LECTURE 1: DIVISIBILITY AND FACTORIZATION

1. Divisibility

Definition 1.1. Let a, b be integers. We say that a *divides* b (written $a \mid b$) if there exists an integer n such that $b = na$.

Note that if a, b, c are integers such that $a|b$ and $a|c$, then $a \mid nb + mc$ for any integers n, m.

Definition 1.2. Let a, b be integers, not both zero. The *greatest common divisor* of a and b (written (a, b)) is the largest positive integer dividing both a and b.

Such an integer always exists since if a is nonzero and $c \mid a$, then $-a \leq c \leq a$.

Definition 1.3. An integer a is *prime* if a has exactly two positive divisors (namely, 1 and a).

Note that by definition, primes can be both positive and negative. In spite of this, in this course when we say "let p be a prime" we will generally mean p is positive.

We will see later in the course that both of these definitions are somewhat naive, and find better formulations of these concepts (i.e. ones that work in much greater generality.)

2. Euclid's algorithm

Proposition 2.1. *Let a and b be integers, not both zero. Then for any integer n, we have $(a, b) = (b, a - nb)$.*

Proof. From the definition of (a, b) it suffices to show that any positive integer divides m both a and b if, and only if, it divides both b and $a - nb$. But if m divides a and b, it clearly divides $a - nb$, and if it divides b and $a - nb$, it clearly divides a. □

This suggests an approach to computing (a, b): replace (a, b) by a pair $(b, a - nb)$ that is "smaller", and repeat until the numbers involved are small enough that it is easy to compute the greatest common divisor. The key to being able to do this is:

Theorem 2.2. *Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that $a = qb + r$ and $0 \leq r < b$.*

Proof. Let q be the largest integer less than $\frac{a}{b}$. Then $0 \leq \frac{a}{b} - q < 1$. Thus $0 \leq a - bq < b$, so we can take $r = a - bq$. □

This gives us an algorithm (Euclid's algorithm) for finding (a,b) for any (a,b) not both zero. Without loss of generality, assume $b \leq a$ and a is positive. (If a is negative we can replace it with $-a$ without changing (a,b).)

(1) Check if $b = 0$. If so then $(a,b) = a$.
(2) Otherwise, replace (a,b) with (b,r), where $a = bq + r$ and $0 \leq r < b$, and return to step 1.

Since at every stage $|a|$ is decreasing, this algorithm terminates; we've shown that $(a,b) = (b,r)$ so the output is always equal to (a,b).

This algorithm gives us more than just a way to compute (a,b): it also allows us to express (a,b) in terms of a and b:

Theorem 2.3. *Let a and b be integers, not both zero. Then there exist integers n, m such that $(a,b) = na + mb$.*

Proof. Let $a_0 = a$, $b_0 = b$, and for each i let a_i, b_i be the result after running i steps of Euclid's algorithm on the pair (a,b). For some r we have $a_r = (a,b)$ and $b_r = 0$. We will show, by downwards induction on i, that there exist integers n_i, m_i such that $(a,b) = n_i a_i + m_i b_i$. For $i = r$ this is clear. On the other hand, for any i we have $a_i = b_{i-1}$ and $b_i = a_{i-1} - q_i b_{i-1}$ for some integer q_i. Thus if $(a,b) = n_i a_i + m_i b_i$, we have

$$(a,b) = n_i b_{i-1} + m_i(a_{i-1} - q_i b_{i-1}) = (n_i - m_i q_i) b_{i-1} + m_i a_{i-1}$$

and the claim follows. □

3. Unique factorization

The fact that (a,b) is an integer linear combination of a and b has strong consequences for factorization and divisibility. First note:

Proposition 3.1. *Let n, a, b be integers, and suppose that $n \mid ab$ and $(n,a) = 1$. Then $n \mid b$.*

Proof. There exist integers x, y such that $ax + ny = 1$. Thus $abx + bny = b$. But n clearly divides abx and bny, so n divides b. □

When n is prime, either n divides a or $(n,a) = 1$. Thus:

Corollary 3.2. *If p is prime, and a, b are integers such that $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

From this we can immediately deduce that factorizations into primes are essentially unique:

Theorem 3.3. *Let n be a positive integer, and suppose we have two factorizations:*

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

with the p_i and q_j prime (and positive). Then $r = s$ and the p_i are a rearrangement of the q_j.

Proof. Suppose otherwise, and let n be the smallest positive integer where this does not hold. We then have $p_1 \mid q_1 q_2 \dots q_s$, so either $p_1 \mid q_1$ or $p_1 \mid q_2 q_3 \dots q_s$. Proceeding inductively, we have $p_1 \mid q_i$ for some i; since q_i is prime this means $p_i = q_i$. We then have:

$$p_2 p_3 \dots p_r = q_1 q_2 \dots q_{i-1} q_{i+1} \dots q_s.$$

Since this product is smaller than n, we must have that $r-1 = s-1$ and the p's (except p_1) are a rearrangement of the q's (except q_i). But since $p_1 = q_i$ we have $r = 2$ and the p's are a rearrangement of the q's. □

4. Linear diophantine equations

Suppose now that we are given a, b, c (all integers) and we want to solve $ax + by = c$ for x, y integers. We first note that (a, b) divides both a and b, so for there to be any solutions, we must have $(a, b) \mid c$. From now on, suppose this is true.

We can write $c = d(a, b)$. We can also find integers m, n such that $(a, b) = ma + nb$. Then $c = d(a, b) = dma + dnb$, so $x = dm$, $y = dn$ is a solution.

Now let x, y be one solution to the equation, and suppose we have a second solution x', y'. Then we find that $a(x - x') + b(y - y') = 0$. We thus have $x' = x + r$, $y' = y + s$, where $ar + bs = 0$. Conversely, if $ar + bs = 0$, then $x + r, y + s$ is a solution to $ax + by = c$. We are thus reduced to finding the solutions to $ar + bs = 0$. For any integer r, to have an s such that $ar + bs = 0$ we must have $s = -\frac{ar}{b}$. So we must determine for which integers r we have $-\frac{ar}{b}$ an integer. This is precisely when $b \mid ar$. Dividing both sides by (a, b), we see that this happens if, and only if, $\frac{b}{(a,b)} \mid \frac{ar}{(a,b)}$. But since $(\frac{b}{(a,b)}, \frac{a}{(a,b)}) = 1$, this happens if, and only if $\frac{b}{(a,b)} \mid r$.

Putting this all together, we find that if x, y is one solution to $ax + by = c$, then the other solutions are of the form $x + n\frac{b}{(a,b)}, y - n\frac{a}{(a,b)}$ for all integers n.

LECTURE 2: CONGRUENCES AND MODULAR ARITHMETIC

1. Congruences

Definition 1.1. Let n be a nonzero integer (usually taken to be positive) and let a and b be integers. We say a is congruent to b modulo n (written $a \equiv b \pmod{n}$) if $n \mid (a-b)$.

For n fixed, it is easy to verify that congruence mod n is an equivalence relation, and therefore partitions $\mathbb{Z}$ into equivalence classes. We let $[a]_n$ denote the equivalence class of a mod n; that is, the set of b such that $b \equiv a \pmod{n}$. The set of equivalence classes modulo n is denoted $\mathbb{Z}/n\mathbb{Z}$.

For any integer a, we can write $a = qn + r$ with $0 \leq r < n$. Then $a \equiv r \pmod{n}$. It follows that the n congruence classes $[0]_n, \dots, [n-1]_n$ exhaust $\mathbb{Z}$. On the other hand, if $0 \neq r, r' < n$, and $r \equiv r' \pmod{n}$, then $|r - r'| < n$ and $n \mid r - r'$, so $r = r'$. We thus have $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \dots, [n-1]_n\}$.

It is easy to check that if a, b, c are integers and $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$. It follows that one can define addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by setting:

$$[a]_n + [b]_n = [a+b]_n$$

$$[a]_n[b]_n = [ab]_n.$$

One easily checks that this satisfies the axioms of a ring, and moreover that the map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ taking an integer a to $[a]_n$ is a ring homomorphism.

Recall that if R is a ring, the *units* of R (denoted $R^\times$) are the elements of R with multiplicative inverses. Let a be an integer and suppose that $[a]_n$ is a unit. Then there exists b such that $ab \equiv 1 \pmod{n}$; it follows that $(a, n) = 1$. Conversely, if $(a, n) = 1$, there exist integers x, y such that $ax + ny = 1$; then $[a]_n[x]_n = [1]_n$, so $[a]_n$ is a unit. Thus we have $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : (a, n) = 1\}$.

Note that if p is a prime, then either $a \equiv 0 \pmod{p}$ or $(a, p) = 1$. Thus every nonzero congruence class mod p is a unit; i.e. $\mathbb{Z}/p\mathbb{Z}$ is a field.

2. Linear congruence equations

Fix integers a and c and a nonzero integer n. Suppose we want to solve $ax \equiv b \pmod{n}$. This is equivalent to finding x, y such that $ax + ny = b$. In particular, by our analysis of linear diophantine equations, there is a solution precisely when (a, n) divides b. Moreover, if x is a solution, the other solutions are of the form $x + r\frac{n}{(a,n)}$ for integers r. In particular they form a single congruence class mod $\frac{n}{(a,n)}$, or a total of (a,n) congruence classes mod n.

3. The Chinese remainder theorem

Let m and n be nonzero integers. Note that if $a \equiv b \pmod{mn}$, then $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$. Thus a congruence class mod mn determines a pair, consisting of a congruence class mod m and a congruence class mod n. More formally, we have a map: $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ that takes $[a]_{mn}$ to the pair $([a]_m, [a]_n)$. It's easy to check that this map is a ring homomorphism.

A natural question to ask is whether the converse is true; that is, given a pair of congruence classes mod m and mod n, is there a congruence class mod mn giving rise to it? In general the answer will be no, but when $(m,n) = 1$, then we have the so-called Chinese Remainder Theorem:

Theorem 3.1. *Let m and n be integers with $(m,n) = 1$, and let a and b be integers. Then there exists an integer x such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. Moreover x is unique modulo mn; that is, if x' is another integer with this property, then $x' \equiv x \pmod{mn}$.*

Proof. We first prove uniqueness. Note that if x and x' both have the required properties, then $x \equiv x' \pmod{n}$ and $x \equiv x' \pmod{m}$. Thus $x - x'$ is divisible by both m and n. Write $x - x' = cm$ for some integers c. We have n divides cm; since $(n,m) = 1$, we must have $n \mid c$. Writing $c = dn$, we have $x - x' = mnd$, so $x \equiv x' \pmod{mn}$.

For existence, we give two proofs. The first is constructive: write $1 = nx + my$. Then $anx + bmy$ is congruent to a mod m and b mod n.

For the second proof, note that the uniqueness we proved above shows that the map:

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

is injective. On the other hand both the source and the target of this map have cardinality mn, so the map is surjective as well, which proves the claim. □

Another way to interpret the Chinese remainder theorem is that the map

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

is an *isomorphism* of rings. Put another way, to prove any statement about $\mathbb{Z}/mn\mathbb{Z}$ that can be formulated purely in ring-theoretic terms, it suffices to prove corresponding statements mod m and mod n, provided that $(m,n) = 1$.

4. Wilson's theorem

Let p be a prime, and consider the congruence class of $(p-1)!$ modulo p. This is the product of all the nonzero congruence classes modulo p. Since inverses exist modulo p, there is a lot of cancellation. In particular, for any a not divisible by p, there exists an integer a^{-1} such that aa^{-1} is congruent to 1 mod p, and a^{-1} is unique up to congruence mod p. Note that $(a^{-1})^{-1} = a$. In particular, either $a = a^{-1}$ or a and a^{-1} are distinct mod p. In the second case, the pair of congruence classes $\{a, a^{-1}\}$ cancels from the product defining $(p-1)!$ mod p. Thus this product is equal to the product of those congruence classes a such that $a = a^{-1}$. These are the classes such that a^2 is congruent to 1 modulo p.

Note that if a^1 is congruent to 1 modulo p, then $(a+1)(a-1)$ is zero mod p. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, this only happens if $a+1$ or $a-1$ is zero, so the classes that are their own inverses are ±1 (modulo p). Since $(p-1)!$ is the product of these classes, we have proved:

Theorem 4.1 (Wilson's Theorem)**.** *Let p be a prime. Then $(p-1)! \equiv -1$ (mod p).*

LECTURE 3: EULER'S THEOREM

1. The Euler Φ-function

We define a function Φ on positive integers n by letting $\Phi(n)$ denote the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$. Explicitly we have $\Phi(n) = \#\{a : 0 \leq a < n, (a,n) = 1\}$; that is, $\Phi(n)$ is the number of integers between 0 and $n-1$ whose greatest common divisor with n is 1.

2. Euler's theorem

Note that the units $(\mathbb{Z}/n\mathbb{Z})^\times$ form a group under multiplication; by definition, $\Phi(n)$ is the order of this group. Recall that for any group G of finite order d, Lagrange's theorem states that for all $g \in G$, g^d is the identity in G. For the group $(\mathbb{Z}/n\mathbb{Z})^\times$, this means that if $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have $[a]_n^{\Phi(n)} = [1]_n$. In other words:

Theorem 2.1. *Let a be an integer with $(a,n) = 1$. Then $a^{\Phi(n)} \equiv 1$ (mod n).*

This is known as *Euler's theorem*. When n is a prime, it becomes the statement that $a^{p-1} \equiv 1 \pmod p$ if p does not divide a; this special case is often called *Fermat's little theorem*.

In fact, Euler's theorem predates Lagrange's theorem by about a century. A more historically accurate proof of Euler's theorem goes like this:

Let a be an integer with $(a,n) = 1$, and consider the product $L = \prod_{1 \leq q < n; (q,n)=1} (aq)$. On the one hand, we have $L = a^{\Phi(n)} \prod_{1 \leq q < n; (q,n)=1} q$. On the other hand, for each q' with $1 \leq q' < n$ such that $(q', n) = 1$, the equation $aq \equiv q' \pmod n$ has a unique solution mod n (since $(a,n) = 1$), and hence there is a unique q, with $1 \leq q < n$ such that $aq \equiv q' \pmod n$.

$$L = \prod_{1 \leq q < n; (q,n)=1} (aq) \equiv \prod_{1 \leq q' < n, (q',n)=1} q' (\text{mod } n).$$

We thus have

$$a^{\Phi(n)} \prod_{1 \leq q < n; (q,n)=1} q \equiv \prod_{1 \leq q' < n, (q',n)=1} q' (\text{mod } n).$$

Cancelling the product from both sides (all of the factors are invertible mod n), we find $a^{\Phi(n)} \equiv 1 \pmod n$.

LECTURE 4: THE Φ-FUNCTION

1. The Euler Φ-function

Recall that $\Phi(n)$ denotes the number of elements of $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

The Chinese Remainder theorem shows that if m and n are positive integers with $(m,n)=1$, we have an isomorphism of rings: $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and hence an isomorphism of groups:

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

It follows that if $(m,n)=1$, then $\Phi(mn)=\Phi(m)\Phi(n)$.

Definition 1.1. A function f on the positive integers is *multiplicative* if for all positive integers m,n such that $(m,n)=1$, we have $f(mn)=f(m)f(n)$. We say f is *strictly multiplicative* if for any pair of positive integers m,n we have $f(mn)=f(m)f(n)$.

Note that Φ is multiplicative but not strictly multiplicative, since for instance $\Phi(2)=1$ but $\Phi(4)=2$.

It is clear that a multiplicative function is determined by its values on prime powers. For p prime we have $(a,p^r)=1$ if, and only if, p does not divide a, so $\Phi(p^r)$ is the number of integers between 0 and p^r-1 that are not divisible by p. There are p^{r-1} numbers in this range divisible by p, so we have $\Phi(p^r)=p^r-p^{r-1}=p^r(1-\frac{1}{p})$.

From this and multiplicativity of Φ one has that $\Phi(n)=n\prod_{p|n}(1-\frac{1}{p})$, where p runs over the primes dividing n.

We have a very important identity involving the Φ-function, namely:

Theorem 1.2. *Let n be a positive integer. Then:*

$$\sum_{d|n}\Phi(d)=n.$$

We will later use this identity in our study of primitive roots. We will give two separate proofs of this theorem.

For the first proof, define two functions f and g by:

$$f(n)=\sum_{d|n}\Phi(d)$$

and $g(n)=n$. Clearly g is multiplicative (it's even strictly multiplicative!). Thus, if we show that f is multiplicative, and $f(p^k)=g(p^k)$ for all primes p and integers k, we must have $f=g$ and the theorem is proved.

