Number Theory in Problem Solving

Konrad Pilch

April 7, 2016

1 Divisibility

Number Theory concerns itself mostly with the study of the natural numbers ($\mathbb{N}$) and the integers ($\mathbb{Z}$). As a consequence, it deals a lot with prime numbers and sometimes with rational numbers ($\mathbb{Q}$). Recall:

Definition. The natural numbers are the numbers $\mathbb{N} = \{1, 2, 3, \dots\}$. The integers are the numbers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. The rational numbers are $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$.

There is significant debate about whether the naturals include 0 or not. It's probably easier to consider the naturals to be just the positive integers. If you want to specify the non-negative integers you may write $\mathbb{N}_0$ or $\mathbb{Z}_{\geq 0}$.

Notation. If an integer a divides an integer b we write $a|b$.

Definition. A prime number is a positive integer $p \neq 1$ such that if p divides ab then p divides a or p divides b. Mathematically, we write this as

$$p|ab \implies p|a \text{ or } p|b$$

Remark. Note, when you get to university and learn about more advanced number theory, negatives of primes will also be included as primes, but we do not worry about that here. Also, note, that this is a different definition than you may have expected! What about the definition that says "p only has two factors: 1 and p"? That is the definition for a number that is *irreducible*. As you can imagine, this ends up being the same thing as prime numbers when you work with integers. Feel free to use that definition, if it suits you better.

Take a step back for a moment and think about the definition of a prime number that I used. Can we include rational numbers? Are there any rational primes? The answer to both questions is an emphatic *no*. The answer at first may be a bit disappointing and baffling, but it all follows from the fact that only certain groups of numbers have a concept of divisibility. We have divisibility in the integers, because of an amazing result called the Fundamental Theorem of Arithmetic.

1.1 Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic allows us to factorise integers. There are other systems of numbers and objects that have this property, but you only learn about them at university. For positive integers, the statement is:

Fundamental Theorem of Arithmetic. *Every positive integer $n \neq 1$ can be written uniquely as a product of powers of primes. Mathematically,*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where the p_i are primes and $\alpha_i \in \mathbb{N}$.

So, how does this give us divisibility? Well, if a integer m can be written as a product of the same primes with the same or smaller powers, then it is called a factor of n and we write $m|n$.
As an example, the integer $20 = 2^2 \times 5$, where the power on the five is a one of course. Then any of the following are factors:

$$1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 5, \quad 2 \times 5 = 10, \quad 2^2 \times 5 = 20.$$

In fact these six positive integers are all the positive factors of 20 as you can easily check for yourself.

Remark. Our discussion, is not complete if we do not mention negative integers. If 4 is a factor of 20, then -4 is a factor of 20 too. The minus does not change whether a number is a factor or not. Moreover, 1 and -1 divide every integer. 0 does not divide any integer, but every non-zero integer divides 0.

1.2 Euclidean Algorithm

One concept you may already be familiar with is the greatest common divisor.

Definition. The *greatest common divisor* of two integers a and b, denoted as $\gcd(a, b)$ (or sometimes just (a, b)), is the largest factor of a that is also a factor of b.

There is a method that allows you to calculate the gcd of two integers very quickly if you do not know their prime factorisation. It is called the *Euclidean Algorithm* and it works as follows:

Euclidean Algorithm. Take two integers: let's say 45 and 159. Take the larger and calculate how many multiples of the smaller fit into it and write the remainder as follows:

$$159 = 3 \times 45 + 24.$$

Now, repeat the same with the last two integers (the smaller integer and remainder).

$$45 = 1 \times 24 + 21$$

Continue until you get a zero as the remainder.

$$\begin{aligned} 24 &= 1 \times 21 + 3 \\ 21 &= 7 \times 3 + 0 \end{aligned}$$

The last remainder above the zero is the gcd! So, $\gcd(45, 159) = 3$.

Corollary 1.1. *The gcd of two integers can be written as a linear combination of the two integers.*

This corollary is really important. You may never use the Euclidean algorithm unless you are coding an algorithm on a computer. However, what it does for us, mathematicians, is it tells us that the gcd can actually be written in terms of the original two integers. I shall do this using the result of the algorithm above.

$$\begin{aligned} \gcd(45, 159) = 3 &= 24 - 1 \times 21 \\ &= 24 - 1 \times (45 - 1 \times 24) \\ &= 2 \times 24 - 1 \times 45 \\ &= 2 \times (159 - 3 \times 45) - 1 \times 45 \\ &= 2 \times 159 - 7 \times 45 \end{aligned}$$

Each of the above lines comes from rearranging one of the lines in the Euclidean algorithm.

Definition. Two integers a and b are *relatively prime* (or *coprime*) if their gcd is 1.

Corollary 1.2. *For any two integers a and b whose gcd is 1, there exist integers s and t such that $as + bt = 1$.*

1.3 Properties of Divisibility

There are two types of divisibility properties that are interesting. The first is divisibility by certain numbers such as 2, 3, 4, 5, 9 and others. I include some of these here:

Theorem 1.3. *A number is divisible by 2 if its last digit is divisible by 2.*
A number is divisible by 3 if the sum of its digits is divisible by 3.
A number is divisible by 4 if its last two digits as a number are divisible by 4.
A number is divisible by 5 if its last digit is 0 or 5.
A number is divisible by 9 if the sum of its digits is divisible by 9.

There are many others, that you should feel free to come up with yourselves.
I now give you some rules about what you can do with divisibility between general numbers.

Theorem 1.4. *1. If $a|b$ and $a|c$, then*

- $a|b + c$
- $a|b - c$
- $a|kb$ *where k is any integer.*

2. *If $d|f$ and $e|f$, then*
   - $\text{lcm}(d,e)|f$ *where lcm is the least common multiple.*
3. *If $g|h$ and $i|j$, then*
   - $gi|hj$.
4. *And recall from the definition, if p is prime and $p|kl$, then*
   - $p|k$ *or* $p|l$.

This is incredible powerful and this can be seen in the following problem.

Problem 1. For what integer n is $\frac{2n-1}{n+7}$ an integer?

Proof. If $\frac{2n-1}{n+7}$ is an integer, then

$$n+7|2n-1.$$

Using Theorem 1.4, we have that

$$n+7|2(n+7).$$

Employing the same theorem again, this time with subtraction we have

$$n+7|2(n+7)-(2n-1)$$

which after simplifying means

$$n+7|15.$$

All the factors of 15 are $-15,-5,-3,-1,1,3,5,15$ and these are all the values that $n+7$ can take, so the solutions are:

$$n=-22,-12,-10,-8,-6,-4,-2,8.$$

□

Notice, that negative solutions are of course allowed if the question does not specify otherwise!

