factors that are 1 or 2 mod 4 is 1 or 2 mod 4. □

Note that this proof will not work to show that there are infinitely many primes that are 1 mod 4, as the product two numbers that are 3 mod 4 is 1 mod 4. We will prove it with a different proof in Chapter 21.

Okay. For what a and b can we say there are infinitely many primes congruent to b mod a? As we observed with 2 mod 4. If $\gcd(a, b) = c$, then any number that is congruent to b mod a is divisible by c. So the only number congruent to b mod a that might be prime is c.

Theorem 12.3 (Dirichelet 1837)**.** *Let* $\gcd(a, b) = 1$. *There are infinitley many primes that are congruent to* b *mod* a.

The proof of this is difficult; we will not do it. But it is called the theorem of primes on arithmetic progressions. An arithmetic progression is a sequence of the form

$$c, c + a, c + 2a, c + 3a, \ldots, .$$

Dirichelet showed that within such progressions, we can find infinitely many primes. Taking $a = 3$ and $b = 1$, we can find infinitely many primes in

$$1, 4, \underline{7}, 10, \underline{13}, 16, \underline{19}, 22, 25, \ldots, .$$

The primes themselves are not in an arithmetic progression. Green and Tao showed in 2004 that the set of all primes contains arbitrarily long arithmetic progressions.

Problems from the Text

Chapter 12: 2, 3(a,b), 5, 6

13 Counting Primes

How many primes are there in $[n] = \{1, 2, \ldots, n\}$?

Let $\pi(n)$ be the number of primes in $[n]$. We know that the function $\pi(n)$ increases to infinity as n goes to infinity, but how quickly?

If you are not familiar with limits, the book gives some nice intuitive discussion on the notion.

To understand the limiting behaviour of $\pi(n)$, let's first look at an easier version. An integer n is *m-prime* if it has no divisors, other than 1 or itself, less than or equal to m.

Example 13.1. A number n is prime if and only if it is $\sqrt{n}$-prime. The number 77 is 5-prime. It is the first 5-prime number that is not prime.

Let $\pi_m(n)$ be the number of m-prime elements of $[n]$. It is easy to see that $\pi_2(n) = \lceil n/2 \rceil$. As a limit, we write this as

$$\lim_{n \to \infty} \frac{\pi_2(n)}{n} = 1/2.$$

To compute $\pi_3(n)$ we can list the numbers $[n]$ then remove the $n/2$ of them that have a divisor 2, and the $n/3$ that have a divisor 3. We've removed the $n/6$ that have a divisor of 6 twice, so we must add that number back it. So

$$\pi_3(n) \approx n(1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{2 \cdot 3}) = n(1 - \frac{1}{2})(1 - \frac{1}{3}) = n \cdot \frac{1}{2} \cdot \frac{2}{3}.$$

Writing this as a limit, we get $\lim_{n\to\infty} \frac{\pi_3(n)}{n} = (1/2)(2/3) = 2/6$. Another way of looking at this, which explains the final form of our equation, is that when we remove the $n/3$ elements with a factor of 3, we remove $1/3$ of the remaining numbers.

Problem 13.1. Show that $\lim_{n\to\infty} \frac{\pi_5(n)}{n} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$.

Now, while the product

$$\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \frac{4}{5} \cdot \frac{5}{6} \cdot \frac{6}{7} \cdot \frac{7}{8} \cdot \ldots \cdot \frac{n-1}{n}$$

is easy to compute, the product

$$\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \ldots \cdot \frac{p-1}{p}$$

is much harder. But deeper analysis yields, as $n \to \infty$, that

$$\frac{\pi(n)}{n} = \frac{\pi_{n-1}(n)}{n} \to \frac{1}{\ln(n)}.$$

We write this as

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

Some Famous conjectures about primes

Goldbach's Conjecture

Every even number is a sum of two primes.

This has been verified up to at least 10^{10}. Vinogradev showed in 1937 that every large enough odd number is the sum of 3 primes. Jing-run showed in 1966 that every large enough even number is the sum of $p + a$ where p is prime and a is either a prime or a product of two primes.

Twin Prime Conjecture

There are infinitely many primes p such that $p + 2$ is also prime.

$N^2 + 1$ Conjecture

There are infinitly many primes of the form $N^2 + 1$.

Iwaniec showed in 1978 that there are infinitely many N such that $N^2 + 1$ is a prime or the product of two primes.

Problems from the Text

Chapter 13: 1, 3, 4

14 Mersenne Primes

We look at the question of when a number of the form $a^n - 1$ can be prime.

Recalling that

$$(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

we see that $a^n - 1$ cannot be prime unless $a = 2$. Further, if n isn't prime, then where $n = ab$ we have

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1)$$

is not prime. So $a^n - 1$ can only be prime if $a = 2$ and n is a prime p.

Primes of the from $2^p - 1$ for prime p are called *Mesenne primes*. There are several.

$$2^2 - 1 = 3 \qquad 2^3 - 1 = 7 \qquad 2^5 - 1 = 31 \qquad 2^7 - 1 = 127$$

are prime, however,

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

isn't.

It seems to start well, but the only primes $2^p - 1$ with $p < 10000$ have

$$p = 2, 3, 5, 7, 13, 61, 89, 107, 127, 521, 607, 1279, 2203,$$
$$2281, 3217, 4253, 4423, 9689, 9941$$

The 48^{th} Mersenne prime is $2^{57\,885\,161} - 1$, found in 2013 by the Great Internet Mersenne Prime Search (GIMPS). The largest know is $2^{82\,589\,933} - 1$, it is believed to be the 51^{st}.

Problems from the Text

Chapter 14: 1, 2, 3

15 Mersenne Primes and Perfect Numbers

A number is *perfect* if it is the sum of its proper factors (its factors less than itself). So

$$6 = 1 + 2 + 3 \qquad \text{and} \qquad 28 = 1 + 2 + 4 + 7 + 14$$

are perfect. Perfect numbers are quite rare. The sums can be too high, or too low:

$$\begin{aligned} 12 &: & 1 + 2 + 3 + 4 + 6 &= 16 \\ 15 &: & 1 + 3 + 5 &= 9 \end{aligned}$$

But we know how to find more.

Theorem 15.1 (Euclid's Perfect Number Formula)**.** *If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect.*

Before we prove this, lets see an example of why it works for the Mesenne prime $2^5 - 1$. The theorem says that $(2^5 - 1)(2^4) = 31 \cdot 16$ is perfect. Well,

$$2^5 - 1 = 31 = 1 + 2^1 + 2^2 + 2^3 + 2^4$$

while $16 = 2^4$ has factors $1, 2, 2^2, 2^3, 2^4$.

Their product $16 \cdot 31$ has proper factors

$$\{1, 2, 2^2, 2^3, 2^4\} \qquad \text{and} \qquad 31 \cdot \{1, 2, 2^2, 2^3\}.$$

Summing these we get

$$\begin{aligned} 1 + 2 + 2^2 + 2^3 + 2^4 \quad &+ \quad 31(1 + 2 + 2^2 + 2^3) \\ 31 \quad &+ \quad 31(2^4 - 1) \qquad\qquad = 16 \cdot 31. \end{aligned}$$

Proof. When $2^p - 1$ is prime, the number $(2^p - 1)2^{p-1}$ has factors

$$\{1, 2, 2^2, \ldots, 2^{p-1}\} \qquad \text{and} \qquad (2^p - 1)\{1, 2, 2^2, \ldots, 2^{p-2}\}$$

which sum to

$$(2^p - 1) \qquad + \qquad (2^p - 1)(2^{p-1} - 1) = (2^p - 1)(2^{p-1})$$

as needed. □

So are these the only perfect numbers? We don't know. But Euler showed the following.

Theorem 15.2 (Euler's Perfect Number Theorem)**.** *If n is an even perfect number, then*

$$n = 2^{p-1}(2^p - 1)$$

where $2^p - 1$ is a Mesenne prime.

Before we prove this, we define a function that we use in its proof. Let $\sigma(n)$ be the sum of the divisors of n.

Example 15.3. $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

Problem 15.1. What is $\sigma(p^k)$?

Clearly n is perfect if and only if $\sigma(n) = 2n$.

Problem 15.2. Show that if $\gcd(m, n) = 1$ then $\sigma(mn) = \sigma(m)\sigma(n)$.

Now we can prove the theorem.

