

B10 lecture course : Elementary Number Theory

Lectures given by Dr Heath-Brown
Notes taken by Tom Womack, extra material supplied by
Paul Rowe, Duncan Archer and Rob Hladky

October 1996

Contents

1	Introduction	3
2	Properties of \mathbb{Z}	3
2.1	Prime Numbers	4
2.2	Estimating $\pi(x)$	4
2.3	Corollaries of PNT	5
3	Congruences	5
3.1	Linear Congruences	5
3.2	Simultaneous congruences	6
4	Arithmetic Functions	7
4.1	Arithmetic Functions	7
4.2	Multiplicative functions	7
4.3	Making multiplicative functions	8
4.4	Perfect Numbers	8
4.5	The Möbius Function	9
5	Congruences to prime moduli	12
5.1	The multiplicative group of \mathbb{Z}_p is cyclic	12
5.2	A very bad primality test	13
5.3	The multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic for $p \geq 3$	13
5.4	Non-linear congruences	15
6	Quadratic Residues	15
6.1	Solving Quadratic Equations	15
6.2	Ways of finding $\left(\frac{n}{p}\right)$	16
6.3	Quadratic Reciprocity	18
6.4	Proof of Quadratic Reciprocity	19

7	Writing numbers as sums of squares	19
7.1	Two squares	19
7.2	Primes of the form $x^2 + 5y^2$	22
7.3	Sums of three squares	22
7.4	Sums of four squares	22
8	Irrational numbers and approximations by rationals	24
8.1	Some irrational numbers	24
8.2	Approximations by rationals	25
8.3	Transcendental numbers	26
9	Diophantine equations	26
9.1	$x^3 + 2y^3 = 13$: Congruences	27
9.2	$x^3 + 2y^3 = 4z^3$: Least counterexample	27
9.3	$x^2 = y^3 + 7$: Using quadratic residues	27
9.4	$x^2 + y^2 = z^2$	27
9.5	$x^4 + y^4 = z^4$	28
9.6	Pell's equation	28
9.7	Mordell's Equation	30
10	More on primes	31
10.1	A lower bound for $\pi(x)$	31
10.2	An upper bound for $\pi(x)$	32
10.3	An upper bound for p_n	34

1 Introduction

I would like to thank Dr Heath-Brown for giving me permission to publish this set of notes. The copyright in the content is his; the errors in the content are mine.

This course is about properties of \mathbb{N} , \mathbb{Z} and \mathbb{Q} ; until you get to a much higher level, no analysis pokes its ugly head anywhere near this subject.

2 Properties of \mathbb{Z}

\mathbb{Z} has a Euclidean algorithm - that is, $\forall a, b \in \mathbb{Z}$, there is a d with $d|a$, $d|b$, $s|a, s|b \implies s|d$. Moreover, $\exists \alpha, \beta \in \mathbb{Z}$ with $\alpha a + \beta b = d$.

Corollary 2.1. *Let p be prime. Then $p|ab \implies p|a$ or $p|b$.*

Proof. Suppose $p \nmid a$. Then $\exists d = (p, a)$, with $d|p$ so $p = dd'$. But p is prime, so $d = 1$ or $d = p$. If $d = p$ then $d|a$ by definition of d , but $p \nmid a$, so $d = 1$.

So $\exists x, y : px + ay = 1$. So $b = pbx + aby$. But $p|ab$, so $ab = pc$. So $b = p(bx + cy)$, so $p|b$. □

Theorem 2.2 (Fundamental Theorem of Algebra). *Every $n \in \mathbb{N}$ can be written as a product of increasing prime numbers in exactly one way.*

There are two parts to this theorem; that every n can be written in this way, and that the expression is unique.

For the first part, let n be the smallest number which can't be written in that way. Then n is composite (since primes are already written in that way), $n = pq$ with $n > p, q > 1$. But p and q are $< n$, so can be written as products of primes; concatenate the expressions.

For the second part, assume that n is the smallest integer with two or more representations :

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = q_1^{e_1} \dots q_s^{e_s}.$$

If $p_1 = q_1$ then $n/p_1 = n/q_1$ - but n/p_1 factorises uniquely. So $p_1 \neq q_1$. WLOG $p_1 < q_1$.

Now, $p_1|n \implies p_1|q_1^{e_1} \dots q_s^{e_s}$. Apply the corollary repeatedly until we have $p_1|q_i$. But q_i is prime, and, by ordering, $q_i \geq q_1 > p_1$. Contradiction.

Corollary 2.3. *Let a, b be coprime positive integers. Then ab is a square iff a and b are both squares.*

Proof. Let $ab = c^2$, and $p_1 \dots p_n$ be all the primes which divide any of a, b or c . Write $a = \prod p_i^{e_i}$, $b = \prod p_i^{f_i}$, $c = \prod p_i^{g_i}$ with $e_i, f_i, g_i \geq 0$.

Now $e_i + f_i = 2g_i$ by definition of multiplication. But, since a and b are coprime, e_i and f_i are never both non-zero. So $e_i = 2g_i$ or $f_i = 2g_i$, so a and b are both squares. □

This concept doesn't hold universally; for example, over $\mathbb{Z}[\exp(2i\pi/23)]$, $ab = c^{23}$ doesn't mean both a and b are 23-rd powers.

2.1 Prime Numbers

It's very easy to make long lists of prime numbers, using the Sieve of Eratosthenes for example (erase multiples of 2 which are ≥ 4 , multiples of 3 which are $\geq 9 \dots$).

Theorem 2.4. *There are infinitely many primes*

Proof. Assume there are only finitely many primes. Multiply them together and add 1 to get λ . If λ is prime, it's a prime not on the list; if it's composite, it's divisible by a prime not on the list. \square

Theorem 2.5. *There are sequences of n consecutive composites for every n*

Proof. $N! + 2 \dots N! + N$, for $N = n + 1$. \square

A corollary of 2.4 is that $p_{n+1} \leq \prod_{i=1}^n p_i + 1$. It's a lousy estimate, though.

At this point, one of the major features of number theory appears; there are an awful lot of unsolved problems about, and a vast number of statements which are easy to make and horrific to prove. For example, we don't know if there are infinitely many primes of the form $n! + 1$, or infinitely many of any prime constellation (for example the twin primes). The answers should be 'yes' and 'yes', but no-one has the proof.

There are earlier sequences of consecutive composites for n ; Marek Wolf conjectured in a recent paper that the first set of n composite numbers appears around $\sqrt{n} \exp(\sqrt{n})$.

We define $\pi(x)$ as the number of prime numbers $\leq x$. For example, $\pi(10^3) = 168$, $\pi(10^4) = 1229$, $\pi(10^6) = 78498$, $\pi(10^8) = 5761455$.

$\pi(x)/x$ is decreasing, but only slowly (roughly as $1/\log x$).

2.2 Estimating $\pi(x)$

Theorem 2.6 (the Prime Number Theorem). $\frac{\pi(x) \log x}{x} \rightarrow 1$ as $x \rightarrow \infty$

Definition 2.7. If $f(x), g(x) > 0 \forall x$, and $\frac{f(x)}{g(x)} \rightarrow 1$ as $x \rightarrow \infty$, we write $f(x) \sim g(x)$.

So the Prime Number Theorem can be written as $\pi(x) \sim \frac{\log x}{x}$. There is a better approximation obtained by $\pi(x) \approx \int_2^x \frac{1}{\log t} dt$; unfortunately, $\frac{1}{\log t}$ can't be integrated using normal functions.

Whilst $\pi(x) > \frac{x}{\log x}$ always, $\pi(x) < \text{Li}(x)$ for small x . This is with 'small' meaning ' $< 10^{18}$ '; Littlewood proved that $\pi(x) > \text{Li}(x)$ for infinitely many x , and Skewes showed that the smallest such x was less than $10^{10^{34}}$. Fortunately, modern results suggest that $x < 10^{1700}$. It's unlikely that x will ever be found, since it's unlikely that $x < 10^{500}$.

The Prime Number Theorem was first proved in 1896; there is still no easy proof, though there's one in Hardy and Wright which is merely fiddly rather than actively incomprehensible.

2.3 Corollaries of PNT

Theorem 2.8. $p_n \sim n \log n$

Proof. Recall that $\pi(p_n) = n$. By theorem 2.6, $n \sim \frac{p_n}{\log p_n}$, so $n \log p_n \sim p_n$.

We want to show, therefore, that $\log p_n \sim \log n$. We know that $p_n \geq n$, so the fraction is always ≥ 1 .

However,

$$n \log p_n \sim p_n \implies \frac{n \log p_n}{p_n} \geq 1/2$$

for large enough n . If ϵ is given, $\log x \leq x^\epsilon$ for large enough x , so $\log p_n \leq p_n^\epsilon$ for n large enough.

So $\frac{np_n^\epsilon}{p_n} \geq 1/2$ for n big enough, so $p_n^{1-\epsilon} \leq 2n$, and $(1-\epsilon) \log p_n < \log 2n$.

So

$$\frac{\log p_n}{\log n} \leq \frac{1}{1-\epsilon} \frac{\log 2n}{\log n},$$

and this tends to 1 as $n \rightarrow \infty$, $\epsilon \rightarrow 0$. □

Corollary 2.9. $p_n < n^2$ for n big enough, since $p_n \leq 2n \log n$ and $2n \log n \leq n^2$

It's not known whether there is always at least one prime between n^2 and $(n+1)^2$, though it seems likely. There is always at least one prime between consecutive cubes, though.

You can model the sequence of primes well by assuming that primes near x occur following a Poisson process with parameter $(\log x)^{-1}$.

3 Congruences

We write $a \equiv b \pmod{n}$ iff $n|(b-a)$. This is an equivalence relation for fixed n . You can add, multiply and subtract congruences, but you can't always divide them ($2 \equiv 8 \pmod{6}$, but $1 \not\equiv 4 \pmod{6}$).

This is just another way of writing arithmetic in $\mathbb{Z}/n\mathbb{Z}$; it means you can work with smaller numbers, so you can check that $2^{30} \equiv (2^5)^6 \equiv (-1)^6 \equiv 1 \pmod{31}$ without ever having to know that $2^{30} = 1073741824$.

3.1 Linear Congruences

You might want to know when you can solve a linear equation like $ax \equiv b \pmod{m}$.

Start off by noticing that, if $d|a$ and $d|m$, $d|ax - b$ (since $ax - b = km$), so $d|b$. So a necessary condition is that $(a, m)|b$.

If this holds, set $d = (a, m)$, so the equation becomes $dAx \equiv dB \pmod{dM}$; we can now divide through by d , since it's not coprime to the modulus, to get $Ax \equiv B \pmod{M}$, with $(A, M) = 1$.

We can go further, in fact; if we can solve $Ax \equiv 1 \pmod{M}$, we have $AxB \equiv B \pmod{M}$. So what we need is

Theorem 3.1. *If $(a, m) = 1$ then the congruence $ax \equiv 1 \pmod{m}$ always has a solution, and it is unique modulo m .*

Proof. $(a, m) = 1$, so, using the Euclidean algorithm, we can find y, z with $ay + zm = 1$. So $m|zm = 1 - ay$, so $ay \equiv 1 \pmod{m}$.

For uniqueness, suppose that $ax \equiv ax' \equiv 1 \pmod{m}$. Then $ax \equiv ax'$, so $m|a(x - x')$. But $(a, m) = 1$, so $m|(x - x')$, so $x \equiv x' \pmod{m}$. \square

So we can solve single linear equations. An obvious next question is how far we can get solving multiple linear equations; simultaneous equations to the same modulus are fairly straightforward using the standard elimination methods, but it would be nice to be able to handle several equations to different moduli.

