Elementary Number Theory - M3P14

Taught by David Helm - d.helm@ic.ac.uk. Office hours: Tuesdays 13:00-15:00, room 672.

Typeset by Rob Rouse. Corrections and suggestions - rr2111@ic.ac.uk.

Autumn 2014

Contents

0 Introduction

0.1 Some Questions

Number Theory is the study of the integers, primes and divisibility. How many primes are there? How common are they? Given n, approximately how many primes are there less than n?

$$\text{Gauss} \sim \frac{n}{\log n}$$

How many primes are there $\equiv a \pmod{b}$ for given a, b?

How can you tell easily that a number is prime? Using a criterion for primality? With factorisation?

0.2 Diophantine Equations

Problem: Given a Diophantine equation, polynomial equations in two or more variables with integer coefficients:

- Do they have integer solutions?
- If they do have solutions, do they have infinitely many?
- If the solution set is not infinite, how many solutions do they have?

The simplest example and the example that gives Diophantine equations their name is the following: Fix $n, m, d \in \mathbb{Z}$ with $nx + my = d$ with x, y unknown - Diophantus. We'll see that for any given choice of n, m, d that this equation will either have no solutions in the integers or infinitely many solutions in the integers.

As an example of a slight increase in complexity, we can look at Pell's equation:

$$x^2 - Dy^2 = \pm 1,\ D > 0$$

We could look at $x^2 + y^2 = a$ [for fixed a]. This is another relatively accessible example. If we want to look at something a bit more tricky, we can consider the Fermat equation:

$$x^n + y^n = z^n \quad [\text{fixed } n]$$

For $n \geq 3$ this equation has no solutions with $x, y, z \neq 0$.

Matiyasevich: An algorithm that such given a collection of Diophantine equations will determine whether they have an integer solution is a logical impossibility.

0.3 Modular Arithmetic

There are a number of primality tests that rely on modular arithmetic. It's also a good tool for studying Diophantine equations.

Solving equations mod p is a finite amount of work. For example, $x^2 + y^2 = 323$. We could check for x up to $\sqrt{323}$. It's a lot easier if we reduce this mod 4:

$$x^2 + y^2 \equiv 3 \pmod{4}$$

$$x \equiv 0 \text{ or } 2 \pmod{4} \implies x^2 \equiv 0 \pmod{4}$$

$$x \equiv 1 \text{ or } 3 \pmod{4} \implies x^2 \equiv 1 \pmod{4}$$

Quadratic Residues. When is an integer a square (mod n)?

Higher residues. When is $a \equiv$ to an m^{th} power (mod n)?

0.4 Notation

We use $\mathbb{Z}$ to denote the integers; $\mathbb{N}$ is the natural numbers [including 0]; $\mathbb{Q}$ is the rationals; $\mathbb{R}$ is the reals; $\mathbb{C}$ is the set of complex numbers.

Definition. *$a, d \in \mathbb{Z}$, $d \neq 0$. We say d <u>divides</u> a, $d|a$. If $\exists n \in \mathbb{Z}$ such that $dn = a$.*

Basic fact: If $d|a$, $d|b$, then $d|na + mb$ for all $n, m \in \mathbb{Z}$.

Proof: Write $a = dk_1$, $b = dk_2$, $k_1, k_2 \in \mathbb{Z}$. $na + mb = ndk_1 + mdk_2 = d(nk_1 + mk_2) \in d\mathbb{Z}$

Theorem 1 (Division Theorem)**.**
$a \in \mathbb{Z}$, $b > 0$. Then $\exists q, r \in \mathbb{Z}$ such that:

1. $a = qb + r$
2. $0 \leq r < b$

Proof. Let $\left\lfloor \frac{a}{b} \right\rfloor$, $\left(\text{largest integer } \leq \frac{a}{b}\right)$

$$0 \leq \frac{a}{b} - q < 1$$

$$0 \leq a - bq < b$$

□

[End lecture 1, 09/10/14]

1 Basics

Definition. *The greatest common divisor [GCD] of two integers [not both zero] is the largest $d \in \mathbb{Z}$ such that $d|a$ and $d|b$.*

Notation: $GCD\{a, b\} = (a, b)$.

How do we compute (a, b)? Let's make the following observations:

- $(0, b) = |b|$
- If $a = bq + r$, then $(a, b) = (b, r)$ [$d|a$ and $d|b \iff d|b$ and $d|r$]

1.1 Euclid's algorithm

Given a, b with $a \geq b \geq 0$ [and a, b not both zero]. If $b = 0$, $(a, b) = a$. Otherwise, we write $a = q_1 b + r_1$ with $0 \leq r_1 < b$ and so $(a, b) = (a, r_1)$. If $r_1 \neq 0$ we write $b = q_2 r_1 + r_2$ with $0 \leq r_2 < r_1$ and so $(b, r_1) = (r_1, r_2)$. Eventually, for some k, $r_k = 0$ and so we'll obtain $(a, b) = (r_{k-1}, r_k) = r_{k-1}$.

Let's look at an example. Consider $(120, 87) = (87, 33) = (33, 21) = (21, 12) = (12, 9) = (9, 3) = (3, 0) = 3$. We obtained this from the following equations:

$120 = 1 \cdot 87 + 33$ $87 = 2 \cdot 33 + 21$ $33 = 1 \cdot 21 + 12$ $21 = 1 \cdot 12 + 9$ $12 = 1 \cdot 9 + 3$
$9 = 3 \cdot 3 + 0$

Corollary: Given $a, b \in \mathbb{Z}$, not both zero, $\exists\ n, m \in \mathbb{Z}$: $na + mb = (a, b)$. To find such coefficients, we simply reverse the above process:

$33 = 120 - 87$ $21 = 87 - 2 \cdot 33$ $12 = 33 - 1 \cdot 21$ $9 = 21 - 1 \cdot 12$ $3 = 12 - 1 \cdot 9$

On substitution: $3 = 12 - 1 \cdot 9 = 12 - 1 \cdot (21 - 1 \cdot 12) = 2 \cdot 12 - 1 \cdot 21 = 2 \cdot (33 - 1 \cdot 21) - 1 \cdot 21 = 2 \cdot 33 - 3 \cdot 21 = 2 \cdot 33 - 3 \cdot (87 - 2 \cdot 33) = -3 \cdot 87 + 8 \cdot 33 = -3 \cdot 87 + 8 \cdot (120 - 87) = 8 \cdot 120 - 11 \cdot 87$

So we see that the GCD $= r_{k-1}$. $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$, so $r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}$. This is a linear combination of r_{k-3}, r_{k-4}, which we can then turn into a linear combination of r_{k-4} and r_{k-5}, and eventually one of r_1 and b and then finally a linear combination of a and b.

Proposition 1. *If $n, a, b \in \mathbb{Z}$, $n \neq 0$, such that $n|ab$ and $(n, a) = 1$, then $n|b$.*

Proof. $\exists\ x, y$ such that $xn + ay = 1$. So $xnb + ayb = b \implies n|b$ since it divides both of the left hand side's parts. □

Proposition 2. *If $d|a$, $d|b$, then $d|(a, b)$.*

Proof. Write $(a, b) = na + mb$. d divides both of the right hand side's parts and so also divides the LHS. □

Up to its sign, (a, b) is uniquely characterised by:

- It divides both a and b
- Any common divisor or a, b divides it, the GCD

Definition. *An integer p is prime if the only divisors of p are ± 1, $\pm p$ [and these are distinct, i.e. $p \neq \pm 1$].*

Proposition 3. *Every integer factors as a product of the form $\pm p_1 p_2 p_3 \cdots p_r$ for some $r \geq 0$ with p_i prime.*

Proof. Suppose some integer did not. WLOG let it be positive. Let n be the smallest positive integer that doesn't factor as so. n is not prime, so $n = ab$ with $a, b \notin \{\pm 1, \pm n\}$. We can assume $a, b > 0$. But $a < n$ and $b < n$ so both a and b factor as products of primes so n must also factor. Contradiction. □

If p is prime, $p \nmid a$, $a \in \mathbb{Z}$, then $(p, a) = 1$. If p is prime and $p|ab$, for $a, b \in \mathbb{Z}$, then either $p|a$ or if not then $p|b$ [by Proposition 1., since $(p, a) = 1$].

Theorem 2 (Fundamental Theorem of Arithmetic)**.**
The factorisation of an integer into primes is unique, i.e. if $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ with p_i, q_j primes, then $r = s$ and $\{\pm p_i\}$ are a reordering of the $\{\pm q_i\}$.

Proof. $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. $p_1|\text{LHS} \implies p_1|\text{RHS}$ and so $p_1 = q_i$, some i. Cancel and continue. □

[End lecture 2, 13/10/14]

1.2 Linear Diophantine equations

Given $a, b, n \in \mathbb{Z}$, find all integers x, y such that $ax + by = n$.

Observe: If $(a, b) \nmid n$ there can't be any solutions [if a solution exists $(a, b)|ax$, $(a, b)|by$, so $(a, b)|n$]

If $(a, b)|n$ we write $n = k(a, b)$. We can use Euclid to write $(a, b) = ax' + by'$ for $x', y' \in \mathbb{Z}$. $n = k(a, b) = a(kx') + b(ky')$. So, $x = kx'$, $y = ky'$ is a solution to $ax + by = n$.

So how do we find all solutions? If:

$$\begin{cases} ax_1 + by_1 = n \\ ax_2 + by_2 = n \end{cases} \quad \text{then } a(x_1 - x_2) + b(y_1 - y_2) = 0$$

Going backwards, if:

$$\begin{cases} ax + by = n \\ ax' + by' = 0 \end{cases} \implies a(x + x') + b(y + y') = n$$

So:

$$\{\text{All solutions}\} = \left\{ (x + x', y + y') : \begin{matrix} (x, y) \text{ is the solution we find} \\ (x', y') \text{ satisfies } ax' + by' = 0 \end{matrix} \right\}$$

N.B.

$$ax' + by' = 0 \implies \frac{a}{(a,b)}x' + \frac{b}{(a,b)}y' = 0 \implies \frac{a}{(a,b)} \Big| \frac{b}{(a,b)}y', \text{ but } \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

So:

$$y' = \frac{a}{(a,b)}y'' \quad \text{and} \quad \frac{a}{(a,b)}x' + \frac{ab}{(a,b)^2}y'' = 0$$

$$\frac{a}{(a,b)}x' = -\frac{ab}{(a,b)^2}y'' \to x' = \frac{-b}{(a,b)}y'' \implies \text{every solution takes the form } x' = \frac{-b}{(a,b)}y'', \quad y' = \frac{a}{(a,b)}y''$$

For some $y'' \in \mathbb{Z}$. Conversely, every (x', y') of this form is a solution!

Definition. *$a, b \in \mathbb{Z}$ are congruent (mod n) $[n \in \mathbb{Z}]$ if n divides $a - b$. We write $a \equiv b \pmod n$*

1. *$a \equiv a \pmod n$ $\forall$ a, $\forall$ n*
2. *$a \equiv b \pmod n \iff b \equiv a \pmod n$*
3. *If $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$*

So, in fact, it's an equivalence relation.

If we let $[a] = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}$, for $a, b \in \mathbb{Z}$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

$\forall\ a \in \mathbb{Z}$, $\exists\ q, r$ such that $a = qn + r$, with $0 \leq r < n$.

$[0], [1], \ldots, [n-1]$ exhaust $\mathbb{Z}$. $\mathbb{Z}/n = \{\text{equivalence classes mod } n\}$. $\mathbb{Z}/n$ has addition given by $[a] + [b] = [x + y]$ and multiplication given by $[a][b] = [xy]$ for $x \in [a]$, $y \in [b]$.

$\mathbb{Z}$ is a ring with above operations and $\phi : \mathbb{Z} \to \mathbb{Z}/n$ such that $\phi(a) = [a]$ is a ring homomorphism. Which elements of $\mathbb{Z}/n$ have inverses? Given $[a]$, when is there an $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{n}$?

Definition. *$a, b \in \mathbb{Z}$ are inverses (mod n) [$n \in \mathbb{Z}$] if ab is congruent to 1 (mod n).*

$ax \equiv 1 \pmod{n} \iff ax - 1 = ny$ for some $y \in \mathbb{Z}$, i.e. $ax - ny = 1$. So $(a, n)|1 \implies (a, n) = 1$. Conversely, if $(a, n) = 1$, $\exists\ x, y \in \mathbb{Z}$ such that $ax + ny = 1 \implies n|ax - 1 \implies [a][x] = [1]$ in $\mathbb{Z}/n$. So we see:

$$(\mathbb{Z}/n)^\times = \{[a] : (a, n) = 1\}$$

Note: $2x \equiv 1 \pmod{51}$: $1 = 51 - 2 \cdot 25$. -25 is a multiplicative inverse of 2 mod 51. We could normalise this and easily say that 26 is a multiplicative inverse of 2 mod 51. These are equally valid statements.

More generally, we can use Euclid's algorithm in this way to solve $ax \equiv b$ in $\mathbb{Z}/n$ for any a, b, n. Exercise: $ax \equiv b$ has any solutions at all in $\mathbb{Z}/n \iff b$ is divisible by (a, n). If this is so, then there are exactly (a, n) solutions when you count the solutions in $\mathbb{Z}/n$.

Theorem 3 (Chinese Remainder Theorem)**.**
If $m, n \in \mathbb{Z} > 0$, $(m, n) = 1$, $a, b \in \mathbb{Z}$, $\exists\ x \in \mathbb{Z}$ such that $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

Proof. Write $1 \equiv rm + sn$, $r, s \in \mathbb{Z}$ $\begin{cases} rm \equiv 1 \pmod{n} \\ rm \equiv 0 \pmod{m} \end{cases}$ $\begin{cases} sn \equiv 0 \pmod{n} \\ sn \equiv 1 \pmod{m} \end{cases}$

Set $x = asn + brm \equiv b \pmod{n} \equiv a \pmod{m}$ □

Observe: If $x, x' \equiv a \pmod{m} \equiv b \pmod{n}$ then $m|x - x'$ and $n|x - x' \implies mn|x - x' \implies x \equiv x' \pmod{mn}$, so x is unique when considered (mod mn).

[End lecture 3, 14/10/14]

Exercise: Find x such that $x \equiv -1 \pmod{9}$ and $x \equiv 13 \pmod{16}$. By Euclid's algorithm, we see $4 \cdot 16 - 7 \cdot 9 = 1$. We can take $x = -1 \cdot 4 \cdot 16 + 13 \cdot (-7) \cdot 9 = -64 - 819 = -883$. $9 \cdot 16 = 144$ and $-883 + 7 \cdot 144 = 125$. Clearly:

$$13 \pmod{16} \equiv 125 \equiv -1 \pmod{9}$$

Abstractly, we have a homomorphism of rings: $\mathbb{Z}/mn \to \mathbb{Z}/m$, $[a]_{mn} \to [a]_m$. Similarly, we get $\mathbb{Z}/mn \to \mathbb{Z}/n$, $[a]_{mn} \to [a]_n$. $\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$, $[a]_{mn} \to ([a]_m, [a]_n)$.

Alternative proof: we could show that $\#(\mathbb{Z}/mn) = (\#\mathbb{Z}/m)(\#\mathbb{Z}/n)$. To do this, it suffices to show that $\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$ is injective, i.e. it has a trivial kernel. Clearly $a \equiv 0 \pmod{m}$ & $a \equiv 0 \pmod{n} \implies a \equiv 0 \pmod{mn}$, and so the homomorphism is indeed injective. [$m|a$, $n|a \implies mn|a \implies a \equiv 0 \pmod{mn}$.]

Recall: $[a] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $(a, n) = 1$.

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{b : 1 \leq b \leq n - 1, (b, n) = 1\}$$

Definition. *The Euler ϕ-function is given by $\phi(n) = \#\{b : 1 \leq b \leq n - 1\,(b, n) = 1\}$. It's defined for $n > 0$.*

Examples:

- $\phi(6) = 2$. Out of $[1, 6] \cap \mathbb{Z}$, 1 & 5 are such that $(b, 6) = 1$. All of $\{2, 3, 4, 6\}$ have factors in common
- $\phi(9) = 6$. $\{1, 2, \not{3}, 4, 5, \not{6}, 7, 8, \not{9}\}$

Definition. *A function $f : \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ is called multiplicative if for all m, n such that $(m, n) = 1$ we have $f(mn) = f(m)f(n)$. We call It strongly multiplicative if $\forall\ m, n \geq 1$, $f(mn) = f(m)f(n)$.*

Strongly multiplicative $\implies$ the function's determined by its value on primes. We write:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \qquad f(n) = f(p_1)^{r_1} f(p_2)^{r_2} \cdots f(p_s)^{r_s}$$

If f is only multiplicative:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \qquad f(n) = f(p_1^{r_1}) f(p_2^{r_2}) \cdots f(p_s^{r_s})$$

In this case, when f is not strongly multiplicative, we can't write $f(p_1^{r_1})$ in terms of $f(p_1)$ as so.

Theorem 4. *ϕ, Euler's function, is a multiplicative function.*

Proof. Let $m, n \in \mathbb{Z}$ with $(m, n) = 1$.

$$\phi(m, n) = \#\left(\mathbb{Z}/mn\right)^\times = \#\left(\mathbb{Z}/m \times \mathbb{Z}/n\right)^\times$$

Note that $(x, y) \in R \times S$ is invertible iff $x \in R^\times$ and $y \in S^\times \iff (x^{-1}, y^{-1})$ is the inverse to (x, y) in $R \times S \implies$ we can write $(x, y)^{-1} = (r, s)$, where $xr = 1$ in R and $ys = 1$ in S.

$$\phi(mn) = \#\left[(\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times\right] = \phi(m)\phi(n)$$

□

N.B. ϕ is not strongly multiplicative: $\phi(4) = 2$ and $\phi(2) = 1$, but $\phi(4) \neq \phi(2)\phi(2)$.

Theorem 5. *Let p be a prime and $r \in \mathbb{Z}_{>0}$:*

$$\phi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$$

Proof: If $(n, p^r) \neq 1$, $p|(n, p^r)$ so $p|n$. So we note that $\#\{b \text{ with } 1 \leq b \leq p^r \text{ and } (b, p^r) \neq 1\} = \#\{\text{multiples of } p \text{ between 1 and } p^r\}$; there are p^{r-1} such numbers. $\phi(p^r) = p^r - \#\{\text{multiples of } p\} = p^r - p^{r-1}$.

In particular:

$$\phi(n) = p_1^{r_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{r_2}\left(1 - \frac{1}{p_2}\right) \cdots p_s^{r_s}\left(1 - \frac{1}{p_s}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) = n \prod_{\substack{p : p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

$\#\left(\mathbb{Z}/n\right)^\times = \phi(n)$. $(\mathbb{Z}/n)^\times$ is a finite group. From Group Theory: G is a finite group of order N. $g \in G \implies g^N = 1$ in G.