Proof of Euler's Perfect Number Theorem. Let n be an even perfect number. As it is even we can write it as $n = 2^k m$ for some $k \geq 1$, some odd m. With this we get that

$$2^{k+1}m = \sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m).$$

As $(2^{k+1} - 1)$ is odd $\sigma(m)$ can be written as $2^{k+1}c$ for some c, and so $m = (2^{k+1} - 1)c$. So m has factors at least : $1, c$ and $(2^{k+1} - 1)c$, which are distinct if $c > 1$, and so

$$2^{k+1}c = \sigma(m) > (2^{k+1} - 1)c + c + 1 = 2^{k+1}c + 1,$$

an impossibility. So we may assume that $c = 1$. But then $n = 2^k m = 2^k(2^{k+1} - 1)$, and we have

$$\sigma(m) = 2^{k+1} = m + 1$$

which means that $m = 2^{k+1} - 1$ is prime, and so a Mersenne prime. □

We do not know if there are any odd perfect numbers.

Problems from the Text

Chapter 15: 1, 2, 3, 5, 6

16 Powers Modulo n and successive squaring

In applications such as cryptography, one often wants to compute

$$a^d \mod m$$

where a, d and m are numbers with 100s of digits.

We clearly can reduce a modulo m without changing the value, and we saw that using Euler's formula, we can reduce d to a residue mod $\phi(m) \approx m$.

But even with these reductions if m is 100 digits, then computing

$$a^d \mod m$$

the 'stupid' way takes m operations:

The stupid way to compute $5^{542} \mod 851$:

$5^1 = 5$ $\quad$ $5^2 = 25$ $\quad$ $5^3 = 125$ $\quad$ $5^4 = 625$

$5^5 = 572$ $\quad$ $5^6 = 307$ $\quad$ $5^7 = 684 \ldots$

Successive squaring

We can speed this up with another idea called successive squaring. There is only one idea: we don't need all of the 5^i, we only need those of the form: $5^1, 5^2, 5^4, 5^8, 5^{16}, \ldots$. As 542 can be written as

$$542 = 2^9 + 2^4 + 2^3 + 2^2 + 2^1$$

we can then compute

$$\begin{aligned} 5^{542} &= 5^{2^9+2^4+2^3+2^2+2^1} \\ &= 5^{2^9} \cdot 5^{2^4} \cdot 5^{2^3} \cdot 5^{2^2} \cdot 5^{2^1}. \end{aligned}$$

The expression of a number n as a 'polynomial in 2'

$$542 = 1(2^9) + 0(2^8) + \cdots + 1(2^1) + 0(2^0)$$

is its *binary expansion*. Its *binary representation* $[n]_2$ is when we record just the co-efficients in its binary expansion:

$$[542]_2 = 1000011110.$$

Problem 16.1. What is the binary representation $[333]_2$ of 333? What number has binary representation $[n]_2 = 0101010$?

To compute $a^d \mod m$ the stupid way we must do our basic operation of 'multiply and reduce modulo m' a total of m times. To compute it by successive squaring, we must do our basic operation about $2 \log_2 m$ times: $\log_2 m$ for computing the powers of d, and at most this for multiplying them together. Oh, we also need to compute $[d]_2$, but this also takes only $\log_2 m$ divisions by 2. (And guess what? Most of the time we are doing this on a computer, so we usually already store d as $[d]_2$.)

Let's summarise our algorithm.

Algorithm 16.1 (Successive squaring)**.** *To compute* $a^d \mod m$*, we*

i). Reduce a *and* d *modulo* m*.*

ii). Compute the numbers $a, a^2, \ldots, a^{2^r}$ *modulo* m *for* $r = \log_2(m)$ *by successively squaring.*

iii). Compute $\Sigma_{i=0}^{r} u_i a^{2^i}$*, modulo* m*, where* $[m]_2 = u_r u_{r-1} \ldots u_0$*.*

Now even if our numbers have 100 digits, we can compute this relatively quickly.

And so, as discussed earler, with Euler's theorem we can now 'check' relatively quickly that a number is prime.

Example 16.2. We show that $m = 69$ is not prime by computing $2^{68} \mod 69$.

Powering, we get:

d	0	1	2	3	4	5	6
2^{2^d}	2	4	16	49	55	58	52

and multiplying we get

$$2^{68} = 2^{64} \cdot 2^4 = 52 \cdot 16 \equiv_{69} 4.$$

As this is not 1 we conclude that 69 is not prime.

Keep in mind, this test only tells us that a number is not prime. We have to be careful using it to say a number is prime. We talk more about this in Chapter 19.

Problems from the Text

Chapter 16: 1, 2(a), 3 (For 3, use a computer, or use smaller numbers in the question.)

17 Computing k^{th} roots modulo m

We can power quickly, but can we undo it? Can we solve the following?

$$x^k \equiv_m b.$$

A solution x to this is called a k^{th} *root of* b *modulo* m?

Note

Notice that the way we find real root does not work modulo m. Modulo 15 the square roots of 10 are 5 and 10. We cannot find this by saying the root is 'between 3 and 4', which is how we would start to find the real square root.

First we observe that there is not always a k^{th} root of b modulo m. If $k = \phi(m)$, then $x^k \equiv_m 1$ for any x so only 1 has any k^{th} roots. The equation

$$x^2 \equiv_6 2$$

has no solutions: $1^2 \equiv_6 5^2 \equiv_6 1$, $2^2 \equiv_6 4^2 \equiv_6 4$, and $3^2 \equiv_6 3$. In general, it is a little tricky to decide if $x^2 \equiv_n r$ has a solution, we will look at this later.

Sometimes though, if $\gcd(b, m) = 1$, then Euler's theorem can help us to find solutions to $x^k \equiv_m b$. If k has an inverse modulo $\phi(m)$– a d such that $dk \equiv_{\phi(m)} 1$– then b^d is our solution. Indeed, in this case $dk + c\phi(m) = 1$ for some c, and so, using $b^{\phi(m)} \equiv_m 1$ in the middle equivalence, we get

$$(b^d)^k = b^{dk} \equiv_m b^{dk+c\phi(m)} = b.$$

So b^d modulo m is our k^{th} root of b. We can find the inverse d of k by EEA as long as $\gcd(k, \phi(m)) = 1$.

We summarise this into an algorithm.

Algorithm 17.1 (k^{th} roots modulo m)**.** *If* $\gcd(b, m) = 1$ *and* $\gcd(k, \phi(m)) = 1$ *then one can find a solution to* $x^k \equiv_m b$ *as follows.*

i). Factor m *and compute* $\phi(m)$*.*

ii). Use EES to find the inverse d *of* k *modulo* $\phi(m)$*.*

iii). Set $x = b^d \mod m$*.*

Example 17.2. To find solution x to $x^5 \equiv_{21} 4$ we use that $\phi(21) = 2 \cdot 6 = 12$. As $\gcd(5, 12) = 1$, the number 5 has an inverse modulo 12 which we can find by the EEA. But clearly $5 \times 5 \equiv_{12} 1$ so it is 5. Thus $x = 4^5 \mod 21 = 16$ is a solution.

Now steps 2 and 3 are okay, we have nice fast algorithms for them, even when m is big. However we haven't looked at factoring m. If m is the product of two large primes, then there is no good way to factor it quickly. This is the fact that many cryptosystems are based on: it is hard to factor a product of two large primes.

We see this in the next section.

Problems from the Text

Chapter 17: 1, 2, 3

18 Powers, Roots and Unbreakable Codes

We can power, ie. compute $a^k \mod m$, quickly. We can undo this, ie. solve $x^k \equiv_m b$ quickly, but only if we know $\phi(m)$. This is all we need to send and receive encrypted (secret) messages.

We look at a public key cryptosystem, called RSA. The 'public key' refers to the fact that the encryption method, for converting the message to a secret message is public. One person, Alice, can decode the messages, but anyone can send them to her.

Suppose we want people to be able to send us secret messages.

$$PICK\ ME\ UP\ AT\ SCHOOL.$$

To send us a message, they first convert it into integer strings. (Or usually binary strings.)

P	I	C	K		M	E	...
15	09	03	12	00	13	05	...

This isn't the secret, anyone can do and undo it. So they have to *encrypt* it. We have to tell them how to do this.

We pick two big primes. Usually they should be at least 80 digits, but we will use smaller primes to make it easier to write.

$$p = 12553 \qquad \text{and} \qquad q = 13007$$

We compute

$$n = pq = 163276871$$
$$\phi(n) = \phi(p)\phi(q) = 163251312.$$

We also choose some e that is relatively prime to $\phi(n)$:

$$e = 79913.$$

Our *public key* (e, n) will not be a secret. We give this to everyone, but we keep p and q and $\phi(n)$ secret.