1.4 Factors and Sigma and Tau

Divisibility allows us to talk about factors. We shall for the moment limit our discussion to the positive integer factors of positive integers. We already know what they look like, but we would like to know a few more things. For example, how many are there? What is their sum?

Definition. For any positive integer n, denote by $\tau(n)$, the number of factors of n. Also, denote by $\sigma(n)$ the sum of the factors of n.

The really amazing thing is that we have formulas for these.

Theorem 1.5. *Let the prime factorisation of n be*

$$n=\prod_{i=1}^{k}p_i^{\alpha_i}=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

then

- $\tau(n)=\prod_{i=1}^{k}(\alpha_i+1)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$, *and*
- $\sigma(n)=\prod_{i=1}^{k}\left(1+p_i+\cdots+p_i^{\alpha_i}\right)=\left(1+p_1+\cdots+p_1^{\alpha_1}\right)\cdots\left(1+p_k+\cdots+p_k^{\alpha_k}\right)$

1.5 Introduction to Diophantine Equations

A huge chunk of number theory problems are Diophantine equations (named after an Ancient Greek mathematician Diophantus).

Definition. *Diophantine equations* are polynomial equations in one or more variables where the only desired solutions are integers.

The polynomial part essentially means you only have powers of variables with addition, subtraction and multiplication. I provide two simple examples.

Problem 2. Solve $2x + 5y = 1$ in integers.

Proof. Note that there are solutions to this since $(2, 5) = 1$. In fact, notice that rearranging yields

$$2x = 1 - 5y$$

In order for the right hand side to be even like the left hand side, it is clear that y must be odd. So, set $y = 2t + 1$. Substituting yields

$$2x = 1 - 5(2t + 1) = -4 - 10t$$

And so, $x = -2 - 5t$. In fact, $(x, y) = (-5t - 2, 2t + 1)$ is the set of all solutions. Yes, it is true there are an infinite number of solutions for all possible integer values of t! □

Another example of a Diophantine equation is Fermat's Last Theorem.

Problem 3. Find all solutions in positive integers of the equation

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

where $n > 1$.

Proof. This went unsolved for over 300 years and the person who solved it, Andrew Wiles, used really powerful mathematics to solve it. There are integer solutions only when $n = 2$ and then $(x, y, z) = (k(a^2 - b^2), 2kab, k(a^2 + b^2))$ for $a, b, k \in \mathbb{N}$. You shall prove the $n = 2$ case in section 4. □

Problems

1.6 Easy

1. Use the definition of prime at the beginning of the section to show that 4 and 6 are not prime. Why is any number that has more than two positive factors not prime?

2. Do there exist integers a and b such that $a + b = 544$ and whose greatest common divisor is 11?

3. Find a rule for divisibility by 8 and 16.

4. Find a rule for divisibility by 11.

5. Show that $3k + 4$ and $4k + 5$ never have a common factor greater than 1.

6. Find the number of zeros at the end of 1000!

7. Find all primes p such that $17p + 1$ is a square.

8. Find all positive integer solutions to
$$x^2 - xy + y^2 = 13.$$

9. Confirm that the formula given for $\sigma(n)$ is correct simply by expanding out the brackets. [Note: the formula is
$$\sigma(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} (1 + p_i + \cdots + p_i^{\alpha_i})]$$

10. Show that $\tau(n)$ is odd iff n is a square.

11. Show that $n! + 1$ and $(n + 1)! + 1$ are relatively prime for all naturals n.

1.7 Hard

1. Prove the formula $\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1)$ when $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

2. Let n be of the form $12k + 2$. Suppose that $6k + 1$ and $4k + 1$ are both prime. Prove that $\tau(n) = \tau(n + 1)$.

3. (Even Perfect Numbers) If n is even, then $\sigma(n) = 2n$ iff $n = 2^{k-1}(2^k - 1)$ with $2^k - 1$ prime.

4. Find the gcd of $2^{50} + 1$ and $2^{20} + 1$. Show further that $(2^m + 1, 2^n + 1) > 1$ if m and n are both odd.

5. Find a formula for the lcm of a and b in terms of a, b and $\gcd(a, b)$.

6. If a, b, m are integers such that $(a, b) = 1$ and $a|m$ and $b|m$, show that $ab|m$.

7. Find the smallest integer n for which
$$10x + 11y = n$$
has exactly 9 solutions in positive integers x, y.

8. Prove that if $n > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime.

2 Congruence

Modulo Arithmetic is a whole new world. It works almost exactly like normal equations, but you do not have to worry about things like size or infinity. Essentially, when working with *modulo* (or *mod* for short), you focus on the remainder upon division. So, if you want to see if something is divisible by 5, work in mod 5 and show that everything is zero!!

The best analogy for modulo arithmetic (to get prepared for the mathematical technicalities) is clock arithmetic: as soon as you hit 12 o'clock, it's like 0 o'clock and then you go to 1, then 2 and so on and the cycle repeats once you hit 12. There is a concept of 13 o'clock, but it's the same as 1 o'clock! That is how I want you to think around mods.

2.1 Modulo Arithmetic

First, the definition:

Definition. Given integers a, b,

$$a - b \text{ is a multiple of } n \iff a \equiv b \pmod{n}.$$

Can you see what is going on? $a \equiv b \pmod{n}$ when a and b leave the same remainder when divided by n.

Remark. Remember that 0 is considered to be multiple of everything, simply because $0 = n \times 0$.

The symbol $\equiv$ works just like $=$ does for the integers. You can perform (most) operations to both sides of an equation, and everything will simply work. This includes addition, subtraction and multiplication. Be careful about division. You cannot always divide (this will be explained a little further on). You can solve equations in exactly the same manner as you would for an ordinary equation.

Problem 4. Solve $(x-1)(x+2) \equiv (x-2)(x+7) \pmod{n}$ if n is odd.