First consider $f(p^k)$. We have:

$$f(p^k) = \sum_{d|p^k} \Phi(d) = \sum_{i=0}^{k} \Phi(p^k) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k.$$

It remains to prove multiplicativity of f. Suppose that m and n are relatively prime integers, so that we have

$$f(mn) = \sum_{d|nm} \Phi(d).$$

Note that for any divisor d of mn, if we set $t = (d, m)$ and $u = (e, n)$, then we have $t|m$, $u|n$, and $tu = d$. Moreover, this gives a bijection between divisors d of mn and pairs (t, u) consisting of a divisor t of m and a divisor u of n. We can thus rewrite the above equation as

$$f(mn) = \sum_{t|m} \sum_{u|n} \Phi(tu).$$

Moreover, for any t, u appearing in the sum, t and u are relatively prime (since any common factor would divide both m and n). We thus have:

$$f(mn) = \sum_{t|m} \sum_{u|n} \Phi(t)\Phi(u) = \left(\sum_{t|n} \Phi(t) \right) \left(\sum_{u|n} \Phi(u) \right) = f(m)f(n).$$

The second proof is more conceptual. Note that $(m, n) = 1$ if, and only if, the additive subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by m is equal to all of $\mathbb{Z}/n\mathbb{Z}$. In other words, $\Phi(n)$ counts the elements of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ that have order exactly n. Another way of saying this is that $\Phi(n)$ is the number of elements of order n in a cyclic group of order n.

Now suppose C is a cyclic group of order divisible by n (but not necessarily equal to n). Then C contains a cyclic subgroup C' of order n. Moreover, this subgroup C' contains every element of C of order dividing n. In particular, the number of elements of C of order n is equal to the number of elements of C' of order n, and this number is of course $\Phi(n)$. Thus $\Phi(n)$ counts the number of elements of order n in *any* cyclic group of order divisible by n!

Now consider the sum:

$$\sum_{d|n} \Phi(d)$$

The above discussion shows that $\Phi(d)$ is the number of elements of order d in a cyclic group C of order n. Since every element of C order d for *some* d dividing n, the total number of such elements is just the number of elements C, so the sum must equal n!

LECTURE 5: MULTIPLICATIVE FUNCTIONS

Recall that a function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ is called *multipllicative* if $f(mn) = f(m)f(n)$ for all m, n with $(m, n) = 1$, and *strictly multiplicative* if $f(mn) = f(m)f(n)$ for *all* m, n.

1. Convolution

There is a natural operation, called *convolution* that allows us to build new multiplicative functions from old ones. Given functions $f, g : \mathbb{Z}_{>0} \to \mathbb{C}$, we define the convolution $f * g$ as follows:

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

This operation has the following nice properties:

Proposition 1.1.

1. *If f and g are multiplicative, so is $f * g$.*
2. *Convolution is commutative: $f * g = g * f$ for all f, g.*
3. *Convolution is associative: $(f * g) * h = f * (g * h)$ for all f, g, h.*
4. *Let δ denote the function defined by $\delta(1) = 1$ and $\delta(n) = 0$ for $n > 1$. Then $f * \delta = f$.*

Proof.

1. Let m and n be relatively prime. We have:

   $$(f * g)(mn) = \sum_{d|mn} f(d)g(\frac{m}{d}).$$

   For each d, set $t = (d, m)$ and $u = (d, n)$, so that $tu = d$, $t|m$, and $u|n$. This gives a bijection between divisors d of mn, and pairs (t, u) consisting of a divisor t of m and a divisor u of n. We can thus rewrite the sum in terms of t and u, obtaining:

   $$(f * g)(mn) = \sum_{t|m} \sum_{u|n} f(tu)g(\frac{mn}{tu}) = \left(\sum_{t|m} f(t)g(\frac{m}{t})\right)\left(\sum_{u|n} f(u)g(\frac{n}{u})\right)$$

   and the right-hand side is $(f * g)(m)(f * g)(n)$.
2. We have $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$. Making the change of variables $e = \frac{n}{d}$, the latter is equal to $\sum_{e|n} f(\frac{n}{e})g(e) = (g * f)(n)$.
3. We have:

   $$((f * g) * h)(n) = \sum_{d|n} (f * g)(d)h(\frac{n}{d}) = \sum_{d|n} \sum_{e|d} f(e)g(\frac{d}{e})h(\frac{n}{d})$$

$$(f*(g*h))(n) = \sum_{d'|n} f(d')(g*h)(\frac{n}{d'}) = \sum_{d'|n}\sum_{e'|\frac{n}{d'}} f(d')g(e')h(\frac{n}{e'})$$

The two sums are related by the change of variables $e = d'$, $d = d'e'$, which has inverse $d' = e, e' = \frac{d}{e}$.

(4) We have $(f*\delta)(n) = \sum_{d|n} f(d)\delta(\frac{n}{d}) = f(n)$ since the only term of the sum for which $\delta(\frac{n}{d})$ is nonzero is $d = n$.

□

The upshot of this proposition is that convolution "almost" makes the set of multiplicative functions into an abelian group; in particular the operation is commutative, associative, and has an identity. Typically, however, a function f will not have an inverse under the convolution operation.

2. Examples

The convolution operation lets us produce interesting multiplicative functions from ones that are obviously multiplicative. For instance, the following functions are clearly multiplicative: the function 1 that takes the value 1 at all integers n, and the function f_k defined by $f_k(n) = n^k$.

It follows that functions built by convolution from the above functions are multiplicative. For instance, the convolution $\sigma_k = f_k * 1$ is, by definition, the function defined by $\sigma_k(n) = \sum_{d|n} d^k$; we immediately see that it is multiplicative.

Another important multiplicative function is the Möbius function μ. It is defined on prime powers by setting $\mu(p^k) = -1$ if p is prime and $k = 1$, and $\mu(p^k) = 0$ for p prime and $k > 1$. It follows that $\mu(n) = 0$ if n is not squarefree, and if n is the product of k distinct primes, then $\mu(n) = (-1)^k$.

The reason the μ function is so important is that it provides an inverse to the function 1 under convolution. That is:

Theorem 2.1 (Möbius Inversion)**.** *The convolution $\mu * 1$ is equal to δ.*

Proof. Both sides are multiplicative, so it suffices to check this for prime powers. For $k \geq 1$ we have:

$$(\mu * 1)(p^k) = \sum_{d|p^k} \mu(d) = \sum_{i=0}^{k} \mu(p^i) = 1 + (-1) + 0 + \cdots + 0 = 0 = \delta(p^k)$$

□

As a corollary, we see for instance that

$$\sigma_k * \mu = (f_k * 1) * \mu = f_k * (1 * \mu) = f_k * \delta = f_k.$$

The function μ is related to the Φ function in the following way:

Theorem 2.2. *We have $\Phi = f_1 * \mu$.*

Proof. It suffices to check this for prime powers as both sides are multiplicative. We have $\Phi(p^k) = p^k - p^{k-1}$. On the other hand

$$(f_1 * \mu)(p^k) = \sum_{i=0}^{k} p^k \mu(p^{k-i}) = 0 + \ldots 0 + (-p^{k-1}) + p^k = p^k - p^{k-1}.$$

□

As a corollary, we obtain yet another proof of the identity:

Corollary 2.3. *Let n be a positive integer. Then:*

$$\sum_{d|n} \Phi(d) = n.$$

Proof. We have $\Phi = f_1 * \mu$. Convolving both sides with 1, we obtain

$$\Phi * 1 = (f_1 * \mu) * 1 = f_1 * (\mu * 1) = f_1 * \delta = f_1.$$

But $f_1(n) = n$, and $(\Phi * 1)(n) = \sum_{d|n} \Phi(d)$. □

3. Perfect Numbers

One application of the theory of multiplicative functions is to the study of perfect numbers. A number n is perfect if the sum of its divisors (other than n itself) is equal to n. For instance 6 is the sum $1+2+3$ of its divisors other than 6. In terms of multiplicative functions, n is perfect if, and only if, $\sigma_1(n) = 2n$. We will write σ for σ_1 in the rest of this section, for brevity.

Observe that if n is an integer such that $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect. Indeed, we have:

$$\begin{aligned} \sigma(2^{n-1}(2^n-1)) &= \sigma(2^{n-1})\sigma(2^n-1) \\ \sigma(2^{n-1}) &= 1 + 2 + \cdots + 2^{n-1} = 2^n - 1 \\ \sigma(2^n - 1) &= 1 + (2^n - 1) = 2^n \end{aligned}$$

so that $\sigma(2^{n-1}(2^n - 1)) = 2^n(2^n - 1)$.

Every known perfect number is of this form. A prime of the form $2^n - 1$ is called a *Mersenne prime*; they can only occur for n prime. (This is because if $n = ab$ we can factor $2^{ab} - 1$ as $(2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1)$.)

There is a partial converse to the above result, due to Euler (although it was claimed by several mathematicians prior to him, without a correct proof).

Theorem 3.1. *Let n be an even perfect number, and write $n = 2^k m$ with $k \geq 1$ and m odd. Then $m = 2^{k+1} - 1$ and is prime. (In particular, every even perfect number arises from a Mersenne prime via the recipe above.)*

Proof. If n is perfect then $\sigma(n) = 2n$. In terms of m and k we have on the one hand $\sigma(2^k m) = 2^{k+1}m$. On the other hand $\sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m)$. So we have $2^{k+1}m = (2^{k+1} - 1)\sigma(m)$. Rearranging, we obtain:

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

Since $\sigma(m)$ and m are integers, so is $\frac{m}{2^{k+1}-1}$; moreover then $\frac{m}{2^{k+1}-1}$ divides m. So the right hand side expresses $\sigma(m)$ as a sum of two divisors of m. Since $\sigma(m)$ is the sum of ALL the divisors of m, it must be that m and $\frac{m}{2^{k+1}-1}$ are the ONLY two divisors of m. Thus $\frac{m}{2^{k+1}-1} = 1$, so $m = 2^{k+1} - 1$. Moreover, since m has exactly two divisors, m is prime. □

By contrast, it is stll not known whether odd perfect numbers exist although it has been shown that such a number has many hard to satisfy properties, and it is strongly suspected that no odd perfect numbers exist.

LECTURE 6: PRIMITIVE ROOTS

1. Basic Definitions

Definition 1.1. Let n be a positive integer and a an integer with $(a, n) = 1$. The *order* of a mod n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Proposition 1.2. *Let a be an integer with $(a, n) = 1$, and let k be the order of a mod n. If $a^d \equiv 1$ (mod n) then k divides d.*

Proof. Write $d = qk + r$ with q, r integers and $0 \leq r < k$. Then $1 \equiv a^d = a^{qk+r} = (a^k)^q(a^r) \pmod{n}$; since $a^k \equiv 1 \pmod{n}$ it follows that $a^r \equiv 1$ mod n. Since $r < k$, r cannot be positive (by the definition of order), so $r = 0$ and $d = qk$. □

It now follows from Euler's theorem that for any a with $(a, n) = 1$, the order of a mod n divides $\Phi(n)$.

Definition 1.3. An integer a with $(a, n) = 1$ is a *primitive root* mod n if the order of a mod n is exactly $\Phi(n)$.

Primitive roots need not exist modulo every n. For instance, if $n = 8$, then $3, 5,$ and 7 have order 2 mod 8, and 1 of course has order 1. Since $\Phi(8) = 4$, there are no primitive roots mod 8.

On the other hand, we have:

Theorem 1.4. *Let p be a prime. Then there exists a primitive root mod p.*

We will prove this shortly. In fact, this is not the strongest result possible; one has:

Theorem 1.5. *Let n be a positive integer. There exists a primitive root mod n exactly in the following cases (and no others):*

1. $n = 1, 2,$ *or* 4,
2. $n = p^r$ *where p is an odd prime and $r > 1$, and*
3. $n = 2p^r$ *where p is an odd prime and $r > 1$.*

We will not prove this, although there are some special cases on the example sheets.

2. Polynomials over a field

The proof of this theorem requires some results about roots of polynomials mod p. Over the rational numbers we all know that a polynomial of degree d has at most d roots. This can fail over other rings; for instance, the polynomial $x^2 - x$ has the roots $[0]_6, [1]_6, [3]_6, [4]_6$ mod 6. The issue here is that $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Lemma 2.1. *Let R be a ring, and $P(X)$ be a polynomial in X with coefficients in R. If $P(\alpha) = 0$, then there exists a polynomial $Q(X)$ with coefficients in R such that $P(X) = Q(X)(X - \alpha)$.*

Proof. We proceed by induction on the degree of P, the degree zero case being clear. Suppose the result is true for polynomials of degree $d - 1$, and let $P(X)$ have degree d. If the leading term of $P(X)$ is cX^d, let $S(X) = P(X) - cX^{d-1}(X - \alpha)$. We have $S(\alpha) = 0$, and $S(X)$ has degree $d - 1$so there exists $T(X)$ with coefficients in R such that $R(X) = T(X)(X - \alpha)$. Then $P(X) = [cX^d + T(X)](X - \alpha)$. □

Theorem 2.2. *Let F be a field, and $P(X)$ a polynomial of degree d with coefficients in F. Then $P(X)$ has at most d distinct roots in F.*

Proof. We again proceed by induction on d; the case $d = 0$ is clear. If $P(X)$ has degree d and α is a root, we can write $P(X) = (x - \alpha)Q(X)$. Now if $P(\beta) = 0$, then $(\beta - \alpha)Q(\beta) = 0$, so (since F is a field) either $\beta = \alpha$ or β is a root of $Q(X)$. By the inductive hypothesis $Q(X)$ has at most $d - 1$ roots in F, so P has at most d roots as claimed. □

As a corollary, we deduce:

Corollary 2.3. *Let p be a prime, and let d divide $p-1$. Then the polynomial $x^d - 1$ has exactly d roots mod p.*

Proof. Note that by Fermat's little theorem, $[1]_p, \dots, [p-1]_p$ are all roots of $x^{p-1} - 1$ mod p. Thus $x^{p-1} - 1$ has exactly $p - 1$ roots. Now fix d dividing $p - 1$ and write $x^{p-1} - 1 = (x^d - 1)Q(X)$ for a polynomial $Q(X)$; $Q(X)$ has integer coefficients so we can view it as a polynomial mod p. Now $x^{p-1} - 1$ has $p - 1$ roots, x^d has at most d roots, and $Q(X)$ has at most $p - 1 - d$ roots. We must thus have equality; i.e. $x^d - 1$ has d roots mod p. □

Another way of stating the corollary is to say that for any d dividing $p-1$, there are exactly d elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ whose order divides d.

3. Existence of primitive roots mod p

We are now ready to prove the existence of primitive roots mod p. We first recall the identity:

$$\sum_{d|n;d>0} \Phi(d) = n.$$

Theorem 3.1. *Let p be a prime. Then for any d dividing $p - 1$, there are exactly $\Phi(d)$ elements of order d in $(\mathbb{Z}/p\mathbb{Z})^\times$. In particular there are $\Phi(p-1)$ primitive roots mod p.*

Proof. We prove this by strong induction on d; the case $d = 1$ is clear. Fix d. The inductive hypothesis tells us that for any d' dividing d and strictly less than d there are $\Phi(d')$ elements of exact order d'. On the other hand there are a total of d elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order dividing d. Thus the number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order exactly d is:

$$d - \sum_{d'|d, 0<d'<d} \Phi(d')$$

and this is precisely $\Phi(d)$. □

4. Discrete logarithms

If g is a primitive root mod n then, by definition, the order of g is $\Phi(n)$. It follows that the powers $g, g^2, \dots g^{\Phi(n)}$ are all distinct mod n (since if $g^i \equiv g^j$ mod n for $0 < i < j < n$ we would have $g^{j-1} \equiv 1 \pmod{n}$.) Since there are only $\Phi(n)$ classes in $(\mathbb{Z}/n\mathbb{Z})^\times$, this says that if g is a primitive root then every class in $(\mathbb{Z}/n\mathbb{Z})^\times$ is a power of g. In other words, the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group of order $\Phi(n)$, generated by g. For this reason primitive roots are often called *generators*.

Another way to say this is that when a primitive root g exists mod n, the map: $\mathbb{Z}/\Phi(n)\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\times$ taking $[a]_{\Phi(n)}$ to $[g^a]_n$ is an isomorphism, from the additive group of $\mathbb{Z}/\Phi(n)\mathbb{Z}$ to $(\mathbb{Z}/n\mathbb{Z})^\times$. It thus has an inverse, which we call the *discrete logarithm to the base g*.

Explicitly, if g is a primitive root mod n, then the discrete logarithm to the base g (denoted $\log_g$) is defined by $\log_g a = [k]_{\Phi(n)}$, where k is an integer such that $g^k \equiv a \pmod{n}$.