Now someone wants to send me the message $m = 150903120$.

To *encode* it, they compute

$$c = m^e \mod n = 150903120^{79913} \equiv_{163276871} 54535292$$

and send me $c = 54535292$.

To *decode* c *back to* m, I have $\phi(n)$, so I can solve

$$x^{79913} \equiv_{163276871} 54535292.$$

I use EEA to compute the inverse $d = 149129$ of $e \bmod \phi(n)$, and then I compute

$$c^d = 54535292^{149129} \equiv_{162376871} 150903120.$$

This is the RSA public key cryptosystem developed by Rivest, Shamir, and Adleman. We summarise it.

RSA public key cryptosystem

Setup: Find large primes p and q; compute $n = pq$ and $\phi = (p-1)(q-1)$, choose e with $gcd(e, \phi)$, compute inverse d of e modulo ϕ.
Private key: p, q, ϕ and d.
Public key: n and e.
Encryption: Encrypt message m to $c = m^e \mod n$.
Decryption: Decrypt codeword c to $m = c^d \mod n$.

Now how secure is this? If anyone else wants to get m, without knowing $\phi(n)$, then have to compute

$$\begin{aligned} 1^e &\mod n \\ 2^e &\mod n \\ &\vdots \end{aligned}$$

Computing any one of these is easy. But even if they are smart about it, they have to do this on average about $\sqrt{n}$ times. We choose m big enough that this is impossible in 1000 years.

They can compute it if they know $\phi(n)$. So our security is based on the fact that finding $\phi(n)$ is hard. We know we can find $\phi(n)$ if we can factor n, our security also depends on the fact that factoring n is hard. Let's see that finding $\phi(n)$ and factoring n are, practically, the same problem. The point of doing this it that factoring n is a much more universal problem. We've been trying to do it for 100s of year. We have not been trying to find $\phi(n)$ for as long.

We show that if we have $\phi(n)$ we can get p and q. Indeed

$$\phi(n) = (p-1)(q-1) = qp - p - q - 1 = n - p - q + 1.$$

From this we get that

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

Finding the zeros of

$$x^2 - (p+q)x + n,$$

we get p and q as this polynomial is $(x-p)(x-q)$.

Problems from the Text

Chapter 18: 1, 2(a,b)

19 Primality Testing and Carmichael Numbers

Recall in Chapter 16 we saw an imperfect primality test: to test if some big number n was prime we calculated

$$a_i^{n-1} \mod n$$

for several a_i and said that if any of these were not equal to 1, then n was not prime. This is called the *Euler Test*. If all of these were 1, then we were not sure that n was prime, but we thought it was likely.

A *(Euler)-witness* (for the non-primality of n) is a number a such that

$$a^{n-1} \not\equiv_n 1.$$

We checked on a computer what percentage of the numbers modulo various composite n are witnesses.

n	190	287	291	314	586	728	808	935
%	95.2	98.6	98.6	99.6	99.8	99.8	99.8	99.1

Seems pretty good. But 561 isn't in our list. For $561 = 3 \cdot 11 \cdot 17$, only about %43 of the numbers from 1 to 560 are witnesses. In fact the only witnesses share a factor with 561. A number n is a *Carmichael* number if for all residues a modulo n we have

$$a^n \equiv_n a.$$

Notice that if this holds, then for all a with $\gcd(a, n) = 1$ we can cancel, and so get

$$a^{n-1} \equiv_n 1.$$

Problem 19.1. Show that if $\gcd(a, n) > 1$ then $a^{n-1} \equiv_n \not\equiv 1$. So checking $a^{n-1} \equiv_n 1$ is a better primality test than checking $a^n \equiv_n a$.

Characterising Carmichael Numbers

Checking for Carmichael numbers by computer, we find that the first couple are

$$561 = 3 \cdot 11 \cdot 17 \qquad 1105 = 5 \cdot 13 \cdot 17$$
$$1729 = 7 \cdot 13 \cdot 19 \qquad 2465 = 5 \cdot 17 \cdot 29$$

They are all products of three distinct odd primes. The 'three' is just because they are small. The following is also a Carmichal number

$$62745 = 3 \cdot 5 \cdot 47 \cdot 89,$$

but are 'distinct odd primes' necessary?

Fact 19.1. *Every Carmichael number is odd.*

Proof. Taking $a = -1$ we get for a Carmichael number n that $-1^n =_n -1$. But this means that n is odd or $n = 2$. We know 2 is not a Carmichael number. □

A number is *square-free* if it is the product of distinct primes.

Fact 19.2. *Any Carmichael number is square-free.*

Proof. Let n be Carmicheal and e be the max integer such that $p^{e+1}|n$. Then as n is Carmicheal we have

$$(p^e)^n \equiv_n p^e \qquad \text{so} \qquad n|(p^e)^n - p^e$$

thus $p^{e+1}|(p^e)^n - p^e$ and dividing through by p^e we get that $p|(p^e)^{n-1} - 1$. This is true only if $e = 0$. □

That n is square-free odd composite number is not sufficient for it to be a Carmichael number though; 15 is not a Carmichael, nor is $3 \cdot 5 \cdot 7 = 105$.

Turns out there is another necessary condition. In problem 19.1 you are asked to show that for any p dividing a Carmichael number n that $(p-1)|(n-1)$. Note that for a square free number this means that p is odd.

This is also sufficeint, so we get the following.

Theorem 19.3. *(Korselt's Criterion for Carmichael Numbers) A composite number n is a Carmichael number if and only if it is square-free, and every prime divisor p has $(p-1)|(n-1)$.*

Proof. We have showed the necessity of square-free, and you showed the necessity of $(p-1)|(n-1)$. So we assume these conditions for some composite number n and show that it is a Carmichael number. As $p - 1|n - 1$ for each p dividing n we have $(p-1)c + 1 = n$ for some c, and so for any a mod n we get

$$a^n = a^{(p-1)c+1} \equiv_p a.$$

This uses Euler if a is prime to p, but is trivial if a is not prime to p. So $p_i|a^n - a$ for all a prime to p_i, and as this is for all p_i, $n|a^n - a$ for all a prime to n. □

We can verify that $561 = 3 \cdot 11 \cdot 1$ by checking that $2, 10, 16$ all divide 560. Can you come up with a good algorithm to find all Carmicheal numbers? Problem 19.6 of the text asks you to do this. Probably you will enumerate the product of distinct odd primes. Can you think of a good formula for constructing Carmichael numbers. Problem 19.4, which is assigned, suggests a way to do this.

The Miller Rabin Test

Because of these pesky Carmichael numbers, we want a better primality test. The Miller-Rabin Test takes the Euler Test a step further. It is based on the following simple idea that mod a prime p, the only square roots of 1 are ± 1.

Fact 19.4. *For prime p, the only solutions to*

$$x^2 \equiv_p 1$$

modulo p are $x \equiv_p \pm 1$.

Proof. If $x^2 \equiv_p 1$ then $p|x^2-1 = (x+1)(x-1)$. As p is prime this gives $p|(x+1)$ or $p|(x-1)$. So $x \equiv_p \pm 1$. □

Example 19.5. Lets use this fact to try to show that 561 is prime. Remember, 561 is Carmichael, so there are many Euler non-witnesses. Say we chose one, such as $a = 13$. The Euler test, computing $13^{560} \equiv_{561} = 1$, is non-conclusive. 561 looks prime, but we don't know. Notice now that $13^{280} \mod 561$ is the square root of $13^{560} \equiv_{561} = 1$. Let's compute this:

$$13^{280} \equiv_{561} 1 \qquad 13^{140} \equiv_{561} 1 \qquad 13^{70} \equiv_{561} = 67.$$

Hey, this says that 67 is the square root of 1 modulo 561. This does not happen modulo a prime, so 561 is not prime.

Here 13 is a witness to the fact that 561 is composite. If it were a non-witness what would happen? That is, if 561 were prime, what would happen? Either we would get that one of the $13^{2^q \cdot 35}$ is -1 (all values before it would have to be 1) or we would never get anything other than 1 and would get that $13^{35} \equiv_{561} 1$.

For an odd composite number n, let $n-1 = 2^k q$ where q is odd. A number $a \in [n-1]$ is a *(Miller) non-witness for n* if

i). $a^q \equiv_p 1$, or

ii). One of $a^q, a^{2q}, \ldots, a^{2^{k-1}q}$ is $\equiv_p -1$.