Proof.

$$\begin{aligned}
& (x-1)(x+2) \equiv (x-2)(x+7) && \pmod{n}\\
\Rightarrow\quad & x^2 + x - 2 \equiv x^2 + 5x - 14 &&\\
\Rightarrow\quad & x - 5x \equiv -14 - (-2) && \text{(collect like terms)}\\
\Rightarrow\quad & -4x \equiv -12 &&\\
\Rightarrow\quad & 4x \equiv 12 && \text{(multiply both sides by } -1)\\
\Rightarrow\quad & x \equiv 3 && \text{(divide both sides by 4)}
\end{aligned}$$

□

As you can see, we can add, subtract, multiply, expand and factorise as freely as you wish. However, we could only divide by 4 because n was relatively prime to 4. In general if you want to divide both sides of a modulo equation, then you have to divide the mod too (but only if you can). For example:

$$\begin{aligned}
& 60x \equiv 480 && \pmod{70}\\
\Rightarrow\quad & 30x \equiv 240 && \pmod{35}\\
\Rightarrow\quad & 15x \equiv 120 && \pmod{35}\\
\Rightarrow\quad & 5x \equiv 40 && \pmod{35}\\
\Rightarrow\quad & x \equiv 8 && \pmod{7}\\
\Rightarrow\quad & x \equiv 1 && \pmod{7}
\end{aligned}$$

This is like the "*never divide by zero*" rule. So, even though we were working mod 70 originally, this reduced down to mod 7 simply because we were dividing by numbers that had factors in common with the mod. So, when we divided by 2 in the first line, the mod had to be divided by 2. But when we did that in the second line, the mod stayed as 35, since $(2, 35) = 1$. In line we divide by 3 and so again the mod stays as 35, but when dividing by 5, we have to reduce the mod too. The last line comes from the fact that $8 \equiv 1 \pmod{7}$. And so, the solution is all $x \equiv 1 \pmod{7}$, which are numbers like $\ldots, -13, -6, 1, 8, 15, \ldots$

- Be careful with indices:

$$a \equiv b \pmod{n} \text{ and } x \equiv y \pmod{n} \quad \not\Longrightarrow \quad x^a \equiv y^b \pmod{n}$$

  There are many counter examples, consider $2^5 = 32 \not\equiv 25 = 5^2 \pmod{3}$. If you want to fiddle with *large* indices in a modulo equation, then you should probably use Fermat's Little Theorem or Euler's Theorem (see later).

- Be careful when square rooting if n is composite:

$$a^2 \equiv b^2 \quad \not\Longrightarrow \quad a \equiv \pm b \pmod{n}$$

  There are many counter examples, like mod 8: we have $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$.

2.2 Modulo p

Prime numbers are way more interesting than composite numbers, In fact, the main reason why prime numbers are so popular is because everything works out nicely in $\pmod{p}$. Here are a few of these extra handy tricks: Remember that the following tools ONLY work if p is prime.

- Polynomial Roots Law:

$$abcd \equiv 0 \quad \Longleftrightarrow \quad a \equiv 0\,,\ b \equiv 0\,,\ c \equiv 0 \text{ or } d \equiv 0$$

  As an example, suppose $5x \equiv 0 \pmod{7}$, then since $5 \not\equiv 0 \pmod{7}$, it follows that $x \equiv 0 \pmod{7}$.

- The "normal" division Law:

$$ab \equiv ac \iff b \equiv c \ \text{(unless } a \equiv 0)$$

  As an example, suppose $2x \equiv 4 \pmod{7}$, then $x \equiv 2 \pmod{7}$.

- The Inverse Law: For any $x \not\equiv 0$, there exists an x^{-1} such that

$$x^{-1}x \equiv 1 \pmod{p}$$

  As an example, in mod 7, $1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 4^{-1} = 2, 5^{-1} = 3$ and $6^{-1} = 6$. Check these! [eg. $2 \times 4 = 8 \equiv 1$]

- Generators: There exists $g \not\equiv 0$ such that $\{1, g, g^2, g^3, \ldots, g^{p-2}\}$ is a rearrangement of $\{1, 2, 3, \ldots, p-1\}$ $\pmod{p}$.

  As an example, in mod 7, there are 2 generators: 3 and 5, because the set $\{1, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\}$ covers the entire set $\{1, 2, 3, 4, 5, 6\}$. The same occurs for 5.

- Quadratic Residue Law:

$$a^2 \equiv b^2 \iff a \equiv \pm b \pmod{p}$$

  As an example, suppose $x^2 \equiv 4 \pmod{7}$, then $x \equiv \pm 2 \pmod{7}$. Remember $-2 \equiv 5 \pmod{7}$.

2.3 Chinese Remainder Theorem

So $\pmod{p}$ is way more fun to work in than $\pmod{n}$, but what if you have to work $\pmod{n}$? Is there a way to conclude something in $\pmod{30}$, whilst only working $\pmod{2}$, $\pmod{3}$ and $\pmod{5}$? There is an answer, and it is called CRT:

Chinese Remainder Theorem. *If you know what x is in* $\pmod{a_1}$, $\pmod{a_2}$, $\pmod{a_3}, \dots,$ $\pmod{a_k}$*, then you must know what x is* $\pmod{a_1 a_2 a_3 \cdots a_k}$*, as long as* $\{a_1, a_2, a_3, \dots a_k\}$ *are pairwise relatively prime.*
More concretely if

$$\begin{aligned} x &\equiv r_1 && \pmod{a_1} \\ x &\equiv r_2 && \pmod{a_2} \\ x &\equiv r_3 && \pmod{a_3} \\ &\dots \\ x &\equiv r_k && \pmod{a_k} \end{aligned}$$

then the Chinese Remainder Theorem guarantees that there exists a unique solution for x in $\pmod{a_1 a_2 a_3 \cdots a_k}$*.*

Let's see this in action.

Problem 5. Find all integers n such that n leaves a remainder of 2 when divided by 3, a remainder of 2 when divided by 4 and a remainder of 1 when divided by 5.

Proof. We have

$$\begin{aligned} n &\equiv 2 \pmod{3} \\ n &\equiv 2 \pmod{4} \\ n &\equiv 1 \pmod{5} \end{aligned}$$

Since $3, 4$ and 5 are pairwise coprime (this means $(3, 4) = 1$ and $(3, 5) = 1$ and $(4, 5) = 1$), we can apply the Chinese remainder theorem. Thus, there is a unique solution for $n \pmod{3 \times 4 \times 5}$. So, there is a unique solution for $n \pmod{60}$. There are many ways to find what this unique value is and I suggest you attempt this yourselves.
The answer, nonetheless, is $n \equiv 26 \pmod{60}$. □

Remark. Don't be confused by what it means to have a *unique* solution $\pmod{60}$. It means that there are an *infinite* number of solutions, and they all leave a remainder of 26 when divided by 60. They are, for example, $\dots, -34, 26, 86, \dots$ Please double check that these numbers satisfy the conditions in the problem.

2.4 Quadratic Residues

We've discussed such things as multiplication, addition, subtraction, division and solving using modulo. I have also made the point that powers of integers don't simplify as easily as one would like. If I am working mod 7, it turns out unfortunately that $9^9 \not\equiv 2^2 \pmod{7}$ [Check this!] even though $9 \equiv 2 \pmod{7}$.
It is true that $9^9 \equiv 2^9 \pmod{7}$ and you can always reduce the base, but the reduction of power works differently. In this and the next three subsections, you will gain a better idea of how to work with powers in modulo.
We begin with quadratic residues.

Definition. A *quadratic residue* modulo n is any number x that is a square in modulo n. Mathematically, this says

$$\exists a, \quad \text{such that} \quad a^2 \equiv x \pmod{n}.$$

As an example, let's write out the quadratic residues for a few numbers.