3.2 Simultaneous congruences

Theorem 3.2 (Chinese Remainder Theorem). *If m_1, \dots, m_k are coprime in pairs, the simultaneous congruences $x \equiv b_1 \pmod{m_1}, \dots, x \equiv b_k \pmod{m_k}$ have a unique solution mod $M = \prod_{i=1}^k m_i$.*

Note that there need not be a solution if the m_i aren't coprime in pairs; $x \equiv 1 \pmod{4}, x \equiv 3 \pmod{8}$ is clearly impossible.

Proof. We need to prove existence and uniqueness.

Existence Let $M = m_i n_i$ (eg $n_3 = m_1 m_2 m_4 \dots m_k$). Then $(m_i, n_i) = 1$, since the m_i are coprime in pairs, so, by theorem 3.1, we can solve $n_i x_i \equiv 1 \pmod{m_i}$ for each i .

Now, let

$$x = x_1 n_1 b_1 + \dots + x_k n_k b_k.$$

Working modulo each m_i in turn, we have $m_i | n_j$ for $j \neq i$, so the only term left is $x_i n_i b_i = b_i$ by definition of the x_i . So x satisfies the simultaneous congruences.

Uniqueness Suppose $x' \equiv b_i \pmod{m_i}$ for all i . Then $x' \equiv x \pmod{m_i} \forall i$ since both $\equiv b_i$. So $m_i | x' - x$. But the m_i are pairwise coprime, so $\prod m_i | x' - x$, so $x' \equiv x \pmod{M}$.

\square

Example 3.3. We solve $10x \equiv 2 \pmod{26}, 7x \equiv 3 \pmod{20}$.

$(26, 20) \neq 1$, but $(10, 2, 26) = 2$, so we can convert the first equation to $5x \equiv 1 \pmod{13}$.

To apply the Chinese Remainder Theorem, we must start off by reducing the equations to the form $x \equiv b_i \pmod{m_i}$. So we solve $5b_1 - 1 = 13y$ getting $b_1 = 8$, and we solve $7b_2 - 3 = 20y$, getting $b_2 = 9$.

Now, we see that $m_i = n_{3-i}$ (that is, there are only two factors so the cofactor in each case is the other one).

So we solve $20x_1 \equiv 1 \pmod{13}$, getting $x_1 = 2$, and $13x_2 \equiv 1 \pmod{20}$, getting $x_2 = 17$. And, by the Chinese Remainder Theorem, we have $x \equiv n_1x_1b_1 + n_2x_2b_2 \equiv 20 \cdot 2 \cdot 8 + 13 \cdot 17 \cdot 9 \equiv 2309 \equiv 229 \pmod{260}$.

4 Arithmetic Functions

4.1 Arithmetic Functions

Definition 4.1. An *arithmetic function* is a function from \mathbb{N} to \mathbb{C} (often from \mathbb{N} to \mathbb{N}).

Examples of arithmetic functions include obvious ones like the polynomials, and also some less usual ones :

$d(n)$, the divisor function, which is $|\{k \in \mathbb{N} : k|n\}|$.

$$\sigma(n) = \sum_{k|n} k$$

$\omega(n)$, the number of prime factors of n

$\phi(n)$, the Euler function, which is $|\{k \in \mathbb{N} : k < n, (k, n) = 1\}|$.

4.2 Multiplicative functions

Definition 4.2. We say that an arithmetic function is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $m, n \in \mathbb{N}$ and $(m, n) = 1$.

For example, d is multiplicative, whilst ω isn't (since $\omega(2) = 1, \omega(3) = 1, \omega(6) = 2 \neq 1$).

Theorem 4.3. ϕ is a multiplicative function

Proof. ϕ is the number of invertible elements in $\mathbb{Z}/n\mathbb{Z}$.

Let a run over a complete set of invertible elements mod m , and b do the same mod n . So there are $\phi(m)a$'s, and $\phi(n)b$'s. We want to show that, if $(m, n) = 1$, $am + bn$ runs over a complete set of invertible elements mod mn . This would imply $\phi(mn) = \phi(m)\phi(n)$.

So we need to show that

- i $am + bn \equiv a'm + b'n \implies a = a', b = b'$. Working mod m gives $bn \equiv b'n$, so $b = b'$ since $(n, m) = 1$; repeating the argument backwards gives $a = a'$.
- ii $(an + bm, nm) = 1$. $(an + bm, m) = (an, m) = 1$ since a and n are each coprime to m . Similarly, $(an + bm, n) = (bm, n) = 1$. So $(an + bm, nm) = 1$.
- iii If c is invertible mod mn , $\exists a, b : c \equiv am + bn \pmod{mn}$. But $mx \equiv c \pmod{n}$ is solvable since $(m, n) = 1$; let b be a solution. If $d > 1$ divides both b and n , $d|c$, so $(c, n) > 1$, so $(c, mn) \neq 1$. So $(b, n) = 1$. Similarly to get $(a, m) = 1$. Now $am + bn \equiv am \equiv c \pmod{n}$, and $am + bn \equiv bm \equiv c \pmod{m}$. So the numbers are congruent mod m and mod n , so mod mn .

□

Corollary 4.4.

$$\phi(n) = n \prod_{p|n} (1 - 1/p).$$

Proof. $\phi(p^e)$ is the number of integers $< p^e$ without a factor p , so is $p^e(1 - 1/p)$. The result follows by multiplicativity. □

4.3 Making multiplicative functions

Theorem 4.5. *If f is multiplicative, then $g(n) = \sum_{d|n} f(d)$ is multiplicative.*

Proof. $g(mn) = \sum_{d|mn} f(d)$. If u and v run over the divisors of m and n respectively, then $d = uv$ runs over the divisors of mn , if $(m, n) = 1$:

If $uv = u'v'$, then $u|u'v'$. But $u|m, v'|n \implies (u, v') = 1$, so $u|u'$. Similarly, $u'|u$, so $u = u', v = v'$, so all the uv are different.

$uv|mn$ trivially (since $(m, n) = 1$).

If $\alpha|mn$, set $u = (\alpha, m)$ and $v = \alpha/u$. Then $\alpha = uv$, and $\alpha|mn \implies \frac{\alpha}{u} | \frac{mn}{u}$. But d/u and m/u are coprime, so α/u divides n . So $v|n, u|m$. □

This produces a number of new multiplicative functions :

$f(x) = 1$ gives the divisor-counting function d , so that's multiplicative.

$f(x) = x$ gives the sum of the divisors, so σ is multiplicative.

Any multiplicative function can be given a direct form in terms of the prime factorisation of the argument :

$$d(p_1^{e_1} \dots) = (e_1 + 1)(e_2 + 1) \dots,$$

$$\sigma(p_1^{e_1} \dots) = \prod \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

4.4 Perfect Numbers

Definition 4.6. $n \in \mathbb{N}$ is *perfect* iff $\sigma(n) = 2n$. If $\sigma(n) < 2n$, n is called *deficient*; if $\sigma(n) > 2n$, n is called *abundant*.

That is, the sum of the proper divisors of a perfect number is the number itself. Some perfect numbers are 6, 28, 496, 33550336 and $2^{60} \cdot (2^{61} - 1)$.

It is an open question whether there are infinitely many perfect numbers (though the answer is clearly 'yes'), and whether there are any odd ones (where the answer is less clear); these are probably the oldest well-defined unanswered questions.

Euclid proved that, if $p = 2^n - 1$ is prime, then $p \cdot (p + 1)/2$ is perfect; such primes are called Mersenne primes, and it's an open question as to whether there are infinitely many of them. 36 are currently known, the largest being $2^{2976221} - 1$.

Theorem 4.7. *If $n = ab$ with $a, b \geq 2$ then $2^n - 1$ is composite*

Proof. $2^n - 1 = x^b - 1$ for $x = 2^a$; $x^b - 1$ factors algebraically as $(x - 1)(x^{b-1} + x^{b-2} \dots + 1)$. \square

Theorem 4.8. *If $q|2^p - 1$ with p, q prime, then $q \equiv 1 \pmod{2p}$.*

Proof. Consider the group of order $q - 1$ of the non-zero residues mod q . By Lagrange's theorem, $2^{q-1} \equiv 1 \pmod{q}$. Now, $2^p \equiv 1 \pmod{q}$, since $q|2^p - 1$.

Now, if $p \nmid q - 1$, $(p, q - 1) = 1$ so $\exists x, y : px + (q - 1)y = 1$. But then $2^{px} 2^{q-1y} \equiv 2^1 \equiv 1^x 1^y = 1$, which is a contradiction. So $p|q - 1$, so $q \equiv 1 \pmod{p}$.

$q \equiv 1 \pmod{2p}$ since q is prime, hence odd. \square

Theorem 4.9 (Euler). *Every even perfect number is of the form $2^{p-1}(2^p - 1)$.*

Proof. An even n is of the form $2^e b$ with $e \geq 1$ and b odd. Now, $\sigma(n) = \sigma(2^e)\sigma(b)$ since σ is multiplicative and $(2^e, b) = 1$ since one has only factors of 2 and the other is odd.

So $\sigma(n) = \sigma(b)2^{e+1} - 1$. So, for n to be perfect, we require

$$2^{e+1}b = (2^{e+1} - 1)\sigma(b).$$

So $2^{e+1}|\sigma(b)$, so $\sigma(b) = 2^{e+1}k$, which means $b = (2^{e+1} - 1)k$. If $k > 1$ then, since 1, k and b are all divisors of b , $\sigma(b) \geq 1 + b + k > k + b = 2^{e+1}k = \sigma(b)$.
Oops.

So $k = 1$, $b = 2^{e+1} - 1$, and $\sigma(b) = 2^{e+1}$ - so b must be prime. \square

So any even perfect number is of Euclid's form. No-one's ever seen an odd perfect number, but you can prove results about them anyway :

Theorem 4.10. *Any odd perfect number has at least three prime factors*

Proof. Suppose $n = p_1^{e_1} p_2^{e_2}$, where p_2 might be 1. Then

$$\sigma(n) = \prod \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right) < \prod \frac{p_i^{e_i+1}}{p_i - 1} = \prod p_i^{e_i} \prod \frac{p_i}{p_i - 1} = n \prod \frac{p_i}{p_i - 1}.$$

So $2 = \prod_{i=1}^k p_i(p_i - 1)^{-1}$.

Write P_i for the i th odd prime number. Assume P_i are written in ascending order, so $p_i \geq P_i$. So $2 < \prod_{i=1}^k \frac{P_i}{P_i - 1}$. But this is impossible if $k = 1$ or $k = 2$, since the product is too small. Increasing k might produce good results after a bit of searching. \square

In fact, it's known that any odd perfect number has at least eight prime factors.

4.5 The Möbius Function

We define $\mu(1) = 1$, and

$$\mu(p_1^{e_1} \dots p_k^{e_k}) = \begin{cases} (-1)^k & e_i = 1 \forall i \\ 0 & \exists i : e_i \geq 2 \end{cases}$$

The function is multiplicative by definition, and equal to zero at any power or number divisible by a power.

Theorem 4.11. $\sum_{d|n} \mu(d) = 0$ unless $n = 1$, whereupon it equals 1.

Proof. $\mu(d)$ is multiplicative, so $f(n) = \sum_{d|n} \mu(d)$ is multiplicative. But $f(p^k) = \mu(1) + \mu(p) + \mu(p^2) \dots = 1 - 1 + 0 + 0 \dots$

So f is 1 iff $n = 1$. □

This function is important because of the following

Theorem 4.12 (The Möbius Inversion Theorem). If $G(n) = \sum_{d|n} F(d)$, then

$$F(n) = \sum_{d|n} \mu(d)G\left(\frac{n}{d}\right) = \sum_{d|n} G(d)\mu\left(\frac{n}{d}\right).$$

Proof.

$$\begin{aligned} \sum_{d|n} \mu(d)G\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) \\ &= \sum_{cd|n} \mu(d)f(c) \\ &= \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) = f(n) \end{aligned}$$

□

Theorem 4.13. If $f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right)$, then $g(n) = \sum_{d|n} f(d)$.