Otherwise it is a *Miller witness* that n is composite.

Notice that we would usually compute 13^{70} before computing 13^{560}, so let's redo the above test a little more efficiently.

Example 19.6. Writing 560 as $560 = 2^4 \cdot 35$ we compute, modulo 561:

$$13^{35} \equiv 208 \qquad 13^{2 \cdot 35} \equiv 67 \qquad 13^{2^2 \cdot 35} \equiv 1.$$

We see that 67 is the square root of 1 modulo 561, so 561 isn't prime.

This is the Miller Rabin Test.

Algorithm 19.7 (Miller Rabin Test)**.** *To test if odd n is prime we write $n-1 = 2^k q$ for odd q. Choose a and compute, mod n:*

$$a^q, a^{2q}, a^{2^2 q}, \ldots, a^{2^k q}.$$

If $a^q = \pm 1$ then a is a non-witness, stop and try with another a. Otherwise if we get an -1 before getting a 1, then a is a non-witness, stop and try another a. Otherwise, we get 1 before -1, a is a witness that n is composite. Really stop.

We saw that only %43 percent of the residues mod 560 are Euler witnesses. It turns out that only 10 of the Euler non-witnesses are Miller non-witnesses. Over %98 of residues are witnesses. It can be shown that if n is an odd composite number, then over %75 of residues are witnesses.

It we run the Miller Rabin test with three different randomly chosen a the probablility falsely assuming n is prime is at most $(1/4)^3 \approx \%1.7$. If we use 10 different a the probablilty is at most %0.0001. Choose 100 and you could run this test 100 times a second and never get a false prime. It is more likely that I am lying to you, and this is all a big ruse to get your secret messages.

Problems from the Text

Chapter 19: 1*, 2, 3 (do a couple), 4, 7

20 Squares modulo p

What numbers are squares modulo p?

b		0	1	2	3	4	5	6	7	...
b^2	mod 13	0	1	4	9	3	12	10	10	...

We know that $-a^2 = a^2$. Modulo an odd prime p, these are different numbers, so every square has at least two square roots. We've also seen that if p is prime, then

$$a^2 \equiv_p b^2 \Rightarrow p | b^2 - a^2 \Rightarrow p | (b-a)(b+a) \Rightarrow b = \pm a$$

So if a is a square mod a prime p, then it has exactly two roots. So exactly $(p-1)/2$ (if p is odd) of the numbers in $[p-1]$ are squares. Only we don't call them squares.

We call a number $a \in [p-1]$ a *QR (quadratic residue) mod p* is if is a square modulo p, and an *NR (quadratic non-residue)* otherwise.

We have proved the following.

Theorem 20.1. *Let p be an odd prime. There are $(p-1)/2$ QRs and $(p-1)/2$ NRs mod p.*

Now. Taking roots is hard. So how do we decide if a given number n is a QR or an NR. We don't want to have to compute the square of every number in $[p-1]$ to decide this, because p might be huge.

Here are some simple properties about QRs and NRs.

Theorem 20.2. *Modulo an odd prime p the following hold.*

i). The product of a QR and a QR is a QR.

ii). The product of a QR and an NR is an NR.

iii). The product of a NR and a NR is a QR.

Proof. Try it. It is not so bad. For part iii), use part ii) and previous theorem. □

These rule perhaps remind us of something:

$$QR \times QR = QR \qquad QR \times NR = QR \qquad NR \times NR = QR.$$

QR and NR act like 1 and -1 under multiplication. This leads to the following definition of the *Legendre Symbol* for prime p and $a \in [p-1]$:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is QR} \mod p \\ -1 & \text{if } a \text{ is } NR \end{cases}$$

With this the previous theorem can be restated.

Theorem 20.3. *For prime p and numbers $a, b \in [p-1]$*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Example 20.4. To decide if 75 is a QR mod 97 we can now compute

$$\left(\frac{75}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5}{97}\right)\left(\frac{5}{97}\right) = \left(\frac{3}{97}\right).$$

It is if and only if 3 is. This time we are lucky because we see that $10^2 \equiv_{97} 3$. But if we are not lucky, how do we decide if 3 is a QR?

Problems from the Text

Chapter 20: 2(a-c), 3

21 When -1 and 2 are QR mod p

We saw that 75 is a QR mod 97 if and only if 3 is, but is 3 a QR? We need a couple more 'rules' about QRs.

Lemma 21.1. *For an odd prime p we have*

$$\left(\frac{a}{p}\right) \equiv_p a^{(p-1)/2}.$$

Proof. We have to show that $a^{(p-1)/2}$ is 1 if a is a QR, and is -1 otherwise. This first statement should be trivial by Euler's theorem (Why?). So let's assume that a is an NR as show that this power is -1. Its square is 1 by Euler's theorem, and the only square roots of 1 are 1 and -1, so it is enough to show that it isn't 1, ie, that a is not a solution to

$$x^{(p-1)/2} \equiv_p 1.$$

Well, this degree $(p-1)/2$ equation mod p has at most $(p-1)/2$ solution mod p by Theorem 8.1 of the text, and those solutions are the QR mod p. So the NR a is not a solution. □

Okay. Powering is easy with a computer. So we can decide if a is a QR mod a prime p. But you still don't want to compute

$$75^{48} \mod 97$$

by hand on a test. With a bit more work, we can get to doing this by hand.

Applying the lemma when $a = -1$ we get the following.

Theorem 21.2 (Quadratic Reciprocity 1)**.** *For odd prime p,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1 \\ -1 & \text{if } p \equiv_4 3 \end{cases}.$$

Recall in Chapter 12 that we showed there are infinitely many primes p with $p \equiv_4 3$. We did not proof the same for primes p with $p \equiv_4 1$. We do this now.

Theorem 21.3. *There are infinitely many primes p with $p \equiv_4 1$.*

Proof. Assume there are finitely many such primes $p_1, \ldots, p_n$, and consider the number $A = (2p_1p_2 \ldots p_n)^2 + 1$. None of $1, p_1, \ldots, p_n$ divide A, and it cannot be prime or we have our contradiction, so it must factor into primes $q_1, \ldots, q_m$ such that $q_i \equiv_4 3$ for all i. But q_1 is odd, and $q_1 | A = (2p_1p_2 \ldots p_n)^2 + 1$, so $x = 2p_1p_2 \ldots p_n$ is a solution to

$$x^2 \equiv_{q_1} -1,$$

meaning that -1 is a QR mod q_1. So by Quadratic Reciprocity $q_i \equiv_4 1$. □

For the next proof, we look at another way of writing the numbers modulo p. Usually we write them as

$$[0, p-1] = \{0, 1, 2, \ldots, p-1\}.$$

This is natural, who doesn't love a positive number? But where $s = (p-1)/2$ we can also write them as

$$[-s, s] = \{-s, -(s-1), \ldots, -1, 0, 1, \ldots, s-1, s\}.$$

We will call this the *symmetric representation* of the integers modulo p.

Applying Lemma 21.1 with $a = 2$, we get the following.

Theorem 21.4 (Quadratic Reciprocity 2)**.** *For odd prime p,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 1 \text{ or } 7 \\ -1 & \text{if } p \equiv_8 3 \text{ or } 5 \end{cases}.$$

Proof. We have that $\left(\frac{2}{p}\right) \equiv_p 2^{(p-1)/2}$ so we compute $2^{(p-1)/2}$.

Consider the following two ways of writing the product S of the even residue's modulo p:

$$S = 2 \cdot 4 \cdot 6 \cdot \cdots \cdot 2s = 2^s(s!)$$

where $s = (p-1)/2$.

We now write this product again using the symmetric representation of the integers modulo p. If s is even we get

$$S = 2 \cdot 4 \cdot \cdots \cdot s \cdot -(s-1) \cdot \cdots \cdot -(3) \cdot -(1) = (-1)^{s/2}(s!).$$

This gives that $2^s = (-1)^{s/2}$, which yields the result for $p \equiv_8 1, 5$ as $s/2$ is even in the first case and odd in the second. Now if s is odd, we get

$$S = 2 \cdot 4 \cdot \ldots (s-1) \cdot (-s) \cdot \cdots \cdot (-3) \cdot (-1) = (-1)^{(s+1)/2}(s!).$$

This gives $2^s = (-1)^{(s+1)/2}$ which yields the result for $p \equiv_8 3, 7$. □

Problems from the Text

Chapter 21: This chapter isn't in the book. Do the following.