One use of the discrete logarithm is to solve exponential equations mod n, if n admits a primitive root g. For instance, by applying $\log_g$ to both sides of the equation $x^d \equiv a \pmod{n}$, we obtain the linear congruence equation $d \log_g x \equiv \log_g a \pmod{\Phi(n)}$ and we can solve those with techniques explained earlier.

LECTURE 7: PRIMALITY TESTING

1. Computational Complexity

The next two lectures will discuss algorithms that make use of the elementary number theory we've developed. In order to discuss them in detail, we must say a few words about what makes an algorithm *efficient*. We measure the complexity of an algorithm by measuring how many operations that algorithm takes to produce an output. Of course this depends on the complexity of the input.

Since computers express both their input and output as strings of bits, we measure the complexity of the input by the length of the bit-string representing it, that is, the number of bits it takes to express that input as a sequence of bits. If (as will usually be the case for us) the input is an integer n, then it takes roughly $\log_2 n$ bits to represent this.

If we have an algorithm, we measure its complexity by asking: for a given length of input, how many operations does it take to produce an output? In particular, if $f : \mathbb{Z}_{>0} \to \mathbb{R}$ is a function, we say that an algorithm "runs in $O(f)$ time" if there exists a constant c, such that for all $\ell \in \mathbb{Z}_{>0}$, and all inputs of length ℓ, the algorithm takes at most $cf(\ell)$ operations to complete.

Of particular interest to us are "polynomial time" algorithms; these are algorithms that run in $O(\ell^n)$ time for some n. For such algorithms, if you double the length of the input, you multiply the run time by a constant factor 2^n for some n; in other words, the difficulty of the problem grows in a reasonable way with the length of the input. By contrast, if an algorithm is only $O(e^{c\ell})$ for some constant c, then doubling ℓ can cause the difficulty of the problem to grow by a very large amount! Such algorithms are said to run in *exponential time* and are generally considered impractical (though they may still be useful for ℓ small).

One subtlety is that we need to make precise what we mean by an operation. For the purposes of this course, we will take a single integer multiplication, addition, or division to be a single operation, regardless of the size of the integer. This is convenient but misleading, as certainly multiplying two 1024-bit integers is harder than multiplying two 32-bit integers! We will ignore this distinction as it does not matter for the purposes of classifying algorithms as "polynomial-time" or "not polynomial-time" (though it can change the particular exponent involved). For more delicate analysis of algorithms this distinction can matter quite a bit.

2. Exponentials mod n

Many of our algorithms will involve computing expressions of the form a^m (mod n). We must show that we can do this in polynomial time. Note that simply multiplying a by itself m times will not work; this takes m operations which is *exponential* in the length $\log_2 m$ of m! On the other hand, we can express m in binary as a sum of powers of 2: $m = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_r}$, with $b_1 > b_2 > \cdots > b_r$. Note that r is bounded by the length of the binary expression for m; that is, roughly $\log_2 m$.

We now compute a^2 mod n, $(a^2)^2 = a^4$ mod n, $(a^4)^2 = a^8$ mod n, etc. It takes $\log_2 m$ squarings to compute a^{2^i} for all i less than b_1. We then have $a^m = a^{2^{b_1}} \cdot a^{2^{b_2}} \cdot \cdots \cdot a^{2^{b_r}}$; computing this takes $r < \log_2 m$ multiplications. The whole process takes at most $2 \log_2 m$ operations, so runs in polynomial time!

It's also worth noting that Euclid's algorithm runs in polynomial time, so that computing greatest common divisors is "efficient".

3. Primality Testing

We now study algorithms to determine, given an integer n, whether n is prime. Certainly one can try all possible divisors on n; since any non-prime n has a divisor less than $\sqrt{n}$, this takes at most $\sqrt{n}$ operations. If $\ell = \log_2(n)$, then $\sqrt{n} = 2^{\frac{\ell}{2}}$, so this is an exponential time algorithm.

A more sophisticated approach is to choose some $a < n$, and compute a^{n-1} (mod n). This can be done in polynomial time, and if a^{n-1} is not 1 mod n, then Euler's theorem tells us that a cannot be prime. (This is often referred to as the *Fermat test*, after Fermat's little theorem.) Unfortunately, as we have seen, there exist Carmichael numbers - composite numbers n such that a^{n-1} is 1 mod n for all a relatively prime to n. We might still hope to randomly stumble upon an a that has a common factor with n, but this is in general unlikely, and most likely takes a number of tries that is exponential in n, so no better than trying divisors at random.

4. The Miller-Rabin Test

Nonetheless, the Fermat test provides the basis for a reliable primality test, called the *Miller-Rabin* test. The idea is to supplement the Fermat test with a second test, that is very likely to be successful in exactly the situations where the Fermat test can fail.

Let us assume that n is odd (it's easy to test whether an even number is prime!) and write $n - 1 = 2^t k$, where k is odd. We then do the following:

(1) Choose $a < n$ uniformly at random.
(2) Compute a^k mod n.
(3) By repeated squaring, compute a^{2k}, $a^{4k}, \ldots, a^{2^t k}$.
(4) If $a^{2^t k} = a^{n-1}$ is not 1 mod n, then n cannot be prime by the Fermat test; stop and return that n is not prime.

(5) If $a^{2^t k} = 1 \bmod n$, let r be the largest integer between 0 and t such that $a^{2^r k}$ is not 1 mod n. If $a^{2^r k}$ is not -1 mod n, return that n is not prime. If $a^{2^r k}$ is -1 mod n, or if there is no r such that $a^{2^r k}$ is not 1 mod n, return that n is "probably prime".

If this test returns that n is not prime, then n cannot be prime. This is clear at step 4, because n has failed the Fermat test. In step 5, the point is that if n is prime, then (as we have seen) the polynomial $X^2 - 1$ has only the roots ± 1. So if $a^{2^r k}$ is not 1 mod n, and $(a^{2^r k})^2 = 1 \bmod n$, then a has to be -1 mod n if n is prime.

On the other hand, if the test returns that n is "probably prime" then n might still be composite (just as in the Fermat test!) The difference between this test and the Fermat test, however, is the following result:

Theorem 4.1 (Miller-Rabin)**.** *Let n be composite. Then the probability of choosing a random a such that the Miller-Rabin test returns "probably prime" for the pair (a, n) is less than $1/2$.*

By running the test repeatedly, we can determine to a very high confidence that n is prime. In particular, if we run the test 1000 times on a composite number, the result of Miller-Rabin shows that the odds of getting "probably prime" every time are less than $\frac{1}{2^{1000}}$, a number so small as to be indistinguishable from zero!

We will only sketch the proof of Miller-Rabin's result here. The key point is a result we've claimed before (but not proven): if p is an odd prime, then $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic for all k.

There are two cases to consider. The first case is when n is a prime power. In this case we can show that n fails the Fermat test for most choices of a. Indeed, if $n = p^k$, Euler's theorem tells us that $a^{p^k - p^{k-1}}$ is 1 mod n for all a prime to n. If $a^{p^k - 1}$ is also 1 mod n, then the order of a divides $p^{k-1}(p-1)$ and $p^k - 1$, and thus divides their gcd $p-1$. But there are only $p-1$ elements of order dividing $p - 1$ modulo n, so the odds of unexpectedly passing the Fermat test are $\frac{p-1}{p^k - 1}$ which is roughly $\frac{1}{p^{k-1}}$. This is very small and certainly less than $\frac{1}{2}$!

In the second case, n is a product $p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ of at least two prime powers. Hence $(\mathbb{Z}/n\mathbb{Z})^\times$ is the product of the cyclic groups $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ for all i. Note that in a product of s cyclic groups there are 2^s elements a such that $a^2 = 1$. Thus we have good reason to suspect that the probability of finding an a that returns "not prime" at step 5 is quite high!

Indeed, for each i let 2^{t_i} be the largest power of 2 dividing $\Phi(p_i^{k_i})$. Then there are 2^{t_i} elements of 2-power order in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$. Of these elements, 1 has order 1, 1 has order 2, 2 have order 4, etc, up to $2^{t_i - 1}$ elements of order 2^{t_i}.

Now suppose we choose an a uniformly at random. Then a^k is distributed uniformly at random among the elements of 2-power order in $(\mathbb{Z}/n\mathbb{Z})^\times$. By the Chinese remainder theorem, $a^k \pmod{p^i}$ is distributed uniformly at random among the 2^{t_i} elements of 2-power order in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$, and each of these classes mod $p_i^{k_i}$ is independent of the others.

We now ask: for which a^k does the test return "probably prime"? For each i, let 2^{r_i} denote the order of a^k mod $p_i^{k_i}$. Let r' be the maximum of the r_i. Then $(a^k)^{2^{r'}}$ is one mod $p_i^{k_i}$ for all i (and hence 1 mod n), but $(a^k)^{2^{r'-1}}$ is not. Fix i such that $r_i = r'$, and suppose that for some j we have $r_j < r'$. Then r' is the smallest integer such that $(a^k)^{2^{r'}}$ is 1 mod n, but $(a^k)^{2^{r_j}}$ is one mod $p_j^{k_j}$. Thus $(a^k)^{2^{r'-1}}$ is one mod $p_j^{k_j}$, so $(a^k)^{2^{r-1}}$ is not -1 mod n. Thus the algorithm correctly determines that n is composite.

The only cases when the algorithm returns "probably prime" are those in which all r_i are equal; a simple but messy counting argument shows that this is less than half of the possible cases. □

The Miller-Rabin test is probabilistic, and although we can use it to determine whether n is prime with very high confidence, it falls short of actually giving a *proof* that n is prime. It was only in this millennium (2002) that a polynomial-time, deterministic primality test was discovered. It is due to Agrawal, Kayal, and Saxena. In practice it tends to be much less efficient than the Miller-Rabin test; typically when searching for primes it is faster to first apply the Miller-Rabin test, and then only apply a deterministic test like the Agrawal-Kayal-Saxena test once you are already quite confident that the number is prime.

LECTURE 8: PUBLIC-KEY CRYPTOGRAPHY

1. Messages as sequences of classes mod n

Since the advent of computers, the idea of representing a message by a string of numbers is a familiar one. In practice, to do this one typically chooses a way of encoding individual characters as binary numbers of a fixed length d (usually 8 or 16 bits, i.e. binary digits.) If we then cut a message up into "blocks" of n characters and concatenate the binary representations of each character in the block, we obtain a dn-bit binary number that represents an n-character block as an integer between 0 and 2^{nd}. If we choose some modulus $m > 2^{nd}$, then we can alternatively represent a block as a class in $\mathbb{Z}/m\mathbb{Z}$. Thus we will be mainly concerned with the problem of communicating a congruence class c mod m, for some large m, between a sender A and a recipient B. The goal is to do this in such a way that any eavesdroppers on the communication can not deduce what c is (but B can).

2. The RSA algorithm

Most traditional forms of cryptography rely on a *shared secret* known to both A and B. This shared secret is effectively some invertible function f from $\mathbb{Z}/m\mathbb{Z}$ to itself. The idea is that rather than sending c to B directly, A computes $f(c)$, sends that to B, and then B computes $f^{-1}(c)$. Since eavesdroppers do not know f, they (at least in principle) can't recover c from $f(c)$.

In practice, for A and B to agree on a function f poses problems. (In particular, they have to communicate to do so, and if eavesdroppers listen to that communication they can learn f.)

The algorithm we describe today avoids this problem completely! It is what is known as a *public-key* algorithm. Instead of secrets being shared between A and B, our recipient B creates a secret *known only to B* (his private key), and then releases additional information (the public key) to *anyone who wants to communicate with him.* For anyone to send B a message, only the public key is required, but decoding the message requires the private key.

Here is how the algorithm works. B first chooses two large prime numbers p and q (in practice, each of these is around 2^{1024} or so) and sets $m = pq$. An integer mod m thus allows you to represent 2048 bits of information, or 256 eight-bit characters. B also chooses a number e such that $(e, \Phi(m)) = 1$, and lets d be a multiplicative inverse of e mod $\Phi(m)$.

The public key, that B shares with everyone, consists of the numbers m and e.

The private part of the key, that B must keep secret, consists of the numbers p, q, and d.

To encode a message c, a sender A computes $s = c^e \pmod{m}$, and sends it to B.

Given an encoded message s, B decodes it by computing $s^d \pmod{m}$. The reason this works is that if $s = c^e$, then one has $(c^e)^d = c^{ed} = c^{1+k\Phi(m)}$, since, by construction, $ed \equiv 1 \pmod{\Phi(m)}$. Thus $s^d = c^{ed} \equiv c \pmod{m}$ by Euler's theorem.

Any eavesdropper who knows c^e and wants to deduce c has to be able to compute an eth root of c mod m. *As far as we know,* this is quite difficult computationally! The best (publicly) known approaches all involve factoring m. For numbers around 2^{2048}, this is not feasible with today's computing equipment (and might well never be feasible)! On the other hand, we have no formal proof that factoring is as computationaly difficult as it seems to be. As far as I'm aware, we don't even have a formal proof that breaking RSA is as computationally difficult as factoring.

For all we know, in fact, it's not outside the realm of possibility that the $P! = NP$ conjecture in computer science is false, in which case *no form of public-key cryptography is secure!*

In spite of these uncertainties, all of our intuition and experience suggests that recovering c from c^e without knowing a factorization of m is computationally infeasible. It is this infeasibility that allows the cryptosystem to work.

3. Signing with RSA

Public-key cryptography can also be used as proof of identity. Suppose B wants to make a declaration to the world, and prove beyond all doubt that it was B who made the declaration, and not an impostor. (Perhaps this declaration is a will, or acceptance of a contract, for instance.)

B first represents the message he wants to sign as a class c mod m. To sign this class, B computes $c^d \pmod{m}$ using the private part of the key, and sends the world the pair (c, c^d).

Suppose A wants to verify that a pair (c, s) was a message signed by B. Then A computes $s^e \pmod{m}$, which requires only the public part of the key. If $s \equiv c^d \pmod{m}$, then $s^e = c^{de} \equiv c$ mod m. So A just needs to check that $s^e \equiv c \pmod{m}$ and if so the signature is verified.

To fake a message signed by B, a forger needs to solve the problem of, given a message c, finding a signature s such that $s^e \equiv c \pmod{m}$. *This is precisely the same problem as deciphering a message sent by the algorithm above.* Thus forging signatures is just as hard as breaking the encryption!

LECTURE 9: QUADRATIC RESIDUES

1. Quadratic Residues

Definition 1.1. Let p be an odd prime and a an integer not divisible by p. We say that a is a *quadratic residue mod p* if there exists an integer d with $d^2 \equiv a \pmod{p}$. If no such d exists, we say that a is a *quadratic non-residue mod n*.

Note that, by convention, integers a divisible by p are neither quadratic residues nor quadratic non-residues mod p.

Proposition 1.2. *Let a, b be integers with $(a,p) = (b,p) = 1$. Then:*

- *If a and b are quadratic residues mod p, then so is ab.*
- *If a is a quadratic residue mod p and b is a quadratic non-residue mod p, then ab is a quadratic non-residue mod p.*
- *If a and b are quadratic non-residues mod p, then ab is a quadratic residue mod p.*

Proof. For the first claim, if $a \equiv d^2 \pmod{p}$ and $b \equiv c^2 \pmod{p}$, then $ab \equiv (cd)^2 (mod \text{p})$. For the second, if $a \equiv d^2 \pmod{p}$ and $ab \equiv c^2 \pmod{p}$, then we have $[b]_p = [a]_p^{-1}[ab]_p = ([d]_p^{-1}[c]_p)^2$.

The third requires more than just the group structure on $(\mathbb{Z}/p\mathbb{Z})^\times$. Choose a primitive root g mod p and write $a \equiv g^r \pmod{p}$, $b \equiv g^s \pmod{p}$. Then r and s are odd since a and b are non-residues. But then $ab \equiv g^{r+s} \pmod{p}$ and $r+s$ is even. □

Definition 1.3. The Jacobi symbol $\left(\frac{a}{p}\right)$, for p prime and a an integer, is defined by:

- $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue mod p,
- $\left(\frac{a}{p}\right) = -1$ if a is a quadratic non-residue mod p,
- $\left(\frac{a}{p}\right) = 0$ if $p \mid a$.

The proposition above then amounts to saying that the map: $(\mathbb{Z}/p\mathbb{Z})^\times \to \pm 1$ defined by $[a]_p \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism.