Proof.

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} f\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu\left(\frac{n}{cd}\right)g(c) \\ &= \sum_{cd|n} \mu\left(\frac{n}{cd}\right)g(c) \\ &= \sum_{c|n} g(c) \sum_{d|\frac{n}{c}} \mu\left(\frac{n}{cd}\right) = g(n) \end{aligned}$$

□

Theorem 4.14. $\sum_{d|n} \phi(d) = n$.

We will present three different proofs of this

Using multiplicativity. ϕ is multiplicative, so $f(n) = \sum_{d|n} \phi(d)$ is also multiplicative. And

$$f(p^e) = \phi(1) + \phi(p) + \dots + \phi(p^e) = 1 + (p-1) + p(p-1) + \dots + p^{e-1}(p-1) = p^e.$$

So $f(n) = n \forall n$. □

Using the inclusion-exclusion principle. Let $m = p_1^{e_1} \dots p_k^{e_k}$. Then

$$\begin{aligned} \phi(m) &= m \cdot 1 - \frac{1}{p_1} \cdot 1 - \frac{1}{p_2} \dots \\ &= m - \left[\sum_{i \leq k} \frac{m}{p_i} \right] + \left[\sum_{i < j \leq k} \frac{m}{p_i p_j} \right] + \dots + (-1)^k \frac{m}{p_1 p_2 \dots p_k} \\ &= \sum_{d|m} \frac{m}{d} \mu(d) \\ &= \sum_{d|m} d \mu\left(\frac{m}{d}\right) \end{aligned}$$

So, by theorem 4.13, $m = \sum_{d|m} \phi(d)$. □

Counting by (m, n) .

$$n = |\{m \in \mathbb{N} : m \leq n\}|.$$

We'll group the m 's according to the value of (m, n) , giving

$$n = \sum_{d|n} |\{m \in N : m \leq n, (m, n) = d\}|.$$

Now, if $m \leq n$ and $(m, n) = d$, we have $m = rd$ and $n = sd$ with $(r, s) = 1$. So

$$n = \sum_{d|n} |\{r \in N : r \leq d, (r, d) = 1\}| = \sum_{d|n} \phi(d)$$
□

This is quite a useful result, because it tells you that ϕ is in some sense the inverse of n .

Theorem 4.15.

$$\sum_{d|n} d \left(\frac{n}{d}\right) \phi(d) = \sigma(n)$$

Proof. Note that $d(k) = \sum_{d|k} 1 = \sum_{uv=k} 1$.
So we have

$$\begin{aligned} \sum_{d|n} d\left(\frac{n}{d}\right)\phi(d) &= \sum_{d|n} \phi(d) \sum_{uv=\frac{n}{d}} 1 = \sum_{d|n} \phi(d) \sum_{d|n} \phi(d) \\ &= \sum_{v|n} \sum_{d|\frac{n}{v}} \phi(d) = \sum_{v|n} \frac{n}{v} = \sigma(n). \end{aligned}$$

□

5 Congruences to prime moduli

For p prime, $\mathbb{Z}/p\mathbb{Z}$ is not merely a ring but a field. It has p elements, and the non-zero ones form a group of order $p - 1$ under multiplication. Applying Lagrange's Theorem gives $n^{p-1} \equiv 1 \pmod{p}$ if $p \nmid n$, which is called Fermat's Little Theorem or FLT.

In general, if n is composite, the residues coprime to n will form a group of order $\phi(n)$ under multiplication, so $a^{\phi(n)} \equiv 1 \pmod{n}$ whenever $(a, n) = 1$. This is called Euler's Theorem.

5.1 The multiplicative group of \mathbb{Z}_p is cyclic

Lemma 5.1. *If $a^u \equiv 1 \pmod{n}$, $a^v \equiv 1 \pmod{n}$ and $(a, n) = 1$ then $a^{(u,v)} \equiv 1 \pmod{n}$*

Proof. $a^u \equiv 1$ means that the order of a has a factor u ; $a^v \equiv 1$ means that it has a factor v , so it has a factor (u, v) . □

Lemma 5.2. *If $e|p-1$, then there are exactly e solutions to $x^e - 1 \equiv 0 \pmod{p}$.*

Note that this only works for prime p ; $x^2 - 1 \equiv 0 \pmod{8}$ has four roots.

Proof. A polynomial of degree d has at most d roots over any field, so we need to prove the polynomial has at least d roots.

$$p - 1 = ef \implies x^{p-1} - 1 = (x^e - 1)(x^{ef-e} + x^{ef-2e} + \dots + x^e + 1).$$

But $x^{p-1} = 1$ by Fermat's little theorem. But the first factor has at most e roots, and the second at most $e(f - 1)$ roots. But $e + e(f - 1) = p - 1$, so both factors must have their full complements of roots. In particular, $x^e - 1$ has e roots. □

Theorem 5.3. *If $e|p - 1$ then there are precisely $\phi(e)$ elements of order e in the multiplicative group mod p .*

Again, this only works for prime p ; there are no elements of order 4 in the multiplicative group modulo 8.

Proof. We work inductively. For $e = 1$, there is 1 element of order 1.

$x^e \equiv 1 \pmod{p} \iff |x| \mid e$. There are exactly e elements with order dividing e , by lemma 5.2; let $f(d)$ be the number of order- d elements, so $\sum_{d \mid e} f(d) = e$.

Now $f(d) = \phi(d)$ for all $d < e$, by the inductive step, so $\sum_{d \mid e} f(d) = \sum_{d \mid e} \phi(d) = e$. Comparing terms in the series gives $f(e) = \phi(e)$. \square

As a corollary to this result, we have that the multiplicative group of \mathbb{Z}_p is cyclic with $\phi(p-1)$ generators, which we call the *primitive roots* of \mathbb{Z}_p .

5.2 A very bad primality test

Theorem 5.4. $x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-(p-1)) \pmod{p}$

Proof. Both sides are polynomials of degree $p-1$ with the same roots, so must be equal to within a constant term, and comparing the coefficient of x^{p-1} gives the constant term equal to 1. \square

Putting $x = 0$ in the above gives (since p is odd)

Theorem 5.5 (Wilson's Theorem).

$$-1 \equiv (-1)^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

This in fact gives a (totally useless) test for primality :

$$d \mid n \implies d \mid (n-1)! \implies (n-1)! \not\equiv -1 \pmod{n},$$

so $(p-1)! \equiv -1 \pmod{p}$ iff p is prime.

Theorem 5.6. Let s be the sum of the primitive roots mod p . Then $s \equiv \mu(p-1) \pmod{p}$.

Proof. Let g be a primitive root. Then the $\phi(p-1)$ primitive roots will be g^n , where $n \in [1, p-1]$ with $(n, p-1) = 1$.

Define $f(n)$ to be 1 iff $(n, p-1) = 1$. Then $s = \sum_{n=1}^{p-1} f(n)g^n$.

But we can also write $f(n)$ as $\sum_{d \mid (n, p-1)} \mu(d)$, by theorem 4.11. So

$$s = \sum_{n=1}^{p-1} g^n \sum_{d \mid (n, p-1)} \mu(d) = \sum_{d \mid p-1} \mu(d) \sum_{d \mid n, n \in [1, p-1]} g^n.$$

Write $s(d) = \sum_{d \mid n} g^n$, so $s = \sum_{d \mid p-1} \mu(d)s(d)$.

If $d = p-1$, $s(d) = g^{p-1} \equiv 1 \pmod{p}$. If $d < p-1$, we have

$$s(d) \equiv \sum_{m=1}^{\frac{p-1}{d}} g^{md} = \frac{(g^d)^{\frac{p-1}{d}+1} - g^d}{g^d - 1}$$

by the formula for the sum of a geometric progression. But $g^{p+1-d} - g^d = g^d - g^d \equiv 0 \pmod{p}$, and $g^d - 1 \not\equiv 0$. So $p|s(d)$ since it divides the numerator and not the denominator, and $s(d)$ is an integer.

So $s(d) \equiv 0$ for $d < p - 1$, so $s \equiv \mu(p - 1)g^{p-1} = \mu(p - 1)$. □

5.3 The multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic for $p \geq 3$

We extend the definition of ‘primitive root’ such that a primitive root of p^n is a generator of the multiplicative group mod p^n .

Theorem 5.7. *The multiplicative group (mod p^n) is cyclic if $p \geq 3$. In fact, there is a g which is a primitive root for $p^r \forall r$.*

Proof. The proof proceeds in three steps :

i $\exists g$, a primitive root mod p , such that $g^{p-1} \not\equiv 1 \pmod{p^2}$.

Let g_1 be any primitive root mod p . Unless $g_1^{p-1} \equiv 1 \pmod{p^2}$, we can take $g = g_1$.

If $g_1^{p-1} \equiv 1 \pmod{p^2}$, consider $g = g_1 + p$. This is still a primitive root mod p , and

$$\begin{aligned} g^{p-1} &= g_1^{p-1} + \binom{p-1}{1} g_1^{p-2} p + \binom{p-1}{2} g_1^{p-3} p^2 \dots \\ &\equiv 1 + (p-1)g_1^{p-2} p \pmod{p^2} \\ &\not\equiv 1 \pmod{p^2} \end{aligned}$$

since p^2 does not divide $p(p-1)g_1^{p-2}$.

ii For such a g , $g^{(p-1)p^r} \not\equiv 1 \pmod{p^{r+2}}$ for $r \geq 0$

For this bit, we work by induction on r . $r = 0$ is given by the previous part.

$g^{(p-1)p^r} = g^{\phi(p^{r+1})} \equiv 1 \pmod{p^{r+1}}$, by Euler’s theorem, so $g^{(p-1)p^r} = 1 + lp^{r+1}$. By induction, we have that the left-hand side $\not\equiv 1 \pmod{p^{r+2}}$, so $p \nmid l$. So

$$\begin{aligned} g^{(p-1)p^{r+1}} &= (g^{(p-1)p^r})^p = (1 + p^{r+1}l)^p \\ &= 1 + p^{r+1}l \binom{p}{1} + \dots \\ &\equiv 1 + p^{r+2}l \pmod{p^{r+3}} \end{aligned}$$

since $p^{r+3} | (p^{r+1}l)^k \binom{p}{k}$ for $k \geq 2$.

iii Such a g is a primitive root mod p^t for all $t \geq 1$.

Let the order of g mod p^t be m . Then $g^m \equiv 1 \pmod{p^t}$, so in particular $g^m \equiv 1 \pmod{p}$, so g is a primitive root mod p and $p-1|m$.

Also, $g^{\phi(p^t)} \equiv 1 \pmod{p^t}$, so $m|(p-1)p^{t-1}$. Write $m = (p-1)k$, where $k|p^{t-1}$.

Then either $k = p^{t-1}$, in which case $m = (p-1)p^{t-1} = \phi(p^t)$ and g is a primitive root of p^t , or $k|p^{t-2}$, whereupon $m|(p-1)p^{t-2}$, so $g^{(p-1)p^{t-2}} \equiv 1 \pmod{p^t}$, which contradicts part ii.

□

5.4 Non-linear congruences

Theorem 5.8 (Chevalley, 1936). *Let $f(x_1, \dots, x_n)$ be an integer polynomial of total degree d . Then, if $n > d$, the number of solutions of $f(x_1, \dots, x_n) \equiv 0 \pmod{p}$ is a multiple of p .*

Corollary 5.9. *If f has zero constant term and $n > d$, there is a solution other than $x_i \equiv 0$. For example, a quadratic form in more than two variables has a non-trivial zero \pmod{p} .*

To prove this theorem, we start with the following

Lemma 5.10. $\sum_{x=0}^{p-1} x^n \equiv 0 \pmod{p}$ for $0 \leq n < p-1$.