1) Show that if a is a QR mod p, then $a^{p-1/2} \equiv_p 1$.
2) Compute the Legendre symbols $\left(\frac{2^3}{29}\right)$ and $\left(\frac{2^3}{7}\right)$.

22 Quadratic Reciprocity

We've seen how to quickly decide if -1 or 2 are QRs modulo a prime p. With one more identity, we can deal with any number a.

Theorem 22.1 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. The following hold.*

i). $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1 \\ -1 & \text{if } p \equiv_4 3 \end{cases}$

ii). $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 1 \text{ or } 7 \\ -1 & \text{if } p \equiv_8 3 \text{ or } 5 \end{cases}$

iii). $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv_4 1 \text{ or } q \equiv_4 = 1 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv_4 3 \text{ and } q \equiv_4 3 \end{cases}$

Before we prove this, in the next chapter, let's see how to use it.

Example 22.2. We see that 70 is an NR modulo 13:

$$\begin{aligned} \left(\frac{70}{13}\right) &= \left(\frac{2}{13}\right)\left(\frac{5}{13}\right)\left(\frac{7}{13}\right) = (-1)\left(\frac{13}{5}\right)(-1)\left(\frac{13}{7}\right) \\ &= \left(\frac{3}{5}\right)\left(\frac{-1}{7}\right) = -\left(\frac{5}{3}\right)(-1) = \left(\frac{-1}{3}\right) - 1 \end{aligned}$$

Problem 22.1. Decide if 75 is a QR modulo 97. How about 14 modulo 137.

Good work. But perhaps you have noticed some shortcomings. We need primes on the bottom, so to use reciprocity, we have to be able to factor the top into primes. But we said that factoring is hard. Jacobi gives us a solution for this.

Definition 22.3. For odd integers a and b, where b has prime decomposition $b = p_1 p_2 \dots p_r$, the *Jacobi symbol* is

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right).$$

With this, Jacobi showed the following.

Theorem 22.4 (Generalised Quadratic Reciprocity)**.** *Let a and b be positive odd integers. The following hold.*

i). $\left(\frac{-1}{b}\right) = \begin{cases} 1 & \text{if } b \equiv_4 1 \\ -1 & \text{if } b \equiv_4 3 \end{cases}$

ii). $\left(\frac{2}{b}\right) = \begin{cases} 1 & \text{if } b \equiv_8 1 \text{ or } 7 \\ -1 & \text{if } b \equiv_8 3 \text{ or } 5 \end{cases}$

iii). $\left(\frac{a}{b}\right) = \begin{cases} \left(\frac{b}{a}\right) & \text{if } a \equiv_4 1 \text{ or } b \equiv_4 = 1 \\ -\left(\frac{b}{a}\right) & \text{if } a \equiv_4 3 \text{ and } b \equiv_4 3 \end{cases}$

Proof. We show the first part, the other parts are in the exercises. Let $b = p_1 p_2 \dots p_s q_1 q_2 \dots q_t$ where p_i are primes with $p_i \equiv_4 1$ and the q_i are primes with $q_i \equiv_4 3$. Then

$$\left(\frac{-1}{p}\right) = \prod \left(\frac{-1}{p_i}\right) \prod \left(\frac{-1}{q_i}\right) = -1^t = \begin{cases} 1 & \text{if } 2 \mid t \\ -1 & \text{if } 2 \nmid t \end{cases}$$

while

$$b \equiv_4 1^s \cdot 3^t \equiv_4 (-1)^t \equiv_4 \begin{cases} 1 & \text{if } 2 \mid t \\ 3 & \text{if } 2 \nmid t \end{cases} .$$

□

Now let's see how this lets us compute $\left(\frac{a}{p}\right)$ without factoring a. Well, we factor out factors of 2, but this is easy.

Example 22.5. We see that 66 is an NR modulo 113.

$$\begin{aligned} \left(\frac{66}{113}\right) &= \left(\frac{2}{113}\right)\left(\frac{33}{113}\right) = \left(\frac{113}{33}\right) = \left(\frac{14}{33}\right) = \left(\frac{2}{33}\right)\left(\frac{7}{33}\right) \\ &= \left(\frac{33}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1 \end{aligned}$$

Notice that we used reduced 113 modulo 33 to 14 to get $\left(\frac{113}{33}\right) = \left(\frac{14}{33}\right)$. We can do this if 33 is prime q because a is a QR mod q if and only if $a \mod q$ is a QR mod q. We can do this with Jacobi symbols too.

Where a and b are odd and $b = p_1 \cdots p_n$, let $\overline{a} = a \mod b$, and let $a_i = a \mod b_i$ for each i. We have that $\overline{a} \equiv_{b_i} a_i$ for each i, and so

$$\left(\frac{a}{b}\right) = \left(\frac{a}{b_1}\right) \cdots \left(\frac{a}{b_n}\right) = \left(\frac{a_1}{b_1}\right) \cdots \left(\frac{a_n}{b_n}\right) = \left(\frac{\overline{a}}{b_1}\right) \cdots \left(\frac{\overline{a}}{b_n}\right) = \left(\frac{\overline{a}}{b}\right).$$

which allows us to reduce odd a modulo b in the Jacobi symbol.

Problem 22.2. Is 3 a QR modulo 141?

Did you get that $\left(\frac{3}{141}\right) = -\left(\frac{141}{3}\right) = -\left(\frac{0}{3}\right)$? Oh yeah! I guess 141 isn't prime. Be careful about that. Even though the Jacobi symbols are defined for all odd numbers, they don't tell us anything when the bottom is not prime. In this case we were lucky. We got a 0. It told us something was funny. Try computing $\left(\frac{3}{119}\right)$. You will get 1, but q is not a quadratic residue modulo $119 = 7 \cdot 17$; it isn't prime, so the Jacobi symbol doesn't tell us anything.

Problems from the Text

Chapter 22: 1, 2, 3, 4, 6, 7

23 Proof of Quadratic reciprocity

Here we give a proof that of the third part of the Quadratic Reciprocity theorem. We show for for distinct odd primes p and q that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{st}$$

where $s = (p-1)/2$ and $t = (q-1)/2$. As s and t are even if and only if $p \equiv_4 1$ and $q \equiv_4 1$ respectively, this gives the result.

Gauss gave several proofs of this, but this one, based on one of Gauss's, is from a paper by G. Rousseau from 1989. It is the most basic proof I could find. Compare it to the proof in the book, which is a classic proof by Eisenstein, it is also nice, but I feel this one is easier. I won't test you on these proofs.

To prove this, we look at the set S of pairs (i, j) in symmetric representation, where i is a non-zero number mod p and j is a non-zero number mod q. So S is the grid $[-s, s] \times [-t, t]$ of integers points in $\mathbb{R}^2$ after we have removed all points on the axes.

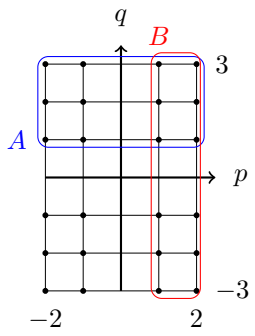


Figure 1: The pairs S in $[-s, s] \times [-t, t]$ for $p = 5, s = 2$ and $q = 7, t = 3$

Let A be all points in S in the first two quadrants of the plane– all points (i, j) such that $i > 0$; and let B be all points in quadrants 1 and 4– points (i, j) such that $j > 0$.

Every point in $(i, j) \in S$ has a negative point $-(i, j) = (-i, -j)$ also in S. Multiplying by -1 switches quadrants 1 and 3, and quadrants 2 and 4. So A

and B both contain one of (i,j) and $-(i,j)$ for each (i,j) in S, and we get from A to B by multiplying the st points in quadrant 2 by -1. Multiplying points componentwise as

$$(i,j)(i',j') = (ii' \mod p, jj' \mod q)$$

we thus get that

$$\Pi A = (-1)^{st} \cdot \Pi B \tag{2}$$

where ΠA and ΠB are the products of all points in A and B respectively.