Theorem (Fermat's Little Theorem)**.**
If $a \in (\mathbb{Z}/p)^\times$ [p prime] then $a^{p-1} \equiv 1$ (mod p).

[End lecture 4, 16/10/14]

Theorem 6 (Euler's Theorem)**.**
If $a \in (\mathbb{Z}/n)^\times$, with $n \in \mathbb{Z}_{\geq 1}$, then $a^{\phi(n)} \equiv 1$ (mod n). [I.e. if $a \in \mathbb{Z}$ such that $(a, n) = 1$ then $a^{\phi(n)} \equiv 1$ (mod n).]

Proof. Consider the products:

$$L = \prod_{[b] \in (\mathbb{Z}/n)^\times} [b] \qquad \text{and} \qquad R = \prod_{[b] \in (\mathbb{Z}/n)^\times} [ab] = [a]^{\phi(n)} \cdot \prod_{[b] \in (\mathbb{Z}/n)^\times} [b]$$

So $R \equiv a^{\phi(n)} \cdot L$. As $a \in (\mathbb{Z}/n)^\times$ on multiplying each $\{[b]\}$ by $[a]$ we merely permute them [if $ab_i = ab_j$ then $i = j$ by a's multiplicative inverse]; so $L \equiv R \equiv a^{\phi(n)} \cdot L \pmod{n}$, i.e. $a^{\phi(n)} \equiv 1 \pmod{n}$ [since $L \in (\mathbb{Z}/n)^\times$]. □

Here's an explanatory example with $n = 9, a = 4$. LHS $\equiv 1{\cdot}2{\cdot}4{\cdot}5{\cdot}7{\cdot}8$. RHS $\equiv (4{\cdot}1){\cdot}(4{\cdot}2){\cdot}(4{\cdot}4){\cdot}(4{\cdot}5){\cdot}(4{\cdot}7){\cdot}(4{\cdot}8) = 4^6 \cdot (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)$. RHS $= 4 \cdot 8 \cdot 7 \cdot 2 \cdot 1 \cdot 5$.

Claim: More formally, with $a \in (\mathbb{Z}/n)$, for any $b \in (\mathbb{Z}/n)^\times$, $\exists!\ b' \in (\mathbb{Z}/n)^\times$ such that $ab' \equiv b \pmod{n}$.

Proof. $(a, n) \equiv 1$. So a has a multiplicative inverse a^{-1}. Then $b' \equiv a^{-1}b \pmod{n}$. □

This is what we applied to the proof of Euler's Theorem. Every factor in L also appears in R and hence $L \equiv R \pmod{n}$. $R \equiv a^{\phi(n)} \cdot L \pmod{n}$ and so $L \equiv a^{\phi(n)} \cdot L \pmod{n}$. Since $L \in (\mathbb{Z}/n)^\times$, we can multiply both sides by L^{-1} to get $1 \equiv a^{\phi(n)} \pmod{n}$.

If p is prime this means that for $(a, p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$. FLT is a specific case of Euler's Theorem.

Naturally, the contrapositive follows: If $n > 0$ $(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$ $[a < n]$ then n is not prime.

Example: We can prove 9 is not prime because $2^8 = 256 \equiv 4 \pmod{9}$ $[(2, 9) = 1]$.

For 100+ digit numbers, this is not so silly. Given a big N, we pick random $1 < a < N$. Compute (a, N) [fast]. If it's not 1, then N is not prime. Otherwise, compute $a^{N-1} \pmod{N}$ [fast]. If it's not 1, N is not prime.

Definition. *A composite number N is a Carmichael number if for all a such that $(a, N) = 1$, we have $a^{N-1} \equiv 1$ (mod N).*

Claim: $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number.

Proof. We need that if $(a, 561) = 1$ then $a^{560} \equiv 1 \pmod{561}$. By the CRT, it suffices to show that if $(a, 561) = 1$, $a^{560} \equiv 1 \pmod{3}$, $\equiv 1 \pmod{11}$, $\equiv 1 \pmod{17}$

Fermat's Little Theorem: $a^2 \equiv 1 \pmod{3}$ if $(a, 3) = 1$ i.e. $3 \nmid a$. $a^{10} \equiv 1 \pmod{11}$ if $(a, 11) = 1$ i.e. $11 \nmid a$. $a^{16} \equiv 1 \pmod{17}$ if $(a, 17) = 1$ i.e. $17 \nmid a$.

$$\begin{aligned} a^{560} &= (a^2)^{280} \equiv 1^{280} \pmod{3} \equiv 1 \\ &= (a^{10})^{56} \equiv 1^{56} \pmod{11} \equiv 1 \\ &= (a^{16})^{35} \equiv 1^{35} \pmod{17} \equiv 1 \end{aligned}$$

□

Application: Diophantine equations. Exercise: $x^2 + y^2 = a$ has no solutions if $a \equiv 3 \pmod{4}$. If you have a Diophantine equation that you think has no solutions and you want to prove this by looking (mod n) for some n, then you should look for an n such that $\phi(n)$ is a small multiple of the exponents appearing in the equation. Here, $\phi(4) = 2$.

Consider $x^5 + y^5 = a$. Find n such that $\phi(n)$ is a small multiple of 5. E.g. $\phi(11) = 10$.

Claim: $\forall\ a \in \mathbb{Z}$, $a^5 \equiv -1, 0$ or $1 \pmod{11}$. If $11|a$, then $a^5 \equiv 0 \pmod{11}$. Otherwise $(a, 11) = 1$. $a^{10} \equiv 1 \pmod{11}$. $a^{10} - 1 \equiv 0 \pmod{11}$, i.e. $(a^5 + 1)(a^5 - 1) \equiv 0 \pmod{11}$. So $a^5 + 1 \equiv 0 \pmod{11}$ or $a^5 - 1 \equiv 0 \pmod{11}$.

So this yields only five possibilities: $x^5 + y^5 \equiv -2, -1, 0, 1, 2 \pmod{11}$. Hence $x^5 + y^5 = a$ has no solutions when $a \equiv 3, 4, 5, 6, 7, 8 \pmod{11}$. E.g. $x^5 + y^5 = 125$ has no solutions because $125 \equiv 4 \pmod{11}$

[End lecture 5, 17/10/14]

2 Applications to Cryptography

Problem: We want to send information in some form to a given recipient in such a way that only the recipient can understand it.

Here are a couple of ways of approaching this:

- Sender and recipient have an agreed upon way to scramble and unscramble messages. E.g. Caesar shift: replace each letter in an alphabet with a successor.
  - Very easy to communicate method
  - Too simple; it's easy to break
- More elaborate systems: Variations: choose a keyword (e.g. CIPHER). We could match congruence classes (mod 26). $A = [0]$, $B = [1]$, &c. For example, using the text 'This is a secret' with keyword, 'cipher':

  $$\begin{aligned} &\text{THISISASECRET} \\ +\ &\text{CIPHERCIPHERC} \\ =\ &\text{VP}\ldots \end{aligned}$$

  However this is still vulnerable to frequency analysis.

- More secure - one time pad. We have a very long string of data [letters, bits]. To encode it, we combine data with the plaintext. We never release the data. We take our message and use a random sting of data known to both the sender and the recipient:

  $$\text{MESSAGEMESSAGE}\ldots$$

  $$\text{XYQREALSRA}\ldots$$

  This has the huge advantage of being theoretically unbreakable as long as the data is truly random and never reused. The disadvantage is that getting the data [the key] to the recipient is just as hard as getting your message to them.

The fundamental problem is how can you communicate securely with someone without any trusted [i.e. private] communication channel? Surprisingly, this is not a hopeless problem.

Idea: It relies on the fact that multiplying big numbers is easy, but factoring big numbers is hard. Let's suppose I generate two very big primes p, q. Then finding $n = pq$ is easy, but even if I tell the world what n is, I'm still the only one who knows p, q.

Can we use this to tell the world how to send us messages only we can decode? The answer is yes! RSA algorithm.

Public information: $n = pq$; a number $e < n$ with $(e, \phi(n)) = 1$, $e \neq 1$
Secret information: Two large primes p, q; $\phi(n) = (p-1)(q-1)$; an integer d such that $ed \equiv 1 \pmod{\phi(n)}$ [we write $1 = de + f\phi(n)$]

Sending me a message:

- Suppose a member of the public wants to send me a message
- They encode that message as a string of integers (mod n) with any agreed-upon scheme
- To send me an integer C (mod n), we compute C^e and reduce (mod n), send me C^e and don't worry about who's listening

So how can we recover C from C^e? The idea is that recipient takes C^e and computes $(C^e)^d \pmod n$.

$$(C^e)^d = C^{ed} = C^{1+k\phi(n)} = C \cdot C^{k\phi(n)} = C \cdot \left(C^{\phi(n)}\right)^k \equiv C \cdot (1)^k \pmod n \equiv C \pmod n \text{ if } (C,n) = 1$$

We should note here that this fails when $(C,n) > 1$. This is very rare; the odds of hitting such a C are:

$$1 - \frac{n}{\phi(n)} = 1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$$

[End lecture 6, 21/10/14]

To summarise, to encode a congruence class $C \pmod n$:

- Compute $C^e \pmod n$ and send it to the recipient

To decode:

- Given C^e, the recipient computes $(C^e)^d \pmod n$.
- Since $ed \equiv 1 \pmod{\Phi(n)} \implies ed = 1 + k\Phi(n)$ for some $k \in \mathbb{Z}$. $(C^e)^d = C^{ed} = C^{1+k\Phi(n)} = C \cdot (C^{\Phi(n)})^k \equiv C \cdot 1^k \pmod n = C$. If $(C,n) = 1$ [Very rarely not the case].

Key generation: Can we generate keys quickly?

- Need to find primes fast
- Need to multiply fast
- Need to compute inverses $\pmod{\Phi(n)}$ fast

Fast will mean 'polynomial time'. I.e. we want the number of steps to be at most a polynomial in $(\log p)$ and $(\log q)$.

Addition: $\sim \log p$ or $\log q$.
Multiplication: Computing $pq \sim (\log p)(\log q)$.

We can improve this with FFT [fast Fourier transform] and such like.

Computing inverses $\pmod{\Phi(n)}$: we need to write $1 = ed + k\Phi(n)$ applying the Euclidean algorithm to $(e, \Phi(n))$. We can choose e, $\Phi(n) = (p-1)(q-1)$. $\log \Phi(n) \cong \log p + \log q$.

How many steps does the Euclidean algorithm take? Given $a, b > 0$, $b \leq a$, we write $\begin{cases} a = q_1 b + r_1 & 0 \leq r_1 < b \\ b = q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \end{cases}$.

We now have (r_1, r_2), $r_1 > r_2$.

Claim: $r_1 \leq \frac{1}{2}a$.

Case 1: $b \leq \frac{1}{2}a$. Then $r_1 < b_1$ so we're okay

Case 2: $b > \frac{1}{2}a$. $q_1 = 1$, $r = a - b \leq \frac{1}{2}a$

Fact: If you pick a large random number n, the odds that it's prime are roughly $\frac{1}{\log n}$. On average, it you keep generating large numbers $\leq n$ until you find a prime it will take roughly $\log n$ attempts.

If you have a way of testing whether p is prime that takes time polynomial in $\log p$, this gives a way of producing primes - keep trying until you find one. We discussed a probabilistic approach to this, which relied on computing exponentials.

Given a, b, how can we quickly compute $a^b \pmod n$? The idea is to compute a, a^2, $a^4 = (a^2)^2$, $a^8 = (a^4)^2$, ..., a^{2^r} where 2^r is the largest power of $2 \leq b$. Save these all in a table so that we have access to these whenever

we need. Now we can express any value of b as the sum of $2^{r_1} + 2^{r_2} + \cdots + 2^{r_k}$ where these are the non-zero bits in the binary expansion for b. Then $a^b = a^{2^{r_1}+2^{r_2}+\cdots+2^{r_k}}$.

Example: $2^{37} \pmod{11}$. $2^0 \equiv 1$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 5$, $2^8 \equiv 3$, $2^{16} \equiv 9$, $2^{32} \equiv 4 \pmod{11}$. So $2^{37} = 2^{32+4+1} = 2^{32} \cdot 2^4 \cdot 2^1 \equiv 4 \cdot 5 \cdot 2 \equiv 7 \pmod{11}$.

So, we can compute $a^b \pmod{n}$ with roughly $2\log_2(b)$ multiplications. So key generation is okay. For encoding and decoding, computing exponentials is all that we need.
RSA is also good for authentication: digital signatures. Idea: You have a private key. You want to sign with docent you're sending with a signature. Encode it as a congruence class $C \pmod{n}$. Use your private key, d, to compute $C^d \pmod{n}$. Then make public both C [the document] and C^d [the signature].

To verify this signature (C, S) the rest of the world needs to check that $S = C^d$. If $S = C^d$, then $S^e = (C^e)^d \equiv C \pmod{n}$. So we can verify the signature by taking S^e and checking that this is the case. Finding S such that $S^e = C$ is exactly like breaking RSA and just as hard.

[End lecture 7, 23/10/14]

Definition. *The order of $a \in (\mathbb{Z}/n)^\times$ is the smallest integer $d > 0$ such that $a^d \equiv 1 \pmod{n}$.*

Euler's Theorem tells us that $a^{\Phi(n)} \equiv 1 \pmod{n}$, so the order of a is $\leq \Phi(n)$.

Lemma 1. *The order of a divides $\Phi(n)$.*

Proof. Let d be the order of a. $a^d \equiv 1 \pmod{n}$, $a^{\Phi(n)} \equiv 1 \pmod{n}$. We write $\Phi(n) = kd + r$, $k \in \mathbb{Z}$, $0 \leq r < d$.

$$\begin{aligned} 1 \equiv a^{\Phi(n)} = a^{kd+r} = a^r (a^d)^k &\equiv a^r (1)^k \pmod{n} \\ &\equiv a^r \pmod{n} \end{aligned}$$

So $a^r \equiv 1 \pmod{n}$. Since $r < d$, we must have $r = 0$. So $\Phi(n) = kd$ and so $d | \Phi(n)$, as required. □

2.1 Primitive Roots

Definition. *A primitive root (mod n) [or generator of $(\mathbb{Z}/n)^\times$] is an element $a \in (\mathbb{Z}/n)^\times$ such that the order of $a = \Phi(n)$.*

Exercise: $n = 5$, $\Phi(n) = 4$. $2^1 \equiv 2\ (5)$, $2^2 \equiv 4\ (5)$, $2^3 \equiv 3\ (5)$, $2^4 \equiv 1\ (5)$. 2, having order 4, is a primitive root.

Note: If a is a primitive root $\pmod{n}$ then the set $\{a, a^2, a^3, \ldots, a^{\Phi(n)}\}$ consists of distinct elements of $\mathbb{Z}/n$.

Proof. If $a^k \equiv a^r \pmod{n}$, with $1 \leq k < r \leq \Phi(n)$ then $a^{r-k} \equiv 1 \pmod{n}$, but $0 < r - k < \Phi(n)$ so this can't happen. □

As a consequence, every element of $(\mathbb{Z}/n)^\times$ is a power of a. [In particular, a generates $(\mathbb{Z}/n)^\times$ as a group.]

In fancier language, we have a map:

$$\mathbb{Z}/\Phi(n) \to (\mathbb{Z}/n)^\times$$
$$[r]_{\Phi(n)} \to [a^r]_n$$

Note: The class of $[a^r]_n$ depends only on $[r]_{\Phi(n)}$. If $r' = r\Phi(n)$, then $r' - r = k\Phi(n)$. $a^{r'} = a^{r+k\Phi(n)} = a^r \left(a^{\Phi(n)}\right)^k \equiv a^r (1)^k = a^r \pmod{n}$.

This map is a homomorphism of groups:

$$a^{r+r'} = a^r \cdot a^{r'}$$

If a is a primitive root, then this homomorphism is an isomorphism. Surjectivity follows from the consequence above; injectivity follows because:

$$\#\left(\mathbb{Z}/\Phi(n)\right) = \#\left(\mathbb{Z}/n\right)^\times$$

The question is, when does $(\mathbb{Z}/n)^\times$ have a generator?

If we look at $(\mathbb{Z}/8)^\times$, by contrast, this actually has no primitive root. $(\mathbb{Z}/8)^\times = \{1,3,5,7\}$. 1 certainly isn't a primitive root. $3^2 \equiv 1\ (8)$, $5^2 \equiv 1\ (8)$, $7^2 \equiv 1\ (8)$ all have order 2. In fact:

$$\mathbb{Z}/2 \times \mathbb{Z}/2 \xrightarrow{\sim} (\mathbb{Z}/8)^\times$$

$$(a,b) \to 3^a 5^b$$

$$(0,0) \to [1]_8$$

$$(1,0) \to [3]_8$$

$$(0,1) \to [5]_8$$

$$(1,1) \to [7]_8$$

Theorem 7. *Let p be a prime. Then there exists a primitive root (mod p). [I.e. $(\mathbb{Z}/p)^\times \cong (\mathbb{Z}/p-1)$.]*

Lemma 2. *Let R be a ring [commutative, with identity] and $P \in R[x]$ a polynomial with coefficients in R. Let's take $\alpha \in R$ such that $P(\alpha) = 0$. Then there exists Q such that $P = (x-\alpha)Q$.*

Proof. Induction of the degree of P. Call this d. Base case: $d = 0 \implies P$ is constant, $P(\alpha) = 0 \implies P \equiv 0$.

Assume this result will hold for polynomials of degree $d-1$ and let's let P have degree d. In this case, we can write $P(x) = ax^d +$ lower order terms. Consider $P' = P(x) - ax^{d-1}(x-\alpha)$. This has degree $d-1$. $P'(\alpha) = P(\alpha) - a\alpha^{d-1}(\alpha-\alpha) = 0$. $P' = (x-\alpha)Q'$. $(x-\alpha)Q' = P - ax^{d-1}(x-\alpha)$. $P = (x-\alpha)(ax^{d-1}+Q')$. □

As a corollary to this, if R is a field then any non-zero polynomial $P \in R[x]$ of degree d has at most d roots in R.