Proof. If $n = 0$ then the sum is equal to p , so $\equiv 0 \pmod{p}$.

Otherwise, the non-one x_i are equivalent to g^{r_i} in some order, where g is a primitive root. So

$$\sum_{i=1}^{p-1} x^n = \sum_{i=1}^{p-1} g^{nr_i} = \sum_{i=1}^{p-1} g^{n_i} = \frac{g^{np} - g^n}{g^n - 1}.$$

The numerator is $g^n((g^n)^{p-1} - 1)$, which is $\equiv 0 \pmod{p}$; the denominator is not divisible by p since $n < p-1$, so the fraction (which is an integer) is divisible by p so $\equiv 0 \pmod{p}$.

□

Proof of 5.8. $1 - f(x_1, \dots, x_m)^{p-1} \equiv 1$ if $f \equiv 0 \pmod{p}$, and 0 otherwise. So the number of solutions to the equation is

$$\sum_{x_1, \dots, x_n} [1 - f(x_1, \dots, x_n)^{p-1}] \pmod{p}.$$

Now, expand f^{p-1} to get terms of the form $cx_1^{e_1} \dots x_n^{e_n}$, of total degree $\leq d(p-1)$, which is $< n(p-1)$. So some exponent must have $e_{i_0} < p-1$.

The contribution from this term is

$$c \sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \dots \sum_{x_n=0}^{p-1} x_1^{e_1} \dots x_n^{e_n} = c \sum_{x_1=0}^{p-1} x_1^{e_1} \dots \sum_{x_n=0}^{p-1} x_n^{e_n}.$$

By the lemma, the i_0 th factor is zero modulo p , so that term contributes 0 modulo p , so the whole sum is 0 modulo p . □

6 Quadratic Residues

6.1 Solving Quadratic Equations

When can we solve $x^2 \equiv n \pmod{p}$?

It's clearly not always possible; the only remainders given by a square modulo 7 are 0, 1, 2, 4.

Definition 6.1. Let p be an odd prime. If $p \nmid n$ and $x^2 \equiv n \pmod{p}$ is solvable, we say that n is a *quadratic residue* of p . If $p \nmid n$ and the congruence is not solvable, we say n is a *quadratic non-residue*. If $p|n$, n is neither.

We summarise this definition with the *Lagrange symbol* :

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{residue} \\ -1 & \text{non-residue} \\ 0 & p|n \end{cases}$$

Note that, if $m \equiv n \pmod{p}$, $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$.

Theorem 6.2. If $p \geq 3$ then there are $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ non-residues. So $\sum_{n=1}^p \left(\frac{n}{p}\right) = 0$.

Proof. We will show that the mapping $n \rightarrow n^2$ is a bijection between the numbers between 1 and $\frac{p-1}{2}$ and the quadratic residues.

1-to-1 If $n^2 \equiv m^2 \pmod{p}$, $p|m^2 - n^2 = (m-n)(m+n)$. $m+n < p$, so we have $p|m-n$ and $m \equiv n \pmod{p}$.

onto If r is a quadratic residue then $s^2 \equiv r \pmod{p}$ for some s . $s \neq 0$ since 0 is not relevant in this context; if $s \leq \frac{p-1}{2}$ then we send s to r , if not we send $p-s$ to r . □

6.2 Ways of finding $\left(\frac{n}{p}\right)$

Theorem 6.3 (Euler's Criterion). $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}$

Proof. If $p|n$, then the left- and right-hand sides are equal.

If $n \equiv x^2 \pmod{p}$, then $p \nmid x$ and $n^{(p-1)/2} = x^{p-1} \equiv 1 = \left(\frac{n}{p}\right)$.

Now, $x^{(p-1)/2} \equiv 1$ has at most $\frac{p-1}{2}$ roots; we have found exactly that many, namely the quadratic residues, so there can be no more. And, letting $m = x^{(p-1)/2}$, we have $m^2 = x^{p-1} \equiv 1 \pmod{p}$, for which we know two roots ± 1 .

So $m \equiv \pm 1 \pmod{p}$ – and we know $m \not\equiv +1$, so $m \equiv -1 = \left(\frac{n}{p}\right)$. □

Corollary 6.4.

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

So the product of two residues or two non-residues is a residue; the product of a non-residue and a residue is a residue.

Corollary 6.5.

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv -1 \pmod{4} \end{cases}$$

So $x^2 + 1 \equiv 0 \pmod{p}$ is solvable if $p \equiv 1 \pmod{4}$, not if $p \equiv -1 \pmod{4}$.

Definition 6.6. The *least positive residue* of $m \pmod{p}$ is the unique $n \in \mathbb{N}$ with $m \equiv n \pmod{p}$ and $m < p$.

Definition 6.7. If $x \in \mathbb{R}$, define $[x] = \max\{n \in \mathbb{N} : n \leq x\}$.

Then the least positive residue of m is $m - p\left[\frac{m}{p}\right]$.

Theorem 6.8 (Gauss' Lemma). If $p \nmid n$, then $\left(\frac{n}{p}\right) = (-1)^\nu$, where ν is the number of integers in $[1, \frac{p-1}{2}]$ for which the least positive residue of mn exceeds $\frac{p}{2}$.

For example, consider $\left(\frac{4}{11}\right)$. We take $m = 1, 2, 3, 4, 5$, $mn = 4, 8, 12, 16, 20$, $mn \equiv 4, 8, 1, 5, 9$, so $\nu = 2$ and $\left(\frac{4}{11}\right) = 1$.

Proof. Consider the numbers mn , reduced to lie between $-\frac{p}{2}$ and $\frac{p}{2}$ (by subtracting p from the numbers $> \frac{p}{2}$ in the list). This produces a list of remainders $r_1, \dots, r_\mu, s_1, \dots, s_\nu$, where $0 \leq r_i, s_j < \frac{p}{2}$ and $\mu + \nu = \frac{p-1}{2}$.

If any of the r_i or s_j are zero, then $p|mn$, which is impossible since $p \nmid m$, $p \nmid n$. So $1 \leq r_i, s_j \leq \frac{p-1}{2}$.

We claim that the r_i and s_j are all different. If $r_i = r_j$ or $s_i = s_j$, then we have $mn \equiv m'n$ for some m, m' , so, since $p \nmid n$, $m \equiv m'$. If $r_i = s_j$, then

$r_i \equiv mn, p - s_j \equiv m'n$, so $mn + m'n \equiv r_i + p - s_j \equiv 0 \pmod{p}$, so $p \mid (m + m')n$, which is impossible since $p \nmid n$ and $m + m' < p$. So r_i, s_j are a rearrangement of $1 \dots \frac{p-1}{2}$.

Now,

$$\prod_{m=1}^{\frac{p-1}{2}} mn = n^{\frac{p-1}{2}} \prod_{m=1}^{\frac{p-1}{2}} m = n^{\frac{p-1}{2}} \frac{p-1}{2}! \equiv \left(\frac{n}{p}\right) \frac{p-1}{2}!$$

And

$$\prod_{m=1}^{\frac{p-1}{2}} mn \equiv \prod_{i=1}^{\mu} r_i \prod_{j=1}^{\nu} (p - s_j) \equiv \prod_{i=1}^{\mu} r_i \prod_{j=1}^{\nu} -s_j = \frac{p-1}{2}! (-1)^{\nu}.$$

$$\text{So } \left(\frac{n}{p}\right) = (-1)^{\nu}.$$

□

Corollary 6.9. 2 is a quadratic residue iff $p \equiv \pm 1 \pmod{8}$. Putting $p = 8n + r$, we have $(p^2 - 1)/8 = 8n^2 + 2nr + \frac{r^2 - 1}{8}$, so $(-1)^{\frac{p^2 - 1}{8}} = 1$ if $p \equiv \pm 1 \pmod{8}$ and $= -1$ otherwise.

Proof. Take $n = 2$ in Gauss' Lemma. So we consider the numbers $2, 4, \dots, p-1$, all of which are equal to their least positive residues, and we want to know how many of them are $> p/2$. $\nu = \frac{p-1}{2} - |\{2r \leq \frac{p}{2}\}|$; $2r \leq \frac{p}{2} \iff r \leq \frac{p}{4}$, so $\nu = \frac{p-1}{2} - [\frac{p}{4}]$.

Now run through the possible residues modulo 8.

□

6.3 Quadratic Reciprocity

Theorem 6.10 (The Law of Quadratic Reciprocity). If p, q are primes ≥ 3 , then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod{4}$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Equivalently,

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

Example 6.11.

$$\begin{aligned}
\left(\frac{1222}{907}\right) &= \left(\frac{315}{907}\right) \\
&= \left(\frac{3}{907}\right)^2 \left(\frac{5}{907}\right) \left(\frac{7}{907}\right) \\
&= 1 \cdot \left(\frac{907}{5}\right) \cdot - \left(\frac{907}{7}\right) \\
&= \left(\frac{2}{5}\right) \cdot - \left(\frac{4}{7}\right) \\
&= \left(\frac{2}{5}\right) \cdot - \left(\left(\frac{2}{7}\right) \cdot \left(\frac{2}{7}\right)\right) \\
&= \left(\frac{2}{5}\right) \cdot -1 \\
&= +1
\end{aligned}$$

since $5 \not\equiv \pm 1 \pmod{8}$.

Lemma 6.12. Let p, q be distinct odd primes, $p = 2p' + 1$, $q = 2q' + 1$.

Write $S(q, p) = \sum_{n=1}^{p'} \left[\frac{nq}{p}\right]$ and $S(p, q) = \sum_{m=1}^{q'} \left[\frac{mp}{q}\right]$.

Then $S(p, q) + S(q, p) = p'q'$.

Proof. Note that $[x] = \sum_{m \leq x} 1$ for $x \geq 0$.

$$S(q, p) = \sum_{n \leq p'} \sum_{m \leq \frac{nq}{p}} 1.$$

Now, $m \leq \frac{nq}{p} \leq \frac{p'q}{p} < \frac{pq}{2p} = \frac{q}{2}$, so $m \leq q'$. So $S(q, p)$ is counting the pairs (n, m) with $n \leq p'$, $m \leq q'$, and $mp \leq nq$. Similarly, $S(p, q)$ is counting the pairs (n, m) with $n \leq p'$, $m \leq q'$, and $mq \leq np$.

So $S(p, q) + S(q, p)$ is counting all the pairs; and none of them are counted twice, since $mp = nq \implies p|n$, which is impossible since $n \leq p' < p$. So $S(p, q) + S(q, p) = p'q'$. \square

6.4 Proof of Quadratic Reciprocity

We apply Gauss' Lemma to $\left(\frac{q}{p}\right)$. Consider nq for $1 < n \leq p'$; these can be written $nq = p\left[\frac{nq}{p}\right] + u_n$ for $1 \leq u_n < p$, and Gauss' Lemma gives us $\left(\frac{q}{p}\right) = (-1)^\nu$, where ν of the u_n are $> p/2$.

We use the notation from the proof of the lemma : $u_n = r_i$ (μ times), and $u_n = p - s_i$ (ν times).

Now,

$$\sum_{n=1}^{p'} u_n = \sum r_i + \sum (p - s_i);$$

working mod 2, this is $\sum r_i + \nu + \sum s_j$. Recalling that the r_i and s_j together cover the whole of $1 \dots p'$, we have $\sum u_n \equiv \nu + \sum_{i=1}^{p'} i \equiv \nu + \frac{p'(1+p')}{2} \pmod{2}$.