Computing the first coordinate of ΠA over A and the second over B using (2) we get

$$\Pi A = ((p-1)!^t, (q-1)!^s(-1)^{st}).$$

Now by the CRT the set $\{(x \mod p, x \mod q) \mid 0 < x < pq \ \ \gcd(x,pq) = 1\}$ is exactly S, and as

$$-(x \mod p, x \mod q) = (-x \mod p, -x \mod q)$$

the set

$$C = \{(x \mod p, x \mod q) \mid 0 < x < (pq-1)/2, \ \gcd(x,pq) = 1\}$$

also contains exactly one of (i,j) and $-(i,j)$ for each (i,j) in S. So $\Pi C = \pm \Pi A$. To compute the first coordinate of ΠC we take the product of the values $x < (pq-1)/2$ that are prime to p, and then divide out those numbers that have a factor of q:

$$\frac{(\Pi_{i=1}^{p-1} i)(\Pi_{i=1}^{p-1} p+i)\ldots(\Pi_{i=1}^{p-1}(t-1)p+i)(\Pi_{i=1}^{s} tp+i)}{1 \cdot q \cdot \cdots \cdot sq}$$

The bottom becomes $q^s \cdot s!$ and reducing the top and bottom modulo p gives

$$\frac{(p-1)!^t s!}{q^s \cdot s!} = \frac{(p-1)!^t}{\left(\frac{q}{p}\right)} = (p-1)!^t \left(\frac{q}{p}\right).$$

Here we used Lemma 21.1 to get $q^s = q^{(p-1)/2} \equiv_p \left(\frac{q}{p}\right)$ on the bottom, and then observed that multiplying by ± 1 is the same as dividing by it. Doing the same for the second coordinate, and comparing with ΠA we get

$$((p-1)!^t, (q-1)!^s(-1)^{st}) = \Pi A = \pm \Pi C = \pm((p-1)!^t \left(\frac{q}{p}\right), (q-1)!^s \left(\frac{p}{q}\right)).$$

Whether $\pm$ is $+$ or $-$, it happens in both coordinates, so cancels, giving

$$(-1)^{st} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right).$$

Problems from the Text

Chapter 23: No problems

24 Which primes are sums of two squares

We look this section at which primes n can be written as

$$n = a^2 + b^2$$

and then in the next section use this to address the same question for general n.

As the only squares are 0 or 1 mod 4 the only such n are $0, 1$ or 2 mod 4. So primes $p \equiv_4 3$ are already eliminated. We know that $2 = 1^2 + 1^2$ so we consider only primes p with $p \equiv_4 1$.

Theorem 24.1. *Any prime p with $p \equiv_4 1$ can be written as the sum of two squares.*

The proof uses a technique called descent, the main steps of which are:

i). Find A, B and M such that

$$A^2 + B^2 = Mp.$$

ii). Use this to find $m < M$ and a and b such that

$$a^2 + b^2 = mp.$$

iii). Keep repeating until we reduce m to 1.

The first step is easy using our Quadratic Reciprocity Theorem.

Problem 24.1. For a prime p with $p \equiv_4 1$, show that we can write

$$A^2 + 1^2 = Mp$$

for some A and some M.

The second step is harder. It uses the following identity that you can (and should) show by simply expanding both sides.

$$(a^2 + b^2)(A^2 + B^2) = (aA + bB)^2 + (bA - aB)^2 \tag{3}$$

This gives us the following.

Fact 24.2. *If n and n' are both sums of two squares, then so is nn'.*

This fact seems like it will be more useful in the next section, but it is the key to descent. Say that

$$A^2 + B^2 = Mp.$$

If we can find m, a and b with $m < M$ such that

$$a^2 + b^2 = mM,$$

then we get from (3) that

$$(aA + bB)^2 + (bA - aB)^2 = mM^2p$$

and if we can divide through by M^2 we get

$$\left(\tfrac{aA+bB}{M}\right)^2 + \left(\tfrac{bA-aB}{M}\right)^2 = mp. \tag{4}$$

These seems like some big 'if's, but the secret is to look at $A^2 + B^2 = Mp$ modulo M. Modulo M it becomes

$$A^2 + B^2 \equiv_M 0$$

but reducing A and B to to a and b respectivley in $[-M/2, M/2]$ we get

$$a^2 + b^2 \equiv_M 0.$$

So $a^2 + b^2 = mM$ for some $m < M$ (this uses $1 < M$). As a and b are the images of A and B mod M we get

$$aA + bB \equiv_M A^2 + B^2 \equiv_M 0 \qquad \text{and} \qquad bA - aB \equiv_M AB - BA = 0$$

so M divides them both giving (4).

This gives the following.

Lemma 24.3. *Let n be a number such that*

$$A^2 + B^2 = Mn$$

for integers A and B and positive integer $M \geq 2$. Where a and b in $[-M/2, M/2]$ are A and B respecively modulo M, we have that

$$\left(\tfrac{aA+bB}{M}\right)^2 + \left(\tfrac{bA-aB}{M}\right)^2 = mn,$$

where the fractions are integers and $m < M$.

Problem 24.2. Use Lemma 24.3 and Problem 24.1 to prove Theorem 24.1

Example 24.4. We use descent to show that $p = 881$ can be written as a sum of squares.

First, we find A_0, B_0 and M_0 such that $A_0^2 + B_0^2 = M_0 \cdot p$. As $p \equiv_4 1$, we have by Quadratic Reciprocity that -1 is a QR mod p. As we did in the Miller Rabin test we write $881 - 1 = 2^4 \cdot 55$, and choosing some a compute powers modulo 881:

	i	0	1	2	3
$2^{55 \cdot 2^i}$	mod 881	1			
$3^{55 \cdot 2^i}$	mod 881	767	662	387	-1

As $a = 2$ didn't help, we tried $a = 3$ and found that $387^2 \equiv_{881} -1$. This lets us start with $A_0 = 387$ and $B_0 = 1$:

$$387^2 + 1^2 = 170 \cdot 881.$$

Reducing A_0 and B_0 modulo 170 we get $a_0 = 47$ and $b_0 = 1$. Dividing by 170 we get

$$M_1 = ((47)^2 + 1^2)/170 = 13$$

and so $47^2 + 1^2 = 13(170)$. So by the lemma, we get

$$107^2 + 2^2 = \left(\tfrac{(47)(387)+(1)(1)}{170}\right)^2 + \left(\tfrac{(1)387-47(1)}{170}\right)^2 = 13 \cdot 881.$$

Repeating, we reduce $A_1 = 107$ and $B_1 = 2$ modulo 13 to get $a_1 = 3$ and $b_1 = 2$, and find

$$M_2 = (3^2 + 2^2)/13 = 1,$$

so

$$25^2 + 16^2 = \left(\tfrac{(3)(107)+(2)(2)}{13}\right)^2 + \left(\tfrac{(2)107-3(2)}{13}\right)^2 = 881.$$

Problems from the Text

Chapter 24: 1, 2, 3, 5

25 What numbers are the sum of two squares

What numbers n can be written as the sum of two squares? Any number n can be written uniquely as

$$n = p_1 p_2 \dots p_r N^2$$

where the p_i are distinct primes, and N^2 is some square.

We have seen that if two numbers can be written as a sum of squares, then so can their product, so we know that if all of the p_i are either 2 or 1 modulo 4, then n is a sum of two squares.

On the other hand, if any one of the p_i is 3 modulo 4, then n is not a sum of two squares. Indeed if

$$a = p_1 p_2 \dots p_r N^2$$

where $p_1 \equiv_4 3$ then applying descent with $n = p_1$ and $M = a/p_1$ and get a representation of p_1 as a sum of squares, but we know that this is impossible.

Notice further that if $n = a^2 + b^2$ where d divides a and b, then d^2 divides n, so the N above is divisible by d.

So the following is also a corollary of Lemma 24.3.

Theorem 25.1. *A number n can be written as $n = a^2 + b^2$ if and only if*

$$n = p_1 p_2 \dots p_r N^2$$

where the p_i are distinct primes with $p_i = 2$ or $p_i \equiv_4 1$ for all i. Further, if $\gcd(a, b) = 1$ then $N = 1$.

That is the if, what is the how.

Example 25.2. Write 90 as a sum of squares. Factoring it as $90 = 2 \cdot 3^2 \cdot 5$, and writing each square-free factor as a sum of squares

$$2 = 1^2 + 1^2 \qquad \text{and} \qquad 5 = 1^2 + 2^2$$

(we would use descent if the numbers were much bigger) we get (using the formula

$$(a^2 + b^2) + (A^2 + B^2) = (aA + bB)^2 + (bA - aB)^2)$$

that

$$10 = (1 \cdot 1 + 1 \cdot 2)^2 + (1 \cdot 1 - 1 \cdot 2)^2 = 3^2 + (-1)^2 = 1^2 + 3^2.$$

Then using the non-square free bit, we get that

$$90 = (1 \cdot 3)^2 + (3 \cdot 3)^2 = 3^2 + 9^2.$$

Back to Pythagorean Triples

In our Theorem about which n can be written as a sum of squares, we were allowing N^2 to be written as

$$N^2 = N^2 + 0^2.$$

This seems like cheating. So which squares can be written as the sum of two non-zero squares. We already considered this problem, this is a Pythagorean Triple.