In fact, the existence of primitive roots gives us an easy description of this map:

Theorem 1.4 (Euler's Criterion)**.** *Let p be an odd prime, and a an integer not divisible by p. Then*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \textit{(mod } p\textit{)}.$$

Proof. If p divides a this is clear. Otherwise, note that $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ by Fermat's little theorem. Thus (since the polynomial $x^2 - 1$ has only two roots mod p) we have $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. If a is a quadratic residue mod p then $a \equiv d^2 \pmod{p}$ for some d, and then $a^{\frac{p-1}{2}} \equiv d^{p-1} \equiv 1 \pmod{p}$. On the other hand, if a is a quadratic non-residue, then $a \equiv g^r \pmod{p}$ for some odd integer r and primitive root g mod p. Then $a^{\frac{p-1}{2}} \equiv g^{\frac{r(p-1)}{2}}$. Since r is odd, $\frac{r(p-1)}{2}$ is not divisible by $p-1$, so (because g has order $p-1$, $g^{\frac{r(p-1)}{2}}$ is not congruent to 1 mod p. It must therefore be -1 mod p. □

2. Computing Jacobi symbols

Euler's criterion lets us determine, for fixed p, which a are quadratic residues mod p. What if we fix a, and ask for which odd primes p is a a quadratic residue?

When $a = -1$, Euler's criterion gives an easy answer: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, so -1 is a quadratic residue mod p if, and only if $\frac{p-1}{2}$ is even. In other words:

Proposition 2.1. *The integer -1 is a quadratic residue mod p if p is 1 mod 4, and a quadratic non-residue if p is 3 mod 4.*

When $a = 2$, the situation is more difficult, but still amenable to a direct approach:

Proposition 2.2 (Gauss' Lemma)**.** *:*

- $\left(\frac{2}{p}\right) = 1$ *if* $p \equiv 1, 7 \pmod{8}$
- $\left(\frac{2}{p}\right) = -1$ *if* $p \equiv 3, 5 \pmod{8}$.

Proof. Let $q = \frac{p-1}{2}$, and set $Q = 2(4)(6)(8)\dots(p-1) = 2^q(q!)$. Reduce all the factors in the product defining Q mod p so that they lie between $-q$ and q (i.e., subtract p from every factor greater than q.) Let Q' be the resulting product $2(4)(8)\dots(-3)(-1)$. We have $Q' \equiv Q \pmod{p}$. On the other hand, the factors in the product defining Q' are the even integers from 1 to q and the negatives of the odd integers from 1 to q. Thus $Q' = (-1)^r q!$, where r is the number of odd integers between 1 and q. We thus have $2^q(q!) \equiv (-1)^r(q!) \pmod{p}$, so $2^q \equiv (-1)^r \pmod{p}$. The result follows by noting that r is even precisely when p is 1 or 7 mod 8, and invoking Euler's criterion. □

Since we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, to answer this question in full generality it suffices to answer it for $a = -1$, for $a = 2$, and for a an odd prime. We will address the case of odd primes in the next lecture.

LECTURE 10: QUADRATIC RECIPROCITY

In the last lecture we reduced the question of computing $\left(\frac{a}{p}\right)$ to the case where a is an odd prime. In this case we have the following remarkable result, which is the crown jewel of 18th-century number theory:

Theorem 0.1 (Law of Quadratic Reciprocity)**.** *Let p and q be odd primes. Then:*

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *if either p or q is 1 mod 4;*
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ *if both p and q are 3 mod 4.*

One can rephrase this a bit more tersely as the equivalent statement:

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

Knowing this, together with the results for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ from last lecture, gives us a way of computing $\left(\frac{a}{p}\right)$ as long as we can factor a. Indeed, given a, we can assume that $0 \leq a < p$, and write $a = \pm 2^r q_1^{k_1} \dots q_n^{k_n}$, with q_i odd primes less than p. Then we have:

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^r \prod_i \left(\frac{q_i}{p}\right)^{k_i}$$

Our results from last lecture let us compute $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$; quadratic reciprocity lets us express $\left(\frac{q_i}{p}\right)$ in terms of $\left(\frac{p}{q_i}\right)$. To compute the latter we can reduce p mod q_i, so that it lies between 0 and $q_i - 1$, and work inductively; at each stage the numbers involved will get strictly smaller.

Note that quadratic reciprocity implies that for each odd prime q, the question of whether q is a quadratic residue mod p has an answer in terms of congruence conditions mod q and mod 4. From this and the Chinese remainder theorem, we can deduce that the question: "for which primes p is a a quadratic residue mod p?" has an answer in terms of congruence conditions on p.

More generally, one can ask, given a monic polynomial f with integer coefficients, for which primes p does f have a root? (The above case is the case of the polynomial $X^2 - a$.) This is a very deep question in number theory! Indeed, we are still extremely far from having a complete answer. One question it is natural to ask is: for which f does the above question have an answer given in terms of congruence conditions on p. A deep branch of algebraic number theory called *class field theory* tells us that this will happen precisely when the field extension determined by f has abelian Galois group. Beyond this we know very little, but there are connections to the theory of modular forms.

LECTURE 11: PROOF OF QUADRATIC RECIPROCITY

Recall that we have claimed:

Theorem 0.1 (Law of Quadratic Reciprocity)**.** *Let p and q be odd primes. Then:*

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *if either p or q is 1 mod 4;*
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ *if both p and q are 3 mod 4.*

1. Proof of Quadratic Reciprocity

Quadratic Reciprocity was one of the deepest results of the 18th century, and there are many approaches to proving it, none of which are particularly simple. The following proof is due to Eisenstein.

Let p and q be odd primes. We can try to compute $\left(\frac{p}{q}\right)$ in the same way we computed $\left(\frac{2}{p}\right)$ above: by considering the product $p(2p)(3p)\dots(\frac{q-1}{2}p)$. On the one hand this is equal to $p^Q Q!$, where $Q = \frac{q-1}{2}$. On the other hand we can reduce this product mod q. In particular, for $1 \leq i \leq Q$ let s_i be the unique integer between $-Q$ and Q such that $s_i \equiv pi \pmod{q}$. Then $p^Q Q! = p(2p)(3p)\dots(Qp) \equiv \prod_{i=1}^{Q} s_i \pmod{q}$. On the other hand, we have:

Lemma 1.1. *For each $1 \leq j \leq Q$, there exists a unique i between 1 and Q such that $s_i = \pm j$.*

Proof. It suffices to show that s_i is never 0, and that s_i is never equal to $\pm s_j$ for $i \neq j$. For the first of these, note that if $s_j = 0$, then $pi \equiv 0 \pmod{q}$; this is impossible since p and i are both invertible mod q. Suppose we have $1 \leq i < j \leq Q$ with $s_i = \pm s_j$. Then either $p(i+j) \equiv 0 \pmod{q}$ or $p(j-i) \equiv 0 \pmod{q}$; this is impossible since $1 \leq j-i < j+i < q$, and p is invertible mod q. □

It follows that we have $\prod_{i=1}^{Q} s_i = (-1)^{S(p,q)} Q!$, where $S(p,q)$ is the number of i between 1 and Q such that $s_i < 0$. Putting this together with the above, we find that $p^Q Q! \equiv (-1)^{S(p,q)} Q! \pmod{Q}$, so that $p^Q \equiv (-1)^{S(p,q)} \pmod{q}$. We thus have:

Lemma 1.2. *Let p and q be odd primes. Then $\left(\frac{p}{q}\right) \equiv (-1)^{S(p,q)} \pmod{q}$.*

Thus we need to understand the parity of $S(p,q)$ and $S(q,p)$, and find a relationship between the two of them. More generally, if a is any odd number, let s_i be the unique integer between $-Q$ and Q such that $s_i \equiv ai$

(mod q), and let $S(a,q)$ be the number of i between 1 and Q such that $s_i < 0$.

Proposition 1.3. *Let a be an odd positive integer, and let $T(a,q)$ denote the sum:*

$$T(a,q) = \sum_{j=1}^{Q} \lfloor \frac{aj}{q} \rfloor.$$

Then $S(a,q) \equiv T(a,q)$ (mod 2).

Proof. For $1 \leq j \leq Q$, let r_j be the unique integer between 1 and q such that $r_j \equiv aj \pmod{q}$. We then have $aj = \lfloor \frac{aj}{q} \rfloor q + r_j$.

Note that $\sum_{j=1}^{Q} j = \frac{Q(Q+1)}{2} = \frac{q^2-1}{8}$. On the other hand, we have seen that as j runs from 1 to Q, $|s_j|$ runs over the integers from 1 to Q. So we have

$$\frac{q^2-1}{8} = \sum_{j=1}^{Q} j = \sum_{j=1}^{Q} |s_j| = \sum_{1 \leq j \leq Q, s_j > 0} s_j - \sum_{1 \leq j \leq Q, s_j < 0} s_j.$$

Note that if $s_j > 0$, then $r_j = s_j$; otherwise $r_j = s_j + q$; the latter happens $S(a,q)$ times. Rewriting the last two sums in terms of the r_j thus gives:

$$\frac{q^2-1}{8} = qS(a,q) + \sum_{j=1}^{Q} r_j - 2 \sum_{j \leq j \leq Q, s_j < 0} r_j.$$

Reducing mod 2, and using that q is odd, we thus find:

$$S(a,q) \equiv \frac{q^2-1}{8} + \sum_{j=1}^{Q} r_j (\text{mod } 2).$$

On the other hand, we have:

$$a\frac{q^2-1}{8} = \sum_{j=1}^{Q} aj = \sum_{j=1}^{Q} \lfloor \frac{aj}{q} \rfloor q + r_j = qT(a,q) + \sum_{j=1}^{Q} r_j.$$

Reducing mod 2, and using that q and a are odd, we find that

$$T(a,q) \equiv \frac{q^2-1}{8} + \sum_{j=1}^{Q} r_j (\text{mod } 2).$$

The result follows. □

On the other hand, we have:

Proposition 1.4. *Let p and q be odd primes. Then $T(p,q) + T(q,p) = \frac{(p-1)(q-1)}{4}$.*

Proof. Consider the set of pairs of integers (x, y) in the rectangle $1 \leq x \leq \frac{p-1}{2}$, $1 \leq y \leq \frac{q-1}{2}$. Clearly there are $\frac{(p-1)(q-1)}{4}$ such pairs.

Now consider the line L given by $qx = py$. Since q and p are prime, there are no x, y in the rectangle that are on this line. For a given x, a point (x, y) lies below L if $y \leq \frac{qx}{p}$. There are thus $\lfloor \frac{qx}{p} \rfloor$ points in the rectangle that lie below L and have x-coordinate x. Summing over all x, we obtain $\sum\limits_{j=1} \frac{p-1}{2} \lfloor \frac{qx}{p} \rfloor$ points in the rectangle below L; this is precisely $T(q, p)$.

Similarly, for a given y, a point (x, y) lies above L if $x \leq \frac{py}{q}$. Summing over all y we find $T(p, q)$ points in the rectangle above L. The claim follows. □

Proof of quadratic reciprocity: Let p,q be odd primes. Then we have:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)}(-1)^{S(q,p)} = (-1)^{T(p,q)}(-1)^{T(q,p)} = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

LECTURE 12: SUMS OF TWO SQUARES

1. Sums of two squares

Here we begin to answer the question: which integers are representable as a sum of two squares?

Definition 1.1. We will say that a positive integer n is a *sum of two squares* if there exist integers x and y such that $n = x^2 + y^2$.

In a negative direction, note that any square is congruent to zero or one mod 4, so if n is a sum of two squares, then n cannot be congruent to 3 mod 4.

On the other hand, we have:

Lemma 1.2. *If m and n are sums of two squares, then so is mn.*

Proof. If $m = x^2 + y^2$, and $n = u^2 + v^2$, then $mn = (x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2$. □

We will later see a more conceptual interpretation of this argument.

In light of this result it makes sense to focus first on which primes are the sum of two squares. Indeed, we have:

Theorem 1.3 ((Fermat's Two-Square Theorem))**.** *Every prime congruent to* 1 *mod* 4 *is the sum of two squares.*

We will prove this in the next section. For now, we note a consequence. Let $\mathrm{ord}_p(n)$ be the largest a such that p^a divides n.

Corollary 1.4. *Let n be a positive integer, and suppose that for each prime p congruent to* 3 *(mod* 4*), we have that* $\mathrm{ord}_p(n)$ *is even. Then n is the sum of two squares.*

Proof. Such an n can be written as the product of a power of 2, powers of primes p congruent to 1 mod 4, and powers of q^2 for q congruent to 3 mod 4. But $2 = 1^2 + 1^2$, every p congruent to 1 mod 4 is a sum of two squares by the theorem, and $q^2 = q^2 + 0^2$ is a sum of two squares. Thus n is a product of sums of two squares and is therefore itself a sum of two squares. □

In fact it will turn out that these are *precisely* the n which can be expressed as the sum of two squares, but we will only prove this later, when we have more tools.

2. Proof of the two square theorem

We first note that if p is a prime congruent to one mod 4, then Euler's criterion tells us that -1 is a quadratic residue mod p. We thus have an n, which we can take between 0 and $p-1$, such that $n^2 \equiv -1 \pmod{p}$. In particular p divides n^2+1, so we can write $n^2+1 = pr$, with $1 \leq r < p$. Note that if $r = 1$ then we are done, as then $p = n^2+1$.

The strategy of the proof will be to inductively reduce the r appearing above. We will use the following proposition to do so:

Proposition 2.1 ((Fermat Descent))**.** *Suppose we have $a^2+b^2 = pr$, with a, b integers and $1 < r < p$. Then there exists $1 \leq r' < r$ and integers x, y such that $x^2+y^2 = pr'$.*

Proof. Choose u, v such that $u \equiv a \pmod{p}$, $v \equiv b \pmod{r}$, and $-\frac{r}{2} \leq u, v \leq \frac{r}{2}$. Then $u^2+v^2 \equiv a^2+b^2 \equiv 0 \pmod{r}$, so we can write $u^2+v^2 = rr'$. Since u^2 and v^2 are at most $\frac{r^2}{4}$, we have that $r' \leq \frac{r}{2}$. On the other hand, we cannot have $r' = 0$, as then $u = v = 0$, so r divides both a and b and then r^2 divides $a^2+b^2 = pr$. It would then follow that r divides p, which is impossible. Thus $1 \leq r' < r$.

Now $(a^2+b^2)(u^2+v^2) = r'r^2p$. Rewriting this as a sum of two squares, we have: $(au+bv)^2 + (av-bu)^2 = r'r^2p$. Set $x = \frac{au+bv}{r}$, $y = \frac{av-bu}{r}$; then $x^2+y^2 = r'p$. We must check that x and y are integers, however.

But $au+bv \equiv a^2+b^2 \equiv 0 \pmod{r}$, and $av-bu \equiv ab-ba \equiv 0 \pmod{r}$, so this is clear. □

Now to express p as a sum of two squares, set $a_0 = n, b_0 = 1, r_0 = r$, and repeatedly apply the proposition to get a_i, b_i, r_i with $a_i^2+b_i^2 = r_ip$ and the r_i decreasing, but always at least one. Eventually one has $r_m = 1$ for some m and the claim follows.

LECTURE 13: QUADRATIC INTEGER RINGS

1. The Gaussian Integers

Definition 1.1. The ring of *Gaussian integers*, denoted $\mathbb{Z}[i]$, is the subring of $\mathbb{C}$ consisting of all complex numbers of the form $a+bi$, where a and b are integers.

To see that $\mathbb{Z}[i]$ is a subring one must of course check that it is closed under addition and multiplication; this is easy.

There is a natural map $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ defined by $N(z) = z\overline{z}$. We have $N(a+bi) = a^2 + b^2$. On the other hand, since $\overline{zw} = \overline{zw}$, we have $N(zw) = N(z)N(w)$.

Let $z = a + bi$, $w = c + di$. We then have $zw = (ac - bd) + (ad + bc)i$. Applying the formula $N(zw) = N(z)N(w)$ we find that $(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$. This gives a conceptual reason for our earlier observation that the product of sums of two squares is a sum of two squares.

2. The ring $\mathbb{Z}[\alpha]$

This suggests that we can deduce interesting results about $\mathbb{Z}$ by considering larger subrings of $\mathbb{C}$. One way to obtain such subrings is to start from $\mathbb{Z}$ and add an extra element α in $\mathbb{C}$. This is slightly more subtle for a general α than it is for $\alpha = i$.

Definition 2.1. Let $\alpha \in \mathbb{C}$. Then the ring $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ containing α.

As usual one has to check that this makes sense. An alternative definition is to take $\mathbb{Z}[\alpha]$ to be the intersection of all subrings of $\mathbb{C}$ containing α. This intersection clearly contains 0, 1 and α, so it is nonempty. It's also closed under addition and multiplication, since it's an intersection of sets that are closed under these operations. Therefore it's a subring of $\mathbb{C}$ that, by construction is contained in any subring of $\mathbb{C}$ that contains α.