On the other hand,

$$\sum_{i=1}^{p'} nq = q \sum_{i=1}^{p'} i = \sum_{i=1}^{p'} p \left[\frac{nq}{p} \right] + u_n = pS(q, p) + \sum_{i=1}^{p'} u_n \equiv S(q, p) + \sum_{i=1}^{p'} i + \nu.$$

So $(q-1) \sum_{i=1}^{p'} i \equiv S(q, p) + \nu$. q is odd, so $S(q, p) + \nu$ is even, so $S(q, p)$ and ν are of the same parity, so $\left(\frac{q}{p}\right) = (-1)^{S(q, p)}$.

So

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{S(q, p)S(p, q)} = (-1)^{p'q'}$$

which is the Quadratic Reciprocity Theorem

7 Writing numbers as sums of squares

$1 = 1^2$, $2 = 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $4 = 2^2$, $5 = 2^2 + 1^2$, $6 = 2^2 + 1^2 + 1^2$, $7 = 2^2 + 1^2 + 1^2 + 1^2$, $8 = 2^2 + 2^2 \dots$

It appears that four squares are enough, and there are clearly numbers which can't be written as a sum of less than four squares.

Now, considering norms in \mathbb{C} is probably the easiest way to establish that

$$(x^2 + y^2)(z^2 + t^2) = (xz - yt)^2 + (xt + yz)^2.$$

So, if a and b can be written as a sum of two squares, so can ab . Clearly the sum of two squares is equal to 0, 1 or 2 (mod 4), so $a \equiv 3 \pmod{4}$ is out of the question.

7.1 Two squares

Theorem 7.1. *Suppose $n \in \mathbb{N}$ and $n \mid N^2 + 1$. Then $\exists a, b \in \mathbb{N}$ with $a \equiv Nb \pmod{n}$ and $n = a^2 + b^2$.*

We will need quite a bit of mechanics to prove this result, so observe first that it implies

Corollary 7.2 (Fermat, 1670). *If p is prime, $p \equiv 1 \pmod{4}$, then p can be written as a sum of two squares*

Proof. If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = +1$, so there is an N with $N^2 \equiv -1 \pmod{p}$, so theorem 7.1 applies. \square

To begin the proof, we need the following result:

Theorem 7.3 (Dirichlet's Approximation Theorem). Let $x \in \mathbb{R}$ and $l \in \mathbb{N}$. Then $\exists u \in \mathbb{Z}$ and $v \in \mathbb{N}$ with $v \leq l$ and $|x - \frac{u}{v}| \leq \frac{1}{v(l+1)}$.

Proof. Consider the $l+1$ complex numbers $y_v = \exp(2\pi i v x)$, where $v \in [0 \dots l]$. These lie on the unit circle.

Since there are $l+1$ of them, there are two with argument differing by $\leq \frac{2\pi}{l+1}$, by the pigeonhole principle. Call these y_v and $y_{v'}$ with $v > v'$.

So $|2v x \pi - 2v' x \pi - 2u \pi| \leq \frac{2\pi}{l+1}$ for some $u \in \mathbb{Z}$. Put $v_2 = v - v'$, a number between 1 and l . So $|2\pi v_2 x - 2\pi u| \leq \frac{2\pi}{l+1}$.

So

$$\left| x - \frac{u}{v_2} \right| \leq \frac{1}{v_2(l+1)}.$$

□

Proof of theorem 7.1. Take $x = \frac{N}{n}$, $l = \lfloor \sqrt{n} \rfloor$.

So $\exists b, c \in \mathbb{Z}$, with $0 < b \leq l$ and $|\frac{N}{n} - \frac{c}{b}| \leq \frac{1}{b(l+1)}$.

But $\sqrt{n} < l+1$, so $\frac{N}{n} - \frac{c}{b} < \frac{1}{b\sqrt{n}}$.

Now set $a = Nb - nc$; $a \equiv Nb \pmod{n}$, and

$$a^2 + b^2 \equiv N^2 b^2 + b^2 \equiv b^2(N^2 + 1) \equiv 0 \pmod{n}.$$

But a and b are quite small;

$$\frac{N}{n} - \frac{c}{b} = \frac{Nb - nc}{nb} = \frac{a}{nb} < \frac{1}{b\sqrt{n}}.$$

so $|a| < \sqrt{n}$, and $|b| < \sqrt{n}$ by definition. So $a^2 + b^2 < 2n$, and is a multiple of n , and is > 0 . So $a^2 + b^2 = n$.

□

Theorem 7.4. If $p \equiv 1 \pmod{4}$ is a sum of two squares, the representation $p = a^2 + b^2$ is essentially unique

Proof. Let $p = a^2 + b^2 = c^2 + d^2$. One of a and b is even, the other odd, and similarly for c and d ; WLOG, a, c are even and b, d odd, with $a > c$ and $b < d$.

So $(a - c, b + d) = 2s$ and $(a + c, d - b) = 2t$. Explicitly, $a - c = 2sA, b + d = 2sB, a + c = 2tC, d - b = 2tD$.

$a^2 - c^2 = d^2 - b^2$, so $4stAC = 4stBD$ and $AC = BD$. $(A, B) = 1$ and $(C, D) = 1$, so $A|BD \implies A|D$; similarly, $D|A$, and $A, D > 0$. So $A = D$ and $B = C$.

So $2a = 2sA + 2tC, 2b = 2sB - 2tD$. So

$$\begin{aligned} p = a^2 + b^2 &= (sA + tC)^2 + (sB - tD)^2 = (sA + Bt)^2 + (Bs - At)^2 \\ &= (A^2 + B^2)(s^2 + t^2) \end{aligned}$$

which is a contradiction, since p is prime and $A, B, s, t > 0$.

□

This means that, if you can write n as a sum of two squares in two different ways, n is composite and can be factored in the following way :

$5141 = 71^2 + 10^2 = 55^2 + 46^2$, so $a = 46, b = 55, c = 10, d = 71$. So $(a - c, b - d) = (36, 126) = 18 = 2 \cdot 9$, so $s = 9$. And $(a + c, d - b) = (56, 16) = 8 = 2 \cdot 4$, so $t = 4$. So $s^2 + t^2 | 5141$, so $97 | 5141$, and $5141 = 53 \cdot 97$.

Theorem 7.5. n is representable as a sum of two squares iff every primes $p \equiv 3 \pmod{4}$ in the factorisation of n appears to an even power.

Proof. One direction is easy : if

$$n = 2^e p_1^{e_1} p_2^{e_2} \dots q_1^{2f_1} q_2^{2f_2} \dots,$$

with $p_i \equiv 1 \pmod{4}$ and $q_i \equiv 3 \pmod{4}$, then we have

$2 = 1^2 + 1^2$, $p_i = a_i^2 + b_i^2$, $q_j^2 = q_j^2 + 0^2$. So n is a product of sums of two squares, so itself a sum of two squares.

For the other way, suppose $a^2 + b^2 = q^g m$, with $q \nmid m$ and $q \equiv 3 \pmod{4}$. Assume g is odd, $g = 2f + 1$. There are two cases :

i If $q^{f+1} | a$, then $q^{2f+1} | a^2$ and so $q^{2f+1} | b^2$. Now, this is an odd power dividing a square, so in fact $q^{2f+2} | b^2$, and $q^{2f+2} | a^2$. So $q^{2f+2} | a^2 + b^2 = q^{2f+1} m$, so $q | m$, which is a contradiction.

ii If $(q^{f+1}, a) = q^g$ for $g \leq f$, we have $q^{2g} | q^{2f+1} m$, and $q^{2g} | a^2$, so $q^{2g} | b^2$ so $q^g | b$.

Put $a = \alpha q^g$, $b = \beta q^g$. Then $\alpha^2 + \beta^2 = q^{2f-2g+1} m$. So $q | \alpha^2 + \beta^2$. But $q \nmid \alpha$, so $\exists \gamma : \alpha \gamma \equiv 1 \pmod{q}$. So $\gamma^2 (\alpha^2 + \beta^2) \equiv 0 \equiv 1 + (\beta \gamma)^2 \pmod{q}$.

But $\left(\frac{-1}{q}\right) = -1$, since $q \equiv 3 \pmod{4}$. So there's a contradiction there.

So g is even. □

7.2 Primes of the form $x^2 + 5y^2$

Working mod 4 and mod 5, we have $p = x^2 + 5y^2 \implies p \equiv \pm 1 \pmod{5}$ and $p \equiv 1 \pmod{4}$, so either $p = 5$ or $p \equiv 1, 9 \pmod{20}$.

These congruences are necessary, but they are in fact also sufficient :

$p = 5$ clearly works. If $p \equiv 1, 9 \pmod{20}$, then

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (+1) \left(\frac{p}{5}\right) = 1,$$

since $p \equiv 1$ or $4 \pmod{5}$.

So $\exists n : n^2 + 5 \equiv 0 \pmod{p}$.

By Dirichlet's Theorem, there exist c, y with $|\frac{n}{p} - \frac{c}{y}| \leq \frac{1}{y(1+l)}$ and $y \in [1, l]$.

Let $x = cy - np$, so $\frac{x}{py} \leq \frac{1}{y(l+1)}$. Moreover, $x^2 + 5y^2 \equiv (Ny)^2 + 5y^2 \equiv y^2(n^2 + 5) \equiv 0 \pmod{p}$.

So $x^2 + 5y^2 = kp$, and $0 < kp \leq \left(\frac{p}{l+1}\right) + 5l^2$. Essentially, the right-hand side has a minimum at $l = \frac{\sqrt{p}}{\sqrt[3]{5}}$.

So let $l = \lfloor p^{1/2}5^{-1/4} \rfloor$, so $l + 1 > p^{1/2}5^{-1/4}$.

So $\left(\frac{p}{l+1}\right)^2 + 5l^2 < \frac{p^2}{p/\sqrt{5}} + \frac{5p}{\sqrt{5}} = 2p\sqrt{5}$, and so k is between 0 and $2\sqrt{5}$.

So $k = 1, 2, 3, 4$. $k = 2$ and $k = 3$ are ruled out by considering the equation modulo 5; if $x^2 + 5y^2 = 4p$, then $4|x^2 + 5y^2$, so x and y are both even (work modulo 4; were x and y both odd, $x^2 + 5y^2 \equiv 2 \pmod{4}$). So halve them to get a solution to $x^2 + 5y^2 = p$.

The problem's not always that easy; there are no necessary and sufficient conditions using only congruences for $p = x^2 + 14y^2$.

7.3 Sums of three squares

There is no nice multiplication identity; $3 \in S_3$, $5 \in S_3$ but $15 \notin S_3$.

Theorem 7.6 (Legendre, 1798). $n \in \mathbb{N}$ is a sum of three or fewer squares iff n is not of the form $4^k(8l + 7)$.

It's easy to prove that you can't write n of that form as a sum of three squares; the proof the other direction is too hard for this course, and also for Legendre.

7.4 Sums of four squares

Theorem 7.7 (Lagrange, 1770). Every positive integer is a sum of 4 squares

We start off with a useful lemma due to Euler :

Lemma 7.8.