Proof. Induction on degree d. If $d = 0$, P is a non-zero constant so no roots. Assume the result holds for $d-1$. Let P have degree d. If P has no roots in R then we're done. Otherwise, we let α be a root of P in $R[x]$. Then, by the previous lemma, we have $P = (x-\alpha)Q$, with the degree of $Q = d-1$. So Q has at most $d-1$ toots in R. Suppose $\beta \in R$ with $P(\beta) = 0$. $(\beta-\alpha)Q(\beta) = 0 \implies (\beta-\alpha) = 0$ (i.e. $\beta = \alpha$) or $Q(\beta) = 0$. Every root of P is either α or a root of Q. Q has $\leq d-1$ roots, so P has $\leq d$ roots. □

Note: $x^2 - 1$ has four separate roots (mod 15). $1^2 \equiv 1\ (15)$, $4^2 \equiv 1\ (15)$, $11^2 \equiv 1\ (15)$, $14^2 \equiv 1\ (15)$. $x^2 - 1 = (x+1)(x-1)$. $(4+1)(4-1) = 5 \cdot 3 = 0\ (15)$. By the Chinese Remainder Theorem: $\mathbb{Z}/pqr$ with p, q, r distinct primes. An element $\alpha \in \mathbb{Z}/pqr$ is a root of $x^2 - 1$ iff α is a root of $x^2 - 1$ (mod p) and a root of $x^2 - 1$ (mod q) and a root of $x^2 - 1$ (mod r) $\iff \alpha \equiv \pm 1$ (mod p), $\alpha \equiv \pm 1$ (mod q), $\alpha \equiv \pm 1$ (mod r). Any combination of choices works, so $x^2 - 1$ has 8 roots mod pqr.

Observation: If m, n odd, relatively prime, then:

$$(\mathbb{Z}/nm)^\times \cong (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$$

which both have even order. So the product is not cyclic. So $(\mathbb{Z}/nm)^\times$ has no generator.

[End lecture 8, 24/10/14]

Theorem 7. claimed that if p is prime then there exists a primitive root (mod p).

We've seen that if R is a field and $P \in R[x]$ a polynomial of degree d, then P has at most d roots in R. In particular, this holds for $R \in \mathbb{Z}/p$. Apply this to polynomials of the form $x^d - 1$, for $d|(p-1)$.

On one hand, we know that $x^d - 1$ has at most d roots (mod p). On the other hand, $x^{p-1} - 1$ (mod p) has exactly $p-1$ roots (mod p). [Fermat's little theorem: if $(x,p) = 1$, $x^{p-1} \equiv 1$ (mod p) so [1], [2], ..., $[p-1]$ are all roots.]

Claim: $\forall d|(p-1)$, $x^d - 1$ has exactly d roots.

Proof. Let's suppose otherwise. Then $\#\{\text{roots of } x^d - 1\} < d$.

$$\begin{array}{ccccc} x^{p-1}-1 & = & (x^d-1) & \left(1 + x^d + x^{2d} + \cdots + x^{p-1-d}\right) \\ p-1 \text{ roots} & & < d \text{ roots} & \leq p-1-d \text{ roots} \end{array}$$

so on the RHS there are $< p-1$ roots but there are $p-1$ on the LHS. Contradiction. □

Corollary: For $d|(p-1)$ the are exactly d elements in $(\mathbb{Z}/p)^\times$ of order divining d.

Claim: There are exactly $\Phi(d)$ elements of order d in $(\mathbb{Z}/p)^\times \ \forall \ d|(p-1)$. [In particular, there are $\Phi(p-1)$ primitive roots!]

Proof. We'll use strong induction on d. The base case here is going to be $d = 1$, and that's easy. 1 is the only element of order 1. We assume the result is true for all $d' < d$, dividing $p-1$. Now, by the above corollary, we have that $\#\{\text{elements of order dividing } d\} = d$. Hence:

$$\#\{\text{elements of order exactly } d\} = d - \sum_{\substack{d'|d \\ d' \neq d}} \#\left\{\text{elements of order } d'\right\}$$

By induction, the number of elements of order $d' = \Phi(d')$ for each $d'|d$, $d' \neq d$.

$$\#\{\text{elements of order } d\} = d - \sum_{\substack{d'|d \\ d' \neq d}} \Phi(d')$$

From the first example sheet, we know:

$$d = \sum_{d'|d} \Phi(d') = \Phi(d) + \sum_{\substack{d'|d \\ d' \neq d}} \Phi(d')$$

So, the number of elements of order $d = \Phi(d)$. □

Corollary: For $g \in (\mathbb{Z}/p)^\times$, a primitive root, the map $(\mathbb{Z}/p-1) \to (\mathbb{Z}/p)^\times$, $[a]_{p-1} \to [g^a]_p$, is an isomorphism of groups.

If g is a primitive root, the map $a \to g^a$ has an inverse $\log_g : (\mathbb{Z}/p)^\times \to (\mathbb{Z}/p-1)^\times$, $g^a \to a$.

Exercise: $p = 7$. $3^1 \equiv 3\ (7)$; $3^2 \equiv 2\ (7)$; $3^3 \equiv 6\ (7)$; $3^4 \equiv 4\ (7)$; $3^5 \equiv 5\ (7)$; $3^6 \equiv 1\ (7)$. $(\text{mod } p = 7)$:

3^a	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$\log_3 3^a$	6	2	1	4	5	3

This has applications in algorithms.

Given p, a primitive root g $(\text{mod } p)$, $a \to g^a$ is easy to calculate. $\log_g$ is quite hard to compute. $a \to g^a$ is a good example of a 'one-way function'. A good application of this is safely storing passwords.

Idea: When a user sets a password, convert it to a binary string. 8-bits per character. Apply a one-way function to it.

Exercise: Choose p prime, larger than $d^{\#\text{ of bits}}$. Treat the bit string as a number a $(\text{mod } p)$. Choose a primitive root g $(\text{mod } p)$. Store $[g^a]_p$. Every time the user enters a password b, compute $[g^b]_p$, compare this to $[g^a]_p$, which you stored. If they match, then $a = b$.

If someone else comes along and steals the password table, then in order to figure out your passwords they'd have to figure out a given g^a [i.e. they'd have to compute $\log_g$].

3 Quadratic Residues

Definition. *$a \in (\mathbb{Z}/p)^\times$ is a quadratic residue [QR] (mod p) if $\exists\ n \in \mathbb{Z}$ such that $a \equiv n^2$ (mod p).*

Exercise: 1 is a quadratic residue (mod 4), but 2 and 3 are not. Working (mod 5): $1^2 \equiv 1$; $2^2 \equiv 4$; $3^2 \equiv 4$; $4^2 \equiv 1$. So $1, 4$ are quadratic residues and $2, 3$ are not.

Note: If $[a]$ is a QR (mod p), then so is $[a]^{-1}$. [If $a \equiv n^2 \pmod p$ then $p \nmid n$ because $p \nmid a$, so $a^{-1} \equiv (n^{-1})^2 \pmod p$.]

If a, b are QR, then so is ab. [If $a \equiv n^2$, $b \equiv m^2 \pmod p$, then $ab \equiv (nm)^2 \pmod p$.]

If a is a QR, b is not, then ab is not a QR. [If ab is a QR, a is a QR, then a^{-1} is a QR so $a^{-1}(ab)$ is a QR $\implies$ b is a QR.]

In summary: If any two of a, b, ab are QRs then so is the third.

Next time: If a, b are not QRs, then ab is a QR. [This uses the existence of a primitive root.]

[End lecture 9, 28/10/14]

Let's recall that there exists a primitive root (mod p). Idea: Every element of $(\mathbb{Z}/p)^\times$ has the form g^n for some n.

If $a \equiv g^n \pmod p$, n even, then a is a quadratic residue. $g^{2k} = (g^k)^2$. What about odd powers of g?

Claim: Let n be odd. Then g^n is not a quadratic residue.

Proof. Suppose $g^n \equiv x^2 \pmod p$. We'll show g is not primitive. By Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod p$, so $(x^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$. So:

$$(g^n)^{\frac{p-1}{2}} \equiv 1 \pmod p \implies g^{n\frac{p-1}{2}} \equiv 1 \pmod p$$

Suppose g were primitive, i.e. $g^{p-1} \equiv 1 \pmod p$. Write $n = 2k+1$:

$$1 \equiv g^{n\frac{p-1}{2}} = g^{(2k+1)\frac{p-1}{2}} = g^{k(p-1)} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod p$$

But g has order $p-1$, a contradiction. So, in particular, there are $\frac{p-1}{2}$ quadratic residues [all even powers of g] and $\frac{p-1}{2}$ quadratic non-residues [all the odd powers of g].

□

Theorem 8 (Euler's Criterion)**.**
$a \in (\mathbb{Z}/p)^\times$. Then a is quadratic residue if, and only if, $a^{\frac{p-1}{2}} \equiv 1$ (mod p). Moreover, a is a quadratic non-residue if, and only if, $a^{\frac{p-1}{2}} \equiv -1$ (mod p).

Proof. For any $a \in (\mathbb{Z}/p)^\times, (a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod p$. So $a^{\frac{p-1}{2}}$ is a root of the polynomial $x^2 - 1$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. If $a \equiv n^2$, then $a^{\frac{p-1}{2}} \equiv (n^2)^{\frac{p-1}{2}} \equiv n^{p-1} \equiv 1 \pmod p$. Conversely, if a is a quadratic non-residue, then a $\equiv g^n \pmod p$ a primitive root, n odd.

So $a^{\frac{p-1}{2}} \equiv (g^n)^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^n \pmod p$. Since g is a primitive root $g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ and so $g^{\frac{p-1}{2}} \equiv -1 \pmod p$. $a^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^n = (-1)^n \equiv -1 \pmod p$, since n is odd in this case. □

Notation:

$$\left(\frac{a}{p}\right) \text{ ['}a \text{ on } p\text{']} = \begin{cases} 1 \text{ if } a \text{ is a QR mod } p \\ \text{-1 if a is a Q. non-residue (mod } p) \\ 0 \text{ if p|a} \end{cases}$$

So from Euler's criterion we note that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

Note: [p odd]

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \equiv \begin{cases} 1 \text{ if } \frac{p-1}{2} \text{ is even} \\ -1 \text{ if } \frac{p-1}{2} \text{ is odd} \end{cases}$$

$\frac{p-1}{2}$ is even $\iff \exists k : \frac{p-1}{2} = 2k \iff p = 4k+1 \iff p \equiv 1 \pmod 4$
$\frac{p-1}{2}$ is odd $\iff \exists k : \frac{p-1}{2} = 2k+1 \iff p = 4k+3 \iff p \equiv 3 \pmod 4$

Corollary: -1 is a QR [i.e. a square] (mod p) $\iff p \equiv 1 \pmod 4$.

Example: $p = 17, 4^2 \equiv -1 \pmod{17}$. $p = 19$, squares are $1, 4, 9, 16, 6, 17, 11, 7, 5$.

Question: When is $\left(\frac{2}{p}\right) = 1$? [I.e., for which p?]

Theorem 9. *p odd. $\left(\frac{2}{p}\right) \equiv 1$ iff $p \equiv 1$ or 7 (mod 8). $\left(\frac{2}{p}\right) \equiv -1$ iff $p \equiv 3$ or 5 (mod 8).*

Example: 2 is a square (mod 7), $2 \equiv 3^2 \pmod 7$. 2 is <u>not</u> a square (mod 11), $2^5 = 32 \equiv -1 \pmod{11}$.

Proof. Let $q = \frac{p-1}{2}$. Consider the product: $2^q \cdot q! = 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdots 2q \equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdot (-5)(-3)(-1) \pmod p$ [arrange for all factors to be between $-q$ and q] $\equiv (-1)^l \cdot q!$ where l is the number of (-1)'s in the equation above. So $2^q \equiv (-1)^l \pmod p$. In particular, $\left(\frac{2}{p}\right) = (-1)^l$. So suffices to show that when $p \equiv 1$ or $7 \pmod 8$ l is even and when $p \equiv 3$ or $5 \pmod 8$ l is odd.

Case 1. $p \equiv 1 \pmod 8$, so $p = 8k+1$, $q = 4k$:
$2 \cdot 4 \cdot 6 \cdot 8 \cdots 8k \equiv 2 \cdot 4 \cdot 6 \cdots 4k \cdot (-4k+1) \cdots (-1)$ [$2k$ pluses and $2k$ minuses]. So $l = 2k$ is even and $\left(\frac{2}{p}\right) = 1$

Case 2. $p = 8k+3, q = 4k+1$:
$2 \cdot 4 \cdot 8 \cdots 8k+2 \equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdots (4k) \cdot (-4k-1) \cdots (-1)$ [$4k+1$ factors, $2k$ positive]
so $l = 2k+1$ is <u>odd</u>. $\left(\frac{2}{p}\right) = -1$

Case 3. $p = 8k+5, q = 4k+2$:
$2 \cdot 4 \cdot 6 \cdots (4k+2)(-4k-1) \cdots (-1)$ [$4k+2$ terms, $2k+1$ positive]. $l = 2k+1$ is odd. $\left(\frac{2}{p}\right) = -1$.

Case 4. $p = 8k+7, q = 4k+3$:
$2' \cdot 4 \cdot 6 \cdot 8 \cdots (4k+2)(-4k-3) \cdots (-1)$ [$4k+3$ terms, $2k+1$ positive]. So $l = 2k+2$ is even. So $\left(\frac{2}{p}\right) = 1$ $\square$

[End lecture 10, 30/10/14]

[This lecture was a problems class.]

[End lecture 11, 31/10/14]

3.1 Quadratic Reciprocity

So, so far we've seen the following:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a QR } \pmod p \\ -1 \text{ if } a \text{ is a QNR } \pmod p \\ 0 \text{ if } p|a \end{cases} \qquad \text{Seen: } \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \qquad \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv 3 \pmod 4 \end{cases} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 \text{ if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

Is $\left(\frac{a}{p}\right)$, for fixed a, always determined by congruence conditions on p? Answer: Yes!

Law 1 (Law of quadratic reciprocity)**.**
p, q distinct odd primes. Then:

$$\begin{cases} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) & \text{if either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Alternatively:

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

Exercises:

- $$\left(\frac{14}{137}\right) = \left(\frac{2}{137}\right)\left(\frac{7}{137}\right) = (1)(1) = 1$$

  $137 = 17 \cdot 8 + 1$, so $137 \equiv 1\ (8)$, $\left(\frac{2}{137}\right) = 1$.

  $$\left(\frac{7}{137}\right) \overset{\text{LQR}}{=} \left(\frac{137}{7}\right) = \left(\frac{4}{7}\right) \overset{\text{QR}}{=} 1$$

- 55 is not a quadratic residue modulo 179:

  $$\left(\frac{55}{179}\right) = \left(\frac{5}{179}\right)\left(\frac{11}{179}\right) = -\left(\frac{179}{5}\right)\left(\frac{179}{11}\right) = -\left(\frac{4}{5}\right)\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$$

- 299 is not a quadratic residue modulo 397:

  $$\left(\frac{299}{397}\right) = \left(\frac{-98}{397}\right) = \left(\frac{-1}{397}\right)\left(\frac{2}{397}\right)\left(\frac{49}{397}\right) = (1)(-1)(1) = -1$$

For which [odd] p is $\left(\frac{7}{p}\right) = 1$? Modulo 7: $1, 2, 4$ are QR, $3, 5, 6$ are not.

$$\text{If } p \equiv 1\ (4): \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \begin{cases} 1 \text{ if } p \equiv 1, 2, 4\ (7) \\ -1 \text{ if } p \equiv 3, 5, 6\ (7) \end{cases}$$

$$\text{If } p \equiv 3\ (4): \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = \begin{cases} -1 \text{ if } p \equiv 1, 2, 4\ (7) \\ 1 \text{ if } p \equiv 3, 5, 6\ (7) \end{cases}$$

Combining these two conditions, we see that if:

$p \equiv 1\ (28)$, $\left(\frac{7}{p}\right) = 1$ $\quad$ $p \equiv 3\ (28)$, $\left(\frac{7}{p}\right) = 1$ $\quad$ $p \equiv 5\ (28)$, $\left(\frac{7}{p}\right) = -1$ $\quad$ $p \equiv 9\ (28)$, $\left(\frac{7}{p}\right) = 1$ $\quad$ &c.

Lemma 3 (Gauss' Lemma)**.**
$a \in \mathbb{Z}$, p odd prime, $p \nmid a$. For each j, let s_j be such that $s_j = a \cdot j \pmod p$:

$$-\left(\frac{p-1}{2}\right) \leq s_j \leq \frac{p-1}{2}$$

Let $S(a,p) = \#\{j : 1 \leq j \leq \frac{p-1}{2}, s_j < 0\}$. Then $\left(\frac{a}{p}\right) = (-1)^{S(a,p)}$.

Proof.

$$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} = a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \equiv (s_1)(s_2)(s_3)\ldots\left(s_{\frac{p-1}{2}}\right) \pmod p$$

Claim: $\left\{|s_1|, \ldots, \left|s_{\frac{p-1}{2}}\right|\right\} = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$. It suffices to show that $1 \leq i < j \leq \frac{p-1}{2} \implies |s_i| \neq |s_j|$ ($\iff s_i \neq \pm s_j$):

- If $s_i = s_j$ then $aj \equiv ai \pmod p \implies p | a(j-i) \implies p|a$ since $0 < j - i < \frac{p-1}{2} < p$
- If $s_i = -s_j$ then $p | a(j+i) \implies p|a$ since $0 \leq j + i < p - 1 < p$

Hence the claim is proved. So we see that:

$$\left(\frac{p-1}{2}\right)!a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)!(-1)^{S(a,p)} \pmod{p}$$

$$\implies a^{\frac{p-1}{2}} \equiv (-1)^{S(a,p)} \pmod{p}$$

□

[End lecture 12, 04/11/14]

Recall the following:

- Law of Quadratic Reciprocity: p, q odd primes, $p \neq q$: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$
- It's been proven that $\left\{|s_1|, |s_2|, \ldots, \left|s_{\frac{p-1}{2}}\right|\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. $s_j \equiv aj \pmod{p}$ and $-\frac{p-1}{2} \leq s_j \leq \frac{p-1}{2}$
- $S(a,p) = \#\{j : 1 \leq j \leq \frac{p-1}{2},\ s_j < 0\}$. Gauss' Lemma: $\left(\frac{a}{p}\right) = (-1)^{S(a,p)}$

Related question: Given $a \in \mathbb{Z}$, for which odd p is $\left(\frac{a}{p}\right) = 1$? We want to control $S(p,q)$, $S(q,p)$, p, q odd.