Let's show that for $\alpha = i$, this agrees with our earlier definition of $\mathbb{Z}[i]$. We've already shown that the set of all integers of the form $a+bi$ is a subring of $\mathbb{C}$. On the other hand, any subring of $\mathbb{C}$ containing i is closed under addition and multiplication, and contains 1, so it contains every complex number of the form $a + bi$. Thus our new definition is consistent with our old one.

Note that for arbitrary α, it is *not necessarily true* that $\mathbb{Z}[\alpha]$ consists of all complex numbers of the form $a + b\alpha$ for a and b integers (although it always contains all complex numbers of that form). To see this, consider examples like $\mathbb{Z}[\pi]$, $\mathbb{Z}[\frac{1}{p}]$ for p some prime, or $\mathbb{Z}[\beta]$ where β is a cube root of

2. (For example, the last ring contains β^2, which is not of the form $a + b\beta$ for any integers a and b.)

3. Quadratic subrings of $\mathbb{C}$

Definition 3.1. An element α of $\mathbb{C}$ is an *algebraic integer of degree two* (alternatively, a *quadratic algebraic integer*) if there exists a polynomial of the form $P(X) = X^2 + aX + b$ with a, b integers roots such that $P(X)$ has no rational roots and $P(\alpha) = 0$.

For instance, i is an algebraic integer of degree two since $(i)^2 + 1 = 0$.

Suppose that α is an algebraic integer of degree two, and let a, b be integers such that $\alpha^2 + a\alpha + b = 0$. Then, for x, y, z, w integers, we have

$$(x+y\alpha)(z+w\alpha) = xz+(xw+yz)\alpha+yw\alpha^2 = (xz-byw)+(xw+yz-ayw)\alpha.$$

In particular the set of complex number of the form $x + y\alpha$ (x,y integers) is closed under addition and multiplication and is therefore a subring of $\mathbb{C}$. Since this subring contains α, it contains $\mathbb{Z}[\alpha]$. On the other hand it is clear that this subring is contained in $\mathbb{Z}[\alpha]$, so the two must be equal. We thus have:

Proposition 3.2. *If α is an algebraic integer of degree two, then $\mathbb{Z}[\alpha]$ is equal to the set of complex numbers of the form $x + y\alpha$, where x and y are integers.*

For α an algebraic integer of degree two, we will say that $\mathbb{Z}[\alpha]$ is a *real quadratic subring of* $\mathbb{C}$ if α is a real number, and an *imaginary quadratic subring of* $\mathbb{C}$ if α is not real.

If $\mathbb{Z}[\alpha]$ is imaginary quadratic, then, as with $\mathbb{Z}[i]$, we can define a *norm* $N : \mathbb{Z}[\alpha] \to \mathbb{Z}_{\geq 0}$ by setting $N(z) = z\overline{z}$. Note that $\overline{\alpha}$ is also a root of $\alpha^2 + a\alpha + b$ in this case, so we have $\alpha + \overline{\alpha} = -a$, $\alpha\overline{\alpha} = b$. Thus we have $N(x + y\alpha) = (x + y\alpha)(x + y\overline{\alpha}) = x^2 + xy(\alpha + \overline{\alpha}) + y^2\alpha\overline{\alpha} = x^2 - axy + by^2$. Note that this is multiplicative: $N(zw) = N(z)N(w)$.

If $\mathbb{Z}[\alpha]$ is real quadratic, we let α^* denote the root of $X^2 + aX + b$ that is not equal to α (note that this is no longer equal to $\overline{\alpha}$.) In this case we define $N(x + y\alpha) = (x + y\alpha)(x + y\alpha^*) = x^2 - axy + by^2$. We thus get a map $N : \mathbb{Z}[\alpha] \to \mathbb{Z}$. This is again multiplicative, but no longer nonnegative. For instance, in $\mathbb{Z}[\sqrt{2}]$, $N(1 + \sqrt{2}) = (1 + \sqrt{2})(1 - \sqrt{2}) = -1$.

4. Factorization in quadratic rings

We can study factorization in quadratic rings in a way analogous to the situation over $\mathbb{Z}$. First, some definitions:

Definition 4.1. An element of $\mathbb{Z}[\alpha]$ is a *unit* if it has a multiplicative inverse; that is, if it lies in $\mathbb{Z}[\alpha]^\times$. Two elements z, w of $\mathbb{Z}[\alpha]$ are *associates* if there exists a unit $u \in \mathbb{Z}[\alpha]^\times$ such that $z = uw$.

Note that if $u \in \mathbb{Z}[\alpha]$ is a unit, there exists v such that $uv = 1$. Taking norms we find that $N(u) = \pm 1$ (if $\mathbb{Z}[\alpha]$ is imaginary quadratic, then this means $N(u) = 1$.) Conversely, if $N(u) = \pm 1$, then $uu^* = \pm 1$, so either u^* or $-u^*$ is a multiplicative inverse of u.

We thus see, for instance, that the units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Definition 4.2. If z, u are elements of $\mathbb{Z}[\alpha]$, we say $z \mid u$ if there exists $r \in \mathbb{Z}[\alpha]$ such that $u = zr$.

Note that every element of $\mathbb{Z}[\alpha]$ is divisible by units and its associates.

Definition 4.3. An element z of $\mathbb{Z}[\alpha]$ is *irreducible* if its only divisors are units and its associates.

Note that for the ring $\mathbb{Z}$, we called such elements prime. Here we will use the word irreducible instead, and save the word prime for a stronger condition (that is equivalent to irreducibility in the ring $\mathbb{Z}$).

It is also possible to definite greatest common divisors over $\mathbb{Z}[\alpha]$, although there is no longer any ordering on $\mathbb{Z}[\alpha]$. We thus need to take a different approach to defining greatest common divisors:

Definition 4.4. Let z and w be elements of $\mathbb{Z}[\alpha]$, not both zero. An element r of $\mathbb{Z}[\alpha]$ is a *greatest common divisor* of z and w if:

- r divides both z and w, and
- if $s \in \mathbb{Z}[\alpha]$ divides both z and w, then s divides r.

You showed in the exercises that over $\mathbb{Z}$, the greatest common divisor had this property, and that this property characterized the greatest common divisor up to sign. It's thus sensible to take this a definition over $\mathbb{Z}[\alpha]$. Note, however, that it is not clear from this definition that greatest common divisors always exist. They are also not unique: if a greatest common divisor does exist, then any associate is a greatest common divisor as well. On the other hand any two greatest common divisors are associates.

A natural question to ask is whether factorizations into irreducibles are unique in $\mathbb{Z}[\alpha]$. In fact, it is not hard to show that factorizations into irreducibles exist:

Proposition 4.5. *Let z be an element of $\mathbb{Z}[\alpha]$. Then z factors into irreducibles.*

Proof. Suppose there is an element of $\mathbb{Z}[\alpha]$ that does not admit a factorization into irreducibles. Then we can find such an element z such that $|N(z)|$ is minimal. Note that z itself cannot be irreducible, so we have $z = uv$ for elements u, v of $\mathbb{Z}[\alpha]$, neither of which is a unit. We have $|N(z)| = |N(u)||N(v)|$ with neither $|N(u)|$ or $|N(v)|$ equal to 1. Thus $|N(u)|, |N(v)| < |N(z)|$, so (by minimality) u and v admit factorizations into irreducibles. But then z does as well. □

On the other hand, it is *not* true, for an arbitrary $\mathbb{Z}[\alpha]$, that such factorizations are unique. For instance, in $\mathbb{Z}[\sqrt{-5}]$, one has $6 = (1+\sqrt{-5})(1-\sqrt{-5}) =$

$2 \cdot 3$, and it is not hard to see (for instance, by considering the norms of possible divisors) that 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all irreducible, and none are associates of each other.

LECTURE 15: SUMS OF TWO SQUARES II

1. Sums of two squares

Note that the norm in $\mathbb{Z}[i]$ is given by $N(a+bi) = a^2+b^2$. We can thus rephrase the question of which integers are representable as a sum of two squares by asking "which integers are norms in $\mathbb{Z}[i]$?". Since the norm is multiplicative, and every element of $\mathbb{Z}[i]$ is a product of primes, we can answer this question by asking "what are the primes in $\mathbb{Z}[i]$, and what are their norms?

Let's try to figure out the primes of $\mathbb{Z}[i]$.

Lemma 1.1. *Let p be a prime in $\mathbb{Z}[i]$. Then there exists an integer prime q such that either $N(p) = q$ or $N(p) = q^2$. In the latter case p is an associate of q. Moreover, $N(p) = q$ if, and only if, q is the sum of two squares.*

Proof. Let $n = N(p)$, and factor $n = q_1q_2\dots q_r$ as a product of integer primes. Since $n = p\overline{p}$, we have that p divides $q_1\dots q_r$, so (since p is prime), p divides q_i for some i. Let $q = q_i$. We have $q = px$. Then $q^2 = N(q) = N(p)N(x)$, so $N(p)$ divides q^2. Since $N(p)$ is not one (if it were p would be a unit), we then have either $N(p) = q$ or $N(p) = q^2$. First suppose that $N(p) = q^2$. Since p divides q we have $pu = q$; since $N(p) = N(q) = q^2$ we must have $N(u) = q$, so u is a unit and p is an associate of q.

Suppose $N(p) = q$. Writing $p = a+bi$ we see that $q = a^2+b^2$. Conversely, if $q = a^2+b^2$, then $q = (a+bi)(a-bi)$. Since p divides q we have either p divides $a+bi$ or p divides $a-bi$; in either case $N(p)$ divides q and must thus equal q. □

Corollary 1.2. $\mathbb{Z}[i]$ *are either of the form $a+bi$, where a^2+b^2 is an integer prime, or q, where q is an integer prime that is not the sum of two squares.*

We have thus reduced the whole question to the question of which primes are the sum of two squares, which we have already answered. However, our new perspective also gives us an alternative approach to this question. In particular, we have the following proof of the two-square theorem via factorization in $\mathbb{Z}[i]$:

Let p be a prime congruent to 1 mod 4. As we have seen in our earlier proof of the two-square theorem, there exists n such that p divides n^2+1. Thus, in $\mathbb{Z}[i]$, we have that p divides $(n+i)(n-i)$. Since neither $\frac{n+i}{p}$ nor $\frac{n-i}{p}$ lie in $\mathbb{Z}[i]$, p does not divide $n+i$ or $n-i$ in $\mathbb{Z}[i]$. Thus p is not prime in $\mathbb{Z}[i]$. By the corollary p must be a sum of two squares.

This proof looks non-constructive, but in fact it isn't; if you want to find a, b such that $p = a^2+b^2$, simply use Euclid's algorithms to find a GCD of p and $n+i$. Since p divides neither $n+i$ nor $n-i$, this GCD is not a unit, nor is it an associate of p, so its norm is neither 1 nor p^2; therefore this GCD has norm exactly p. In fact, this is precisely what the Fermat descent in our original proof is doing!

Since we have also shown that primes congruent to 3 mod 4 are not the sum of two squares, we have the following complete characterization of sums of two squares:

Theorem 1.3. *An integer n is a sum of two squares if and only if its prime factorization is of the form:*

$$n = 2^r p_1^{s_1} \dots p_k^{s_k} q_1^{t_1} \dots q_h^{t_h}$$

where the p_i are primes congruent to 1 *mod* 4*, the q_i are primes congruent to* 3 *mod* 4*, and the t_i are* even.

Proof. Suppose n is of the above form, and write:

$$z = (1+i)^r (a_1 + b_1 i)^{s_1} \dots (a_k + b_k i)^{s_k} q_1^{\frac{t_1}{2}} \dots q_h^{\frac{t_h}{2}},$$

where $p_i = N(a_i + b_i)$. Then $N(z) = n$. Conversely, if n is a sum of two squares, we can write $n = N(z)$, and factor $z = u(1+i)^r p_1^{s_1} \dots p_k^{s_k} q_1^{t_1} \dots q_h^{t_h}$ in $\mathbb{Z}[i]$, where the p_i are primes in $\mathbb{Z}[i]$ whose norm is a prime congruent to 1 mod 4, and the q_i are primes in $\mathbb{Z}$ congruent to 3 mod 4. Then $N(z)$ has the claimed form. □

We can go further and compute the number of ways of representing n as a sum of two squares. Indeed, if we count the representations: $n = (\pm a)^2 + (\pm b)^2$ and $n = (\pm b)^2 + (\pm a)^2$ as being equivalent, then we are counting the number of ways to write $n = z\overline{z}$, with $z \in \mathbb{Z}[i]$, up to replacing z with an associate, or interchanging z and its conjugate.

By considering the factorization of n over $\mathbb{Z}$, and then further factoring over $\mathbb{Z}[i]$, it is not hard to see that (assuming n can be written as a sum of squares at all) the number of inequivalent ways to write n as a sum of two squares is given by:

$$\frac{1}{2}(s_1+1)(s_2+1)\dots(s_r+1)$$

if at least one s_i are odd, and

$$\frac{1}{2}[1+(s_1+1)(s_2+1)\dots(s_r+1)]$$

if all s_i are even, where the s_i are the exponents of the primes congruent to 1 mod 4 in the factorization for n.

LECTURE 16: REPRESENTING INTEGERS BY NORM FORMS

1. Representing primes by quadratic forms

The advantage of this newer proof of the two square theorem, and the related characterization of sums of two squares is that it is now clear how to generalize this approach to other Euclidean domains. Let α be an imaginary quadratic algebraic integer, and b, c integers such that $\alpha^2 + b\alpha + c = 0$. We have

$$N(x + y\alpha) = (x + y\alpha)(x + y\overline{\alpha}) = x^2 - bxy + cy^2;$$

we will refer to the polynomial $P(x, y) = x^2 - bxy + cy^2$ as the *norm form* for α.

As the norm is multiplicative, representing integers by norms reduces to the question of representing primes by norms. Here we have:

Theorem 1.1. *Suppose that unique factorization holds in $\mathbb{Z}[\alpha]$, and let p be an integer prime such that the polynomial $P(x, 1) = x^2 - bx + c$ has a root mod p. Then there exist integers x and y such that $P(x, y) = p$. Conversely, if there exist such x and y, then $x^2 - bx + c$ has a root mod p.*

Proof. We have $x^2 - bx + c = (x + \alpha)(x + \overline{\alpha})$. So if $x^2 - bx + c$ has a root mod p, then there exists x such that p divides $(x + \alpha)(x - \alpha)$ in $\mathbb{Z}[\alpha]$. Since neither $\frac{x+\alpha}{p}$ nor $\frac{x-\alpha}{p}$ lies in $\mathbb{Z}[\alpha]$, p is not prime in $\mathbb{Z}[\alpha]$. Therefore p must be reducible in $\mathbb{Z}[\alpha]$, so $p = uv$ with neither u nor v units. Then $N(u)N(v) = p^2$, and neither $N(u)$ nor $N(v) = 1$, so $N(u) = p$ and the result follows.

Conversely, suppose there exist x and y such that $P(x, y) = p$. Then y is not divisible by p: if it were, then we would have $x^2 - bxy + cy^2 = p$, which implies that x is divisible by p as well. But then $x^2 - bxy + cy^2$ is divisible by p^2 so can't be equal to p. Thus y is invertible mod p, and mod p we have $P(x, y) = 0$. But mod p, we have $P(x, y) = y^2 P(\frac{x}{y}, 1) = 0 \pmod{p}$, where by $\frac{x}{y}$ we mean x times the multiplicative inverse of y. So $\frac{x}{y}$ is a root of $P(X, 1) = X^2 - bX + c \pmod{p}$. □

Moreover, it is not hard to see that when p is odd, the polynomial $x^2 - bx + c$ has a root mod p if, and only if, the discriminant $b^2 - 4c$ is a square mod p:

Lemma 1.2. *Let p be an odd prime. The polynomial $x^2 - bx + c$ has a root mod p if, and only if, $b^2 - 4c$ is zero or a quadratic residue mod p.*

Proof. Suppose $b^2 - 4c \equiv d^2 \pmod{p}$, and let $x = 2^{-1}(b+d)$. Then $x^2 - bx + c = 4^{-1}(b^2 + 2bd + d^2 - 2b(b+d) + 4c) = 0$. Conversely, if x is a root of $x^2 - bx + c$, then $(2x-b)^2 = 4x^2 - 4bx + b^2 = b^2 - 4c$. □

Since b and c are fixed we can use quadratic reciprocity to turn this into a congruence condition on p.