$\pmod{3}$	
x	x^2
0	0
1	1
2	1

$\pmod{4}$	
x	x^2
0	0
1	1
2	0
3	1

$\pmod{5}$	
x	x^2
0	0
1	1
2	4
3	4
4	1

Notice, how I filled out the table for numbers $\{0, 1, 2, \ldots, n-1\}$. The reason is that as soon as you hit n again, it's back to zero (like clock arithmetic), so the value for n^2 in the table will be the same as 0^2. Similarly, for 1^2 and $(n+1)^2$ and so on.

Problem 6. Find any solutions for $x^2 + y^2 = 765483$ in integers.

Proof. Consider the left hand side modulo 4. Each square (x^2 or y^2) is either 0 or 1 if we consult the appropriate table. So, the left hand side is $\equiv 0, 1$ or $2 \pmod 4$. On the other hand, the right hand side $765483 \equiv 3 \pmod 4$, so the two sides can never be equal and there are no solutions! □

2.5 Higher Residues

This idea of quadratic residues generalises of course to higher powers. In fact, all we are doing is calculating the remainder in mod n when we take certain powers. The real question is why do we do this? As we saw in the example problem above, these residues can give us more information than we expect. For example, in mod 3 and 4, squares are only $\equiv 0, 1$. Mod 5 is slightly less useful because we have 0,1 and 4 being quadratic residues, so there are many more options available.

It would be good to know which mod to use when certain powers are present in a problem. Here is a rough guide (although I would always recommend finding the right mod yourself as it may depend on the problem itself):

Squares: mod 3, 4, 8

(mod 8)	
x	x^2
0	0
1	1
2	4
3	1
4	0
5	1
6	4
7	1

Cubes: mod 7, 9

(mod 7)	
x	x^3
0	0
1	1
2	1
3	6
4	1
5	6
6	6

(mod 9)	
x	x^3
0	0
1	1
2	8
3	0
4	1
5	8
6	0
7	1
8	8

Fourth Powers: mod 5

(mod 5)	
x	x^4
0	0
1	1
2	1
3	1
4	1

Remark. This is even better than it looks, since $8 \equiv -1 \pmod 9$ and $6 \equiv -1 \pmod 7$.

How did I get these numbers? They come from Euler's Theorem below. The corresponding result for prime numbers is called Fermat's Little Theorem.

2.6 Fermat's Little Theorem

One of the oldest results in number theory is Fermat's little theorem:

Fermat's Little Theorem. *For all x and primes p,*

$$x^p \equiv x \pmod{p}$$

Also, if x is coprime to p (has no factor of p), then

$$x^{p-1} \equiv 1 \pmod{p}$$

The second form is more common and more useful, since the first version has to take into account what happens to numbers $\equiv 0 \pmod{p}$, which is easy anyway.

Problem 7. What is the remainder when you divide 655^{758} by 7?

Proof. Since $655 \equiv 4 \pmod{7}$, we really are trying to work out the remainder when 4^{758} is divided by 7. But since $(4,7) = 1$, we can apply Fermat's little theorem to get that $4^6 \equiv 1 \pmod{7}$. We now have enough information to solve the problem.

$$\begin{aligned} 655^{758} &\equiv 4^{758} && \pmod{7} \\ &\equiv \left(4^6\right)^{126} \times 4^2 && \pmod{7} \\ &\equiv 1^{126} \times 16 && \pmod{7} \\ &\equiv 1 \times 2 = 2 && \pmod{7} \end{aligned}$$

So, the remainder is 2. □

2.7 Euler's Theorem

If you're not working with primes, as will often happen it is important to be able to simplify large powers in a similar way. There is a theorem called Euler's Theorem that does exactly this, however, first you need to know about the Euler totient function, ϕ.

Definition. The *Euler totient function*, or *Euler phi function*, denoted by $\phi(n)$ counts how many numbers are coprime to n and less than or equal to it.

So, for example, clearly

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \phi(5) = 4, \quad \phi(6) = 2.$$

One can see that $\phi(p) = p - 1$ when p is prime and this is easy to verify from the definition. It gets way more complicated when n is not prime. But there is a formula for it.

Theorem 2.1. *For $n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, we have*

$$\phi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1} = (p_1 - 1) \cdots (p_k - 1) p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}.$$

We shall prove this is in one of the problems for this section. We are now ready to see Euler's theorem.

Euler's Theorem. *For integers a and n such that $(a, n) = 1$, it follows that*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Problems

2.8 Easy

1. If p is a prime and $a^2 \equiv b^2 \pmod{p}$, prove that $a \equiv \pm b$.
2. Verify that $2^{-1} \equiv 3^{-1} + 6^{-1}$ (mod 7).
3. Prove that there is no triangular number which is one less than a multiple of 11.
4. Does there exist a pair of integers (x, y) such that $x^2 + y^2 = 7007$?
   What about a triplet of integers (x, y, z) such that $x^2 + y^2 + z^2 = 7007$?
5. I am thinking of a number. When you divide it by n it leaves a remainder of $n - 1$, for $n = 2, 3, 4, 5, 6, 7, 8, 9$ and 10. What is my number?
6. Find all integer solutions to the equation $15x - 19y = 1$.
7. What are the last two digits (units and tens digits) of 123^{456}?
8. Show that no prime number of the form $3n - 1$ can be expressed as $x^2 + 3y^2$ for any x or y.
9. Find the remainder when 19^{19} is divided by 5.
10. Find $\phi(n)$ for $n = 35, 100, 51200$.
11. Find the last two digits of 7^{7^7}.

2.9 Medium

1. Determine all integers n, m such that $m^2 = n! + 3$.
2. Determine all integers n such that $n^4 - 3n^3 - n^2 + 4n + 1$ is a multiple of 7.
3. Let d be any positive integer not equal to 2, 5, or 13. Show that one can find distinct a, b in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.
4. Find all integer solutions to the equation $x^2 = 65y - 1$.
5. The integers a, b and c are the sides of a right angled triangle. Prove that abc is a multiple of 60.
6. If p is a prime, solve the modulo equation:

$$x^{p-3} + x^{p-4} + \cdots x^2 + x + 1 \equiv p - 1 \pmod{p}$$

7. Let n be a positive integer and let $a_1, a_2, a_3, \ldots, a_k$ $(k \geq 2)$ be distinct integers in the set $\{1, 2, \ldots, n\}$ such that n divides $a_i(a_{i+1} - 1)$ for $i = 1, 2, \ldots, k - 1$. Prove that n does not divide $a_k(a_1 - 1)$.