Lemma 4. *Let a be odd and p be an odd prime such that p does not divide a.*

$$S(a,p) \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor \ \ (mod\ 2)$$

Proof. Idea:

$$aj = \left\lfloor \frac{aj}{p} \right\rfloor \cdot p + r_j \quad 0 \leq r_j < p$$

- If $s_j > 0$: $r_j = s_j$
- If $s_j < 0$: $r_j = s_j + p$

$$\frac{p^2-1}{8} = \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} |s_j| = \sum_{\substack{j=1 \\ s_j>0}}^{\frac{p-1}{2}} s_j + \sum_{\substack{j=1 \\ s_j<0}}^{\frac{p-1}{2}} (-s_j) = \sum_{\substack{j=1 \\ s_j>0}}^{\frac{p-1}{2}} r_j - \sum_{\substack{j=1 \\ s_j<0}}^{\frac{p-1}{2}} (r_j - p)$$

$$= \sum_{\substack{j=1 \\ s_j>0}}^{\frac{p-1}{2}} r_j - \sum_{\substack{j=1 \\ s_j<0}}^{\frac{p-1}{2}} r_j + pS(a,p) \equiv \sum_{j=1}^{\frac{p-1}{2}} r_j + S(a,p) \pmod{2}$$

Also:

$$a\frac{p^2-1}{8} = \sum_{j=1}^{\frac{p-1}{2}} aj = \sum_{j=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{aj}{p} \right\rfloor \cdot p + r_j\right) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor \cdot p + \sum_{j=1}^{\frac{p-1}{2}} r_j$$

$$\overset{\text{reduce (mod 2)}}{\implies} \frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} r_j \pmod{2}$$

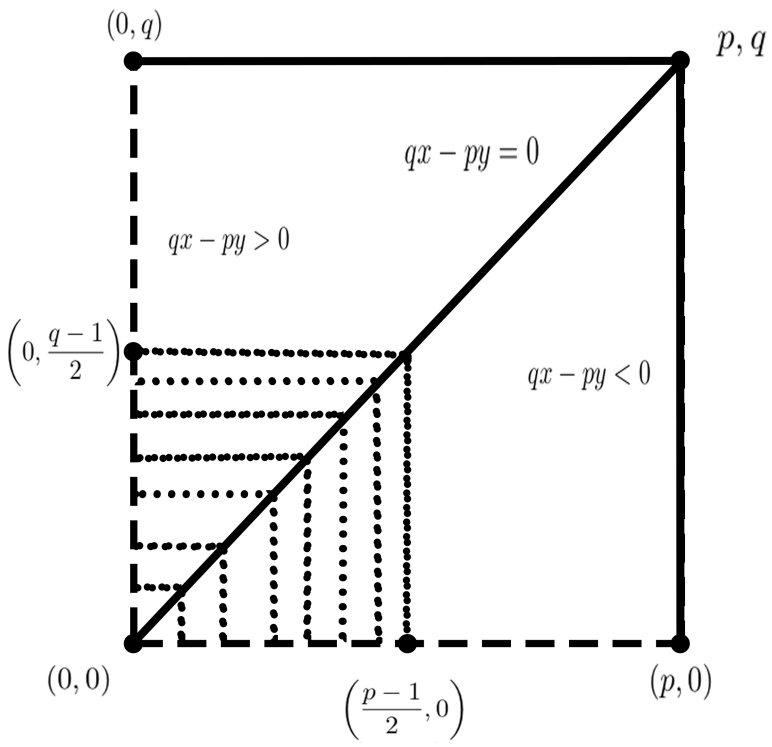
Combine:

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor + \underbrace{\sum_{j=1}^{\frac{p-1}{2}} r_j}_{\text{CANCEL}} \equiv \sum_{j=1}^{\frac{p-1}{2}} r_j + S(a,p)$$

□

$\left(\frac{a}{p}\right) = (-1)^{S(a,p)}$. If a is odd, $S(a,p) \equiv T(a,p) \pmod 2$, where $T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{aj}{p} \right\rfloor$.

So, if a is odd, $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$. The final step: p, q odd primes, $p \neq q$. Then $T(p,q)+T(q,p) = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.



Consider the points $(x,y) : 1 \leq x \leq \frac{p-1}{2}$, $1 \leq y \leq \frac{q-1}{2}$. The total number of such points is $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$. The first thing to note is that there are no lattice points on the diagonal except for $(0,0)$ and (p,q) because if (x,y) is on the diagonal then we have, by definition, $qx - py = 0 \implies q|y$ and $p|x$, which isn't possible.

The points below the diagonal: When $x = j$, y ranges from 1 to the largest possibly y such that $qx - py > 0 \implies y < \frac{qx}{p}$. When $x = j$, this is $\left\lfloor \frac{qj}{p} \right\rfloor$.

So, the number of points below the diagonal $= \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor = T(q,p)$.

The points above the diagonal: When $y = j$, x ranges from 1 to the largest possible x such that $qx - py < 0 \implies x < \frac{py}{q}$. When $y = j$, this is $\left\lfloor \frac{pj}{q} \right\rfloor$.

So, the number of points above the diagonal $= \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor = T(p,q)$.

The total number of points $= T(p,q) + T(q,p) = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.

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

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

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(p,q)+T(q,p)} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

This finally proves the Law of Quadratic Reciprocity.

[End lecture 13, 06/11/14]

3.2 Sums of Two Squares

$$x^2 + y^2 = n, \quad n \in \mathbb{Z}, \quad n \geq 0$$

1. For a given n, does $x^2 + y^2 = n$ have any integer solutions? If so, we'll say n is 'a sum of two squares'. Example: $3^2 + 2^2 = 13$.

2. If there are solutions, how many are there? Note: Only finitely many: $x^2 + y^2 = n$, $-\sqrt{n} \leq x, y \leq \sqrt{n}$.

Observation: $x, y \in \mathbb{Z}$,

$$x^2 \equiv 0, 1 \pmod 4$$
$$y^2 \equiv 0, 1 \pmod 4$$

So $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. If $n \equiv 3 \pmod 4$, then there are no solutions to $x^2 + y^2 = n$.

The converse is not true. $21 \equiv 1 \pmod 4$, but 21 is not a sum of two squares.

Note: If $n = x^2 + y^2 = (x + iy)(x - iy)$, $i^2 = -1$. So if $n = x^2 + y^2 = (x + iy)(x - iy)$ and $m = z^2 + w^2 = (z + iw)(z - iw)$ then:

$$\begin{aligned} mn &= (x + iy)(x - iy)(z + iw)(z - iw) \\ &= (xz - yw + i(xw + yz))(xz - yw - i(xw + yz)) \\ &= (xz - yw)^2 + (xw + yz)^2 \end{aligned}$$

Furthermore, obviously if n is a sum of two squares then so is $m^2 n$. $n = x^2 + y^2$, $m^2 n = (nx)^2 + (my)^2$.

Corollary: If $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, p_i prime, and for each i either r_i is even or p_i is the sum of two squares, then n is the sum of two squares. [Indeed, if all r_i are even there we can take $0^2 + \sqrt{n}^2 = n$.]

Theorem 10 (Fermat's Two-Square Theorem)**.**
Every prime $p \equiv 1$ (mod 4) is the sum of two squares.

Proof. $p \equiv 1 \pmod 4 \implies \left(\frac{-1}{p}\right) = 1$. Let $x \in \mathbb{Z}$ such that $x^2 \equiv -1 (\text{mod } p)$, $p | x^2 + 1$.

We can assume $0 \leq x < p$ [because otherwise for some $n \geq 1$, $x^2 \equiv (x \pm np)^2 \pmod p$]. $x^2 + 1 = pM$, $M \in \mathbb{Z}$ and so $1 \leq M < p$. [Note that $M \neq p$ as this $\implies x^2 + 1 = p^2$, which is clearly impossible.]

If $M = 1$, we're done [as $p = x^2 + 1^2$]. So suppose $M > 1$. Set: $a_0 := x$; $b_0 := 1$; $M_0 := M$. $a_0^2 + b_0^2 = M_0 p$.

We're going to construct a_i, b_i, M_i such that $a_i^2 + b_i^2 = M_i p$ with $1 \leq M_i < M_{i-1}$, inductively.

Suppose we have $a_i^2 + b_i^2 = M_i p$, $M_i > 1$. Choose:

$$x_i \equiv a_i \pmod{M_i}$$
$$y_i \equiv b_i \pmod{M_i}$$

such that $-\frac{M_i}{2} \leq x_i, y_i \leq \frac{M_i}{2}$.

$a_i^2 + b_i^2 = M_i p \equiv 0 \pmod{M_i}$ so $x_i^2 + y_i^2 \equiv 0 \pmod{M_i}$. $x_i^2 + y_i^2 = M_i \cdot r$ for some $r \in \mathbb{Z}$. $0 \leq r \leq \frac{M_i}{2}$.

$$\begin{aligned} &M_i p = a_i^2 + b_i^2 \\ &M_i r = x_i^2 + y_i^2 \end{aligned} \implies M_i^2 pr = (x_i^2 + y_i^2)(a_i^2 + b_i^2)$$
$$= (x_i a_i + y_i b_i)^2 + (x_i b_i - y_i a_i)^2$$

$x_i a_i + y_i b_i \equiv a_i^2 + b_i^2 \equiv 0 \pmod{M_i}$ So $M_i | x_i a_i + y_i b_i$

$x_i b_i - y_i a_i \equiv a_i b_i - a_i b_i = 0 \pmod{M_i}$ So $M_i | x_i b_i - y_i a_i$

Set $a_{i+1} := \frac{x_i a_i + y_i b_i}{M_i}$, $b_{i+1} := \frac{x_i b_i - y_i a_i}{M_i} \implies a_{i+1}^2 + b_{i+1}^2 = pr$, $r \leq \frac{M_i}{2}$. Set $M_{i+1} := r$. Repeat until $M_n = 1$. $\square$

Example : $8^2 \equiv -1 \pmod{13}$. $8^2 + 1^2 = 65 = 5 \cdot 13$. $\{a_0 = 8, b_0 = 1, M_0 = 5\}$, $x_0 = -2$, $y_0 = 1$. $a_1 = \frac{-2\cdot 8+1}{5} = -3$, $b_1 = \frac{-2\cdot 1-8}{5} = -2$. $a_1^2 + b_1^2 = (-3)^2 + (-2)^2 = 13$. [In this case $M_1 = 1$ and we're done.]

Corollary: If any number, n, is of the form:

$$n = (\text{perfect square}) \cdot \prod_{\substack{p_i:\ p_i \text{ prime} \\ p_i=2 \text{ or } p_i \equiv 1\ (4)}} p_i$$

then n is a sum of two squares. [Note that $p_i = 2$ follows since $2n := 2(x^2 + y^2) = (x + y)^2 + (x - y)^2$.]

Theorem 11. *Every sum of two square of this form.*

[The only-if counterpart of Fermat's Two Square Theorem, as it was stated in lectures, is trivial. Since p is an odd prime it's either $\equiv 1$ or 3 (mod 4), but a sum of two squares obviously cannot be $\equiv 3 \pmod 4$.]

[End lecture 14, 07/11/14]

3.3 Gaussian Integers

Definition. *The set of Gaussian integers [denoted $\mathbb{Z}[i]$] is the set $\{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$.*

Note: $\mathbb{Z}[i]$ is closed under addition and multiplication. [Multiplication: $(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$.]

Definition. *Let $x, y \in \mathbb{Z}[i]$. We say that x divides y $[x|y]$ if there exists $d \in \mathbb{Z}[i]$ such that $dx = y$.*

Question: Which elements of $\mathbb{Z}[i]$ divide 1? Example: $(i)(-i) = 1$.

Definition. *For $x \in \mathbb{Z}[i]$ let $N(x)$, the norm of x, denote the product $x \cdot \overline{x}$. E.g. $N(a + bi) = a^2 + b^2$.*

Useful properties:

- N takes integer values on $\mathbb{Z}[i]$.
- $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$.

Corollary: If $x|y$ in $\mathbb{Z}[i]$ then $N(x)|N(y)$ in $\mathbb{Z}$.

Proof. $x|y \implies y = dx \implies N(y) = N(d)N(x) \implies N(x)|N(y)$. □

If $x|1$ in $\mathbb{Z}[i]$, then $N(x)|N(1) = 1$ so $N(x) = 1$.

If $x \in \mathbb{Z}[i]$ with $N(x) = 1$ then we can write $x = a + ib$, $N(x) = a^2 + b^2 = 1$. So we must either have $a^2 = 1$, $b^2 = 0$, $x = \pm 1$ or $a^2 = 0$, $b^2 = 1$, $x = \pm i$.

Definition. *An element of $\mathbb{Z}[i]$ is a unit if it divides 1.*

Units divide every element of $\mathbb{Z}[i]$. If u is a unit then $u^{-1} \in \mathbb{Z}[i]$ and so we can rewrite n as follows: $n = uu^{-1}n$ and this holds $\forall n \in \mathbb{Z}[i]$ and all units u; both u and un divide n.

Definition. *An associate of $n \in \mathbb{Z}[i]$ is an element of the form un, where u is a unit in $\mathbb{Z}[i]$.*

Definition. *An element of $\mathbb{Z}[i]$ is irreducible if its only divisors are units and its associates.*

Example: 3 is irreducible in $\mathbb{Z}[i]$. Let's suppose that we have $x|3$ in $\mathbb{Z}[i]$, then $N(x)|N(3) = 9$:

- If $N(x) = 1$, then x is a unit
- If $N(x) = 9$, $x = a+bi$, $a^2+b^2 = 9 = 3^2+0^2$ [this is the only way of writing 9 as the sum of two squares] so either $\{a^2 = 9, b^2 = 0, x = \pm 3\}$ or $\{a^2 = 0, b^2 = 9, x = \pm 3i\}$. So x is an associate of 3
- If $N(x) = 3$, $x = a + bi$, $a^2 + b^2 = 3$. This obviously can't happen

Example: 5 is not irreducible in $\mathbb{Z}[i]$. E.g. $5 = (2 + i)(2 - i)$, neither of which is a unit.

An odd prime $p \in \mathbb{Z}$ is irreducible in $\mathbb{Z}[i]$ if and only if p is not the sum of two squares.

Proof. If $p = a^2 + b^2$, then $p = (a+bi)(a-bi)$, so p is not irreducible. If p is not irreducible, then p has a divisor x that is a unit or an associate. $p = xd$. $N(p) = N(x)N(d)$. $p^2 = N(x)N(d)$, but d, x are not a units, so $N(x), N(d) \neq 1 \implies N(x) = p$. But on writing $x = a + bi$, $p = a^2 + b^2$, i.e. it's the sum of two squares. □

Clearly over $\mathbb{Z}$, given $a, b \in \mathbb{Z}$ such that $a > b > 0$, $\exists!$ q, r such that $a = bq + r$ with $0 \leq r < b$.

Theorem 12 (Gaussian Division Theorem)**.**
Given $a, b \in \mathbb{Z}[i]$ there exist $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$ with $N(r) < N(b)$.

Proof. Let $q' := \frac{a}{b} \in \mathbb{C}$. So $q' = \frac{a\bar{b}}{N(b)} =: x' + iy'$ with $x', y' \in \mathbb{Q}$. Now choose $x, y \in \mathbb{Z}$ such that $|x - x'| \leq \frac{1}{2}$, $|y - y'| \leq \frac{1}{2}$. Let $q := x + iy \in \mathbb{Z}[i]$:

$$N(q' - q) = |x' - x|^2 + |y' - y|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Set $r := a - bq = bq' - bq = b(q' - q)$. So:

$$N(r) = N(b)N(q' - q) \leq \frac{N(b)}{2} < N(b)$$

□

Definition. *Let $a, b \in \mathbb{Z}[i]$. An element x of $\mathbb{Z}[i]$ is a greatest common divisor of a and b if:*

- *$x|a$ and $x|b$*
- *For any $d \in \mathbb{Z}[i]$ such that $d|a$ and $d|b$ we have $d|x$*

Result: If x, y are both GCDs of a, b then x and y are associates.

Proof. By the first property, $x|a$, $x|b$. By the second property, y is a GCD so $x|y$. Symmetrically, $y|x$.

$$\begin{cases} x = uy \\ y = u'x \end{cases} \implies x = uu'x \implies uu' = 1 \text{ so } u, u' \text{ are units.}$$

□

Theorem 13. *If $a, b \in \mathbb{Z}[i]$, $b \neq 0$, then there exists a GCD, x, of a, b in $\mathbb{Z}[i]$. Moreover, x is of the form $ra + sb$ with $r, s \in \mathbb{Z}[i]$.*

[End lecture 15, 11/11/14]

Proof. Assume WLOG $N(b) \leq N(a)$. If $b = 0$ we're done [$1 \cdot a + 0 \cdot b = a$ is a GCD of a and b]. If $b \neq 0$, write:

$$\begin{aligned} a &= q_1 b + r_1 && N(r_1) < N(b) \\ b &= q_2 r_1 + r_2 && N(r_2) < N(r_1) \quad [\text{if } r_1 \neq 0] \\ r_1 &= q_3 r_2 + r_3 && N(r_3) < N(r_2) \quad [\text{if } r_2 \neq 0] \\ &&& \&\text{c.} \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

Claim: r_k is a GCD of a and b.

Proof. $r_k | r_{k-1}$ by the last equation. $r_{k-2} = q_k r_{k-1} + r_k$ so $r_k | r_{k-2}$. Similarly $r_k | r_i$ $\forall i \leq k-1$. Furthermore $b = q_2 r_1 + r_2$ so $r_k | b$ and $a = q_1 b + r_1$ so $r_k | a$. Unwinding this algorithm we see that we can write r_k as $ra + sb$ with $r, s \in \mathbb{Z}[i]$. If $d|a$ and $d|b$ then $d|ra + sb$ so $d|r_k \implies r_k$ is a GCD. □

□

Definition. *$a, b \in \mathbb{Z}[i]$ are relatively prime if a, b have no common divisors other than units. [In this case 1 is a GCD of a and b.]*

Theorem 14. *If a and b are relatively prime and $a|bc$, then $a|c$.*

Proof. We can write $1 = ra + sb$, $r, s \in \mathbb{Z}[i]$. Then $c = rac + sbc$, with both terms on the RHS divisible by a, so $a|c$. □

Theorem 15. *In particular, if p is irreducible in $\mathbb{Z}[i]$ and $p|bc$ then $p|b$ or $p|c$.*

Proof. Let d be a GCD of p and b. Then $d|p$, so d is either a unit or an associate of p. If d is a unit then b, p are relatively prime so $p|c$: if d is an associate of p, then $d|b \implies p|b$. □

Definition. *An element $p \in \mathbb{Z}[i]$ is prime if $\forall b, c \in \mathbb{Z}[i]$ $p|bc \implies p|b$ or $p|c$.*

So, in fact, Theorem 15. just says all irreducible elements are also prime.