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (z_1^2 + z_2^2 + z_3^2 + z_4^2),$$

where

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$

$$z_2 = x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3$$

$$z_3 = x_1y_3 - x_3y_1 - x_4y_2 + x_2y_4$$

$$z_4 = x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2$$

Proof. As a cop-out, I could suggest evaluating both sides and showing that they're equal. Alternatively, use the representation of the quaternions as 2×2 matrices over \mathbb{C} :

$$\begin{pmatrix} \alpha_1 & -\alpha_2 \\ \bar{\alpha}_2 & \bar{\alpha}_1 \end{pmatrix} \begin{pmatrix} \beta_1 & -\beta_2 \\ \bar{\beta}_2 & \bar{\beta}_1 \end{pmatrix} = \begin{pmatrix} \gamma_1 & -\gamma_2 \\ \bar{\gamma}_2 & \bar{\gamma}_1 \end{pmatrix}$$

where $\gamma_1 = \alpha_1\beta_1 - \alpha_2\bar{\beta}_2$ and $\gamma_2 = \bar{\alpha}_2\beta_1 + \alpha_1\bar{\beta}_2$; put $\alpha_1 = x_1 + ix_2$, $\alpha_2 = x_3 + ix_4$, $\beta_1 = y_1 + iy_2$, $\beta_2 = y_3 + iy_4$, $\gamma_1 = z_1 + iz_2$, $\gamma_2 = z_3 + iz_4$ with x_i, y_i, z_i as in the statement of the problem, and note that the determinants of the matrices are respectively $\sum x_i^2$, $\sum y_i^2$ and $\sum z_i^2$. \square

So, to prove Lagrange's theorem, we need to prove it for prime numbers not equal to 2.

Lemma 7.9. *If $p \geq 3$ is prime, then $\exists x, y$ with $p|1 + x^2 + y^2$.*

Proof. This is automatic by Chevalley's Theorem. Alternatively, let x run through the numbers from 0 to $\frac{p-1}{2}$. Then x^2 are distinct mod p , so $-(x^2 + 1)$ are also distinct, and there are $\frac{p+1}{2}$ of these.

Similarly, let y run through $0 \dots \frac{p-1}{2}$. These all have distinct squares, and there are $\frac{p+1}{2}$ of those. But there are only p residue classes in total, and $p + 1$ elements in the union of the sets. So there's an overlap somewhere.

So $-1 - x^2 \equiv y^2 \pmod{p}$ has a solution, which is a solution to $1 + x^2 + y^2 \equiv 0 \pmod{p}$ also. \square

Proof of theorem 7.7. Take p an odd prime, and x, y with $p|1 + x^2 + y^2$. $x, y < \frac{p}{2}$, so $x^2 + y^2 + 1 = kp \leq \frac{p^2}{2} + 1 < p^2$. So $k < p$.

Let k_0 be the least number such that k_0p is a sum of four squares. It's defined (since k would work), and in $[1, p]$.

Now, k_0 is odd. For, if $k_0 = 2k_1$, we have $2k_1p = a^2 + b^2 + c^2 + d^2$. Arrange these with $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2}$, and notice that

$$k_1p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$$

with $k_1 < k_0$. But k_0 was minimal. So k_0 is odd.

So we have $k_0p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ with $k_0 < p$ and odd. Choose b_i with $x_i = y_i + k_0b_i$, so $x_i \equiv y_i \pmod{k_0}$, and $-\frac{k_0}{2} < y_i \leq \frac{k_0}{2}$. Since k_0 is odd, $|y_i| < \frac{k_0}{2}$. If all the y_i are zero, $k_0|x_i$ for each i , so $k_0^2|x_i^2$, so $k_0^2|k_0p$. So $k_0|p$, and $k_0 = 1$.

If not, at least one of them is non-zero, $\sum y_i^2 > 0$. Also, $\sum y_i^2 < \sum \frac{k_0^2}{4} < k_0^2$. And $x_i \equiv y_i \pmod{k_0}$, so $\sum y_i^2 \equiv \sum x_i^2 \equiv 0 \pmod{k_0}$. So

$$\sum y_i^2 = k_0k_1, 0 < k_1 < k_2.$$

Now use lemma 7.8 to write $\sum x_i^2 \sum y_i^2 = \sum z_i^2$. It emerges (since $x_i \equiv y_i$), that each of the $z_i \equiv \sum y_i^2 \pmod{k_0}$, and in fact are zero mod k_0 . So we can divide through by k_0^2 , to get

$$pk_1 = \sum_{i=1}^4 \left(\frac{z_i}{m_0}\right)^2.$$

So k_0 isn't minimal. This is a contradiction, so all the y_i must be zero, so $k_0 = 1$. \square

8 Irrational numbers and approximations by rationals

Theorem 8.1. *Let $f(x) \in \mathbb{Z}(x)$ be a monic polynomial. Then any rational root is an integer which divides the constant term of f .*

Proof. $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$. $f(\frac{u}{v}) = 0$, with $(u, v) = 1$. We need to show that $v = 1$ and $u|a_0$.

Multiply through by v^n to get $u^n + a_{n-1}u^{n-1}v + \dots + a_0v^n = 0$. v clearly divides all but the first term of this, so $v|u^n$. But $(u, v) = 1$, so $v = 1$.

Similarly, $u|a_0v^n$, since it divides all the other terms, so $u|a_0$. □

So non-trivial algebraic numbers are irrational.

8.1 Some irrational numbers

Theorem 8.2. $\log_{10}(n)$ is irrational unless $n = 10^\alpha$ for $\alpha \in \mathbb{Z}$.

Proof. Suppose $\log_{10}(n) = \frac{a}{b}$. Then $n = 10^{a/b}$, so $n^b = 10^a$. Now compare prime factors for a contradiction. □

Theorem 8.3 (Lambert, 1761). e is irrational

Proof. $e = 2 + \frac{1}{2!} + \frac{1}{3!} + \dots$; suppose $e = \frac{m}{n}$ with $(m, n) = 1$.

If $n \geq 1$, then

$$n!e = 2n! + \frac{n!}{2!} + \frac{n!}{3!} + \dots + s + t$$

where $s = \frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} \dots$ is an integer, and t is strictly positive and < 1 by comparison with the geometric progression $(n+1)^{-1} + (n+1)^{-2} \dots$

So $n!e - s \in \mathbb{Z}$, but also $n!e - s \in (0, 1)$. But there are no integers strictly between 0 and 1, so this is a contradiction □

Theorem 8.4 (Lambert, 1761). π is irrational

His proof was rather fiddly; what we're giving here is a much later proof of the irrationality of π^2 .

Proof due to Niven, 1947. Suppose $\pi^2 = \frac{a}{b}$, with $(a, b) = 1$, and $a, b \in \mathbb{N}$.

We define

$$f(x) = \frac{x^n(1-x)^n}{n!} = \frac{1}{n!} \sum_{i=n}^{2n} c_i x^i.$$

So

$$f^{(m)}(0) = \begin{cases} 0 & m < n, m > 2n \\ \frac{m!}{n!} c_m \in \mathbb{Z} & m \in [n, 2n] \end{cases}$$

$f(x) = f(1-x)$, so the same thing happens at $x = 1$. Define

$$G(x) = b^n(\pi^{2n}f(x) - \pi^{2n-2}f^{(2)}(x) + \pi^{2n-4}f^{(4)}(x) \dots).$$

Putting $x = 0$, and noting that $b^n\pi^{2k} = b^{n-k}a^k \in \mathbb{Z}$, we have $G(0) \in \mathbb{Z}$, $G(1) \in \mathbb{Z}$.

Now,

$$\frac{d}{dx}(G' \sin \pi x - \pi G \cos \pi x) = G'' \sin \pi x + G' \pi \cos \pi x - G' \pi \cos \pi x + \pi^2 G \sin \pi x.$$

But

$$G'' + \pi^2 G = b^n \pi^{2n+2} f(x) = \pi^2 a^n f(x)$$

since all the other terms cancel. So

$$\int_0^1 \pi a^n f(x) \sin \pi x = \left[\frac{1}{\pi} (G'(x) \sin \pi x - \pi G \cos \pi x) \right]_0^1 = G(1) + G(0).$$

since $\sin \pi x$ vanishes at the endpoints. This is an integer.

But $f(x) \in (0, \frac{1}{n!})$, and $\sin \pi x \in [0, 1]$. So the integral is $\leq \frac{\pi a^n}{n!}$, which tends to 0 as $n \rightarrow \infty$, and so is < 1 for n large enough. So it's not an integer. This is the desired contradiction. \square

8.2 Approximations by rationals

\mathbb{Q} is dense in \mathbb{R} , so $x \in \mathbb{R} \implies \exists$ a sequence of rationals tending to x . We ask how close you can get with a restricted denominator.

By Dirichlet's theorem, $x \in \mathbb{R}$, $q \in \mathbb{N} \implies \exists a \in \mathbb{Z}, p \in [1, q] \cap \mathbb{N}$, with $|x - \frac{a}{p}| < \frac{1}{p(q+1)} < \frac{1}{p^2}$.

This isn't a very exciting result for rationals, since you could simply take $\frac{a}{p} = x$.

If $\frac{a}{q} \neq \frac{u}{v}$, $|\frac{u}{v} - \frac{a}{q}| = |\frac{uq - av}{vq}|$. $uq - av \neq 0 \implies |\frac{u}{v} - \frac{a}{q}| \geq \frac{1}{vq} \implies q \leq v$.

This suggests the following theorem :

Theorem 8.5. $x \in \mathbb{Q}$ has only finitely many good rational approximations; x irrational has infinitely many.

8.3 Transcendental numbers

Theorem 8.6 (Liouville). Let α be an irrational root of a polynomial over \mathbb{Z} of degree n . Then there is a constant c , depending on the polynomial, such that

$$|\alpha - \frac{p}{q}| \geq \frac{c(f)}{q^n} \forall p \in \mathbb{Z}, \forall q \in \mathbb{N}.$$

Definition 8.7. $\alpha \in \mathbb{C}$ is *transcendental* iff there is no polynomial over \mathbb{Z} of which α is a root.

Theorem 8.8. $x = 10^{-1!} + 10^{-2!} + 10^{-3!} \dots$ is transcendental.

Proof. x is clearly irrational, since its decimal expansion never repeats. Suppose $f(x) = 0$ for some polynomial in x of degree n . Then $\exists c > 0 : |\alpha - \frac{p}{q}| > \frac{c}{q^n}$.

But, if you take $q = 10^{k!}$ and $a = 10^{k!}(10^{-1!} + 10^{-2!} + \dots + 10^{-k!})$, you find an approximation with

$$\begin{aligned} \left| \alpha - \frac{q}{a} \right| &= 10^{-(k+1)!} + 10^{-(k+2)!} \dots \\ &< 10^{-(k+1)!}(1 + 10^{-1} + 10^{-2} \dots) \\ &= \frac{10}{9} 10^{-(k+1)!} = \frac{10}{9} q^{-(k+1)} \end{aligned}$$

Taking k large enough makes it impossible for α to be a root of a polynomial of any degree. □

Theorem 8.9 (Roth, 1955). Let $f(x) \in \mathbb{Z}[x]$ be non-constant with an irrational root. Then

$$\exists c(f, \epsilon) : \left| \alpha - \frac{p}{q} \right| \geq \frac{c(f, \epsilon)}{q^{2+\epsilon}}.$$

This improves q^n to $q^{2+\epsilon}$ in Liouville's theorem; it is a best possible result, since there are infinitely many approximations to (say) $\sqrt{2}$ with error $\leq \frac{1}{q^2}$. The proof is difficult.

9 Diophantine equations

These were studied by Diophantus, around 250AD.

Definition 9.1. A *Diophantine equation* is a polynomial equation with integer coefficients, usually in several variables, to be solved in the integers or over \mathbb{Q} .

Probably the most famous Diophantine equation is Fermat's Last Theorem. There is no general theory of Diophantine equations; we've already met two, namely the equations $x^2 + y^2 = n$ and $x^2 + y^2 + z^2 + t^2 = n$. We'll go through a number of Diophantine equations to find methods that come in useful in general.

9.1 $x^3 + 2y^3 = 13$: Congruences

We work modulo 9; $x^3 \equiv 0, \pm 1 \pmod{9}$, so $x^3 + 2y^3 \equiv 0, 1, 8, 2, 3, 1, 6, 7, 8 \pmod{9}$. In particular, $x^3 + 2y^3 \not\equiv 4 \pmod{9}$, so the value 13 is impossible.