2.10 Hard

1. (Euler Phi Function) We shall prove the formula for $\phi(n)$. As usual, assume $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.
   (a) First, simplify the problem and assume $n = ab$ where $(a, b) = 1$. Prove $\phi(ab) = \phi(a)\phi(b)$. [Hint: it's really important to use the fact that a and b are coprime.]
   (b) Using (a), show that

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{\alpha_i}).$$

(c) Now, compute $\phi(p^\alpha)$ where p is prime.

(d) Put all the preceding parts together to find the formula for $\phi(n)$.

2. Let a, b and c be positive integers, no two of which have a common divisor greater than 1. Show that $2abc - ab - bc - ca$ is the largest integer which cannot be expressed in the form $xbc + yca + zab$, where x, y and z are non-negative integers.

3. For any positive integer n, prove that
$$98^n - 68^n - 31^n$$
is always one less than a multiple of 2010.

4. Find one pair of positive integers a and b such that:
   - $ab(a+b)$ is not divisible by 7;
   - $(a+b)^7 - a^7 - b^7$ is divisible by 77.

   Justify your answer.

5. Determine all positive integers relatively prime to all the terms of the infinite sequence
$$a_n = 2^n + 3^n + 6^n - 1\,, \qquad n \geq 1.$$

3 Bounding Arguments

We have talked in great detail about one of the unique properties of integers: divisibility. First, in the Divisibility section we discussed when a number divides another. Then, in the Congruences section, we discussed when a number does not divide a number (and hence leaves a remainder). Now, it's time to use the other major property of integers: they are discrete.
The discreteness of integers essentially means that there is a gap between each consecutive integer.

Discrete Inequality. *If m and n are both integers and $m > n$, then $m \geq n + 1$.*

It's such a simple fact, and yet it gives us powerful tools as well. The following subsections expand on this, even if the connection to discreteness is not evident (see if you can work it out!)

3.1 Factorisation

Before, we start on any techniques associated to bounding here is a key fact about positive integers:

Theorem 3.1. *If a and b are positive integers, and $a|b$, then $a \leq b$.*

This immediately suggests trying to factorise complicated expressions wherever possible. Very often, one will have an expression with variables on one side and integers on the other, so it gives one an idea of what the variable factors are likely to be. We begin with a very important problem, since many problems reduce to something similar.

Problem 8. Solve in integers a, b, the equation

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{2}.$$

Proof. Multiplying the whole equation by $2ab$ yields $2b + 2a = ab$, which rearranges to

$$ab - 2a - 2b = 0.$$

This is the important form I was referring to. Factorising this is easy, if you add an integer to make it work. Specifically, if we rewrite this as

$$ab - 2a - 2b + 4 = 4$$

the left hand side is simply $(a-2)(b-2)$, so we have that $a-2$ and $b-2$ are factors of 4, which we can easily see are $-4, -2, -1, 1, 2, 4$. This gives the solutions $(a, b) = (-2, 1), \cancel{(0,0)}, (1, -2), (3, 6), (4, 4), (6, 3)$, where we remove the $(0, 0)$ because it wouldn't allow the fractions of the problem. □

3.2 WLOG and cases

Now, the reason why this previous theorem is so crucial is because it limits the possible solutions. Remember at the beginning of the problem if all you know is that the number (or numbers) you are looking for are integers or even just positive integers, then there are still an infinite number of possibilities! Cutting it down to a finite number of possibilities is (mind the pun!) infinitely better. At that point, you can continue trying to make the bound stronger, or alternatively, try each remaining case.
Trying a small amount of cases that are left is called a case bash and it's really important that it covers *all* the remaining cases for the proof to be rigorous.

Remark. Regardless of whether or not the solutions have been successfully bounded yet, you *should* definitely try the small cases anyway, in case they give you a good intuition for how to do the problem in general!

One of the methods that you have already seen that is very good for bounding is the use of 'Without Loss of Generality' (or WLOG). When the problem is symmetric in some variables, you may assume an ordering of them, which can give you some ideas about the size of the solutions. For more details consult the Method of Proof series of notes. Using the same problem, I will demonstrate the use of WLOG.

Problem 9. Solve in integers a, b, the equation

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{2}.$$

Proof. Since the problem is symmetric in a, b, WLOG $a \leq b$.
If a is negative, then let $a = -A$, where A is a positive integer. Then

$$\frac{1}{b} = \frac{1}{2} + \frac{1}{A}$$

which implies $\frac{1}{b} > \frac{1}{2}$. So, b is both positive and $b < 2$. So, clearly $b = 1$ and substituting back gives $a = -2$.
Since a cannot be zero, we are left with a, b both positive. Also, since $a \leq b$ we have $\frac{1}{a} \geq \frac{1}{b}$ and it follows that

$$\frac{1}{2} = \frac{1}{a} + \frac{1}{b} \leq \frac{2}{a}.$$

Multiplying by $2a$ gives $a \leq 4$. We have a great bound. So, we now substitute in $a = 1, 2, 3, 4$. We find that the only solutions are $a = 3, b = 6$ and $a = 4, b = 4$.
Removing the WLOG and combining the negative and positive case gives us the same solutions: $(a, b) = (-2, 1), (1, -2), (3, 6), (4, 4), (6, 3)$. □

3.3 Square Bounding

The idea here is quite an easy one: there are no perfect squares between the squares of consecutive integers! Of course this generalises to all powers. You can see this in action here:

Problem 10. For what integers n is $n(n+3)$ a perfect square?

Noting that $n(n+3) = n^2 + 3n$, we realise that it already kind of looks like a square! Squares near n^2 include:

$$(n-1)^2 = n^2 - 2n + 1, \quad n^2, \quad (n+1)^2 = n^2 + 2n + 1, \quad (n+2)^2 = n^2 + 4n + 4.$$

Of course there are others but these are the most likely to equal the expression from the problem.

Proof. We need to be systematic. First, suppose $n = 0$, then $n(n+3) = 0$ which is a square.
Second, suppose n is a positive integer. Then $n \geq 1$, so

$$(n+2)^2 = n^2 + 4n + 4 > n^2 + 3n \geq n^2 + 2n + 1 = (n+1)^2$$

so, if $n(n+3) \neq (n+1)^2$, then it is strictly between two consecutive squares and therefore not a square. This would contradict what we want and so, $n(n+3) = (n+1)^2$. Expanding and simplifying gives $n = 1$.
Lastly, suppose n is negative. With the negative value, it's a bit harder to pin down where the square will lie. But, notice that if $-3 < n \leq -1$, then $n(n+3)$ is actually negative (and hence not a square), since the bracketed term is positive while n is negative. So, we are clearly working with $n \leq -3$. It's easier to work with positive integers, so let $n = -N$ and so, $N \geq 3$ and we are trying to make $-N(-N+3) = N^2 - 3N$ a square. Since, $N \geq 3$, notice that $N^2 - 6N + 9 \leq N^2 - 3N$. Also, $N^2 - 3N < N^2 - 2N + 1$, so together we have

$$(N-3)^2 = N^2 - 6N + 9 \leq N^2 - 3N < N^2 - 2N + 1 = (N-1)^2.$$

So, $N^2 - 3N = (N-3)^2$ or $N^2 - 3N = (N-2)^2$. Expanding both possibilities and simplifying yields $N = 3$ and $N = 4$ respectively.
Thus, all the solutions for n in the problem are $n = -4, -3, 0$ and 1. □

3.4 Polynomial Division

In the first handout on divisibility, we talked about divisibility of integers. The same idea works for polynomials, which are evaluated at integer values. The idea is to have a higher degree polynomial dividing a smaller degree polynomial. This is unlikely to be true for many integers, so the idea is to work out after what number the higher degree expression becomes too big to divide the other expression. Then just try all the remaining values.