Theorem 16. *Any $x \in \mathbb{Z}[i]$ factors into a product of irreducibles. This factorisation is unique up to reordering of associates. If $x = p_1 \dots p_r = q_1 \dots q_s$ with all p_i, q_j irreducible then the number of factors on both sides is the same ($r = s$) and $\exists$ a reordering of the q_i's such that q_i is an associate of p_i $\forall i$.*

Question: Given $p \in \mathbb{Z}$ prime, does p remain prime in $\mathbb{Z}[i]$? Not always.

Examples: $2 = (1-i)(1+i)$; $5 = (2-i)(2+i)$.

3 is prime in $\mathbb{Z}[i]$. Indeed, in Lecture 15 we saw that 3 is irreducible in $\mathbb{Z}[i]$ and so is also prime in $\mathbb{Z}[i]$.

Theorem 17. *In fact if $p \in \mathbb{Z}$ is a prime satisfying $p \equiv 3 \pmod 4$ then p remains prime in $\mathbb{Z}[i]$.*

Proof. Similarly to $p = 3$, it suffices to show that p is irreducible in $\mathbb{Z}[i]$ in order to show that it's prime in $\mathbb{Z}[i]$. $N(p) = p^2$ so if $d|p \implies N(d) = 1, p, p^2$:

- $N(d) = 1 \implies d$ is a unit
- $N(d) = p^2 \implies d$ is an associate [$p^2 + 0^2 = p^2$ is the only way of writing p^2 as such a sum]
- $N(d) = p \implies p = d_x^2 + d_y^2$, which can't happen as p is not a sum of two squares

□

Theorem 18. *If $p \in \mathbb{Z}$ is prime and $p \equiv 1 \pmod 4$, then p is not prime in $\mathbb{Z}[i]$.*

Proof. $\left(\frac{-1}{p}\right) = 1 \implies \exists n \in \mathbb{Z}$ such that $p|n^2+1$ so $p|(n+i)(n-i)$ in $\mathbb{Z}[i]$ [recall that we can assume $0 \leq n < p$]. But $p \not| (n \pm i)$ so p can't be prime. □

Corollary: Every prime $p \equiv 1 \pmod 4$ is the sum of two squares.

Proof. $p \in \mathbb{Z}$ is not prime in $\mathbb{Z}[i]$ so p cannot be irreducible. So $\exists d|p \in \mathbb{Z}[i]$, such that d is neither a unit nor an associate. $N(d) \in \{1, p, p^2\}$ but $N(d) \neq 1$ [as d is not a unit] and $N(d) \neq p^2$ [as d is not an associate of p], so $p = N(d)$. On writing $d = a + ib$, we see that $p = N(d) = a^2 + b^2$.

□

Key point: We can write down all primes in $\mathbb{Z}[i]$:

- $p = i + 1$ and associates [$N(p) = 2$ so $1 + i$ is irreducible and thus prime]
- $p \in \mathbb{Z}$: $p \equiv 3 \pmod 4$ and associates [$N(p) = p^2$ and $N(d) \neq p$ for $d|p \implies$ irreducible $\implies$ prime]
- $a \pm bi$ such that $N(a \pm bi) = a^2 + b^2 = p$ is an odd prime

Claim: Every prime, p, of $\mathbb{Z}[i]$ is an associate of a prime on that list.

Proof. It suffices to show that there is an integer $p_i \in \mathbb{Z}$, prime [as an element of $\mathbb{Z}$], such that $p|p_i$. Now $p\overline{p} = N(p)$, so $p|N(p)$. Writing $N(p) = p_1 p_2 \dots p_r$, with p_i's being integer primes. $p|N(p) \implies p|p_i$ for some i.

So p does indeed divide an integer prime, which means, since the above list contains the factorisations of all integer primes, p is on that list. □

[End lecture 16, 13/11/14]

[This lecture was a problems class.]

[End lecture 17, 14/11/14]

We have previously shown: If every prime p dividing $n \in \mathbb{Z}_{\geq 0}$ such that $p \equiv 3 \pmod 4$ appeared with even exponent in the prime factorisation, then n is the sum of two squares. We can now prove that every sum of two squares has this form.

Theorem 19. *Suppose $n \in \mathbb{Z}$ is the sum of two squares [$n = a^2 + b^2$]. Then the exponent of any prime $p \in \mathbb{Z}$ that appears in the factorisation of n such that $p \equiv 3 \pmod 4$ is even.*

Proof. $n = a^2+b^2 = (a+bi)(a-bi)$. Consider the prime factorisation of n in $\mathbb{Z}[i]$. Let p be a prime $\equiv 3 \pmod 4$. Then p is prime in $\mathbb{Z}[i]$. Note: $p^k | a+bi \iff p^k | a$ and $p^k | b \iff p^k | a-bi$. Let k be the largest power of p such that $p^k | a+bi$ in $\mathbb{Z}[i]$, so k is also the largest power of p such that $p^k | a-bi$. So p^{2k} is the largest power of p dividing n. □

Examples:

- $21 = 3 \cdot 7$ and so is not the sum of two squares.
- p prime $\equiv 1 \pmod 4$, $p = (a+bi)(a-bi)$.
- $n = p^2 q$, $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$. $q = a^2 + b^2$. $n = p^2(a+bi)(a-bi)$.

  $$n = pu(a+bi) \cdot pu^{-1}(a-bi) \qquad 4 \text{ ways } (\pm pa)^2 + (\pm pb)^2$$
  $$n = pu(a-bi) \cdot pu^{-1}(a+bi) \qquad 4 \text{ ways } (\pm pb)^2 + (\pm pa)^2$$

  So in total there are 8 ways of writing this n as the sum of two squares.
- $n = p^2$, $p \equiv 1 \pmod 4$, $p = a^2 + b^2$ so $p^2 = (a+bi)^2(a-bi)^2$. $(a+bi)^2 = a^2 - b^2 + 2abi$:

  $$n = u(a+bi)^2 \cdot u^{-1}(a-bi)^2 \to p^2 = (a^2-b^2)^2 + (2ab)^2 \qquad +3 \text{ associates}$$
  $$n = u(a+bi)(a-bi) \cdot u^{-1}(a+bi)(a-bi) \to p^2 = (a^2+b^2)^2 + 0^2 \qquad +3 \text{ associates}$$
  $$n = u(a-bi)^2 \cdot u^{-1}(a+bi)^2 \to p^2 = (2ab)^2 + (a^2-b^2)^2 \qquad +3 \text{ associates}$$

If every $p \equiv 3 \pmod 4$ appears with even exponent in the factorisation of n, then the number of ways to write n as the sum of two squares is:

$$4 \prod_{\substack{p|n \\ p \equiv 1(4)}} (1 + ord_p(n))$$

where $ord_p(n)$ is the largest power of p dividing n.

Definition. *Let $\omega = \frac{-1+\sqrt{-3}}{2}$, $\omega^2 + \omega + 1 = 0$ [so $\omega^3 = 1$]. The <u>Eisenstein integers</u>, $\mathbb{Z}[\omega]$, form the subset of $\mathbb{C}$ consisting of elements of the form $a + b\omega$, $a, b \in \mathbb{Z}$, closed under multiplication and addition.*

$N : \mathbb{Z}[\omega] \to \mathbb{C}$. $a+b\omega \to (a+b\omega)(a+b\overline{\omega}) = a^2+ab(\omega+\overline{\omega})+b^2\omega\overline{\omega} = a^2-ab+b^2$. So N is the integer valued on $\mathbb{Z}[\omega]$.

Question: Which $n \in \mathbb{Z}$ are of the form $n = a^2 - ab + b^2$, $a, b \in \mathbb{Z}$? It's connected to factorisation in $\mathbb{Z}[\omega]$.

If $n = a^2 - ab + b^2$, $m = c^2 - cd + d^2$ then nm is also of this form. $\omega^2 = -\omega - 1$, $\overline{\omega}^2 = -\overline{\omega} - 1$, $\omega\overline{\omega} = 1$.

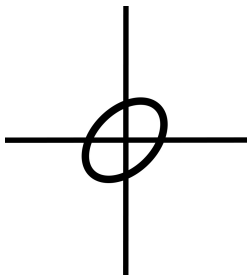
$$n = (a + b\omega)(a + b\overline{\omega})$$
$$m = (c + d\omega)(c + d\overline{\omega})$$
$$nm = (a + b\omega)(c + d\omega)(a + b\overline{\omega})(c + d\overline{\omega})$$
$$nm = (ac + bd\omega^2 + (ad + bc)\omega)(ac + bd\overline{\omega}^2 + (ad + bc)\overline{\omega})$$
$$nm = (ac - bd + (ad + bc - bd)\omega)(ac - bd + (ad + bc - bd)\overline{\omega})$$

So $mn = (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 = (a^2 - ab + b^2)(c^2 - cd + d^2)$.

So $N(xy) = N(x)N(y)$. Question: Is there unique factorisation in $\mathbb{Z}[\omega]$. Answer: Yes!

[End lecture 18, 18/11/14]

Units: In $\mathbb{Z}[\omega]$, $N(xy) = N(x)N(y)$. N takes values in $\mathbb{Z}_{\geq 0}$. So if $xy = 1$. $N(x)N(y) = 1 \implies N(x), N(y) = 1$. We want $(a, b) : a^2 - ab + b^2 = 1$. $\{\pm(1,0), \pm(1,1), \pm(0,1)\}$ fit this equation, so the units are ± 1, $\pm\omega$, $\pm(1+\omega)$.



Definition. *$x, y \in \mathbb{Z}[\omega]$, we say that x <u>divides</u> y, $x|y$, if $\exists d \in \mathbb{Z}[\omega] : y = dx$.*

Definition. *$x \in \mathbb{Z}[\omega]$ is <u>irreducible</u> if its only divisors are of the form u or ux, with u a unit in $\mathbb{Z}[\omega]$.*

Definition. *$x \in \mathbb{Z}[\omega]$ is <u>prime</u> if x is not a unit, $x \neq 0$, and whenever $x|yz$, either $x|y$ or $x|z$ [$y, z \in \mathbb{Z}[\omega]$].*

Question: Are all irreducible elements also prime elements? Key point for $\mathbb{Z}[i]$: Given $a, b \in \mathbb{Z}[i]$, $b \neq 0$, $\exists q, r \in \mathbb{Z}[i]$: $a = qb + r$, $N(r) < N(b)$.

Theorem 20. *Let $a, b \in \mathbb{Z}[\omega]$, $b \neq 0$. $\exists q, r \in \mathbb{Z}[\omega] : a = qb + r$, $N(r) < N(b)$.*

Proof. Let $q' := \frac{a}{b} =: x' + y'\omega$, $x', y' \in \mathbb{Q}$. Let $x, y \in \mathbb{Z}$ such that $|x - x'|, |y - y'| \leq \frac{1}{2}$. Take $q := x + y\omega$ so $r = a - qb$. Hence $r = a - qb = b(q' - q) = b[(x' - x) + (y' - y)\omega]$.

Now $N(r) = N(b) \cdot N[(x-x') + (y-y')\omega] = N(b) \cdot [(x-x')^2 - (x-x')(y-y') + (y-y')^2] \leq N(b) \cdot \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) \leq \frac{3}{4}N(b) < N(b)$. So $N(r) < N(b)$, as required. □

3.4 Euclidean Algorithm

Definition. *$d \in \mathbb{Z}[\omega]$ is a <u>GCD</u> of $a, b \in \mathbb{Z}[\omega]$ if $d|a$, $d|b$, and $\forall x \in \mathbb{Z}[\omega]$ such that $x|a, x|b$, we have $x|d$.*

Theorem 21. *For any $a, b \in \mathbb{Z}[\omega]$, not both zero, a GCD of $a, b \in \mathbb{Z}[\omega]$ exists. More precisely, $\exists x, y \in \mathbb{Z}[\omega]$ such that $xa + by$ is a GCD of a, b.*

Proof. Omitted. It's near identical to that with $\mathbb{Z}[i]$.

□

Corollary: Irreducibles in $\mathbb{Z}[\omega]$ are prime in $\mathbb{Z}[\omega]$.

Proof. Let x be irreducible and suppose $x|yz$, $y, z \in \mathbb{Z}[\omega]$. If $x|y$ we're done. Otherwise, x irreducible $\implies 1$ is a GCD of x and y. $\exists a, b \in \mathbb{Z}[\omega]$ such that $ax + by = 1$. Then $axz + byz = z$. $x|axz$, $x|byz$ [since $x|yz$] so $x|z$. □

Corollary: Unique factorisation in $\mathbb{Z}[\omega]$.

Application: Representability by $a^2 - ab + b^2$:

- For which $n \in \mathbb{Z}$ is n of the form $a^2 - ab + b^2$?
- For which $n \in \mathbb{Z}$ is n of the form $N(x)$, $x \in \mathbb{Z}[\omega]$?

Let's look (mod 3) at $(a^2 - ab + b^2)$:

$$\begin{pmatrix} \underline{[b]\backslash[a]} & | & \underline{[0]} & \underline{[1]} & \underline{[2]} \\ [0] & | & [0] & [1] & [1] \\ [1] & | & [1] & [1] & [0] \\ [2] & | & [1] & [0] & [1] \end{pmatrix}$$

So $a^2 - ab + b^2 \not\equiv 2 \pmod 3$. Recall that if n, m are representable [of the form $a^2 - ab + b^2$] then so is mn.

Question: Which primes are of the form $a^2 - ab + b^2$?

There are three cases:

- $p \equiv 0 \pmod 3 \implies p = 3$. $3 = 2^2 - (2 \cdot 1) + 1^2$ is representable
- $p \equiv 2 \pmod 3$. This is never representable, as we've just seen
- $p \equiv 1 \pmod 3$. This is a hard case

Theorem 22. *Let p be a prime $\in \mathbb{Z}$. $p \equiv 1 \pmod 3$. Then $\exists a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.*

Proof. We'll show that p is not prime in $\mathbb{Z}[\omega]$. Then $p = xy$ for some $x, y \in \mathbb{Z}[\omega]$ such that neither x nor y are units. Then $N(p) = N(x)N(y)$, $p^2 = N(x)N(y)$, so we must have $N(x) = N(y) = p$ so on writing $x = a + b\omega$, we have $p = a^2 - ab + b^2$.

So it does indeed suffice to show that p is not prime in $\mathbb{Z}[\omega]$. Consider the equation $x^2 + x + 1 = 0$ in $\mathbb{Z}/p$. Because $(x^2 + x + 1)(x - 1) = x^3 - 1$, the solutions to $x^2 + x + 1$ are solutions to $x^3 - 1 = 0$.

Claim: If $p \equiv 1 \pmod 3$, then there are three distinct solutions to $x^3 \equiv 1 \pmod p$.

Proof. Let g be a primitive root. $\forall x \in \left\{g^{p-1}, g^{\frac{p-1}{3}}, g^{\frac{2(p-1)}{3}}\right\}$, $x^3 \in \left\{g^{3(p-1)}, g^{p-1}, g^{2(p-1)}\right\} \equiv \{1\} \pmod 3$. □

So $x^2 + x + 1$ has two roots (mod p). Let α be one such root, then $a := -\alpha$ is a root of $x^2 - x + 1$. So $\exists a \in \mathbb{Z}$: $p | a^2 - a + 1$. We can assume that $0 \leq a < p$ since $(a \pm np)^2 - (a \pm np) + 1 \equiv a^2 - a + 1 \pmod p$ $[\forall n \geq 1]$.

Now in $\mathbb{Z}[\omega]$, $a^2 - a + 1 = (a + \omega)(a + \overline{\omega})$. So in $\mathbb{Z}[\omega]$, $p | (a + \omega)(a + \overline{\omega})$. But p cannot divine either of these so p is not prime in $\mathbb{Z}[\omega]$ and we're done! □

[End lecture 19, 21/11/14]

In $\mathbb{Z}[i]$ we were able to conclude that every $p \equiv 1 \pmod 4$ is of the form $a^2 + b^2$. In $\mathbb{Z}[\omega]$ we discovered that every $p \equiv 1 \pmod 3$ is of the form $a^2 - ab + b^2$. $[a, b \in \mathbb{Z}]$.

Question: Given $z \in \mathbb{C}$, when is $\{a + bz : a, b \in \mathbb{Z}\}$ closed under $+, \circ$? $+$: always. $\circ$: harder.

Observe: If $\{a + bz : a, b \in \mathbb{Z}\}$ is closed under multiplication, then z^2 is in this set $\implies z^2 = a + bz$ for some $a, b \in \mathbb{Z}$. So $z^2 - bz - a = 0$, i.e. z satisfies a quadratic polynomial that is monic with integer coefficients.

Conversely, suppose $z^2 - bz - a = 0$ for some $a, b \in \mathbb{Z}$. Then $[c, d, e, f \in \mathbb{Z}]$:

$$\begin{aligned}(c + dz)(e + fz) &= ce + cfz + dez + dfz^2 \\ &= ce + (cf + de)z + df(bz + a) \\ &= (ce + dfa) + (cf + de + dfb)z \; [\in \mathbb{Z}[z]]\end{aligned}$$

Definition. *Let $z \in \mathbb{C}$ satisfy $P(z) = 0$, where P is a monic polynomial of degree 2 with integer coefficients. Then the quadratic subring generated by z, $\mathbb{Z}[z]$, is the set $\{a + bz : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.*

Examples:

- $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, the Gaussian and Eisenstein integers
- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$

Note: Unique factorisation fails in $\mathbb{Z}[\sqrt{-5}]$. Units: If $uv = 1$ in $\mathbb{Z}[\sqrt{-5}]$, $N(u)N(v) = 1 \implies N(u) = N(v) = 1$. So $u, v = \pm 1$. 2 is irreducible but it's not prime:

- If $uv = 2$, then $N(u) \cdot N(v) = 4$ so $N(u) = 1$ $[u = \pm 1, v = \pm 2]$ or $N(u) = 2$ [can't happen] or $N(u) = 4$ $[N(v) = 1$, so $v = \pm 1]$
- 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$: $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. $2|6$ in $\mathbb{Z}[\sqrt{-5}]$. $2 \nmid (1 + \sqrt{-5})$. $2 \nmid (1 - \sqrt{-5})$
- Unique factorisation fails: $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ are all irreducible. None are associates. But $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

Question: Which quadratic subrings of $\mathbb{C}$ have unique factorisation? We needed to be able to repeatedly write:

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$

&c. in such a way that we were eventually guaranteed $r_k = 0$.

Definition. *Let R be a non-zero commutative ring, with no zero divisors. [I.e. if $ab = 0$ in R, then $a = 0$ or $b = 0$.] Then R is an integral domain.*

Definition. *A Euclidean norm on an integral domain, R, is a function $N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that:*

For all $a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ such that:

- $a = qb + r$
- Either $r = 0$ or $N(r) < N(b)$

Exercise: $R = \mathbb{Z}[i]$, $N(a + bi) = a^2 + b^2$ is Euclidean. $R = \mathbb{Z}[\omega]$, $N(a + b\omega) = a^2 - ab + b^2$ is Euclidean.