9.2 $x^3 + 2y^3 = 4z^3$: Least counterexample

If $z = 0$ then either $x = y = 0$ or $\frac{x^3}{y^3} = -2$, the latter of which is impossible. So we look for a solution with $z \neq 0$.

Take a solution with minimal value of $|z|$. Then $2|4z^3 = x^3 + 2y^3$, so $2|x^3$, so $2|x$, so $x = 2X$.

So $8X^3 + 2y^3 = 4z^3$, so $4X^3 + y^3 = 2z^3$, so $2|y^3$, so $2|y$, so $y = 2Y$.

So $4X^3 + 8Y^3 = 2z^3$, so $2X^3 + 4Y^3 = z^3$, so $2|z^3$, so $2|z$, so $z = 2Z$.

So $2X^3 + 4Y^3 = 8Z^3$, so $X^3 + 2Y^3 = 4Z^3$, with $Z = z/2$. But z was supposed to be minimal and non-zero, so this is impossible.

9.3 $x^2 = y^3 + 7$: Using quadratic residues

Theorem 9.2. $x^2 = y^3 + 7$ has no solutions

Proof. If $2|y$ then $8|y^3$, so $x^2 \equiv 7 \pmod{8}$, which is impossible. So y is odd, so x is even.

If $y \equiv 3 \pmod{4}$ then $x^2 = y^3 + 7 \equiv 2 \pmod{4}$ – which is also impossible. So $y \equiv 1 \pmod{4}$.

But $x^2 + 1 \equiv y^3 + 8 = (y+2)(y^2 - 2y + 4)$. $y+2$ is odd, so, letting p be any prime divisor of $y+2$, we have $p|x^2 + 1$, so $\left(\frac{-1}{p}\right) = +1$, so $p \equiv 1 \pmod{4}$.

So $y+2$ is entirely a product of primes of the form $4k+1$, so $y+2 \equiv 1 \pmod{4}$ provided that it's positive. But $y \equiv 1 \pmod{4}$, so $y+2 < 0$, so $y < -2$, so $y^3 < -8$, so $y^3 + 7 < -1$, so can't possibly be a square \square

9.4 $x^2 + y^2 = z^2$

Theorem 9.3. If $x^2 + y^2 = z^2$ with $x, y, z \in \mathbb{N}$, then there exist $a, b, c \in \mathbb{N}$ such that either (x, y, z) or (y, x, z) are of the form $(a(b^2 - c^2), 2abc, a(b^2 + c^2))$.

Proof. Obviously, anything of that form satisfies $x^2 + y^2 = z^2$.

For the converse, let $a = (x, y)$. Then $a^2|x^2 + y^2 = z^2$, so $a|z$. Put $x = aX, y = aY, z = aZ$.

So $X^2 + Y^2 = Z^2$, with $(X, Y) = 1$. So X and Y aren't both even, and, were they both odd, we'd have $Z^2 \equiv 2 \pmod{4}$. So, WLOG, X is odd and Y is even, so Z is odd.

So $\frac{X+Z}{2}$ and $\frac{X-Z}{2}$ are integral and coprime, so $\frac{Y^2}{4} = \frac{X+Z}{2} \frac{X-Z}{2}$. Multiplying through by 4, we have that $X+Z$ and $X-Z$ have product a square; being coprime, they must both be squares. Call them b^2 and c^2 to get the form above. \square

9.5 $x^4 + y^4 = z^4$

Theorem 9.4. $x^4 + y^4 = z^4$ has no solutions in \mathbb{N}

The proof of this theorem uses infinite descent, otherwise known as least-counterexample or backwards induction.

Proof. Suppose $(x, y) = d > 1$. Then $d^4 | x^4 + y^4 = z^2$, so $d^2 | z$. So

$$\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{z}{d^2}\right)^2.$$

So we may take $(x, y) = 1$.

Then $(x^2)^2 + (y^2)^2 = z^2$. Using the general solution for the order-2 equation, we have $x^2 = b^2 - c^2$, $y^2 = 2bc$, $z^2 = b^2 + c^2$ with b, c coprime and of opposite parity.

If b is even, c is odd, and then $x^2 \equiv 3 \pmod{4}$. So b is odd, c is even, and $y^2 = 2bc$ is even, so y is even.

Now, $(\frac{y}{2})^2 = \frac{bc}{2}$. b and $\frac{c}{2}$ are coprime, their product is a square, so they are both squares. $b = B^2$, $\frac{c}{2} = C^2$. So $\frac{y}{2} = BC$, $x^2 = b^2 - c^2$, so $b^2 = x^2 + c^2 = x^2 + 4C^4 = B^4$. So $z = B^4 + 4C^4$.

Now, $(B^2)^2 = (x^2 + (2C^2)^2)$ with $(B^2, 2C^2) = (b, c) = 1$. So $B^2 = u^2 + v^2$, and either $x = u^2 - v^2$, $C^2 = uv$ or $x = 2uv$, $2C^2 = u^2 - v^2$.

But $2C^2$ is even, so B^2 is odd, so x is odd. So $x = u^2 - v^2$, $C^2 = uv$, with u, v coprime with opposite parities. So we can put $u = m^2$, $v = n^2$. So $B^2 = m^4 + n^4$ with $B < z$. So we can go on down forever. \square

A very similar proof to that one gives that $X^4 + 4Y^4 = Z^4$ has no solutions in \mathbb{N} .

9.6 Pell's equation

Pell's equation is $x^2 - Dy^2 = 1$ with $x, y \in \mathbb{N}$ and a fixed $D \in \mathbb{N}$.

If $D = d^2$, we have $(x - dy)(x + dy) = 1$, so $x = 1$, $y = 0$.

Theorem 9.5. *Given $D \in \mathbb{N}$ not a square, and x_0, y_0 with $x_0^2 - Dy_0^2 = 1$, y_0 minimal non-zero, all solutions to Pell's equation are of the form $x + y\sqrt{D} = (x_0 + y_0\sqrt{D})^n$.*

Proof. Define $N : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ as $N(a, b) = a^2 - Db^2$ - this is the norm function. Then $(a + b\sqrt{D})(c + d\sqrt{D}) = e + f\sqrt{D} \implies e = ac + Dbd, f = bc + ad$.

So $N(a, b)N(c, d) = N(e, f)$.

It's now fairly clear that, for any solution (x, y) , $N(x, y) = N(x_0, y_0)^n = 1$. The hard bit is proving that those are the only solutions.

Let x, y be a solution. Note that $x_0, y_0 \in \mathbb{N}$, so $x_0 + y_0\sqrt{D} > 1$. So

$$\exists n > 0 : (x_0 + y_0\sqrt{D})^n \leq x + y\sqrt{D} \leq (x_0 + y_0\sqrt{D})^{n+1}.$$

Now, consider $(x + y\sqrt{D})(x_0 - y_0\sqrt{D})^n = a + b\sqrt{D}$ for some $a, b \in \mathbb{Z}$. $N(a, b) = 1$, so $a^2 - bD^2 = 1$. $(x_0 + y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = x_0^2 - Dy_0^2 = 1$, so $x_0 - y_0\sqrt{D} > 0$.

So

$$\begin{aligned} (x_0 + y_0\sqrt{D})^n (x_0 - y_0\sqrt{D})^n &\leq (x + y\sqrt{D})(x_0 - y_0\sqrt{D})^n \\ &\leq (x_0 + y_0\sqrt{D})^{n+1} (x_0 - y_0\sqrt{D})^n. \end{aligned}$$

Divide through to get $1 \leq a + b\sqrt{D} < x_0 + y_0\sqrt{D}$. So either $a + b\sqrt{D} = 1$, or it leads to a solution less than the minimal one.

$$(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 = 1; a + b\sqrt{D} \geq 1, \text{ so } 0 < a + b\sqrt{D} \leq 1.$$

In particular, we have $a - b\sqrt{D} \leq 1 < a + b\sqrt{D}$, so $b \geq 0$. $a - b\sqrt{D} > 0$, so $a > 0$. If $b > 0$, then $b \geq y_0$ to avoid violating minimality, so $a^2 = 1 + b\sqrt{D} \geq 1 + y_0^2 D = x_0 D$, making $a \geq x_0$. But the last inequality was strict.

So $a = 1, b = 0$.

□

So we know how to find a complete set of solutions given one. But we haven't yet proved that there is one - which is what the next theorem is for.

Theorem 9.6. *If $D \in \mathbb{N}$ is not a square, $x^2 - Dy^2 = 1$ has solutions in integers.*

This is not an obvious theorem; for $D \leq 50$, there are 43 non-square numbers, only 41 of which have solutions to this with $y < 1000$. With $D = 151$, the minimal solution is $x = 1728148040, y = 140634693$. Nonetheless, it's true.

Lemma 9.7. *There are infinitely many solutions to $|x^2 - Dy^2| < 1 + 2\sqrt{D}$ with x, y coprime*

Proof. Suppose the set of solutions S were finite.

For each solution (except for the trivial one $(1, 0)$), $\frac{x}{y} \in \mathbb{Q}$, whilst $\sqrt{D} \notin \mathbb{Q}$. So $|\sqrt{D} - \frac{x}{y}|$ is strictly positive $\forall x, y \in S$.

Choose $L \in \mathbb{N}$ with $|\sqrt{D} - \frac{x}{y}| \geq \frac{1}{L}$ for all the solutions. Now apply theorem 7.3 (Dirichlet's approximation theorem) to get $u, v \in \mathbb{N}$ with $v \leq L, \sqrt{D} - \frac{u}{v} \leq \frac{1}{v(L+1)} < \frac{1}{L}$, u, v coprime, and $(u, v) \notin S$ by definition of L .

But $|\sqrt{D} - \frac{u}{v}| \leq \frac{1}{v^2}$ since $v < L$, so

$$|\sqrt{D} - \frac{u}{v}| = |2\sqrt{D} + (\frac{u}{v} - \sqrt{D})| \leq 2\sqrt{D} + |\sqrt{D} - \frac{u}{v}| \leq 2\sqrt{D} + 1.$$

So

$$|D - \frac{u^2}{v^2}| = (\sqrt{D} - \frac{u}{v})(\sqrt{D} + \frac{u}{v}) \leq \frac{2\sqrt{D} + 1}{v^2}.$$

So $v^2 D - u^2 < 2\sqrt{D} + 1$, so (u, v) satisfies the conditions to be in S but isn't there - but S contains all the solutions. Contradiction. □

Proof of theorem 9.6. By the lemma, there is at least one k such that $x^2 - Dy^2 = k$ has infinitely many solutions with $(x, y) = 1$.

We divide these solutions into k^2 classes according to the residues of x and y modulo k ; at least one of these classes must be infinite, so in particular it must have ≥ 2 elements. So take different solutions (x, y) and (x', y') in the same class; $x, x' \equiv i \pmod{k}, y, y' \equiv j \pmod{k}$.

$$((xx' - Dyy')^2 - D(xy' - yx')^2) = (x^2 - Dy^2)(x'^2 - Dy'^2) = k^2.$$

$xy' - yx' \equiv ij - ji = 0 \pmod{k}$, and $xx' - Dyy' \equiv i^2 - Dj^2 \equiv x^2 - Dy^2 \equiv 0 \pmod{k}$. So, writing $xx' - Dyy' = kx^*$ and $xy' - yx' = ky^*$, we have $x^{*2} - Dy^{*2} = 1$.

So we've got a solution, unless $y^* = 0$. But, in that case, $xy' = yx'$. But x and y are coprime, so $y|xy' \implies y|y'$. The same argument gives $y'|y$, so $y = y'$, and also $x = x'$ - but we chose them to be different. So the argument can't fail in that way □

That result is very nearly a constructive argument, given an algorithm for finding the approximation whose existence is known from Dirichlet's lemma.