Problem 11. Find all positive integers a, b such that $a|b+1$ and $b|a+1$.

Polynomial division is really going to help us out here. In each of the division statements in the problem, we have a degree 1 term dividing a degree 1 term, but there is no easy simplification, since we don't know any relation between a and b. The 1s are really going to help us out. The trick is multiplying the two expressions together.

Proof. Multiplying the two division statements together yields $ab|ab+a+b+1$. Since $ab|ab$, this gives us

$$ab|a+b+1.$$

Your intuition should immediately tell you that the left hand side looks to big. Since the statement is completely symmetric in a and b, WLOG $a \leq b$ and we get

$$ab \leq a+b+1 \leq 2b+1 \leq 3b.$$

So $a \leq 3$. Try $a = 1$. From the statements in the problem, we get $b|2$, so $b = 1$ or $b = 2$ and both work!.
Try $a = 2$. From the statements in the problem, we get $2|b+1$ and $b|3$. So, from the second of these we get $b = 3$ (since $b \geq a$) and this satisfies the first, so it's a valid solution.
Try $a = 3$. We get $3|b+1$ and $b|4$. Since $b \geq a$, $b = 4$, but this does not satisfy $a|b+1$, so there is no solution here.
So, all the solutions are $(a, b) = (1, 1), (1, 2), (2, 1), (2, 3), (3, 2)$ (after we remove the WLOG). □

3.5 How fast functions grow

Having studied mathematics at school, you are probably getting quite familiar with many functions: constant, linear, quadratic, polynomial, exponential, logarithmic etc. You probably have an intuition for how quickly they grow. So, if the problem contains two or more different functions, for really large numbers one of the functions is quite likely to be significantly bigger than the others.
As a rough guide, here is the order in how quickly functions grow.

- constant functions: $f(x) = c$ (these functions *do not* grow),
- logarithm functions: $f(x) = \log(x)$,
- linear functions: $f(x) = ax + b$,
- higher degree polynomial functions: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$,
- exponential functions: $f(x) = a^x$.

Remark. This is only a very rough guide and it won't be true at all values of x. Also, importantly the other numbers in these functions can make things wrong if you aren't careful. Make sure you are very comfortable with these types of functions.

Proving that something grows faster and hence is eventually much bigger is actually quite hard to do. Induction is often very useful. Also, to prove higher degree polynomials or exponentials grow faster than linear functions, the following is a cool inequality to know.

Theorem 3.2. *For every integer $r \geq 2$ and every real number $x \geq -1$, it follows that*

$$(1+x)^r > 1 + rx.$$

Remark. This is also called Bernoulli's Inequality. It's very useful when you want to explain that higher degree powers grow way faster than linear functions.

Remark. Clearly, this inequality is actually an equality for $r = 0, 1$. Also, note if r is even, then it's true for all reals x. The inequality also generalises to all real numbers $r > 1$ and interestingly is reversed for $r \in (0, 1)$.

For an example of this being used, see the next example problem in the Greatest Common Divisor subsection below.

3.6 Greatest Common Divisor

Any two positive integers always have a greatest common divisor. The idea is to make use of this to simplify problems. For example, suppose your problem involves m and n. Call $d = \gcd(m, n)$. Then let $m = ad$ and $n = bd$. Since d is the greatest common divisor, it follows that $(a, b) = 1$.

Remark. Don't forget to utilise the fact that $\gcd(m, p)$ where p is prime is either 1 or p. Similarly, the gcd of two distinct primes is of course 1.

It is a little subtle how the gcd can help, but here is an example where the use of the gcd actually shows one of the numbers is a multiple of the other very easily.

Problem 12. Solve $m^n = n^m$ in positive integers m, n.

Proof. First, WLOG $m \geq n$. Next, call $d = \gcd(m, n)$. Then let $m = ad$ and $n = bd$, and hence, it follows that $(a, b) = 1$ and $a \geq b$. Substituting yields $(ad)^n = (bd)^m$. Since $m \geq n$, it follows that

$$a^n = b^m d^{m-n}.$$

The key here is that, therefore, $b^m | a^n$, so any prime that divides b must also divide a, but $(a, b) = 1$, so there are no primes that divide b. So, $b = 1$. [Note, this actually means $n | m$, since $n = d$.]
We now, have

$$a^n = n^{an-n}.$$

Since $n^{an-n} = \left(n^{a-1}\right)^n$, both sides are powers of n, so we take the n^{th} root of both sides. Thus,

$$a = n^{a-1}.$$

It is really intuitive that the right hand side is almost always way bigger than the left hand side. We shall use Bernoulli's inequality to reduce the amount of cases we need to check significantly.

- $a = 1$. Then $1 = n^0$, which works. This corresponds to the obvious solution $m = n$.
- $a = 2$. Then $2 = n^1$, which means $(m, n) = (4, 2)$.
- $n = 1$. Then $a = 1^{a-1}$, which means $(m, n) = (1, 1)$ which we have actually covered already.
- $n \geq 2$ and $a \geq 3$. In Bernoulli's inequality, set $x = n - 1$ and $r = a - 1$. This means $x \geq 1$ and $r \geq 2$, since we've already dealt with $a = 1, 2$ and $n = 1$. So, we can apply the strict version of Bernoulli's Inequality. Substituting gives

  $$n^{a-1} > 1 + (a-1)(n-1) = 2 - a - n + an$$

  It is now sufficient to show that when $a \geq 3$ and $n \geq 2$, we have $2 - a - n + an \geq a$. This is true since subtracting a from both sides and factorising yields $(a-1)(n-2) \geq 0$ which is obviously true from the fact that $a \geq 3$ and $n \geq 2$. So, $n^{a-1} > a$ and there are no solutions in this case.