$R = K[x]$ where K a field, $N(P) :=$ degree of P is a Euclidean norm.

Proof. Given polynomials $a(x), b(x), \exists q(x), r(x)$ such that $a = bq + r$ and $deg(r) < deg(b)$ or $r = 0$. □

If $deg(a) < deg(b)$, take $q = 0$, $r = a$ and done. If $deg(a) \geq deg(b)$, then $\exists c \in K^*$, $m \geq 0$ such that $cx^m = b$ has the same leading term as a i.e. $deg(a - cx^m b) = deg(a) - 1$. We can keep subtracting off multiples of b until the difference has degree smaller than $deg(b)$.

Example: $a = x^4 - x + 1$, $b = x^2 + x + 1$. [So $q = x^2 - x$, $r = 1$.] $a - x^2b = x^4 - x + 1 - x^4 - x^3 - x^2 = -x^3 - x^2 - x + 1$. $a - x^2b + xb = 1$ i.e. $a = b(x^2 - x) + 1$.

Definition. *We call a ring R with Euclidean N a Euclidean domain.*

Theorem 23. *In a Euclidean domain, R, given a, b not both zero, there exists a GCD r of a, b in R , and $x, y \in R$, such that $r = xa + yb$.*

Corollary: If R is a Euclidean domain, then the irreducibles in R are prime.

Definition. *$a \in R$ is irreducible if its only divisors are units and associates. $a \in R$ is prime if whenever $a|xy$ [$x, y \in R$], $a|x$ or $a|y$.*

Definition. *A quadratic subring of $\mathbb{C}$ is imaginary if it is not contained in $\mathbb{R}$.*

Example: $\mathbb{Z}[i]$ is imaginary. $\mathbb{Z}[\sqrt{2}]$ is not imaginary.

The following are the only Euclidean quadratic subrings of $\mathbb{C}$:

$$\mathbb{Z}[i] \qquad \mathbb{Z}[\sqrt{-2}] \qquad \mathbb{Z}[\omega] \qquad \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \qquad \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$$

There are four more imaginary quadratic subrings with unique factorisation:

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \qquad \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right] \qquad \mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right] \qquad \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$$

Theorem 24 (Heegner)**.** *These nine are the only imaginary quadratic rings with unique factorisation.*

Open question: Are there infinitely many real quadratic rings with unique factorisation?

[End lecture 20, 21/11/14]

3.5 Pell's Equation

$$x^2 - dy^2 = 1 \text{ [sometimes } x^2 - dy^2 = -1\text{]}$$

This is Pell's equation; we will be studying this equation for fixed $d \in \mathbb{N}_{>0}$ such that d is non-square to restrict to real quadratic situations. [d wasn't specified to necessarily be an integer in lectures.]

If $d = a^2$, $x^2 - dy^2 = (x + ay)(x - ay)$. If $(x + ay)(x - ay) = 1$, then $x + ay = x - ay \implies y = 0$, $x = \pm 1$.

When d is not a square, we work in $\mathbb{Z}[\sqrt{d}]$. In the imaginary quadratic case, we could define $N(z) := z\overline{z} \in \mathbb{Z}$. In the real case, every $z \in \mathbb{Z}[\sqrt{d}]$ is its own complex conjugate, so $z\overline{z}$ does not necessarily land in $\mathbb{Z}$.

Variation: Given $z = x + y\sqrt{d}$, define $z^* := x - y\sqrt{d}$. Then $N(z) := zz^* = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$. $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$. This is never Euclidean, but multiplicativity does hold; observe $z_i = x_i + y_i\sqrt{d_i}$:

$$(z_1 z_2)^* = x_1 x_2 + d y_1 y_2 - (x_1 y_2 + x_2 y_1)\sqrt{d}$$

So $N(z_1 z_2) = z_1 z_2 z_1^* z_2^* = z_1 z_1^* z_2 z_2^* = N(z_1)N(z_2)$.

Corollary: Given $x_1, y_1, a_1, x_2, y_2, a_2$ such that $x_i^2 - dy_i^2 = a_i$, then $\exists x_3, y_3$ such that $x_3^2 - dy_3^2 = a_1 a_2$.

Proof. Let $z_1 = x_1 + y_1\sqrt{d}$, $N(z_1) = x_1^2 - dy_1^2 = a_1$ and $z_2 = x_2 + y_2\sqrt{d}$, $N(z_2) = a_2$. Let $z_3 = z_1 z_2 = x_3 + y_3\sqrt{d} \implies N(z_3) = N(z_1)N(z_2) \implies x_3^2 - dy_3^2 = a_1 a_2$. Explicitly: $x_3 = (x_1 x_2 + d y_1 y_2)$, $y_3 = (x_1 y_2 + x_2 y_1)$. □

In particular, if $x_1^2 - dy_1^2 = 1$, $x_2^2 - d_1^2 = 1$ then $(x_1 x_2 + d y_1 y_2)^2 - d(x_1 y_2 + x_2 y_1)^2 = 1$. In fact, solutions to Pell's equation form a group under multiplication in $\mathbb{Z}[\sqrt{d}]$:

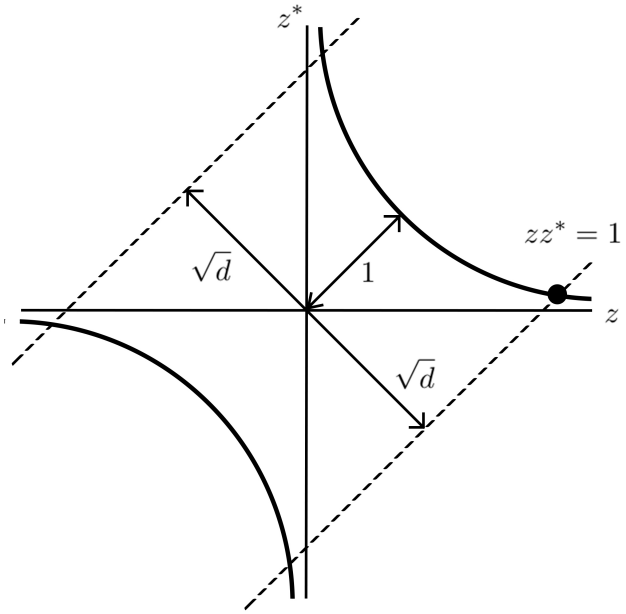
$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 + d y_1 y_2, x_1 y_2 + x_2 y_1)$$

The identity is $1_{\mathbb{Z}[\sqrt{d}]} = (1, 0)$. Inverses are given by $z \to z^*$ in $\mathbb{Z}[\sqrt{d}]$ corresponding to $(x_1, y_1) \to (x_1, -y_1)$.

Let $\mathbb{Z}[\sqrt{d}]^{\times,1}$ be the set of $\{z \in \mathbb{Z}[\sqrt{d}] : N(z) = 1\}$. This is a subgroup of $\mathbb{Z}[\sqrt{d}]^\times$, under multiplication. $\mathbb{Z}[\sqrt{d}]^{\times,1} \equiv \{\text{solutions to Pell's equation}\}$. Note: If $u \in \mathbb{Z}[\sqrt{d}]^\times$, then $\exists y \in \mathbb{Z}[\sqrt{d}]$ such that $uy = 1$. Then $N(u)N(y) = 1$, so $N(u) = \pm 1$. $\{\text{elements in } \mathbb{Z}[\sqrt{d}] \text{ of norm } -1\} \equiv \{\text{solutions to } x^2 - dy^2 = -1\}$.

Let's look for easy elements and generators of $\mathbb{Z}[\sqrt{d}]^{\times,1}$. Note: $\pm 1 \in \mathbb{Z}[\sqrt{d}]^{\times,1}$ [the 'trivial units', the trivial solutions to $x^2 - dy^2 = 1$. Suppose there are other solutions ...

Picture: Plot $\mathbb{Z}[\sqrt{d}]$ in $\mathbb{R}^2$. $x + y\sqrt{d} = z \in \mathbb{Z}[\sqrt{d}] \to (z, z^*) = (x + y\sqrt{d}, x - y\sqrt{d})$:



This picture shows that solutions to $zz^* = 1$, $z \in \mathbb{Z}[\sqrt{d}]$ are discrete in $\mathbb{R}$. If there are solutions other than ± 1, let z be such a solution. If $z < 0$, replace z with $-z$ so $z > 0$. If $z < 1$, replace z with z^{-1} $[= z^*]$ so we can assume $z > 1$. So, if there are solutions to Pell's equation other than ± 1 then there is a solution > 1. Such solutions form a discrete set.

Definition. *Suppose $\exists$ non-trivial solutions to $x^2 - dy^2 = 1$. Then the fundamental 1-unit of $\mathbb{Z}[\sqrt{d}]$ is the smallest $\epsilon \in \mathbb{Z}[\sqrt{d}]^{\times,1}$ such that $\epsilon > 1$.*

[End lecture 21, 25/11/14]

Suppose we have $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]^{\times,1}$ with $z_2 > z_1 > 1$. Write $z_i = x_i + y_i\sqrt{d}$. Claim: $x_i, y_i > 0$.

Proof. $N(z_i) = 1 = z_i \cdot z_i^* \implies z_i^{-1} = z_i^* = x_i - y_i\sqrt{d}$. For y_i, since $z_i > 1, 0 \leq z_i^{-1} \leq 1$ and so $z_i > z_i^{-1} \implies x_i + y_i\sqrt{d} > x_i - y_i\sqrt{d} \implies y_i > 0$. For x_i: $z_i + z_i^{-1} > 1 > 0 \implies 2x_i = z_i + z_i^{-1} > 0 \implies x_i < 0$. □

Moreover, if $z_2 > z_1$ then $y_2 > y_1$.

Proof. $z_i - z_i^{-1} = 2y_i\sqrt{d}$, but for $z > 1, z - \frac{1}{z}$ is obviously an increasing function of z. So $z_2 > z_1 \implies z_2 - z_2^{-1} > z_1 - z_1^{-1} \implies y_2 > y_1$. □

Corollary: The fundamental 1-unit in $\mathbb{Z}[\sqrt{d}]^{\times,1}$ is the element $x + y\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]^{\times,1}$ with $x, y > 0$ and y as small as possible.

Example: $3 + 2\sqrt{2}$ is a fundamental 1-unit in $\mathbb{Z}[\sqrt{2}]$.

Proof. $N(3 + 2\sqrt{2}) = (3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 9 - (2\sqrt{2})^2 = 1$. Suffices to show that $x + y\sqrt{2}$ is never a 1-unit when $y = 1$. When $y = 1, (x + \sqrt{2})(x - \sqrt{2}) = 1 \iff x^2 - 2 = 1$, and this doesn't happen.

□

Theorem 25. *If a fundamental 1-unit, ϵ, exists in $\mathbb{Z}[\sqrt{d}]^{\times,1}$ then every element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ has the form $\pm z^n$ for some $n \in \mathbb{Z}$. [Otherwise the only 1-units are ± 1.]*

Proof. Let $\alpha \in \mathbb{Z}[\sqrt{d}]^{\times,1}$. If $\alpha < 0$, replace it with $-\alpha$ so that $\alpha > 0$. If $\alpha < 1$, replace it with $\alpha^{-1}[= \alpha^*]$ so we can assume $\alpha > 1$. Now $\epsilon > 1$, so $\lim_{n\to\infty} \epsilon^n = +\infty$. So $\exists n : \epsilon^n \leq \alpha < \epsilon^{n+1}$. Now $\frac{\alpha}{\epsilon^n}$ is in $\mathbb{Z}[\sqrt{d}]^{1,\times}$ and $1 \leq \frac{\alpha}{\epsilon^n} < \epsilon$. But ϵ was the smallest 1-unit > 1 so we must have $\epsilon^n = \alpha$. □

Going back to our last example, the solutions to $x^2 - 2y^2 = 1$:

$$(x, y) : (x + y\sqrt{2}) = \pm(3 + 2\sqrt{2})^n, n \in \mathbb{Z}$$

Incidentally, note that $(1, 1)$ is a solution to $x^2 - 2y^2 = -1$. $(1 + \sqrt{2})$ is a (-1)-unit in $\mathbb{Z}[\sqrt{2}]^\times$, so:

$$\mathbb{Z}[\sqrt{2}]^{\times,-1} = \{\pm(1 + \sqrt{2})(3 + 2\sqrt{2})^n : n \in \mathbb{Z}\}$$

It still remains to be shown that if $d > 0$ is not a square, then there exists x, y with $y \neq 0$ such that $x^2 - dy^2 = 1$.

$x^2 - dy^2 = 0$ happens only if $x^2 = dy^2 \iff \left(\frac{x}{y}\right)^2 = d$.

To solve $x^2 - dy^2 = 1$, look for rational numbers 'unusually close to $\sqrt{d}$'.

Theorem 26 (Dirichlet)**.**
Let $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ be irrational and $Q \in \mathbb{Z}_{>1}$. Then $\exists p, q \in \mathbb{Z}$, $q < Q$, such that $|p - q\alpha| < \frac{1}{Q}$.

Proof. For $k = 1, \ldots, Q - 1$, let $a_k = \lfloor k\alpha \rfloor \in \mathbb{Z}$. So $0 < k\alpha - a_k < 1$. Break $[0, 1]$ into Q subintervals:

$$\left[0, \frac{1}{Q}\right], \left[\frac{1}{Q}, \frac{2}{Q}\right], \ldots, \left[\frac{Q-1}{Q}, 1\right]$$

By the pigeonhole principle, of the $Q + 1$ numbers $\{0, \alpha - a_1, 2\alpha - a_2, \ldots, 1\}$ two of them must land in same subinterval. Let these two be β_1, β_2. But $\beta_1 - \beta_2$ must have the form $q\alpha - p$ with $p, q \in \mathbb{Z}$, $q < Q$. With them being in the same subinterval, $|\beta_2 - \beta_1| < \frac{1}{Q}$ and so $|p - q\alpha| < \frac{1}{Q}$ as was claimed. □

[End lecture 22, 27/11/14]

[This lecture was a problems class.]

[End lecture 23, 28/11/14]

Remark [on the Dirichlet Theorem]: $\left|\frac{p}{q}-\alpha\right| < \frac{1}{Qq} < \frac{1}{q^2}$. This is saying that $\exists$ infinitely many p, q such that $\left|\frac{p}{q}-\alpha\right| < \frac{1}{q^2}$; to see this, pick $Q > \frac{1}{|p-q\alpha|}$ and apply Dirichlet's theorem again to get a new pair p_2, q_2.

Theorem 27. *$\exists$ a solution (x, y) such that $x^2 - dy^2 = 1$ if d is non-square.*

Proof. We approximate $\sqrt{d}$ by rational numbers $\frac{p_i}{q_i}$. Fix $Q_1 > 1$. $\exists p_1, q_1$ such that $\left|p_1 - q_1\sqrt{d}\right| < \frac{1}{Q_1}$, $q_1 < Q_1$. Choose Q_2 such that $Q_2 > \frac{1}{\left|p_1 - q_1\sqrt{d}\right|}$ [in particular, $Q_2 > Q_1$]. $\exists p_2, q_2$ such that $\left|p_2 - q_2\sqrt{d}\right| < \frac{1}{Q_2} < \left|p_1 - q_1\sqrt{d}\right|$, $q_2 < Q_2$. Iterating, we obtain p_i, q_i such that:

$$\left|p_i - q_i\sqrt{d}\right| < \frac{1}{Q_i} < \frac{1}{q_i}$$

Consider $N(p_i - q_i\sqrt{d}) = (p_i - q_i\sqrt{d})(p_i + q_i\sqrt{d})$. Now:

$$\left|N(p_i - q_i\sqrt{d})\right| < \frac{1}{q_i} \cdot \left|p_i + q_i\sqrt{d}\right| \leq \frac{1}{q_i}\left[\left|p_i - q_i\sqrt{d}\right| + 2q_i\sqrt{d}\right] < \frac{1}{q_i}\left[3q_i\sqrt{d}\right] = 3\sqrt{d}$$

Of course there are only finitely many integers between $-3\sqrt{d}$ and $3\sqrt{d}$, so $\exists M \in \mathbb{Z}$ such that $|M| < 3\sqrt{d}$ and infinitely many p_i, q_i such that $N(p_i - q_i\sqrt{d}) = M$. [We want to divide one by another to get something of norm 1, but we need integer coefficients.]

Consider, for each such (p_i, q_i), the congruence class of $p_i \pmod M$. Since there are only a finite number of congruence classes $\pmod M$, $\exists p_0 \in \mathbb{Z}$ such that $p_i \equiv p_0$ for infinitely many i [since $\exists$ infinitely many (p_i, q_i) such that $N(p_i - q_i\sqrt{d}) = M$]. Now consider $q_i \pmod M$; $\exists q_0 \in \mathbb{Z}$ such that $q_i \equiv q_0 \pmod M$ for infinitely many i.

Summary: $\exists$ infinitely many (p_i, q_i) such that $N(p_i - q_i\sqrt{d}) = M$ with $p_i \equiv p_0 \pmod M$ and $q_i \equiv q_0 \pmod M$. So $\exists p, q, p', q'$ such that $N(p - q\sqrt{d}) = N(p' - q'\sqrt{d}) = M$, $p \equiv p'$ and $q \equiv q' \pmod M$.

Consider:

$$z = \frac{p - q\sqrt{d}}{p' - q'\sqrt{d}} = \frac{(p - q\sqrt{d})(p' + q'\sqrt{d})}{M} = \frac{(pp' - qq'd) + (pq' - qp')\sqrt{d}}{M}$$

So if $z = \frac{p - q\sqrt{d}}{p' - q'\sqrt{d}} \in \mathbb{Z}[\sqrt{d}]$ then we're done [as z has norm 1]. So we need to show that this holds true, i.e:

$$M | (pp' - qq'd) \tag{1}$$
$$M | (pq' - qp') \tag{2}$$

(1). $pp' - dqq' \equiv p^2 - dq^2 \pmod M = (p + q\sqrt{d})(p - q\sqrt{d}) = N(p - q\sqrt{d}) = M \equiv 0 \pmod M$

(2). $pq' - qp' \equiv pq - qp \pmod M = 0$

So $z \in \mathbb{Z}[\sqrt{d}]$ and $N(z) = 1$ so $z =: x + y\sqrt{d}$ solves $x^2 - dy^2 = 1$, as required. □

Big question in Number Theory: Given [suitable] subrings of $\mathbb{C}$ [rings of algebraic integers], what do the units look like?