We saw that the triples (a, b, c) for which

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

and for which $\gcd(a, b) = 1$ are exactly the triples

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad c = \frac{s^2 + t^2}{2}$$

for relatively prime odd integers $s > t \geq 1$.

For such a triple, we have that $2c = s^2 + t^2$ and so c is a product of distinct primes $p \equiv_4 1$.

Theorem 25.3. *A number c is the hypotenuse of a PPT (a, b, c) if and only if it is the product of distinct primes $p_i \equiv_4 1$.*

Problems from the Text

Chapter 25: 1, 2, 5

27 Euler's Phi Function and Sums of Divisors

Recall the Euler Phi function $\phi(n)$ which counts the elements modulo n that are relatively prime to n. We prove a neat identity involving the ϕ function.

It arises as follows. Let $F(n) = \sum_{d|n} \phi(n)$ be the sum of $\phi(d)$ over all factors d of n. For $n = 15$ we get:

$$F(15) = \phi(1) + \phi(3) + \phi(5) + \phi(15) = 1 + 2 + 4 + 8 = 15$$

Theorem 27.1. *For all integers $n \geq 1$ we have $F(n) = n$.*

Proof. The identity clearly holds for all primes p. Indeed one gets that

$$F(p^d) - F(p^{d-1}) = \phi(p^d) = p^d - p^{d-1}$$

and so it holds for powers of primes by induction.

Too quick? Our proof that $F(p^d) = p^d$ is by induction on d. For $d = 1$ it is true as

$$F(p) = \phi(p) + \phi(1) = (p - 1) + 1 = p.$$

Assuming now that $d > 1$ and that $F(p^{d-1}) = p^{d-1}$ we get

$$F(p^d) = \phi(p^d) + F(p^{d-1}) = (p^d - p^{d-1}) + p^{d-1} = p^d.$$

That $F(p^d) = p^d$ thus holds by induction.

To prove the theorem it is now enough to show that $F(AB) = F(A)F(B)$ when A and B are relatively prime. Well, observe that the set of numbers dividing AB is

$$\{ab: \qquad a \mid A \qquad \text{and} \qquad b \mid B \}.$$

So

$$\begin{aligned} F(AB) &= \sum_{a|A\,,\,b|B} \phi(ab) = \sum_{a|A} \sum_{b|B} \phi(ab) \\ &= \sum_{a|A} \sum_{b|B} \phi(a)\phi(b) = \sum_{a|A} \phi(a) \sum_{b|B} \phi(b) = F(A)F(B) \end{aligned}$$

□

Problems from the Text

Chapter 27: 1, 2, 3

28 Powers modulo p and primitive roots

The *order* $e_p(a)$ *modulo* p of a number a is the minimum $d \geq 1$ such that

$$a^d \equiv_p 1.$$

By Fermat's Little Theorem we know that the order of a modulo p is at most p for every $a \not\equiv_p 0$. If there are elements a of order $p-1$, then for any d dividing $p-1$ there are elements such as a^d with order $(p-1)/d$.

Must the $e_p(a)$ always divide $p-1$? Are there always elements a with $e_p(a) = p-1$?

Theorem 28.1 (Order Divisibility Property)**.** *Let a be an integer not divisible by the prime p. If $a^n \equiv_p 1$ then $e_p(a)$ divides n. In particular, the order of any element modulo p divides $p-1$.*

Proof. Let $a^n \equiv_p 1$ and let $d = e_p(a)$. As $d < n$ we can divide n by d and get $n = cd + q$ for some q with $0 \leq q < d$. But then

$$1 \equiv_p a^n = a^{cd+q} \equiv_p a^q.$$

So $q = 0$ or we contradict the fact $d = e_p(a)$. □

An element g such that $e_p(g) = p-1$ is called a *primitive root* modulo p; it is also often called a primitive element, or a generator.

Problem 28.1. Show that an element g mod p is a primitive root if and only if

$$\{g, g^2, \ldots, g^{p-1}\} \equiv_p \{1, 2, \ldots, p-1\}.$$

Problem 28.2. Show that if g is a primitive root modulo p, then g^d is a primitive root modulo p if and only if $\gcd(d, p-1) = 1$. Conclude that if there is a primitive root modulo p, then there are $\phi(p-1)$ of them.

Theorem 28.2. *For every prime p there are $\phi(p-1)$ primitive roots mod p.*

If you have taken algebra, you can get this easily from the fact that the multiplicative group of any field is cyclic. But we haven't taken algebra.

Proof. We know that the order d of any element modulo p divides $p-1$.

Claim 28.3. *For any d dividing $p-1$ there are exactly d elements mod p with order dividing d.*

Proof. Elements of order d are roots of $x^d - 1 \bmod p$ so there are at most d distinct ones. As

$$(x^{p-1} - 1) = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1).$$

and the roots of $x^{p-1} - 1$ are distinct, the roots of $x^d - 1$ are also distinct, so there are exactly d of them. ◇

For every divisor d of $p-1$ let $\psi(d)$ be the number of elements of order d. Our goal is to show that $\psi(p-1) = \phi(p-1)$. We do so by showing, by induction on the number of divisors of d that $\psi(d) = \phi(d)$ for all d dividing $p-1$.

If d dividing $p-1$ is prime, all elements of order dividing d are of order 1 or d, and only one is of order 1, so $\psi(d) = d - 1 = \phi(d)$.

Assume now that d dividing $p-1$ is not prime. By the claim we have

$$d = \sum_{d'|d} \psi(d')$$

and by induction that $\psi(d') = \phi(d')$ except when $d' = d$ so

$$d = \sum_{d'|d} \phi(d') - \phi(d) + \psi(d) = d - \phi(d) + \psi(d)$$

where we use Theorem 27.1 in the second equality. Thus $\phi(d) = \psi(d)$, as needed. □

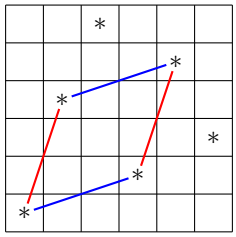
Although we know how many primitive roots there are modulo p, so we tend to be able to find one quickly, and if we find one primitive root a then a^r is another for any r with $\gcd(r, p-1) = 1$. (This immediatly shows that there are $\phi(p-1)$ primitive roots if there is one, but the proof we gave is basically the proof we would use to show there is one.) But there is no predicting which elements mod p will be primitive roots.

Conjecture 28.4 (Artin)**.** *For any non-square $a \neq -1$ there aer infnitely many primes p such that a is primitive modulo p.*

There are no non-square $a \neq -1$ for which this is known to hold or not hold. However, it is known to hold for at least one of $2, 3$ and 5, and to not hold for at most two different a.

Costas Arrays

Can you put n dots in the n^2 squares of an $n \times n$ grid so that there is exactly one dot in each row and column? Of course you can. But how about without any four dots that make a parallelogram:



A placement of dots on the $n \times n$ grid is easy to describe as an n-tuple

$$(a_1, a_2, \ldots, a_n)$$

of distinct numbers in $[n]$. It is a *Costas Array* if there is no d with $1 \geq |d| < n$ and distinct $1 \leq i < j \leq j$ such that

$$a_{i+d} - a_i = a_{j+d} - a_j.$$

Notice that this has no parallelograms, but is a slighly stronger condition, it also omits three dots in a line, which we can view as a kind of squished parallelogram.

The following is due to Welch.

Theorem 28.5. *Where g is a primitive element modulo p, the tuple*

$$(g^1, g^2, \ldots, g^{p-1})$$

where g^i is computed mod p, is a Costas Array.

Proof. If $g^{i+d} - g^i \equiv_p g^{j+d} - g^j$ then we have that

$$g^i(g^d - 1) \equiv_p g^j(g^d - 1).$$

As $|d| < p - 1$, and so $g^d - 1 \neq 0$ is invertible, we get $g^i \equiv_p g^j$. This implies that $i = j$ as g is primitive. □

Notice that this is even stronger than we were asking for. Here there are no parallelograms 'modulo p'.