So, all the solutions are $(m, n) = (2, 4), (4, 2), (k, k)$ for all $k \in \mathbb{N}$. □

Problems

3.7 Easy

1. Find all integers m, n such that $mn + 4 = m + n$.
2. Find all integers m, n such that $mn + a = bm + cn$ for fixed integers a, b, c. [Hint: try to factorise the three higher degree terms.]
3. Prove that for all non-negative integers $2^n \geq n^2$.
4. Find all positive integers m such that $m^3 > m!$
5. Find all integers a, b such that
$$\frac{1}{a} + \frac{2}{b} = \frac{3}{5}.$$
6. Find all integers m, n such that $m^2 + 4n$ and $n^2 + 4m$ are both squares.
7. Find all integers m, n such that $1 + m + m^2 + m^3 = 2^n$.
8. Show that in every primitive Pythagorean triple (all three numbers don't have common factor), exactly one of the numbers is even, exactly one of the numbers is divisible by 3 and exactly one of the numbers is divisible by 5.
9. Find all positive integers x such that $x^2 + 2$ is divisible by $2x + 3$.
10. Find all k such that $k^2 + k + 1 | k^3 + 2k + 2$.
11. Solve in primes: $p(q - r) = q + r$.

3.8 Hard

1. If a, b, c are all positive integers, is it possible for $a^2 + b + c$, $b^2 + c + a$ and $c^2 + a + b$ to all be perfect squares?
2. Suppose a, b, c are distinct positive integers greater than 1. Solve
$$(a - 1)(b - 1)(c - 1) | abc - 1.$$
3. Given positive integers $a > b > 2$, which is bigger: a^b or b^a?
4. Find all n such that $2^n = n! + n + 1$.
5. In how many ways can 1 be expressed as the sum of the reciprocals of three positive integers?
6. Find all pairs of integers m, n such that $n^2(m - 1) = m^5 - 1$.
7. Find all integers m, n such that $m^2 - n! = 2010$.
8. Find all integers m, n such that $m^2 = n^5 - 5$.
9. Find all positive integers m, n such that
$$\frac{m^2n + m + n}{mn^2 + n + 7}$$
is also a positive integer.
10. Let p be a prime. Prove that there are no solutions to $2^p + 3^p = a^n$ if $n > 1$.
11. Let p be an odd prime. Find all positive integers m, n that satisfy $(p - 1)(p^n + 1) = 4m(m + 1)$.

4 Number Theory Theorems

In the previous three number theory handouts, you will have learnt a rather expansive amount about divisibility, remainders (modulo) and about bounding techniques. Of course, there are many other less common techniques that you will need to learn the hard way: by finding them yourself by solving problems.
The problems at the end of this set of notes are general number theory problems for you to practice what you have learnt so far.
In this hand out, I provide some very key results in elementary number theory that it would be prudent to know.

4.1 Pell's Equation

Definition. A *Pell's equation* is of the form

$$x^2 - ay^2 = 1$$

where a, x, y are all integers and a is not a square.
A *generalised Pell's equation* is of the form

$$x^2 - ay^2 = b$$

where a, b, x, y are all integers and a is not a square.

As you can see Pell's equation is a Diophantine equation, and interestingly, is actually an equation that Diophantus himself worked on. Pell's equations do come up a bit and so it is worth knowing the following facts.

Theorem 4.1. *Given a Pell's equation*

$$x^2 - ay^2 = 1,$$

if the equation has a solution, then it has an infinite number of solutions.

The theorem above is what we call an existence theorem since it does not tell us how to find these solutions, rather it tells us they exist (under certain circumstances). There is a modern solution to Pell's equation, which follows easily from continued fractions (which is a rather difficult concept in itself). I sketch the ideas here, and you will prove the details in the problems attached.

Definition. Given a Pell's equation $x^2 - ay^2 = 1$ with a fixed, consider all pairs (x_i, y_i) with $x_i, y_i \in \mathbb{N}$, which are solutions to the equation. The *fundamental solution* (x_1, y_1) is the pair such that $x_1 + \sqrt{a}y_1$ is a minimum over all (x_i, y_i). [In other words, $x_1 + \sqrt{a}y_1 \leq x_i + \sqrt{a}y_i$ for all i.]

It actually follows the fundamental solution is unique.

Lemma 4.2. *If a solution to the Pell's equation $x^2 - ay^2 = 1$ exists for a fixed a, then by the well-ordering principle, a fundamental solution exists. Call it (x_1, y_1) as standard. Then all the other positive integer solutions are given by*

$$x_n + \sqrt{a}y_n = (x_1 + \sqrt{a}y_1)^n.$$

What this means is that when you expand the right hand side and collect all the non- $\sqrt{a}$ terms and all the $\sqrt{a}$ terms separately, then the coefficients will be x_n and y_n respectively.

Problem 13. Find all solutions in positive integers x, y to $x^2 - 3y^2 = 1$.

Proof. We immediately, see that $(x, y) = (2, 1)$ is a solution. It turns out to be the fundamental solution, since the only solution that could be smaller is $(1, 1)$, but that does not satisfy the Pell's equation. So, all the solutions are given by

$$x_n + \sqrt{a}y_n = (2 + \sqrt{3})^n.$$

As an example, we calculate that the first few solutions are $(2, 1), (7, 4), (26, 15), \ldots$ [Check this!] □

If we are dealing with a generalised Pell's equation, then the lemma can be altered as follows:

Lemma 4.3. *If there is at least one solution to the Pell's equation $x^2 - ay^2 = 1$ and to the generalised Pell's equation $x^2 - ay^2 = b$ for fixed a and b, then by the well-ordering principle, a fundamental solution exists for both. Call them (x_1, y_1) and (x_1', y_1') respectively. Then all the other positive integer solutions are given by*

$$x_n + \sqrt{a}y_n = (x_1 + \sqrt{a}y_1)^{n-1}(x_1' + \sqrt{a}y_1').$$

Remark. If a solution does not exist for the generalised Pell's equation, try using a quadratic residue argument to prove it.

4.2 Pythagoras's Theorem

We are all familiar with Pythagoras' Theorem for geometry. In number theory, we are less interested in the right angled triangle and more interested in the equation

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

This is in fact, very famous on its own as the case $n = 2$ of Fermat's Last Theorem, which turns out to only have solutions in this particular case. Look this up!

Definition. A triple of non-zero integers (x, y, z) satisfying the equation $x^2 + y^2 = z^2$ is called a *Pythagorean triple*. Moreover, it is called a *primitive Pythagorean triple* if there is no prime that simultaneously divides x, y and z.

Turns out that Pythagoras' theorem has been solved in integers. In fact, you will solve it in the problems attached.