For instance, if $\alpha = \frac{-1+\sqrt{-3}}{2}$, then $b = c = 1$ and $\mathbb{Z}[\alpha]$ is a Euclidean domain. We thus see that any prime such that $x^2 - x + 1$ has a root mod p is of the form $x^2 + xy + y^2$, and conversely. On the other hand the lemma shows that $x^2 - x + 1$ has a root mod p if, and only if, -3 is a zero or a quadratic residue mod p.

Thus in particular $x^2 - x + 1$ has a root mod p if, and only if, -3 is a square mod p; by quadratic reciprocity this holds precisely when $p = 3$ or $p \equiv 1 \pmod{3}$. Conversely, by directly checking mod 3 we see that $x^2 - xy + y^2$ is always 0 or 1 mod 3, so the primes of the form $x^2 - xy + y^2$ are precisely 3 and the primes congruent to 1 mod 3.

When unique factorization fails in $\mathbb{Z}[\alpha]$ the above result is false. For instance, when $\alpha = \sqrt{-5}$ ($a = 0$, $b = 5$), then $P(x) = x^2 + 5y^2$. In particular 3 is not of the form $P(x, y)$, even though $x^2 + 5$ has a root mod 3. In this situation the question of finding the primes of the form $P(x, y)$ has connections to class field theory and is a very deep part of modern algebraic number theory. For a taste of this, Cox's book *Primes of the form* $x^2 + ny^2$ is very good.

LECTURE 17: SUMS OF FOUR SQUARES

1. The ring of quaternions

We've used the arithmetic of the ring $\mathbb{Z}[i]$ to determine precisely which integers are the sum of two squares. On the other hand, it is a fact (first proved by Lagrange) that every positive integer is the sum of *four* integer squares. This fact is connected with the arithmetic of a noncommutative ring, which we now describe.

Definition 1.1. The ring $\widetilde{H}$ of quaternions is the ring whose elements are formal sums $a + bi + cj + dk$, with $a, b, c, d \in \mathbb{R}$. Addition is given by the rule:

$$(a+bi+cj+dk)+(x+yi+zj+wk) = (a+x)+(b+y)i+(c+z)j+(d+w)k.$$

Multiplication is given by the rules:

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

extended by $\mathbb{R}$-linearity and the distributive law.

Let $z = a + bi + cj + dk$ be a quaternion. The *conjugate* z^* of z is the quaternion $a - bi - cj - dk$. Note that if z and w are quaternions, then $(zw)^* = w^*z^*$.

The *norm* $N(z)$ of z is given by $N(z) = zz^* = a^2+b^2+c^2+d^2$. Note that this is a *real* number, and hence commutes with all elements of $\widetilde{H}$. Thus we have:

$$N(zw) = zw(zw)^* = zww^*z^* = zN(w)z^* = zz^*N(w) = N(z)N(w).$$

As was the case with $\mathbb{Z}[i]$, this gives an expression for the product of two sums of four squares as a sum of four squares. Explicitly, one has:

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) = N(a+bi+cj+dk)N(x+yi+zj+wk)$$
$$= N((a+bi+cj+dk)(x+yi+zj+wk))$$
$$= (ax-by-cz-dw)^2+(ay+bx+cw-dz)^2+(az-bw+cx+dy)^2+(aw+bz-cy+dx)^2.$$

In particular if m and n are integers that are representable as the sum of four integer squares, then so is their product mn. Thus to prove Lagrange's theorem it sufficies to prove that every prime is the sum of four integer squares.

2. Proof of Lagrange's theorem

Let p be a prime. If $p = 2$, or p is 1 mod 4, then we have already shown that p is a sum of two squares, hence also a sum of four squares. It thus remains to prove that primes congruent to 3 mod 4 are sums of four squares. We will do this via a descent argument, similar to that used in the proof of the two square theorem.

Lemma 2.1. *Let p be a prime congruent to 3 mod 4. Then there exist x and y such that $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.*

Proof. It suffices to find an integer a such that a is a square mod p and $a+1$ is not. Since -1 is not a quadratic residue mod p we would then have $-a-1$ a quadratic residue mod p. Taking x such that $x^2 \equiv a$ mod p and y such that $y^2 \equiv -a-1 \pmod{p}$ the claim would follow.

Suppose that we cannot do this. Then for each square a mod p, $a+1$ would also be a square mod p. In particular every congruence class mod p would be a square; since this doesn't happen we are done. □

Fix a prime congruent to 3 mod 4. By the lemma we can find x and y such that $x^2 + y^2 + 1 = pr$ for some integer r. Since we only care about x and y mod p, we can further arrange that $|x|, |y| \leq \frac{p}{2}$. Then $r < p$. We are now ready to begin our descent:

Proposition 2.2. *Suppose that for some $p > r > 1$, we have x, y, z, w such that $x^2 + y^2 + z^2 + w^2 = rp$. Then there exist x', y', z', w', r' integers with $1 \leq r' < r$ and $(x')^2 + (y')^2 + (z')^2 + (w')^2 = r'p$.*

Proof. There are two cases we must treat separately. First suppose that r is even. Then either all of x, y, z, w have the same parity, or two of them are odd and two are even. Permuting x, y, z, w as necessary, we can assume x and y have the same parity, as do z and w. Then set:

$$\begin{aligned} x' &= \frac{x+y}{2} \\ y' &= \frac{x-y}{2} \\ z' &= \frac{z+w}{2} \\ w' &= \frac{z-w}{2} \end{aligned}$$

It is then easy to verify that $(x')^2 + (y')^2 + (z')^2 + (w')^2 = \frac{r}{2}p$.

Now suppose that r is odd. Choose a, b, c, d such that $-\frac{r}{2} < a, b, c, d < \frac{r}{2}$ and $a \equiv x \pmod{r}$, $b \equiv y \pmod{r}$, etc. (we can get away with strict inequalities here because r is odd.)

Since $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{r}$, our congruences imply that $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{r}$. Write $a^2 + b^2 + c^2 + d^2 = r'r$, and note that $r' < r$ since $a^2, b^2, c^2, d^2 < \frac{r^2}{4}$. On the other hand r' is nonzero (if it were zero, all of x, y, z, w would be divisible by r, and we would have $r^2|rp$, hence $r|p$. This cannot happen since $1 < r < p$. Thus we have $1 \leq r' < r$.

We then have:

$$r'r^2p = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2)$$

$= (ax+by+cz+dw)^2+(-ay+bx+cw-dz)^2+(-az-bw+cx+dy)^2+(-aw+bz-cy+dx)^2.$ Note that $ax + by + cz + dw \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{r}$. Similarly each of the other terms are congruent to zero mod r.

We thus have integers:

$$\begin{aligned} x' &= \frac{ax + by + cz + dw}{r} \\ y' &= \frac{-ay + bx + cw - dz}{r} \\ z' &= \frac{-az - bw + cx + dy}{r} \\ w' &= \frac{-aw + bz - vy + dx}{r} \end{aligned}$$

and $(x')^2 + (y')^2 + (z')^2 + (w')^2 = r'p$ as desired. □

To complete the proof, one begins with $x^2 + y^2 + 1 = pr$ and repeatedly applies the proposition until $r = 1$.

Remark 2.3. The descent in the proof of the two square theorem is really Euclid's algorithm for $\mathbb{Z}[i]$ in disguse. This descent is also Euclid's algorithm in a noncommutative setting. The associated ring is the ring of quaternions of the form $a + bi + cz + dw$, where either a, b, c, d are all integers, or a, b, c, d are all half-integers (that is, fractions of the form $\frac{r}{2}$ with r odd.)

3. Sums of three squares

At this point it's natural to ask which positive integers are the sum of *three* integer squares. This turns out to be much more difficult. In one direction, you showed on an earlier example sheet that no integer of the form $4^t(8k+7)$ (t, k integers) is a sum of three squares. Conversely, one has:

Theorem 3.1. *Every integer not of the form $4^t(8k + 7)$ is a sum of three squares.*

The proof of this requires tools beyond the scope of the class, such as the Hasse principle for quadratic forms. One place to read about this is in Serre's *A course in arithmetic.*

LECTURE 18: PELL'S EQUATION I

1. Pell's Equation

Let $d > 0$ be a nonsqure integer, and consider the equation $x^2 - dy^2 = 1$. This is called Pell's equation.

Note that $ZZ[\sqrt{d}]$ is a real quadratic subring of $\mathbb{C}$, and its norm form is given by $N(x + y\sqrt{d}) = x^2 - dy^2$. Thus the problem of finding integer solutions to Pell's equation is equivalent to finding elements of norm 1 in $\mathbb{Z}[\sqrt{d}]$. Since such elements are units, and the norm is multiplicative, these elements form a subgroup $\mathbb{Z}[\sqrt{d}]^{\times,1}$ of $\mathbb{Z}[\sqrt{d}]^{\times}$.

There are two obvious elements of $\mathbb{Z}[\sqrt{d}]^{\times,1}$, namely ± 1. All others are of the form $x + y\sqrt{d}$, with x and y integers and y nonzero. We have:

Lemma 1.1. *Let $x + y\sqrt{d}$ be an element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$. Then:*

- *We have $x, y > 0$ if and only if $x + y\sqrt{d} > 1$.*
- *We have $x > 0, y < 0$ if and only if $0 < x + y\sqrt{d} < 1$.*
- *We have $x < 0, y > 0$ if and only if $-1 < x + y\sqrt{d} < 0$.*
- *We have $x, y < 0$ if and only if $x + y\sqrt{d} < -1$.*

Proof. It is clear that if $x, y > 0$ then $x + y\sqrt{d} > 1$. But then $x - y\sqrt{d} = (x+y\sqrt{d})^{-1}$ lies between 0 and -1. Similary, $-x+y\sqrt{d}$ lies between -1 and 0, and $-x - y\sqrt{d}$ is less than -1. Thus we have the rightward implication in each of the four claims above. But since the four cases are mutually exclusive and exhaust all the possibilities, the leftward implications hold as well. □

Lemma 1.2. *Let $z = x + y\sqrt{d}$, $z' = x' + y'\sqrt{d}$ be two elements of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ with x, y, x', y' all positive. Then $z > z'$ if, and only if, $y > y'$.*

Proof. We have $z - \frac{1}{z} = x + y\sqrt{d} - (x - y\sqrt{d}) = 2y\sqrt{d}$. Since $z - \frac{1}{z}$ is an increasing function for z positive, we have $z > z'$ iff $z - \frac{1}{z} > z' - \frac{1}{z}'$ iff $y > y'$. □

Suppose we have a nontrivial element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ (that is, one other than ± 1). Without loss of generality we can take x and y positive. There then exists $\epsilon = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^{\times,1}$ such that x and y are both positive and y is as small as possible. We will call ϵ the *fundamental 1-unit* in $\mathbb{Z}[\sqrt{d}]$. By the previous two lemmas it is the smallest element of $\mathbb{Z}[\sqrt{d}]^{\times}$ that is greater than one.

Proposition 1.3. *Suppose there exists a nontrivial element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$. Then every element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ is of the form $\pm\epsilon^n$ for some n in $\mathbb{Z}$, where ϵ is the fundamental 1-unit.*

Proof. Let z be an element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$. After negating z and/or replacing z by $\frac{1}{z}$, as necessary, we can assume $z > 1$. Since ϵ is also greater than one, there exists n such that $\epsilon^n \leq z < \epsilon^{n+1}$. Then $\epsilon^{-n}z$ is a 1-unit with $1 \leq \epsilon^{-n}z < \epsilon$; since ϵ is the smallest 1-unit greater than one we have $\epsilon^{-n}z = 1$. □

LECTURE 19: PELL'S EQUATION II

1. Constructing the fundamental 1-unit

Let $d > 0$ be a nonsquare integer, and consider the equation $x^2 - dy^2 = 1$. We have seen that solutions x, y to this equation correspond to norm one units $x + y\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]^{\times,1}$. Moreover, we have seen that if there are solutions other than $(\pm 1, 0)$, and we take $\epsilon = x + y\sqrt{d}$ with y positive and as small as possible then the group $\mathbb{Z}[\sqrt{d}]^{\times,1}$ is the set $\pm\epsilon^n$ for $n \in \mathbb{Z}$.

In fact, we will show that there are always elements of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ other than ± 1, so that there are always infinitely many solutions to Pell's equation as above. The key idea is to note that $x^2 - dy^2 = 0$ precisely when $\frac{x}{y}$ is a square root of d, and thus, when d is not a square, $x^2 - dy^2 = 1$ when $\frac{x}{y}$ is in some sense "as close as possible" to $\sqrt{d}$. This suggests we should think about approximating $\sqrt{d}$ by rational numbers.

It's clear that if p and q are integers, and α is an irrational number, then we can make $|\frac{p}{q} - \alpha|$ as small as we want. However, in order to do so we might need to make q large. We will thus be interested in approximations to α where the error $|\frac{p}{q} - \alpha|$ is small *compared to* $\frac{1}{q^n}$ *for various* n. As n gets larger it will become harder and harder to find such approximations.

When $n = 1$ the situation is very easy: for any α, and any q, there exists p such that $|\frac{p}{q} - \alpha| < \frac{1}{q}$.

When $n = 2$ things are much less trivial, but we have the following important result, due to Dirichlet:

Theorem 1.1. *Let α be an irrational number, and $Q > 1$ an integer. Then there exist p, q integers, with $1 \le q < Q$, such that $|p - q\alpha| < \frac{1}{Q}$.*

Proof. For $1 \le k \le Q - 1$, let $a_k = \lfloor k\alpha \rfloor$, so that $0 < k\alpha - a_k < 1$.

Partition the interval $[0, 1]$ into Q subintervals of length $\frac{1}{Q}$. One of these intervals contains two elements of the set:

$$\{0, \alpha - a_1, 2\alpha - a_2, \dots, (Q-1)\alpha - a_{Q-1}, 1\}$$

The difference between these two elements is of the form $p - q\alpha$, where p and q are integers and q is less than Q, and this difference is less than $\frac{1}{Q}$. □

Corollary 1.2. *For any irrational α there are infinitely many $\frac{p}{q}$ such that $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.*

Proof. It suffices to show, given any $\frac{p}{q}$ with $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$, that we can find another $\frac{p'}{q'}$ with $|\alpha - \frac{p'}{q'}| < \frac{1}{(q')^2} < |\alpha - \frac{p}{q}|$.

Suppose given such a $\frac{p}{q}$, and choose Q such that $\frac{1}{Q} < |\alpha - \frac{p}{q}|$. Then by the theorem there exist p', q' with $q' < Q$, and $|\alpha - \frac{p'}{q'}| < \frac{1}{Qq'} < \frac{1}{(q')^2}$. The claim follows. □

We can now show:

Theorem 1.3. *For any nonsquare d there is a nontrivial solution to $x^2 - dy^2 = 1$.*

Proof. The corollary gives us infinitely many pairs (p_i, q_i) such that $|p_i - q_i\sqrt{d}| < \frac{1}{q_i}$. Note that then $|p_i + q_i\sqrt{d}| < \frac{1}{q_i} + 2q_i\sqrt{d} < 3q_i\sqrt{d}$. We thus have $|N(p_i - q_i\sqrt{d})| = |(p_i - q_i\sqrt{d})(p_i + q_i\sqrt{d})| < 3\sqrt{d}$.

Thus for some M between $-3\sqrt{d}$ and $3\sqrt{d}$ there are infinitely many pairs (p_i, q_i) such that $N(p_i + q_i\sqrt{d}) = M$.

Since there are finitely many congruence classes mod M, there is some pair (p_0, q_0) such that there are infinitely many pairs (p_i, q_i) with $N(p_i + q_i\sqrt{d}) = M$, $p_i \equiv p_0 \pmod{M}$, and $q_i \equiv q_0 \pmod{M}$.

Now for (p_i, q_i) and (p_j, q_j) any two such pairs, consider the quotient:

$$\frac{p_i - q_i\sqrt{d}}{p_j - q_j\sqrt{d}} = \frac{(p_ip_j - dq_iq_j) + (p_iq_j - p_jq_i)\sqrt{d}}{M}.$$

The congruence conditions show that this quotient lies in $\mathbb{Z}[\sqrt{d}]$, and it has norm 1 by multiplicativity of the norm. □

2. The equation $x^2 - dy^2 = -1$.

Note that we can also apply these techniques to solving $x^2 - dy^2 = -1$. Solutions correspond to elements of norm -1 in $\mathbb{Z}[\sqrt{d}]$; if $x + y\sqrt{d}$ is one solution, the others are given by $\pm(x + y\sqrt{d})\epsilon^n$, where ϵ is the fundamental 1-unit. Note, however, that unlike for 1 units there may be no -1-units at all (consider, for instance, $d = 3$, where the equation has no solutions mod 3 and thus no integer solutions.)