Problems from the Text

Chapter 28: 1, 2, 3, 4, 5, 7, 16, 17

29 Primitive Roots and Indices

We have seen that for prime p there is always a primitive root– an element g such that

$$\{g^1, g^2, \ldots, g^{p-1}\} \equiv_p \{1, 2, \ldots, p-1\}.$$

These are the same as sets, but there order is all mixed up. Indeed for prime $p = 13$ the element 2 is a generator. We compute mod 13:

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
2	4	8	3	6	12	11	9	5	10	7	1

Given a primitive root g mod an prime p, the index $I(a)$ of a number a mod p is the value such that

$$g^{I(a)} =_m a.$$

So, for example, with primitive root 2 modulo p, the index $I(7) = 11$ as $2^{11} \equiv_{13} 7$. Reversing the above table, we get the index table for the generator 2 mod 13.

a	1	2	3	4	5	6	7	8	9	10	11	12
$I(a)$	12	1	4	2	9	5	11	3	8	10	7	6

A table like this is not as useful as it was before computers, but it is still useful on math tests. It allows me to ask you to multiply big numbers mod p:

Example 29.1. $8 \cdot 4 \equiv_{13} 2^3 \cdot 2^2 = 2^5 \equiv 6$

This $I(a)$ is just the logarithm of a in the base g right? In a cryptography class, $I(a)$ is often called the *discrete log* of a to the base g mod p. It satisfies those conditions you would expect of a logarigthm.

- $I(ab) \equiv_{p-1} I(a) + I(b)$
- $I(a^k) \equiv_{p-1} kI(a)$

Why am I writing '$\equiv_{p-1}$'? This is because we are using Euler: $2^{p-1} \equiv_p 1$.

Example 29.2. $7 \cdot 12 \equiv_{13} 2^{11} + 2^6 \equiv_{13} 2^{17} \equiv_{13} 2^5 \equiv_{13} 9$

Let's take a slightly bigger modulus to get into some meatier examples.

Here is the index table modulo $p = 31$ for the primitive root $g = 3$.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$I(a)$	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21
a	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$I(a)$	6	7	26	4	8	29	17	27	13	10	5	3	16	9	15

Example 29.3. Solve the congruence $17x \equiv_{31} 9$. Usually we have to invert 17 modulo 31, but as we have the indices, we write the congruence in our base g as

$$3^{I(17)}3^{I(x)} \equiv_{31} 3^{I(9)} \qquad \text{or} \qquad I(17) + I(x) \equiv_{30} I(9).$$

The second form is easy to solve:

$$I(x) \equiv_{30} I(9) - I(17) = 2 - 7 \equiv_{30} 25$$

So $x = 6$ as $I(6) = 25$.

Example 29.4. Solve the congruence $5x^{35} \equiv_{31} 26$. We convert this to an index equation $20 + 35I(x) \equiv_{30} 5$, which become $5I(x) \equiv_{30} -15$. This has a solution as -15 is a multiple of $\gcd(30, 5) = 5$, so has not only the solution $-3 \equiv_{30} 27$, but has 5 solutions: $I(x) = 3, 9, 15, 21, 27$. Thus $x = 27, 29, 30, 15, 23$.

Problems from the Text

Chapter 29: 1a, 3, 4

30 The equation $x^4 + y^4 = z^4$

Fermat's Last Theorem, proved by Wiles, tells us that the equation

$$x^n + y^n = z^n$$

has no positive integer solutions for $n \geq 4$.

For $n = 4$ we show the following stronger statement.

Theorem 30.1. *The equation $x^4 + y^4 = z^2$ has no positive integer solutions.*

Proof. Again we use descent. We assume, towards contradiction, that there is a solution. Let $x^4 + y^4 = z^2$ be one that minimizes z. We will find one with smaller z, contradicting our choice of solution.

There are two main steps.

i). We find u and v such that $x^2 + 4v^2 = u^4$ for $u < z$, then use this to

ii). find X and Y such that $X^4 + Y^4 = u^2$.

Clearly x, y and z do not share a common factor, or we can factor it out and get a solution with a smaller z. Now, letting $a = x^2$ and $b = y^2$, we have a PPT $a^2 + b^2 = z^2$ and so there are odd integers $s > t$ such that

$$x^2 = a = st \qquad \text{and} \qquad y^2 = b = \frac{s^2 - t^2}{2} \qquad \text{and} \qquad z = c = \frac{s^2 + t^2}{2}.$$

As st is an odd square, we have $st \equiv_4 1$, so s and t are both 1 mod 4 or both 3 mod 4:

$$s \equiv_4 t.$$

Claim 30.2. *We can write $s+t = 2u^2$ and $s-t = 4v^2$ for some u and v such that u and $2v$ are relatively prime.*

Proof. Any number dividing $(s-t)$ and $(s+t)$ divides $2s$ and $2t$, so $\gcd(s-t, s+t) = 1$ or 2. As s and t are both odd, it is 2. Further, we know that $(s-t)(s+t) = s^2 - t^2 = 2y^2$ is twice a square. Now 4 divides $s-t$, so it cannot divide $s+t$, so $s+t$ is $2b$ for some b. As $y^2 = (s-t)b$ and $(s-t)$ and b are relatively prime, we have that both $(s-t)$ and b are squares. So $s+t = 2u^2$ for some u, and $s-t = 4v^2$ for some v. ◇

We can write this as

$$s = u^2 + v^2 \qquad \text{and} \qquad t = u^2 - 2v^2,$$

so $x^2 = st = u^4 - 4v^4$ which gives us the required

$$x^2 + 4v^4 = u^4.$$

Also $2z = s^2 + t^2 = 2(u^4 + 4v^2)$ so $u < z$.

Now, this is a PPT $(x, 2v^2, u^2)$ so

$$x = ST \qquad \text{and} \qquad 2v^2 = \frac{S^2 - T^2}{2} \qquad \text{and} \qquad u^2 = \frac{S^2 + T^2}{2}$$

for odd relatively prime $S > T$.

As we argued for s and t we can argue that $\gcd(S-T, S+T) = 2$, and $(S-T)(S+T) = 4v^2$ is a square, so we can write

$$S + T = 2X^2 \qquad \text{and} \qquad S - T = 2Y^2.$$

Solving gives

$$S^2 = X^2 + Y^2 \qquad \text{and} \qquad T = X^2 - Y^2$$

and so

$$u^2 = \frac{S^2 + T^2}{2} = X^4 + Y^4.$$

This is our smaller solution, as required for the contradiction.

□

Problems from the Text

Chapter 30: Nothing here.

31 Square-Triangular Numbers

Recall that all the triangular numbers were of the form $m(m+1)/2$ so a square triangular number is a number n^2 where

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

for some m. We look for solutions (m, n) to this equation. Our first two square-triangular numbers 1 and 36 come from the solutions $(m, n) = (1, 1)$ and $(8, 6)$.

We observed in an exercise that for a solution (m, n) to this equation, we get, by multiplying both sides by 8 the equation

$$8n^2 = 4m^2 + 4m = (2m+1)^2 - 1$$

and so $(x, y) = (2m+1, 2n)$ is solution to the equation

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

We get a solution $(x, y) = (3, 2)$ to this for our solution $(m, n) = (1, 1)$.

So lets solve $x^2 - 2y^2 = 1$. This is called a Pell equation, these are covered in the next section. We won't get there, but we show how to find infinitely many solutions (x, y) to this this one. As long as x is odd and y is even, $(m, n) = ((x-1)/2, y/2)$ gives us a square-triangle number n^2.

If $x^2 - 2y^2 = 1$, then

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

So we are trying to find x and y satisfying this. Well from one, we get many. Using our solution $(x, y) = (3, 2)$, we have

$$1 = (3 + 2\sqrt{2})(3 - 2\sqrt{2}). \tag{5}$$

Squaring this, we get

$$1^2 = 1 = (3 + \sqrt{22})^2(3 - \sqrt{22})^2 = (17 + 12\sqrt{2})(17 - 12\sqrt{2}).$$

The solution $(x, y) = (17, 12)$ gives $(m, n) = (9, 6)$ for the square-triangular number 36.

But taking (5) to any power works. For example, taking it to the fifth power gives

$$1^5 = 1 = (3 + \sqrt{22})^5(3 - \sqrt{22})^5 = (3363 + 2278\sqrt{2})(3363 - 2278\sqrt{2}),$$

and we get $(m, n) = (1681, 1189)$ so 1189^2 is another square-triangle number.

Using another descent argument, we can show that the only integer solutions to $x^2 - 2y^2 = 1$ are (x_k, y_k) where

$$(3 + 2\sqrt{2})^k = x_k + y_k\sqrt{2}.$$

I'll let you look at that on your own.

Problems from the Text

Chapter 31: Nothing here.