Theorem 4.4. *All primitive integer solutions to $x^2 + y^2 = z^2$ are given by*

$$(x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2) \qquad \textit{for some } a, b \in \mathbb{N} \textit{ and } a > b.$$

This, of course means that if you want *all* Pythagorean triples, just multiply all three numbers by any integer k to get

$$(x, y, z) = \Big((a^2 - b^2)k, 2abk, (a^2 + b^2)k\Big) \qquad \text{for some } a, b, k \in \mathbb{N} \text{ and } a > b.$$

4.3 Quadratic Reciprocity

Quadratic reciprocity is one of the most famous results in elementary and non-elementary number theory. First proven by Gauss, it basically refers to whether or not a number is a quadratic residue modulo a prime.

Definition. For all integers a and primes p define the *Legendre symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod{p} \\ 1 & a \not\equiv 0 \text{ is a quadratic residue } \pmod{p} \\ -1 & a \not\equiv 0 \text{ is not a quadratic residue } \pmod{p} \end{cases}$$

Be careful, the Legendre symbol looks just like a fraction. Unless something is specified to be the Legendre symbol, it is just a fraction. Then the following is the classical statement of quadratic reciprocity:

Quadratic Reciprocity Theorem. *For odd primes, p, q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}.$$

Moreover,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

where all the lefthand sides are Legendre symbols.

We shall not prove this, but there are more than 200 proofs in existence, so I would strongly suggest having a look at the literature out there.

4.4 Primes as sums of squares

A very interesting fact that is a very specific corollary of the quadratic reciprocity is the following amazing theorem:

Theorem 4.5. *A prime p can be written as the sum of two squares iff $p = 2$ or $p \equiv 1 \pmod 4$.*

We shall prove this in the attached problems.

Problems

4.5 Medium (not easy)

1. (Pell's Equation) Consider a Pell's equation $x^2 - ay^2 = 1$ for fixed a. Suppose there exists a solution in positive integers x, y.

   - By using the well-ordering principle, explain why there is a fundamental solution (x_1, y_1).
   - Prove that the fundamental solution (x_1, y_1) is unique.
   - Show that if $x_2 + \sqrt{a}y_2 = \left(x_1 + \sqrt{a}y_1\right)^2$, then $x_2 - \sqrt{a}y_2 = \left(x_1 - \sqrt{a}y_1\right)^2$. [Hint: expand both equations]
   - Use the same working to show that if $x_n + \sqrt{a}y_n = \left(x_1 + \sqrt{a}y_1\right)^n$, then $x_n - \sqrt{a}y_n = \left(x_1 - \sqrt{a}y_1\right)^n$.
   - Hence, show that $x_n^2 - ay_n^2 = 1$. [Hint: difference of squares]
   - Hence, explain why (x_n, y_n) are all solutions to $x^2 - ay^2 = 1$.
     Remark. These are actually all the solutions because of the Dirichlet unit theorem (super hard!).
   - Show that an alternate way of writing down x_n and y_n is

     $$x_n = x_{n-1}x_1 + ay_{n-1}y_1, \qquad y_n = y_{n-1}x_1 + x_{n-1}y_1.$$

     [Hint: use $\left(x_1 + \sqrt{a}y_1\right)^n = \left(x_1 + \sqrt{a}y_1\right)^{n-1}\left(x_1 + \sqrt{a}y_1\right)$.]
   - Find all the positive integer solutions to $x^2 - 2y^2 = 1$.
   - Find all the integer solutions to $x^2 - 2y^2 = 1$.

2. (Pythagorean Triples) We will find all solutions to $x^2 + y^2 = z^2$ in positive integers x, y, z.

   - Prove that if a Pythagorean triple is not primitive, then dividing by the common factor of x, y and z gives a primitive Pythagorean triple.
     Remark. So, it is sufficient to find all *primitive* Pythagorean triples.
   - Show that if (x, y, z) is a primitive Pythagorean triple, then

     $$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

     and the fractions are in simplest form.
     Remark. So, finding a solution of $X^2 + Y^2 = 1$ for rational X, Y (simplified) will give us a Pythagorean triple.
   - Draw a unit circle in the X-Y plane. What is the equation of this circle?
   - Draw a straight line from $(-1, 0)$ with slope t. What is the equation of this line?
   - We now put $0 < t < 1$. Where is the line going to intersect the circle other than at $(-1, 0)$?
   - To find the intersection point of the line with the circle, substitute the equation of the line into the equation of the circle.
   - Solve the quadratic for X. [One solution should be -1 as we know $(-1, 0)$ is an intersection point of the line and circle. The other solution should simplify nicely and be in terms of t]
   - Use that to find the corresponding solution for Y.
   - We want X and Y to be rational. Show that X and Y are rational iff t is rational.
   - Setting $t = \frac{b}{a}$ with $a, b \in \mathbb{N}$ and $(a, b) = 1$, show that $X = \frac{a^2 - b^2}{a^2 + b^2}$ and $Y = \frac{2ab}{a^2 + b^2}$ and hence,

     $$(x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2).$$

3. Heron's formula says that the area of a triangle with side lengths a, b, c is

   $$\text{Area} = \sqrt{s(s-a)(s-b)(s-c)}$$

   where $s = \frac{1}{2}(a + b + c)$. Find all triangles that have consecutive integer sidelengths and whose area is an integer. [Hint: you should get a Pell's equation.]

4.6 Hard

1. (Primes as sums of squares) Let p be a prime. We will show that $p = x^2 + y^2$ where $x, y \in \mathbb{N}$ iff $p = 2$ or $p \equiv 1 \pmod 4$.

   - Suppose $p = 2$, find integers x and y such that $p = x^2 + y^2$.
   - Show that if $p \equiv 3 \pmod 4$, it can never be expressed as the sum of two perfect squares.
   - Suppose $p \equiv 1 \pmod 4$. Show that there exists an integer in the set $\{1, 2, \ldots, p-2, p-1\}$ whose square is one less than a multiple of p. [Try to do this without using quadratic reciprocity.]
   - Hence, show that for every number from the set $\{1, 2, \ldots, p-2, p-1\}$, there is a different number in the same set, such that the sum of their squares is a multiple of p.
   - Show that at least one of these sums of squares is actually equal to p.

2. Find all positive integers a, b, m, n such that $a^m b^n = (a+b)^2 + 1$.

3. Let $p > 2$ be prime and n, x be positive integers. Suppose $x - 1$ has exactly a factors of p in its prime factorisation, and n has exactly b factors of p where $a \geq 1$ and $b \geq 0$. Prove that $x^n - 1$ has exactly $a + b$ factors of p in it.

4. Find all positive integers k that can be written as

   $$k = \frac{x+1}{y} + \frac{y+1}{x}$$

   where x and y are also positive integers.

5. Determine the maximum value of $m^2 + n^2$ where $m, n \in \mathbb{Z}$, $1 \leq m, n \leq 1981$ and $(n^2 - mn - m^2)^2 = 1$.