LECTURE 20: DIOPHANTINE APPROXIMATION

1. Liouville's theorem

We've shown that for any irrational real number α, there are infinitely many rational numbers $\frac{p}{q}$ with $|\frac{p}{q} - \alpha| < \frac{1}{q^2}$. What happens if we ask for something stronger? For instance, can we find infinitely many $\frac{p}{q}$ with $|\frac{p}{q} - \alpha| < \frac{1}{q^e}$ for some $e > 2$?

It turns out that there for many irrational α, the answer is *no.* In particular, let's make the following definition:

Definition 1.1. Let d be a positive integer. A complex number α is *algebraic of degree d* if there is a degree d (not necessarily monic) polynomial $P(x)$, with integer coefficients, such that $P(\alpha) = 0$, and no such polynomial of degree less than d.

We then have:

Theorem 1.2 (Liouville's theorem)**.** *Let α be a real number that is algebraic of degree d. Then for any real number $e > d$, there are at most finitely many rational numbers $\frac{p}{q}$ such that $|\frac{p}{q} - \alpha| < \frac{1}{q^e}$.*

Proof. Let $P(x)$ be a polynomial of degree d, with integer coefficients, such that $P(\alpha) = 0$. Choose ϵ such that $P(x)$ has no roots other than α on the closed interval $[\alpha - \epsilon, \alpha + \epsilon]$.

Write $P(x) = (x - \alpha)Q(x)$; $Q(x)$ is a monic polynomial with real coefficients, of degree $d - 1$. Since $|Q(x)|$ is a continuous, real valued function, there is a real number $K > 0$ such that $|Q(x)| \leq K$ on the compact set $[\alpha - \epsilon, \alpha + \epsilon]$.

Now suppose we have $\frac{p}{q}$ with $|\frac{p}{q} - \alpha| < \frac{1}{q^e}$. There are only finitely many q such that $\frac{1}{q^e} \geq \epsilon$, so we may assume $\frac{1}{q^e} < \epsilon$.

Now on the one hand, we have:

$$|P(\frac{p}{q})| = |(\frac{p}{q} - \alpha)||Q(\frac{p}{q}| < \frac{1}{q^e}K.$$

On the other hand, since P has degree d and integer coefficients, the denominator of $P(\frac{p}{q})$ (when written in lowest terms) is a divisor of q^d. But $\frac{p}{q}$ is NOT a root of $P(x)$, so $P(\frac{p}{q})$ is nonzero and hence $|P(\frac{p}{q})| \geq \frac{1}{q^d}$.

Putting the inequalities together, we get:

$$\frac{1}{q^d} \leq |P(\frac{p}{q})| < \frac{1}{q^e}K.$$

Rewriting, we find $q^{e-d} < K$; since $e - d > 0$ there are only finitely many q for which this is possible. □

2. Constructing transcendentals

Recall that a complex number α is *transcendental* if there is no polynomial $P(x)$, with integer coefficients, such that $P(\alpha) = 0$, and *algebraic* otherwise.

The set of polynomials $P(x)$ with integer coefficients is countable; since each such polynomial has finitely many roots the set of algebraic numbers is countable. Since the set of reals is uncountable this means that, in a very strong sense, almost every real number is transcendental.

In spite of this it is very hard to give an example of a single real number that is provably transcendental. (In fact, e and π are examples of transcendental numbers, but this is much harder than what we'll do.)

Liouville's theorem gives one approach to proving that a given number is transcendental: show that it admits too many good rational approximations. If we can show that for any e, there exist infinitely many $\frac{p}{q}$ such that $|\frac{p}{q} - \alpha| < \frac{1}{q^e}$, then Liouville's theorem tells us that α can't be algebraic of any degree, and hence must be transcendental.

As an example, define a real number α by

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

This clearly converges.

We can find rational approximations to α simply by truncating the series; for each k, let α_k be the sum:

$$\alpha_k = \sum_{n=1}^{k} \frac{1}{10^{n!}}.$$

On one hand, α_k is rational with denominator $10^{k!}$. On the other hand, we have:

$$|\alpha - \alpha_k| = \sum_{n=k+1}^{\infty} \frac{1}{10^{n!}} < \frac{2}{10^{(k+1)!}}.$$

Fix a positive integer d. For any $k > d$, we have $\frac{2}{10^{(k+1)!}} < \frac{1}{(10^{k!})^d}$. Thus there are infinitely many k such that $|\alpha - \alpha_k| < \frac{1}{(10^{k!})^d}$. Liouville's theorem thus tells us that α cannot be algebraic of degree d. Since d was arbitrary, α must be transcendental.

3. Roth's theorem

Liouville's theorem tells us that algebraic numbers are difficult to approximate well by rationals. In fact, they are even more difficult to approximate than Liouville's theorem would suggest. For instance, we have:

Theorem 3.1 (Roth's Theorem)**.** *Suppose α is algebraic. Then for any $\epsilon > 0$, there are only finitely many rational numbers $\frac{p}{q}$ such that $|\frac{p}{q} - \alpha| < \frac{1}{q^{2+\epsilon}}$.*

In other words, for algebraic numbers, you cannot do any better than Dirichlet's theorem.

Roth's theorem is considerably harder to prove than Liouville's, and we will not give a proof in this course. Note that the stronger bound gives proofs that additional real numbers are transcendental; for instance, one can prove with Roth's theorem that the number

$$\beta = \sum_{n=1}^{\infty} \frac{1}{10^{3^n}}$$

is transcendental, which is not possible with Liouville's theorem.

LECTURE 21: CONTINUED FRACTIONS

1. Rational Continued Fractions

Given a rational number $\frac{p}{q}$, we can write $\frac{p}{q} = a_0 + r_0$, where a_0 is an integer and $0 \leq r_0 < 1$ is between 0 and 1. If r_0 is not zero, then we can write $\frac{1}{r_0} = a_1 + r_1$, with a_1 and integer and $0 \leq r_1 < 1$. We then have:

$$\frac{p}{q} = a_0 + r_0 = a_0 + \frac{1}{a_1 + r_1}.$$

Continuing in this way, as long as r_i is nonzero we set $\frac{1}{r_i} = a_{i+1} + r_{i+1}$, with a_i an integer and $0 \leq r_{i+1} < 1$. The denominators of the r_i are strictly decreasing, so eventually some $r_n = 0$ and we have:

$$\frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}}.$$

This expression is called the *continued fraction expansion* of $\frac{p}{q}$. It is closely related to Euclid's algorithm; indeed, it's not hard to see that the a_i are the quotients q_i from Euclid's algorithm applied to the pair p, q. Note that each a_i is an integer and for $i \geq 1$, $a_i \geq 1$.

2. Infinite Continued Fractions

Now let α be an irrational real number. As above, we can write $\alpha = a_0 + r_0$, where a_0 is an integer and $0 \leq r_0 < 1$, and then for each i set $\frac{1}{r_i} = a_{i+1} + r_{i+1}$ with a_{i+1} an integer and $0 \leq r_{i+1} < 1$. Note that unlike in the rational case, this sequence will never terminate, as r_i is always irrational and thus never zero. We write:

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

and call this the *continued fraction expansion* of α. Note that so far this is just a formal expression! In fact, we can make mathematical sense of this expression, but it requires some justification.

First, we introduce some useful notation: For $a_0, \dots a_n$ real numbers, we define $[a_0; a_1, \dots, a_n]$ to be the real number:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}}$$

when this expression is well-defined (that is, when it does not involve a division by zero.)

The value of this expression can computed by a recurrence relation, as follows:

Lemma 2.1. *Given $a_0, \dots, a_n$ real numbers, define p_i, q_i for $0 \leq i \leq n$ by $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1 + 1$, $q_1 = a_1$, together with the recurrences:*

$$p_i = a_i p_{i-1} + p_{i-2}$$

$$q_i = a_i q_{i-1} + q_{i-2}.$$

Then $[a_0; a_1, \dots, a_n] = \frac{p_n}{q_n}$, assuming no q_i is zero.

Proof. We prove this by induction on n; the cases $n = 0$ and $n = 1$ are clear. Let p'_i and q'_i be the numbers defined by the recurrence attached to the sequence $a_0, a_1, \dots, a_{n-2}, a_{n-1} + \frac{1}{a_n}$. The induction hypothesis tells us that $[a_0; a_1, \dots, a_{n-2}, a_{n-1} + \frac{1}{a_n}] = \frac{p'_{n-1}}{q'_{n-1}}$. By the recurrence defining the p' and q', we have

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

Since the sequences defining p'_i,q'_i and p_i,q_i agree for $i \leq n-2$, the latter is equal to:

$$\frac{(a_{n-1} + \frac{1}{a_n})p_{n-2} + p_{n-3}}{(a_{n-1} + \frac{1}{a_n})q_{n-2} + q_{n-3}}.$$

Multiplying both numerator and denominator by a_n, and using $p_{n-1} = a_{n-1}p_{n-2} + p_{n-3}$, $p_n = a_n p_{n-1} + p_{n-2}$ (and similarly for q_n) we find that this expression is equal to $\frac{p_n}{q_n}$.

Thus we have:

$$[a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_{n-2}, a_{n-1} + \frac{1}{a_n}] = \frac{p_n}{q_n}$$

as claimed. □

Note that if $a_i \geq 1$ for all i (as will be the case, for instance, if the a_i come from taking a continued fraction expansion of some real number), then the q_i are all nonzero and form a strictly increasing sequence. (Indeed, if all a_i are at least one, then $q_i \geq q_{i-1} + q_{i-2} \geq 2q_{i-2}$, so this sequence increases exponentially fast.)

Now suppose we have an infinite sequence $a_0, a_1, a_2, \dots,$ of real numbers, and assume that $a_i \geq 1$ for $i \geq 1$. Define p_i and q_i by the recurrence given above. We call $\frac{p_i}{q_i}$ the *ith convergent* to the continued fraction:

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

Lemma 2.2. *We have $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$.*

Proof. This is again by induction on n; the base case $n = 1$ is clear. Assume this is true for $n - 1$. Then by the defining recurrence for the p_i and q_i, we have:

$$p_nq_{n-1}-q_np_{n-1} = (a_np_{n-1}+p_{n-2})q_{n-1}-(a_nq_{n-1}+q_{n-2})p_{n-1} = p_{n-2}q_{n-1}-q_{n-2}p_{n-1} = -(-1)^{n-2}$$

and the claim follows. □

It follows that $|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| < \frac{1}{q_nq_{n-1}}$. Since the q_n increase exponentially, it follows that the $\frac{p_i}{q_i}$ form a Cauchy sequence, and hence converge to a real number.

A natural question to ask at this point is: "if the sequence $a_0, a_1, \ldots$ arises from the continued fraction expansion of an irrational number α, is the limit of the convergents $\frac{p_n}{q_n}$ equal to α?". This is indeed the case:

Lemma 2.3. *Let α be an irrational real number, and let $a_0, a_1, \ldots$ be the sequence of integers arising from its continued fraction expansion. Let $\frac{p_n}{q_n}$ be the nth convergent. Then $\frac{p_n}{q_n} < \alpha$ if n is even, and $\frac{p_n}{q_n} > \alpha$ if n is odd.*

Proof. Once again we use induction on n; the case $n = 0$ is clear. Note that $[a_1; a_2, \ldots, a_n]$ is the $(n-1)$st convergent to $\frac{1}{\alpha - a_0}$. Thus, by the induction hypothesis, if n is odd we have:

$$[a_1; a_2, \ldots, a_n] < \frac{1}{\alpha - a_0}$$

and thus

$$\alpha < a_0 + \frac{1}{[a_1; a_2 \ldots, a_n]} = [a_0; a_1, a_2, \ldots, a_n].$$

If n is even the same argument works with the inequalities reversed. □

Corollary 2.4. *Let α be an irrational real number, and let $a_0, a_1, \ldots$ be the sequence of integers arising from its continued fraction expansion. Let $\frac{p_n}{q_n}$ be the nth convergent. Then $|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_nq_{n+1}}$. In particular the limit $\frac{p_n}{q_n}$ as n approaches infinity is α.*

Proof. Since exactly one of $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ is less than α, we have

$$|\alpha - \frac{p_n}{q_n}| < |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = \frac{1}{q_nq_{n+1}}.$$

Since the q_n increase exponentially quickly the second claim is clear. □

Note that since $\frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}$, this gives a second, *completely constructive* proof of Dirichlet's theorem on rational approximations!

LECTURE 22: BEST APPROXIMATIONS

1. Best Approximations

Last lecture we saw that the convergents $\frac{p_n}{q_n}$ of the continued fraction expansion of α provide good rational approximations to α (and in particular converge to α). In fact, there is a sense in which the convergents to the continued fraction expansion of α are the best possible rational approximations to α. We will make this precise below.

Fix α real and irrational, and as above define a_i and r_i by setting $\alpha = a_0 + r_0$, with a_0 an integer and $0 \leq r_0 < 1$, and $\frac{1}{r_i} = a_{i+1} + r_{i+1}$ with a_{i+1} an integer and $0 \leq r_{i+1} < 1$. Define p_n and q_n from the sequence $a_0, a_1, \ldots$ by the recurrences of the previous section.

Lemma 1.1. *For all n, we have:*

$$\alpha = \frac{p_n + p_{n-1}r_n}{q_n + q_{n-1}r_n}.$$

Proof. For $n = 1$ this is easy. Assume it is true for $n - 1$; that is, that we have:

$$\alpha = \frac{p_{n-1} + p_{n-2}r_{n-1}}{q_{n-1} + q_{n-2}r_{n-1}}.$$

We have $\frac{1}{r_{n-1}} = a_n + r_n$; substituting $\frac{1}{a_n+r_n}$ for r_{n-1} in the above and using the relations $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$ yields the claimed result. □

Corollary 1.2. *For all n, $|\alpha - \frac{p_n}{q_n}| < |\alpha - \frac{p_{n-1}}{q_{n-1}}|$.*

Proof. We have:

$$|\frac{\alpha - \frac{p_n}{q_n}}{\alpha - \frac{p_{n-1}}{q_{n-1}}}| = \frac{q_{n-1}}{q_n}|\frac{q_n\alpha - p_n}{q_{n-1}\alpha - p_{n-1}}|.$$

Substituting $\alpha = \frac{p_n+p_{n-1}r_n}{q_n+q_{n-1}r_n}$, we find that the right hand side is equal to:

$$\frac{q_{n-1}}{q_n}|\frac{q_n\frac{p_n+p_{n-1}r_n}{q_n+q_{n-1}r_n} - p_n}{q_{n-1}\frac{p_n+p_{n-1}r_n}{q_n+q_{n-1}r_n} - p_{n-1}}|.$$

Simplifying, we find that this is equal to:

$$\frac{q_{n-1}}{q_n}|\frac{q_n p_{n-1}r_n - p_n q_{n-1}r_n}{q_{n-1}p_n - p_{n-1}q_n}| = \frac{q_{n-1}}{q_n}r_n < 1.$$

The claim follows. □

Theorem 1.3. *Let h, k be integers with $|k| \leq q_n$. Then $|\frac{h}{k} - \alpha| \geq |\frac{p_n}{q_n} - \alpha|$. In other words, $\frac{p_n}{q_n}$ is the best rational approximation to α with denominator at most q_n.*

Proof. Suppose that $|\frac{h}{k} - \alpha| < |\frac{p_n}{q_n} - \alpha|$. Then by the corollary we also have $|\frac{h}{k} - \alpha| < |\frac{p_{n-1}}{q_{n-1}} - \alpha|$. Suppose that n is even. Then we have:

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n-1}}{q_{n-1}},$$

and our inequalities then imply that we also have

$$\frac{p_n}{q_n} < \frac{h}{k} < \frac{p_{n-1}}{q_{n-1}}.$$

If n is odd the same holds with the inequalities reversed, by a similar argument. Either way we have

$$|\frac{h}{k} - \frac{p_{n-1}}{q_{n-1}}| < |\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{1}{q_n q_{n-1}}.$$

On the other hand, the left hand side of this is a positive rational number with denominator kq_{n-1}, so must be at least $\frac{1}{kq_{n-1}}$. This is a contradiction since $k \leq q_n$. □

LECTURE 23: PERIODIC CONTINUED FRACTIONS

1. Periodic Continued Fractions

In this lecture we single out certain irrationals with particularly nice continued fraction expansions:

Definition 1.1. The continued fraction expansion $[a_0; a_1, a_2, \dots]$ of an irrational number α is *eventually periodic* if there exist positive integers N and d such that $a_n = a_{n+d}$ for all $n \geq N$. It is *periodic* if there exists a positive integer d such that $a_n = a_{n+d}$ for all n.