On the other hand, there are better algorithms for this problem, involving the continued-fraction expression of the square root.

9.7 Mordell's Equation

Mordell's Equation is $x^2 + k = y^3$ for $x, y \in \mathbb{Z}$ and k given.

We've already demonstrated that there are no solutions for $k = 7$ (in theorem 9.2). It turns out there are finitely many solutions for each k , and Baker has produced what must be one of the most useless theorems ever :

Theorem 9.8 (Baker's Bound). *If $x^2 + k = y^3$, then*

$$\max(|x|, |y|) < \exp(10^{10}|k|^{10000}).$$

Fermat proved that $x^2 + 2 = y^3$ has solution $x = \pm 5, y = 3$, and that $x^2 + 4 = y^3$ has solutions $x = \pm 2, y = 2$ and $x = \pm 11, y = 5$. We'll prove

Theorem 9.9. *$x^2 + 1 = y^3$ has only the trivial solution $x = 0, y = 1$.*

Proof. Working mod 8 gives that y must be odd and positive, and x even.

Recall theorem 7.1 : 'if $n \in \mathbb{N}$ divides $N^2 + 1$ then n may be written as $a^2 + b^2$ with $a \equiv Nb \pmod{n}$ '. Here, $y|x^2 + 1$, so $y = a^2 + b^2$, with $a \equiv xb \pmod{y}$.

We will work in $\mathbb{Z}[i]$, though purely formally (that is, we won't have to use unique factorisation). First, we prove that $x + i = \eta(a + bi)^3$ where η is a unit of $\mathbb{Z}[i]$.

Set $(a + bi)^3 = p + qi$ ($p = a^3 - 3ab^2, q = 3a^2b - b^3$). Now,

$$\begin{aligned} (a - bx)^3 &= a^3 - 3a^2bx + 3ab^2x^2 - b^3x^3 \\ &= (a^3 - 3ab^2) + 3ab^2(x^2 + 1) - (3a^2b - b^3)x - b^3x(1 + x^2) \\ &\equiv p - qx \pmod{y^3} \end{aligned}$$

since $y^3 = x^2 + 1$. But $y|a - bx \implies y^3|(a - bx)^3 \implies y^3|p - qx$.

Now, let $\frac{x+i}{(a+bi)^3} = \lambda \in \mathbb{C}$. $y \neq 0$, so the division will work.

i λ has integer real and imaginary parts.

$$\begin{aligned}(x+i)(p-qi) &= \lambda(a+bi)^3(p-qi) \\ &= \lambda(a+bi)^3 \bar{a+bi}^3 \\ &= \lambda|a+bi|^3 = \lambda(a^2+b^2)^3 = \lambda y^3.\end{aligned}$$

Now, $(x+i)(p-qi) = xp+q+(p-qx)i$, and $y^3|p-qx$, $xp+q \equiv xp-qx^2 \pmod{y^3} = x(p-qx) \equiv 0$.

So

$$\lambda = m + ni = \frac{xp+q}{y^3} + \frac{p-qx}{y^3}i,$$

so m and n are integers.

ii $|\lambda|^2=1$

$$|x+i|^2 = x^2+1 = |\lambda|^2|(a+bi)^3|^2 = |\lambda|^2|(a^2+b^2)^3 = |\lambda|^2 y^3.$$

So $|\lambda|^2 = 1$, since $x^2+1 = y^3$.

So $x+i = \eta(a+bi)^3$. $\eta^4 = 1$ since $\eta^2 = \pm 1$, so $\eta^9 = \eta$. So $x+i = (\eta^3(a+bi))^3$.

Let $\alpha + \beta i = \eta^3(a+bi)$. Then $x+i = (\alpha + \beta i)^3$.

So $x = \alpha^3 - 3\alpha\beta^2$ and $1 = 3\alpha^2\beta - \beta^3 = \beta(3\alpha^2 - \beta^2)$. So $\beta|1$, so $\beta = \pm 1$. So $3\alpha^2 - \beta^2 = \pm 1$. $\beta^2 = 1$, so $3\alpha^2 = 0$ or 2 . But $\alpha \in \mathbb{Z}$, so $\alpha = 0$.

So $(x, y) = (0, 1)$.

□

10 More on primes

Some time ago, we defined $\pi(x)$ as the number of primes $\leq x$. The Prime Number Theorem states that $\pi(x) \sim \frac{x}{\log x}$; it is quite hard to prove the exact statement, but there are elementary proofs that $\pi(x) = O(\frac{x}{\log x})$.

10.1 A lower bound for $\pi(x)$

Theorem 10.1. For $x \geq 3$, we have

$$\pi(x) \geq \frac{(x-3) \log 2}{\log x}.$$

To prove this, we show that

$$\pi(2n+1) \geq \frac{2n \log 2}{\log(2n+1)};$$

then, for $x \geq 3$, we let $2n + 1$ be the largest odd number $\leq x$ with $n \geq 1$;

$$\pi(x) \geq \pi(2n + 1) \geq \frac{2n \log 2}{\log x} \geq \frac{(x - 3) \log 2}{\log x}$$

since $2n + 3 \geq x$, so $2n \geq x - 3$.

Proof. Let

$$I = \int_0^1 x^n (1 - x)^n dx,$$

a function we've seen before. Using the binomial theorem, we have

$$I = \int_0^1 \sum_{r=0}^n (-1)^r \binom{n}{r} x^{n+r} dx = \sum_{r=0}^n (-1)^r \binom{n}{r} \frac{1}{n+r+1}$$

Now, set $d_k = \text{lcm}(1 \dots k)$ (for example, $d_7 = 420$). So $d_{2n+1}I$ is an integer since the denominators of each of the summands divide d_{2n+1} .

$x^n(1-x)^n$ has a maximum value of 4^{-n} at $x = \frac{1}{2}$, so $I < 4^{-n}$. So

$$0 < d_{2n+1}I < \frac{d_{2n+1}}{4^n}.$$

But $d_{2n+1}I$ is a positive integer, so at least 1, so $d_{2n+1} \geq 4^n$.

If p is prime, and $p^a | d_{2n+1}$, $p^{a+1} \nmid d_{2n+1}$, then $\exists m \leq 2n + 1 : p^a | m$. So $p^a \leq 2n + 1$.

So

$$4^n \leq d_{2n+1} = \prod_{p_i^{e_i} \leq 2n+1} p_i^{e_i} \leq (2n + 1)^{\pi(2n+1)}.$$

Taking logs, we have

$$n \log 4 \leq \log(d_{2n+1}) \leq \pi(2n + 1) \log(2n + 1)$$

Dividing through, and discarding the d_{2n+1} term as having served its purpose, we have

$$\pi(2n + 1) \geq \frac{2n \log 2}{\log(2n + 1)}$$

□

10.2 An upper bound for $\pi(x)$

As is fairly common in number theory, we start off with something superficially completely different.

Definition 10.2. $\theta(x) = \sum_{p \leq x} \log p$

Theorem 10.3. $\theta(x) \leq x \log 4$

Proof. Set

$$M = \binom{2m+1}{m} = \frac{(2m+1)(2m)(2m-1)\dots(m+2)}{m!}.$$

This is divisible by every prime between $m+2$ and $2m+1$, and is an integer. So $\prod_{m+1 < p \leq 2m+1} p | M$, so that product is $\leq M$. Taking logs gives

$$\theta(2m+1) - \theta(m+1) \leq \log M.$$

Now consider expanding $(1+1)^{2m+1}$ by the binomial theorem, to get

$$2 \cdot 4^m = 2^{2m+1} = \sum_{i=0}^{2m+1} \binom{2m+1}{i} \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2M.$$

So we have $\theta(2m+1) - \theta(m+1) \leq m \log 4$. All we need do now is work by induction to get the form required by the problem.

Since $\theta(x) = \theta([x])$, we can confine ourselves to integer x . We work by induction; for $n=1$ we have $0 \leq 2 \log 2$, $n=2$ gives us $\log 2 \leq 4 \log 2$, which is a start.

Suppose the result holds for all $n < n_0$, and consider n_0 .

If n_0 is even, it's composite, so $\theta(n_0) = \theta(n_0-1) \leq 2(n_0-1) \log 2 \leq 2n_0 \log 2$.

If n_0 is odd, write $n_0 = 2m+1$. Then

$$\begin{aligned} \theta(n_0) &= \theta(2m+1) \\ &= \theta(2m+1) - \theta(m+1) + \theta(m+1) \\ &\leq 2m \log 2 + 2(m+1) \log 2 \\ &\leq 2(2m+1) \log 2 = 2n_0 \log 2. \end{aligned}$$

□

Before we can use that result to provide a bound for $\pi(x)$, we need the following

Lemma 10.4. *For $x > 1$, we have*

$$\begin{array}{ll} i & \frac{\log x}{x} \leq 1/e \\ ii & \sqrt{x} \leq \frac{2x}{e \log x} \end{array}$$

Proof. i Differentiate; the function has a maximum at $x = e$, value $1/e$.

ii Put $t = \sqrt{x}$ and apply the previous part to get $\frac{\log \sqrt{x}}{\sqrt{x}} \leq 1/e$. So $\frac{\log x}{2\sqrt{x}} \leq 1/e$; multiply by x and rearrange to get $\sqrt{x} \leq \frac{2x}{e \log x}$. \square

We have that $\theta(x) - \theta(\sqrt{x}) \leq \theta(x) \leq 2x \log 2$. But the first term can be written in terms of $\pi(x)$ by:

$$\begin{aligned} \theta(x) - \theta(\sqrt{x}) &= \sum_{\sqrt{x} \leq p \leq x} p \\ &\leq \sum_{\sqrt{x} \leq p \leq x} \log \sqrt{x} \\ &= (\pi(x) - \pi(\sqrt{x})) \log \sqrt{x} \end{aligned}$$

So,

$$\pi(x) - \pi(\sqrt{x}) \leq \frac{\theta(x)}{\log \sqrt{x}} \leq \frac{2x \log 2}{\log \sqrt{x}} = \frac{4x \log 2}{\log x}.$$

And the remainder is bounded above by something of the right form since

$$\pi(\sqrt{x}) \leq \sqrt{x} \leq \frac{2x}{e \log x}.$$

So

$$\pi(x) \leq (4 \log 2 + 2/e) \frac{x}{\log x} \leq 3.51 \frac{x}{\log x}.$$

So $\pi(x) = O(\frac{x}{\log x})$, with the constant lying between $\log 2$ and 3.51 .

10.3 An upper bound for p_n

Theorem 10.5. *The n th prime number, p_n , satisfies $p_n < n^2$.*

Proof. By experiment, the result holds for $n < 8$.

p_n is odd, so we'll write $p_n = 2k+1$; now use theorem 10.1, and the knowledge that $\pi(p_n) = n$, to get

$$n \geq \frac{2k \log 2}{\log p_n} = \log 2 \frac{p_n - 1}{\log p_n}.$$

Now, taking derivatives shows that $\frac{\log x}{x-1}$ is decreasing for $x \geq 3$, so $\frac{x-1}{\log x}$ is increasing. To obtain a contradiction, assume $p_n \geq n^2$. Then

$$\frac{p_n - 1}{\log p_n} \geq \frac{n^2 - 1}{\log n^2} = \frac{n^2 - 1}{2 \log n}.$$

So

$$\begin{aligned}n \geq \frac{(n^2 - 1) \log 2}{2 \log n} &\implies n + 1 \geq \frac{(n^2 - 1) \log 2}{2 \log n} \\ &\implies 1 \geq \frac{(n - 1) \log 2}{2 \log n} \geq \frac{(8 - 1) \log 2}{2 \log 8}\end{aligned}$$

since the function is decreasing. But the right-hand side is equal to $7/6$; this is the desired contradiction. \square