4 Continued Fractions

Suppose we're given $\alpha \in \mathbb{R}$. We can write $\alpha = a_0 + r_0$ where $a_0 = \lfloor \alpha \rfloor$ and such that $0 \leq r_0 < 1$. If $\alpha \notin \mathbb{Z}$, $r_0 \neq 0$ and $\frac{1}{r_0} > 1$, so we can define $a_1 = \lfloor \frac{1}{r_0} \rfloor$ and then $0 \leq r_1 < 1$ such that $\alpha = a_0 + \frac{1}{a_1 + r_1}$. We continue in this way:

$$\begin{aligned} \alpha &= \alpha_0 + r_0, & \alpha_0 &= \lfloor \alpha \rfloor, 0 \leq r_0 < 1 \\ \frac{1}{r_0} &= \alpha_1 + r_1, & \alpha_1 &= \lfloor \frac{1}{r_0} \rfloor, 0 \leq r_1 < 1 \\ \frac{1}{r_1} &= \alpha_2 + r_2, & \alpha_2 &= \lfloor \frac{1}{r_1} \rfloor, 0 \leq r_2 < 1 \\ &\&c. & &\&c. \end{aligned}$$

If this stops, α is rational. $\alpha \in \mathbb{Q} \implies r_{k+1} = 0 \implies$ this terminates:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_k + \cfrac{1}{a_{k+1}}}}}}$$

$a_0, \ldots, a_{k+1}$ are integers.

Example:

$$\frac{40}{19} = \alpha = 2 + \frac{2}{19} = 2 + \frac{1}{\frac{19}{2}} = 2 + \frac{1}{9 + \frac{1}{2}} = 2 + \frac{1}{9 + \frac{1}{2+0}}$$

If α is rational, then numerator$(r_0) <$ denominator$(r_0) \implies$ denominator$(r_1) =$ numerator(r_0), numerator$(r_1) <$ denominator(r_1) &c.

If $\alpha \in \mathbb{R} \backslash \mathbb{Q}$, i.e. α is irrational, then we get an infinite sequence $a_0, a_1, a_2, \ldots$ We write:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

[End lecture 24, 02/12/14]

Example: $\alpha = \sqrt{3}$. $\alpha_0 = 1$, $r_0 = \sqrt{3} - 1$.

$$\begin{aligned} \alpha &= \sqrt{3} = 1 + \left(\sqrt{3} - 1\right), & \alpha_0 &= \left\lfloor \sqrt{3} \right\rfloor = 1, \ 0 \leq r_0 < 1 \\ \frac{1}{r_0} &= \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2}, & a_1 &= \left\lfloor \frac{1}{\sqrt{3} - 1} \right\rfloor = 1, \ 0 \leq r_1 < 1 \\ \frac{1}{r_1} &= \frac{2}{\sqrt{3} - 1} = \sqrt{3} + 1, & a_2 &= \left\lfloor \frac{2}{\sqrt{3} - 1} \right\rfloor = 2, \ 0 \leq r_2 < 1 \\ \frac{1}{r_2} &= \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2}, & a_3 &= \left\lfloor \frac{1}{\sqrt{3} - 1} \right\rfloor = 1, \ 0 \leq r_3 < 1 \\ &\&c. & &\&c. \end{aligned}$$

$$\frac{1}{r_2} = \frac{1}{r_0} \implies a_3 = a_1, \ r_3 = r_1 \implies a_4 = a_2$$

We would like to say the following, but it doesn't [yet] make sense:

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cdots}}}}}$$

Notation: If $a_0 \in \mathbb{R}$, $a_1, \ldots, a_r \in \mathbb{R}_{>0}$, let $[a_0; a_1, \ldots, a_r]$ denote:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_r}}}}$$

Suppose we have an infinite continued fraction expression:

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

Definition. *The n^{th} convergent to this expression is the rational number $[a_0; a_1, \dots, a_n]$.*

Let α be an irrational number and:

$$\alpha = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

its continued fraction expansion. Then $\forall n$, $[a_0; a_1, \dots, a_n] = \frac{p_n}{q_n}$ rational. Claim:

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha$$

The zeroth convergent is $\frac{p_0}{q_0} = \frac{a_0}{1}$. The 1^{st} convergent is $[a_0; a_1] = \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1}$.

Let $a_0 \in \mathbb{R}$, $a_1, a_2, \dots \in \mathbb{R}_{>0}$. Set $p_0 = a_0$, $q_0 = 1$. $p_1 = a_1 a_0 + 1$, $q_1 = a_1$. For given n, set $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$.

Claim: $\forall n$, $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$. By induction on n, $n = 0$, $n = 1$ are clear.

Suppose that this is true for $n - 1$. Then $[a_0; a_1, \dots, a_n] = \left[a_0; a_1, \dots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\right]$:

$$a_0 + \cfrac{1}{a_1 + \frac{\dots}{\dots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}$$

By the inductive hypothesis, this is $\frac{p'_{n-1}}{q'_{n-1}}$ where $p'_i = p_i$ for $0 \le i \le n-2$.

$$p'_{n-1} = \left(a_{n-1} + \frac{1}{a_n}\right) p'_{n-2} + p'_{n-3} = \left(a_{n-1} + \frac{1}{a_n}\right) p_{n-2} + p_{n-3}$$

$$q'_{n-1} = \left(a_{n-1} + \frac{1}{a_n}\right) q'_{n-2} + q'_{n-3} = \left(a_{n-1} + \frac{1}{a_n}\right) q_{n-2} + q_{n-3}$$

so it suffices to show:

$$\frac{p_n}{q_n} = \frac{\left(a_{n-1} + \frac{1}{a_n}\right) p_{n-2} + p_{n-3}}{\left(a_{n-1} + \frac{1}{a_n}\right) q_{n-2} + q_{n-3}}$$

Expanding:

$$\frac{\left(a_{n-1} + \frac{1}{a_n}\right) p_{n-2} + p_{n-3}}{\left(a_{n-1} + \frac{1}{a_n}\right) q_{n-2} + q_{n-3}} = \frac{a_{n-1} p_{n-2} + p_{n-3} + \frac{1}{a_n} p_{n-2}}{a_{n-1} q_{n-2} + q_{n-3} + \frac{1}{a_n} q_{n-2}} = \frac{p_{n-1} + \frac{1}{a_n} p_{n-2}}{q_{n-1} + \frac{1}{a_n} q_{n-2}} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}$$

Corollary: $p_n \cdot q_{n-1} - q_n \cdot p_{n-1} = (-1)^{n-1}$.

Proof. Base case is $n = 1$: $p_1 q_0 - p_0 q_1 = a_1 a_0 + 1 - a_1 a_0 = 1$. Assume it's true for $n - 1$:

$p_n q_{n-1} - p_{n-1} q_n = (a_n p_{n-1} + p_{n-2})\, q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) = p_{n-2} q_{n-1} - p_{n-1} q_{n-2} = (-1)(-1)^{n-2} = (-1)^{n-1}$

by the inductive hypothesis. □

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$$

In fact, if $[a_0; a_1, \dots]$ gives the continued fraction expansion for α, then we have the following observation:

$$\begin{cases} \frac{p_n}{q_n} < \alpha & \text{if } n \text{ is even} \\ \frac{p_n}{q_n} > \alpha & \text{if } n \text{ is odd} \end{cases}$$

Proof. By induction. $n = 0$ is clear because $\frac{p_0}{q_0} = a_0 = \lfloor \alpha \rfloor < \alpha$. Assume that it's true for $n-1$ and all α.

$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n]$. What we'll do instead is we'll consider the continued fraction expansion of $\frac{1}{\alpha - a_0} = \frac{1}{r_1}$. This is $[a_1; a_2, a_3, \ldots]$. By the inductive hypothesis:

$$\begin{cases} [a_1; a_2, \ldots, a_n] < \frac{1}{\alpha - a_0} & \text{if } n \text{ is odd} \\ [a_1; a_2, \ldots, a_n] > \frac{1}{\alpha - a_0} & \text{if } n \text{ is even} \end{cases}$$

$$\frac{p_n}{q_n} = a_0 + \frac{1}{a_1 + \frac{\cdots}{\cdots + \frac{1}{a_n}}} = a_0 + \frac{1}{[a_1; a_2, \ldots, a_n]} \quad \begin{cases} < a_0 + \alpha - a_0 = \alpha & \text{if } n \text{ is even} \\ > a_0 + \alpha - a_0 = \alpha & \text{if } n \text{ is odd} \end{cases}$$

□

[End lecture 25, 04/12/14]

Recall the definitions of p_n and q_n and note that q_n is increasing and $\forall n$, $q_n > 0$.

Theorem 28.

$$\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha$$

Proof.

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = (-1)^{n-1} \frac{1}{q_n q_{n-1}}$$

Note that:

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = (-1)^{n-1} \frac{1}{q_n q_{n-1}} + (-1)^{n-2} \frac{1}{q_{n-1} q_{n-2}}, \text{ which is } \begin{cases} > 0 \text{ if } n \text{ is even} \\ < 0 \text{ if } n \text{ is odd} \end{cases}$$

Hence, we note that the sequences:

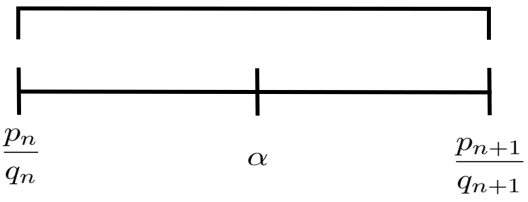
- $\left\{ \frac{p_n}{q_n} \right\}_{n \text{ even}}$ is <u>increasing</u> and bounded above by α. So it converges to a limit $\alpha^- \leq \alpha$
- $\left\{ \frac{p_n}{q_n} \right\}_{n \text{ odd}}$ is <u>decreasing</u> and bounded below by α. So it converges to a limit $\alpha^+ \geq \alpha$

$$\alpha^+ - \alpha^- = \lim_{n \to \infty} \left[\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} \right] = \lim_{n \to \infty} \left[\frac{1}{q_{2n+1} q_{2n}} \right] = 0$$

So $\alpha^+ = \alpha^-$ which implies $\alpha^- = \alpha = \alpha^+$. □

Diagrammatically, for an even n:

$$\frac{1}{q_n q_{n+1}}$$



$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

Conclusion: $\exists$ infinitely many $\frac{p}{q}$ such that $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$.

Recall:

$$\sqrt{3} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \cdots}}}}} = 1 + \frac{1}{[1; 2, 1, 2, 1, 2, 1, \ldots]}$$

The sequence $a_0, a_1, \ldots$ is <u>eventually periodic</u> i.e. $\exists p \in \mathbb{Z}$, $k \in \mathbb{Z}$ such that $\forall n > k$, $a_{n+p} = a_n$.

Theorem 29. *Let α be an irrational # whose continued fraction expansion is eventually periodic. Then α is the root of a quadratic polynomial with rational coefficients. Equally, α has the form $x+y\sqrt{D}$ with x, y rational and D an integer. [This is the root of $t^2 - 2xt + (x^2 - Dy^2)$.]*

Proof. Firstly observe the following: Let $\alpha = [a_0; a_1, \dots]$, $\alpha_n = [a_n; a_{n+1}, \dots]$, then $\exists P_n, Q_n, R_n, S_n \in \mathbb{Z}$ such that $\alpha = \frac{P_n\alpha_n + Q_n}{R_n\alpha_n + S_n}$.

Proof. Induction on n. The base case, $n = 0$, is clear: $P_0 = S_0 = 1$, $Q_0 = R_0 = 0$. Assume it's true for $n-1$:

$$\alpha = \frac{P_{n-1}\alpha_{n-1} + Q_{n-1}}{R_{n-1}\alpha_{n-1} + S_{n-1}}$$

If we write this out in continued fraction form, we have that:

$$\alpha_{n-1} = a_{n-1} + \frac{1}{a_n + \frac{1}{a_{n+1} + \frac{1}{a_{n+2}+\cdots}}} = a_{n-1} + \frac{1}{\alpha_n}$$

$$\implies \alpha = \frac{P_{n-1}\left(a_{n-1} + \frac{1}{\alpha_n}\right) + Q_{n-1}}{R_{n-1}\left(a_{n-1} + \frac{1}{\alpha_n}\right) + S_{n-1}} = \frac{\left(P_{n-1}a_{n-1} + Q_{n-1}\right)\alpha_n + P_{n-1}}{\left(R_{n-1}a_{n-1} + S_{n-1}\right)\alpha_n + R_{n-1}}$$

And so we let $P_n := P_{n-1}a_{n-1} + Q_{n-1}$, $\quad Q_n := P_{n-1}$, $\quad R_n := R_{n-1}a_{n-1} + S_{n-1}$, $\quad S_n := R_{n-1}$. □

Suppose that $[a_0; a_1, \dots]$ is periodic, i.e. $\exists p$: $a_{n+p} = a_n \ \forall n \geq 0$. Then, in this case, $\alpha = [a_0; a_1, \dots]$, $\alpha_p = [a_p; a_{p+1}, \dots] = \alpha$. So $\alpha = \frac{P_p\alpha + Q_p}{R_p\alpha + S_p}$. $R_p\alpha^2 + S_p\alpha = P_p\alpha + Q_p$, i.e. α satisfies $R_p\alpha^2 + (S_p - P_p)\alpha - Q_p = 0$.

So if α is periodic, α is a quadratic root! Now assume α is only eventually periodic. Then α_n is periodic for some $n \implies \alpha_n$ is a quadratic root so we can write $\alpha_n = x + y\sqrt{D}$, $D \in \mathbb{Z}$, $x, y \in \mathbb{Q}$. But now:

$$\begin{aligned}\alpha &= \frac{P_n\alpha_n + Q_n}{R_n\alpha_n + S_n} \\ &= \frac{x_1 + y_1\sqrt{D}}{x_2 + y_2\sqrt{D}}, \ \ x_1, x_2, y_1, y_2 \in \mathbb{Q} \\ &= \frac{(x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D})}{x_2^2 - Dy_2^2}\end{aligned}$$

which has the form $x_3 + y_3\sqrt{D}$, $x_3, y_3 \in \mathbb{Q}$. So we have proved it for eventually periodic α's too. □

[The converse is also true, but it's harder to prove.]

[End lecture 26, 05/12/14]

Theorem 30. *The convergents $\frac{p_n}{q_n}$ to a continued fraction expansion for α are the 'best' rational approximations to α with denominator $\leq q_n$. I.e. if $\frac{h}{k} \in \mathbb{Q}$ satisfies $\left|\frac{h}{k} - \alpha\right| < \left|\frac{p_n}{q_n} - \alpha\right|$, then $k > q_n$.*

Proof. We also know that $\left|\frac{p_n}{q_n} - \alpha\right| < \left|\frac{p_{n-1}}{q_{n-1}} - \alpha\right|$ so approximations get better. Let's look at the two cases:

- For n even: $\frac{p_n}{q_n} < \alpha < \frac{p_{n-1}}{q_{n-1}}$.

  $$\frac{p_n}{q_n} \to \left[\left|\frac{p_n}{q_n} - \alpha\right|\right] \leftarrow \alpha \rightarrow \left[\left|\frac{p_n}{q_n} - \alpha\right| + \epsilon\right] \leftarrow \frac{p_{n-1}}{q_{n-1}}$$

  so if $\frac{h}{k}$ is closer to α than than $\frac{p_n}{q_n}$ is, we have $\frac{p_n}{q_n} < \frac{h}{k} < \frac{p_{n-1}}{q_{n-1}}$.

- For n odd: $\frac{p_n}{q_n} > \alpha > \frac{p_{n-1}}{q_{n-1}}$. The same argument $\implies \frac{p_{n-1}}{q_{n-1}} < \frac{h}{k} < \frac{p_n}{q_n}$.

Obviously in either case $\left|\frac{h}{k} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n-1}q_n}$.

Since $\frac{h}{k} \neq \frac{p_{n-1}}{q_{n-1}}$, $\left|\frac{h}{k} - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{hq_{n-1} - p_{n-1}k}{kq_{n-1}}\right| \geq \frac{1}{kq_{n-1}}$ so $\frac{1}{q_nq_{n-1}} > \frac{1}{kq_{n-1}} \implies k > q_n$, as required. □

$$\alpha = 1 + \frac{1}{10^{1000000}} + \frac{1}{10^{10^{1000000}}} + \frac{1}{10^{10^{10^{1000000}}}} + \cdots = \sum_{i=0}^{\infty} \frac{1}{10^{\cdots\{i \text{ times}\}\ldots^{1000000}}}$$

Definition. *An element α of $\mathbb{C}$ is algebraic if there exists a polynomial P with rational coefficients such that $P(\alpha) = 0$. The degree of α is the degree of the smallest such P [i.e. the lowest degree of such P].*

Examples:

- $\frac{p}{q} \in \mathbb{Q}$ has degree 1. It's the root of $px - q = 0$.
- $\sqrt{D}$ with $D \in \mathbb{Q}$ has degree 2. It's a root of $x^2 - D = 0$

Definition. *$\alpha \in \mathbb{C}$ is transcendental if α is not algebraic.*

Theorem 31. *Transcendental numbers exist.*

Proof. $\mathbb{C}$ is uncountable. There are countably many polynomials with coefficients in $\mathbb{Q}$, but each has only finitely many roots. A countable union of finite sets is countable and so the algebraic numbers are countable. □

Philosophy 1. *Real algebraic numbers tend to be hard to approximate rationally.*

Theorem 32 (Louiville)**.**
α algebraic of degree d. $\forall e \in \mathbb{Z}_{>d}$ $\exists$ only finitely many $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^e}$

Proof. Let $f = \sum_{i=0}^{d} a_i x^i$, $a_i \in \mathbb{Q}$ such that $f(\alpha) = 0$. Let N be a common denominator for the a_i then we can rewrite $a_i =: \frac{c_i}{N}$ where $c_i \in \mathbb{Z}$. Now take $F = \sum_{i=0}^{d} c_i x^i$. $F = Nf$, so $F(\alpha) = 0$. $(x - \alpha)|F$ in $\mathbb{R}[x]$. I.e. $\exists Q(x)$, with coefficients in $\mathbb{R}$, such that $(x - \alpha)Q(x) = F(x)$.

$|Q(x)|$ is a continuous function on $\mathbb{R}$ and so it's bounded on $[\alpha-1, \alpha+1]$. Let $k = \max\{|Q(x)| : \alpha - 1 \leq x \leq \alpha + 1\}$ and suppose we have a $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^e}$. Clearly $F\left(\frac{p}{q}\right) \neq 0$: $F\left(\frac{p}{q}\right) = 0 \implies (qx - p)|F \implies \frac{F(x)}{qx-p}$ has rational coefficients, vanishes at α, and has degree $< d$. But this can't happen because α has degree d. So:

$$F\left(\frac{p}{q}\right) = \sum_{i=0}^{d} c_i \left(\frac{p}{q}\right)^i = \frac{(\text{something}) \in \mathbb{Z}}{q^d} \implies \left|F\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$$

Now $F(x) = Q(x)(x - \alpha) \implies \left|F\left(\frac{p}{q}\right)\right| = \left|\frac{p}{q} - \alpha\right| \left|Q\left(\frac{p}{q}\right)\right| \implies \frac{1}{q^d} \leq \left|\frac{p}{q} - \alpha\right| \left|Q\left(\frac{p}{q}\right)\right| < \frac{k}{q^e} \implies q^{e-d} < k.$

For $e > d$, only finitely many q work so clearly there can only be finitely many $\frac{p}{q}$. □

Theorem 33. *The following α is transcendental:*

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

Proof. Suppose α is algebraic of degree d. Let $\alpha_r = \sum_{n=1}^{r} \frac{1}{10^{n!}}$ so α_r is rational with $denom(\alpha_r) = 10^{r!}$. Then:

$$|\alpha - \alpha_r| = \left|\sum_{n=r+1}^{\infty} \frac{1}{10^{n!}}\right| \approx \frac{1}{10^{(r+1)!}} = \frac{1}{(10^{r!})^{r+1}} < \frac{1}{(10^{r!})^{r}}$$

So $\forall e \in \mathbb{Z}_{>d}$, $\forall r > e$, we see $|\alpha - \alpha_r| < \frac{1}{(denom)^r} < \frac{1}{(denom)^e}$. But there are infinitely many such r and so infinitely many such α_r so by Louiville's Theorem, α can't have degree $d \implies \alpha$ is not algebraic. □

The following theorem is 'state of the art' [we won't prove it in this course]:

Theorem 34. *If α is algebraic, then $\forall \epsilon > 0$ $\exists$ only finitely many $\frac{p}{q}$ such that $\left|\frac{p}{q} - \alpha\right| < \frac{1}{q^{2+\epsilon}}$.*

[End lecture 27, 09/12/14]

5 Sums of Squares

We know $n \in \mathbb{Z}$ is of the form a^2+b^2 iff all primes $p \equiv 3 \pmod 4$ appear as even powers in the factorisation of n.

$n = a^2 + b^2 + c^2 \implies n$ is not of the form $4^t(8k+7)$ for $t, k \in \mathbb{Z}_{\geq 0}$. Claim: The converse is true!

Furthermore, we will soon see that every non-negative integer is the sum of 4 squares.

Theorem 35. *If n, m are both sums of 4 squares then so is nm.*

Proof. LOL. We 'notice' that we can express $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2)$ as:

$$= (xa + yb + zc + wd)^2 + (xd + yc - zb - wa)^2 + (xb - ya + zd - wc)^2 + (xc - yd - za + wb)^2$$

$$= (xa - yb - zc - wd)^2 + (xd - yc + zb + wa)^2 + (xb + ya - zd + wc)^2 + (xc + yd + za - wb)^2$$

Expand if you dare. The second of these is a variant of the first, sending y, z, w to $-y, -z, -w$. □

Definition. *A quaternion is a formal sum $x+yi+zj+wk$ where $x, y, z, w \in \mathbb{R}$ and i, j, k are symbols satisfying $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$.*

Extend this to a product that is $\mathbb{R}$-linear, distributable over addition:

$$(x + yi + zj + wk)(a + bi + cj + dk) = xa + xbi + \cdots + ayi + yicj[= yck] + \ldots$$

This makes the quaternions into a ring, $\mathbb{H}$; it's not commutative. Given $x + yi + zj + wk$, its conjugate is $x - yi - zj - wk$.

Definition. *The norm on the quaternions is defined as follows:*

$$N(x + yi + zj + wk) = (x + yi + zj + wk)(x - yi - zj - wk) = x^2 + y^2 + z^2 + w^2$$

It's not automatic that if $u, v \in \mathbb{H}$ that $N(uv) = N(u)N(v)$ since $N(uv) = uv(uv)^*$ and $N(u)N(v) = uu^*vv^*$ and multiplication is not commutative. However, in this case it is multiplicative. [We leave this as an exercise for those of us who have far too much time on their hands.]

Theorem 36. *Every $n \in \mathbb{Z}$, $n \geq 0$ is a sum of four squares.*

Proof. By Theorem 35., it suffices to show that every prime is the sum of 4 squares. $p = 2 = 1^2 + 1^2$. $p \equiv 1 \pmod 4 \implies p = a^2 + b^2$. So we only need now concern ourselves with $p \equiv 3 \pmod 4$.

Recall that $p \equiv 1 \pmod 4 \iff -1$ is QR [i.e. a square] (mod p), so $p | n^2 + 1$ for some n. After writing $Mp = n^2 + 1$, we then used Fermat descent to reduce M until $M = 1$.

Lemma 5. *$p \equiv 3$ (mod 4) $\implies \exists a, b \in \mathbb{N}$ such that $a^2 + b^2 + 1 \equiv 0$ (mod p).*

Proof. It suffices to find a QR $a^2 \pmod p$ such that $a^2 + 1$ is not a QR. Then, since $a^2 + 1$ is not a QR and -1 isn't [since $p \not\equiv 1 \pmod 4$], we must have $(-1)(a^2 + 1) = -a^2 - 1$ is a QR $\implies \exists b : b^2 \equiv -a^2 - 1 \pmod p$. But then $a^2 + b^2 + 1 \equiv a^2 - a^2 - 1 + 1 = 0 \pmod p$ if there's such an a.

If for every QR a, $a + 1$ is also a QR $\implies$ every congruence class (mod p) is a QR. Since there are only $\frac{p-1}{2}$ QR's, this can't happen. So $\exists a$ satisfying the above. □

[End lecture 28, 11/12/14]

[This lecture was a Problems Class]

[End lecture 29, 12/12/14]

Theorem 37. *Suppose, for some $r > 1$, we have $x^2 + y^2 + z^2 + w^2 = rp$. Then $\exists x', y', z', w'$ and $\exists l$ with $1 \leq l < r$ such that $(x')^2 + (y')^2 + (z')^2 + (w')^2 = lp$.*

Proof. Consider the two cases:

1. r even. Let $l := \frac{r}{2}$. The number of x, y, z, w that are even is then $0, 2, 4$. Rearranging x, y, z, w, we can assume WLOG that $x \equiv y \pmod 2$ and $z \equiv w \pmod 2$:

$$x' := \frac{x+y}{2} \qquad y' := \frac{x-y}{2} \qquad z' := \frac{z+w}{2} \qquad w' := \frac{z-w}{2}$$

Then $(x')^2 + (y')^2 + (z')^2 + (w')^2 = \frac{1}{4}(2x^2 + 2y^2 + 2z^2 + 2w^2) = \frac{rp}{2} = lp$

2. r odd. Take a, b, c, d such that $-\frac{r}{2} < a, b, c, d, < \frac{r}{2}$ [we can employ strict inequality as r is odd] and $a \equiv x \pmod r$, $b \equiv y \pmod r$, $c \equiv z \pmod r$, & $d \equiv w \pmod r$.

$$a^2+b^2+c^2+d^2 \equiv x^2+y^2+z^2+w^2 = rp \equiv 0 \pmod r \implies \exists l\text{: } a^2+b^2+c^2+d^2 = lr. \left[a^2, b^2, c^2, d^2 < \tfrac{r^2}{4}\right].$$

This last equation $\implies l < r$, but we also know that $l \geq 1$: If $l = 0$, then $a, b, c, d = 0 \implies r|x, y, z, w.$ $\implies r^2 | \left(x^2 + y^2 + z^2 + w^2\right) = rp \implies p = r$. So $x^2 + y^2 + z^2 + w^2 = r^2$ with $r|x, y, z, w$. But this $\implies x = \pm r$, $y, z, w = 0$ [or similar permutations]. So $1 \leq l < r$.

Now consider the following:

$$\begin{aligned} lr^2p &= (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) \\ &= (xa + yb + zc + wd)^2 + (xd + yc - zb - wa)^2 + (xb - ya + zd - wc)^2 + (xc - yd - za + wb)^2 \end{aligned}$$

Set:

$$x' = \frac{xa + yb + zc + wd}{r} \quad y' = \frac{xd + yc - zb - wa}{r} \quad z' = \frac{xb - ya + zd - wc}{r} \quad w' = \frac{xc - yd - za + wb}{r}$$

So that now we have $lp = (x')^2 + (y')^2 + (z')^2 + (w')^2$ with $1 \leq l < r$.

Now all that remains to do is to show that $x', y', z', w' \in \mathbb{Z}$:

$$\begin{aligned} x' &: xa + yb + zc + wd \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod r \\ y' &: xd + yc - zb - wa \equiv xw + yz - zy - wx = 0 \pmod r \\ z' &: xb - ya + zd - wc \equiv xy - yx + zw - wz = 0 \pmod r \\ w' &: xc - yd - za + wb \equiv xz - yw - zx + wy = 0 \pmod r \end{aligned}$$

And we're done. [We can thus iteratively reduce any $r > 1$ until $l = 1$.] □

Corollary: Every prime p can be expressed as a sum of four squares. □

Theorem 38. *n is a sum of 3 squares iff n is not of the form $4^t(8k + 7)$, $t, k \geq 0$.*

Proof. The 'only if' follows from the fact that squares (mod 8) are congruent to one of $\{0, 1, 4\}$. The 'if' uses a Theorem of Dirichlet: Let $(a, n) = 1$, then there are infinitely many primes p such that $p \equiv a \pmod n$ □

Question: Given $a, n \in \mathbb{Z}$, are there infinitely many primes $p \equiv a \pmod n$? Note that if $(a, n) = d > 1$, then d divides every $x \equiv a \pmod n$. So we should assume $(a, n) = 1$.

Theorem 39. *There are infinitely many primes p: $p \equiv 3$ (mod 4).*

Proof. Suppose there are only finitely many $p \equiv 3 \pmod 4$. Call them $p_1, \ldots, p_r$.

Let $n = (p_1 \ldots p_r)^2 + 2$. Then all $p_i \nmid n$, $n = 3 \pmod 4$. If every $p|n$ were $\equiv 1 \pmod 4$, then $n \equiv 1 \pmod 4$. So $\exists p|n$ with $p \equiv 3 \pmod 4$ $\implies \{p_1, \ldots, p_r\}$ is not a complete list of primes $\equiv 3 \pmod 4$, a contradiction. □

We can also use this to prove that $\exists$ infinitely many p: $p \equiv 5 \pmod 6$.

Theorem 40. *$\exists$ infinitely many primes $p > 0$ with $p \equiv 1 \pmod 4$.*

Proof. We're going to use the fact that -1 is a QR $\pmod p \iff p \equiv 1 \pmod 4$.

Suppose $p_1, \ldots, p_r$ are primes $\equiv 1 \pmod 4$. Define $n := (p_1 p_2 \ldots p_r)^2 + 1 \equiv 2 \pmod 4$, for some $n > 2$.

So $\exists$ and odd prime p such that $p|N$. Clearly $p_1, \ldots, p_r \neq p$. Reducing $n \pmod p$, we have $(p_1 \ldots p_r)^2 \equiv -1 \pmod p$ so -1 is a QR and so $p \equiv 1 \pmod 4$.

□

Variant: Given a, $\exists$ infinitely many primes p such that a is a QR $\pmod p$.

[End lecture 30, 16/12/14]

Theorem 41. *$\exists$ infinitely many primes $p > 0$ with $p \equiv 1 \pmod n$ $\forall n$.*

We need a way of producing numbers that are only divisibly by $p \equiv 1 \pmod n$.

Definition. *$n \geq 1$. The n^{th} cyclotomic polynomial, $\Phi_n(x)$, is the polynomial:*

$$\Phi_n(x) = \prod_{\substack{1 \leq d \leq n \\ (d,n)=1}} \left(x - e^{\frac{2\pi i d}{n}}\right)$$

The roots of Φ_n are $e^{\frac{2\pi i d}{n}}$, $1 \leq d \leq n$, $(n, d) = 1$. These are roots of unity with exact order n.

$\left(e^{\frac{2\pi i d}{n}}\right)^n = e^{2i\pi d} = 1$. If $\left(e^{\frac{2\pi i d}{n}}\right)^k = 1$, then $\frac{dk}{n}$ is an integer, so $n|dk \implies n|k$.

Observation:

$$\prod_{e|n} \Phi_e(x) = \prod_{g|n} \prod_{\substack{1 \leq d \leq g \\ (d,g)=1}} \left(x - e^{\frac{2\pi i d}{g}}\right)$$

If $n = gf$:

$$\prod_{e|n} \Phi_e(x) = \prod_{g|n} \prod_{\substack{1 \leq d \leq g \\ (d,g)=1}} \left(x - e^{\frac{2i\pi df}{n}}\right)$$

{The pairs (d, g) such that $g|n$, $1 \leq d \leq g$, $(d, g) = 1\} \leftrightarrow \{1 \leq t \leq n$ in that the bracketed term in the above product cycles through the n^{th} roots of unity, $e^{\frac{2i\pi t}{n}}$ for $1 \leq t \leq n\}$.

$\frac{d}{g} \to \frac{df}{n}$. $df \overset{n=fg}{=} \frac{dn}{g}$. $t \to \left(\frac{n}{(t,n)}, \frac{t}{(t,n)}\right)$. So we see:

$$\prod_{g|n} \Phi_g(x) = \prod_{1 \leq t \leq n} \left(x - e^{\frac{2i\pi t}{n}}\right) = x^n - 1$$

Corollary: Φ_n has integer coefficients.

Proof. Strong induction on n. $\Phi_1 = x - 1$. Assume Φ_g has integer coefficients $\forall g < n$. We know:

$$x^n - 1 = \Phi_n(x) \prod_{\substack{g|n \\ g \neq n}} \Phi_g(x)$$

but both of these have integer coefficients. Suppose Φ_n does not have integer coefficients. Let $c_i x^i$ be the term of highest degree in $\Phi_n(x) =: \sum_{i=0}^{deg(\phi(n))} c_i x^i$ that doesn't have integer coefficients.

$d := deg\left(\prod_{g|n, g\neq n} \Phi_g =: P(x) := \sum_{s=0}^{d} a_s x^s\right)$. By the hypothesis, $a_i \in \mathbb{Z}$. The coefficients of x^{i+d} in $x^n - 1$ is:

$$c + \sum_{s=0}^{d-1} a_s c_{i+d-s} \; [= (\text{coefficients of } \Phi_n \text{ degree} > i) \cdot (\text{coefficients of } P)]$$

as all terms in the sum are $\in \mathbb{Z}$ and $x^n - 1$ has integer coefficients, this cannot happen. [Note that $P(x)$ is a product of monic polynomials, so $a_d = 1$. So $\nexists$ such a c_i. □

$$\Phi_1 = x - 1$$
$$\Phi_2 = x + 1$$
$$\Phi_3 = x^2 + x + 1$$
$$\Phi_4 = x^2 + 1$$

Theorem 42. *Let p be a prime not dividing n. Then Φ_n has distinct roots (mod p).*

Proof. $\Phi_n(x)|(x^n - 1)$, so it suffices to show that $x^n - 1$ has distinct roots (mod p).

Definition. *Let $P(t) = \sum_{i=0}^{d} c_i t^i$ be a polynomial with coefficients $\in \mathbb{Z}\backslash p\mathbb{Z}$. The <u>derivative</u> $P'(t) = \sum_{i=1}^{d} ic t^{i-1}$.*

Note that $(PQ)' = P'Q + PQ'$ [check]. So if $(x-a)^2|P$, $P = (x-a)^2 Q \implies P' = (x-a)^2 Q' + 2(x-a)Q \implies x - a$ is a root of P'.

Suppose $x^n - 1$ had a double root a (mod p), $(x-a)^2|(x^n - 1)$ in $\mathbb{Z}/p[x]$. So $(x-a)|nx^{n-1} \implies a^{n-1} \equiv 0 \pmod{p}$. If $p\nmid n$, we must then have $a \equiv 0$. But 0 is not a root of $x^n - 1$, a contradiction, so $\nexists$ a double root. □

Corollary: If $p\nmid n$ and $p|\Phi_n(a)$ for some $a \in \mathbb{Z}$ then $p \equiv 1 \pmod{n}$.

Proof. Since $p|\Phi_n(a)$, $\phi_n(x)|x^n - 1$, so $p|a^n - 1$. So $a^n \equiv 1 \pmod{p}$. Suppose $a^d \equiv 1 \pmod{p}$ for some $d \neq n$, $d|n$. Then a is a root of $x^d - 1 \pmod{p} \implies (x - a)|x^d - 1 = \prod_{g|d} \Phi_g(x)$. So $(x - a)|\Phi_g(x)$, $(x - a)|\Phi_n(x)$.

But $x^n - 1 = \prod_{g|n} \Phi_g(x)$ so the above shows $(x - a)^2|x^n - 1$. We just showed this can't happen. So a has <u>exact order</u> n (mod p) and $a^{p-1} \equiv 1 \pmod{p}$ hence $n|p - 1$, i.e. $p \equiv 1 \pmod{n}$. □

Let $p_1, \ldots, p_r$ be a finite list of primes > 0 with $p \equiv 1 \pmod{n}$. $X := \Phi_n(np_1 \ldots p_r)$. Claim: no p_i divides X.

Proof. $\Phi_n(np_1 \ldots p_r) \equiv \Phi_n(0) \pmod{p_i}$, but $\Phi_n(0)|(0^n - 1) \pmod{p_i}$ so is non-zero. □

For an integer k, let $X_k = \Phi(knp_1 \ldots p_r)$. Claim: no prime dividing n divides X_k [uses the same argument].

Theorem 43. *$\exists$ infinitely many primes $p > 0$ with $p \equiv 1$ (mod n) $\forall n$.*

Proof. Let p be a prime dividing X_k, then as stated above $p\nmid n$, so by the corollary to Theorem 42., $p \equiv 1 \pmod{n}$. p is not any of the p_i so $\exists$ infinitely many primes $p \equiv 1 \pmod{n}$.

Let p be a prime dividing X_k fails if $X_k = \pm 1$. We thus need $\exists k \in \mathbb{Z}$: $X_k \neq \pm 1$. But since Φ_n is a polynomial, there are only finitely many roots α, β such that $\phi_n(\alpha) = +1$, $\phi_n(\beta) = -1$ and so $\Phi_n(knp_1 \ldots p_r)$ can't be ± 1 for all values of k.

□

[End lecture 31, 18/12/14]

[This lecture was a Q & A session.]

[End lecture 32, 19/12/14]