Definition 1.2. An irrational number α is a *quadratic irrational* if there is a polynomial $ax^2 + bx + c$, with a, b, c integers, that has α as a root.

We then have:

Proposition 1.3. *Suppose that α has an eventually periodic continued fraction expansion. Then α is a quadratic irrational.*

Proof. We first show this when α is periodic. We then have a d such that

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{d-1} + \frac{1}{\alpha}}}}.$$

Simplifying the right hand side, we find integers x, y, z, w such that

$$\alpha = \frac{x\alpha + y}{z\alpha + w}.$$

Then $z\alpha^2 + (w - x)\alpha - y = 0$; since α is irrational z cannot be zero, so α is a quadratic irrational.

If α is only eventually periodic there is a β with periodic continued fraction expansion such that we have:

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{N-1} + \frac{1}{\beta}}}}.$$

Then β is quadratic irrational. It thus suffices to show that if β is quadratic irrational, so is $\frac{1}{\beta}$ and $n + \beta$ for integer n.

Note that if β is a root of $ax^2 + bx + c$, then $\frac{1}{\beta}$ is a root of $a + bx + cx^2$, and $n + \beta$ is a root of $a(x - n)^2 + b(x - n) + c$, so these claims are clear. □

In fact, all quadratic irrationals have eventually periodic continued fraction expansions, so that the converse to the above proposition also holds.

To see this, fix a real, quadratic irrational α. Then there exist a, b, c integers such that $a\alpha^2 + b\alpha + c = 0$. Let $\alpha = [a_0; a_1, a_2, \dots]$ be the continued fraction expansion of α, and set $s_n = [a_{n+1}; a_{n+2}, \dots]$; note that $s_n = \frac{1}{r_n}$, where r_n is the nth remainder. To show that the continued fraction expansion is eventually periodic it suffices to show we get the same remainder twice (that is, $s_i = s_j$ for some $i \neq j$, since the continued fraction expansion of α past s_n depends only on s_n. Moreover, to show that some s_i occurs twice it suffices to show that the set of distinct remainders $\{s_n : n \geq 1\}$ is finite (as then at least one of them must occur infinitely many times!)

We will do this by constructing a finite set of quadratic polynomials such that each s_n is the root of one such polynomial. Since each such polynomial has at most two roots, this will mean that there are finitely many possible s_n, and thus prove the periodicity.

Recall that we have shown that for any n, $\alpha = \frac{p_n + p_{n-1} r_n}{q_n + q_{n-1} r_n}$, where $\frac{p_n}{q_n}$ is the nth convergent. Rewriting in terms of $s_n = \frac{1}{r_n}$ we have: $\alpha = \frac{p_n s_n + p_{n-1}}{q_n s_n + q_{n-1}}$. If we substitute this into $a\alpha^2 + b\alpha + c = 0$ we get the following expression (after clearing denominators):

$$a(p_n s_n + p_{n-1})^2 + b(p_n s_n + p_{n-1})(q_n s_n + q_{n-1}) + c(q_n s_n + q_{n-1})^2 = 0$$

and rewriting this as a quadratic in s_n we find that $A_n s_n^2 + B_n s_n + C_n = 0$, where:

$$\begin{aligned} A_n &= ap_n^2 + bp_n q_n + cq_n^2 \\ B_n &= 2ap_n p_{n-1} + b(p_n q_{n-1} + p_{n-1} q_n) + 2cq_n q_{n-1} \\ C_n &= ap_{n-1}^2 + bp_{n-1} q_{n-1} + cq_{n-1}^2 \end{aligned}$$

Note in particular that $C_n = A_{n-1}$. Moreover, computing the discriminant $B_n^2 - 4A_n C_n$ we find (after some algebra) that

$$B_n^2 - 4A_n C_n = (b^2 - 4ac)(p_n q_{n-1} - q_n p_{n-1})^2 = b^2 - 4ac$$

since we had shown previously that $p_n q_{n-1} - q_n p_{n-1} = \pm 1$.

The idea is now to bound the A_n from above; that is, to show that for some M, $|A_n| \leq M$ independently of n. If we can do this for $|A_n|$, then it is also true that $|C_n| \leq M$ for all M. There would therefore be only finitely many possiblitlies for the pair (A_n, C_n) as n varies. But once A_n, C_n are fixed, there are at most two possibilities for B_n, since we know that $B_n^2 - 4A_n C_n = b^2 - 4ac$, with a, b, c fixed. Thus if we can bound $|A_n|$, there are only finitely many quadratic polynomials satisfied by the s_n, and thus (as explained above) only finitely many possible s_n, so the continued fraction must be periodic!

It thus remains to show that $|A_n|$ is bounded above. To do this recall that we have shown that $|\frac{p_n}{q_n} - \alpha| < \frac{1}{q_n q_{n+1}}$. Rewriting this we find:

$$|p_n - q_n \alpha| < \frac{1}{q_{n+1}} < \frac{1}{q_n}.$$

As a result we can write $p_n = \alpha q_n + \frac{\delta}{q_n}$ with $|\delta| < 1$. Substituing into $A_n = ap_n^2 + bp_nq_n + cq_n^2$ we find:

$$A_n = a\alpha^2 q_n^2 + 2a\alpha\delta + \frac{\delta^2}{q_n^2} + b\alpha q_n^2 + b\delta + cq_n^2$$

which we can rewrite as

$$q_n^2(a\alpha^2 + b\alpha + c) + 2a\alpha\delta + \frac{\delta^2}{q_n^2} + b\delta.$$

Note that the first term here is zero, as α is a root of $aX^2 + bX + c$, the second and fourth terms are bounded independently of n, and the third term is less than 1 in absolute value. Thus the whole expression is bounded independently of n and the result follows.

LECTURE 24: CONTINUED FRACTIONS AND PELL'S EQUATION

We saw when we were first proving the existence of nontrivial solutions to Pell's equation $X^2 - dY^2 = 1$ (d not a square) that if (X, Y) was a solution with Y nonzero then $\frac{X}{Y}$ was close to the irrational $\sqrt{d}$. This led us to construct solutions by considering rational approximations to $\sqrt{d}$.

Now that we know that continued fraction expansions give good rational approximations, it's natural to ask if there is a relationship between the convergents $\frac{p_n}{q_n}$ to the continued fraction expansion of $\sqrt{d}$ and solutions to $X^2 - dY^2 = 1$.

In fact, we have:

Theorem 0.1. *Let (X, Y) be a solution to $X^2 - dY^2 = 1$, with $X, Y > 0$. Then there exists an integer n such that $(X, Y) = (p_n, q_n)$, where $\frac{p_n}{q_n}$ is the nth convergent to the continued fraction expansion of $\sqrt{d}$.*

Note that (as you can easily check in examples) the converse is false: not every convergent $\frac{p_n}{q_n}$ gives rise to a solution to Pell's equation. Nonetheless, this gives a much more efficient way to find solutions to Pell's equation than the "try increasing values of Y until one works" approach we were using previously! In particular, (since the q_n are an increasing sequence) the first $\frac{p_n}{q_n}$ in the continued fraction expansion of $\sqrt{d}$ such that $p_n^2 - dq_n^2 = 1$ gives the fundamental solution to $X^2 - dY^2 = 1$.

1. Best Approximations Revisited

The key to proving this is to first establish a strengthening of our results on good rational approximations. We already know that the best possible rational approximations are convergents; the following theorem gives us a very strong criterion for detecting these convergents:

Theorem 1.1. *Let α be a real quadratic irrational and let $\frac{p_n}{q_n}$ be the convergents to its continued fraction expansion. Let p, q be integers with q positive and $q < q_{n+1}$. Suppose that $|p - q\alpha| \leq |p_n - q_n\alpha$. Then $\frac{p}{q} = \frac{p_n}{q_n}$.*

Proof. Let $x = pq_n - qp_n$, and $y = pq_{n+1} - qp_{n+1}$. Then we have:

$$p_{n+1}x - p_n y = pp_{n+1}q_n - pp_n q_{n+1} = (-1)^n p$$

$$q_{n+1}x - q_n y = -qp_n q_{n+1} + qp_{n+1}q_n = (-1)^n q$$

(using $p_{n+1}q_n - p_n q_{n+1} = (-1)^n$.) Note that since q_n, q_{n+1} are positive and $q < q_{n+1}$, this is only possible if x and y have the same sign (consider the absolute values).

Using these expressions we can write:

$$q\alpha - p = (-1)^n[q_{n+1}x - q_ny]\alpha - (-1)^n[p_nx - p_ny]$$

$$= (-1)^n[(q_{n+1}\alpha - p_{n+1})x - (q_n\alpha - p_n)y]$$

Recall that we have shown that as n increases, the sign of $\alpha - \frac{p_n}{q_n}$ alternates. Thus $q_{n+1}\alpha - p_{n+1}$ has sign opposite to $q_n\alpha - p_n$. Since x and y have the same sign, we can take absolute values in the above equality and obtain:

$$|q\alpha - p| = |x||q_{n+1}\alpha - p_{n+1}| + |y||q_n\alpha - p_n|.$$

Since we have assumed that $|q\alpha - p| \leq |q_n\alpha - p_n|$, and x, y are integers, we must have either $y = 0$ or $|y| = 1$, $x = 0$. But if $y = 0$ we have $\frac{p}{q} = \frac{p_{n+1}}{q_{n+1}}$ which is impossible since $\frac{p_{n+1}}{q_{n+1}}$ is in lowest terms and $q < q_{n+1}$. So we must have $|y| = 1$, $x = 0$, but this implies that $\frac{p}{q} = \frac{p_n}{q_n}$. □

As a corollary, we can deduce that "sufficiently good rational approximations are convergents:

Corollary 1.2. *Let α be a real quadratic irrational and p, q positive integers such that $|\frac{p}{q} - \alpha| < \frac{1}{2q^2}$. Then $\frac{p}{q} = \frac{p_n}{q_n}$ for some n.*

Proof. Since the q_n are increasing, we can find a unique n such that $q_n \leq q < q_{n+1}$.

Suppose $|p - q\alpha| \leq |p_n - q_n\alpha|$. Then the previous theorem shows immediately that $\frac{p}{q} = \frac{p_n}{q_n}$. So we may assume that $|p - q\alpha| > |p_n - q_n\alpha|$.

Then if $\frac{p}{q} \neq \frac{p_n}{q_n}$, we have:

$$\frac{1}{qq_n} \leq |\frac{p}{q} - \frac{p_n}{q_n}| \leq |\frac{p}{q} - \alpha| + |\frac{p_n}{q_n} - \alpha|.$$

By assumption, $|\frac{p}{q} - \alpha| < \frac{1}{2q^2}$. Moreover, we know that $|\frac{p_n}{q_n} - \alpha| = \frac{1}{q_n}|p_n - q_n\alpha|$ and $|p_n - q_n\alpha| < |p - q\alpha| < \frac{1}{2q}$. Thus $|\frac{p_n}{q_n} - \alpha| < \frac{1}{2qq_n}$. In particular we have

$$\frac{1}{qq_n} \leq |\frac{p}{q} - \alpha| + |\frac{p_n}{q_n} - \alpha| < \frac{1}{2q^2} + \frac{1}{2qq_n} = \frac{q + q_n}{2q^2q_n}.$$

We thus deduce that:

$$\frac{q + q_n}{2q^2q_n} \geq \frac{1}{qq_n}.$$

Clearing denominators we find that $q + q_n > 2q$ which implies that $q_n \geq q$. Since we chose n such that $q_n \leq q$ we must have $q_n = q$; then p must equal p_n and we are done. □

2. Pell's Equation

We now return to Pell's equation. Fix a nonsquare positive integer d. We then have:

Theorem 2.1. *If p, q satisfy $p^2 - dq^2 = 1$, then $\frac{p}{q}$ is a convergent to $\sqrt{d}$.*

Proof. It suffices to show that $|\sqrt{d} - \frac{p}{q}| < \frac{1}{2q^2}$, by the corollary. We have:

$$|\sqrt{d} - \frac{p}{q}| = |\frac{q\sqrt{d} - p}{q}| = |\frac{q^2 d - p^2}{q(q\sqrt{d} + p)}|$$

Since $p^2 - dq^2 = -1$, the right hand expression can be rewritten as $|\frac{1}{q^2(\sqrt{d} + \frac{p}{q})}$. But $\sqrt{d} > 1$, and $\frac{p}{q} > q$ since $p = \sqrt{1 + dq^2} > q$, so the result follows. □

LECTURE 25: PRIMES IN ARITHMETIC PROGRESSIONS I

1. Primes in arithmetic progressions

A natural question to ask is how the primes are distributed mod n. It's easy to see that for any a with $(a, n) > 1$, there is at most one prime congruent to a mod n, so we can refine this question by asking:

Question 1.1. Given a positive integer n, and an integer a with $(a, n) = 1$, are there infinitely many primes congruent to a mod n?

The answer to this question is *yes*; this was first proven by Dirichlet. The methods involved belong to analytic number theory; see for instance Serre's *A course in arithmetic* for a proof of this statement.

We will instead concern ourselves with special cases of this problem that can be approached by elementary methods.

2. Elementary Results

We first recall the proof that there are infinitely many primes; the structure of this proof will form a template for our arguments.

Theorem 2.1. *There are infinitely many primes.*

Proof. It suffices to construct, for any finite set S of primes, a prime not in S. Given such a set S, let $Q = 1 + \prod_{p \in S} p$. Then Q is divisible by at least one prime, but not by any prime in S. □

It's easy to adapt this proof to show that there are infinitely many primes congruent to 3 mod 4:

Theorem 2.2. *There are infinitely many primes congruent to* 3 *mod* 4.

Proof. Let S be a set of primes congruent to 3 mod 4, and let $Q = 2 + \prod_{p \in S} p^2$. Then Q is congruent to 3 mod 4, so Q is divisible by at least one prime congruent to 3 mod 4. On the other hand, Q is not divisible by any primes in S. □

A very similar argument works to show there are infinitely many primes congruent to 5 mod 6. Handling cases beyond that requires new ideas. For instance:

Lemma 2.3. *Let x be an even integer and let p be a prime dividing $x^2 + 1$. Then p is congruent to* 1 *mod* 4.

Proof. On the one hand p is clearly odd. On the other hand, $x^2 \equiv -1 \pmod{p}$, so -1 is a quadratic residue mod p. Hence p is 1 mod 4. □

Theorem 2.4. *There are infinitely many primes congruent to* 1 *mod* 4.

Proof. Let S be a finite set of primes congruent to 1 mod 4, and set $Q = 1 + \prod_{p \in S} p^2$. By the lemma, every prime dividing Q is congruent to 1 mod 4, but no prime in S divides Q. □

This suggests a strategy for proving there are infinitely many primes congruent to a mod n for some pair a, n: if we can find a polynomial P such that for any integer x, every prime dividing $P(nx)$ is congruent to a mod n, then we can try to mimic the proof that there are infinitely many primes congruent to 1 mod 4 to show that there are infinitely many primes congruent to a mod n. When $a = 1$ it turns out this is possible. Indeed, in the following lecture we will show:

Theorem 2.5. *For any positive integer n, there are infinitely many primes congruent to* 1 *mod n.*

LECTURE 26: PRIMES IN ARITHMETIC PROGRESSIONS II

We claimed at the end of the last lecture that we could prove:

Theorem 0.1. *For any positive integer n, there are infinitely many primes congruent to* 1 *mod n.*

1. Cyclotomic polynomials

The key to studying the primes congruent to 1 mod n is a family of polynomials known as the *cyclotomic polynomials* Φ_n.

Definition 1.1. The nth cyclotomic polynomial Φ_n is the product:

$$\Phi_n = \prod_{1 \le a < n; (a,n)=1} (x - e^{\frac{2\pi a i}{n}}).$$

In other words, Φ_n is the monic polynomial whose roots are the primitive nth roots of unity, all with multiplicity one.

A priori, Φ_n is a polynomial with complex coefficients. However, we observe:

Lemma 1.2. *For any n, we have:*

$$x^n - 1 = \prod_{d|n, d>0} \Phi_d.$$

Proof. The roots of $x^n - 1$ are the n roots of unity, each with multiplicity one. In other words, they are the primitive dth roots of unity for d dividing n, each with multiplicity one. These are the same as the roots of the product of the Φ_d. □

From this it is easy to deduce:

Lemma 1.3. *For any n, the polynomial Φ_n has integer coefficients.*

Proof. We prove this by strong induction on n; the case $n = 1$ is clear. Suppost that Φ_d has integer coefficients for all $d < n$. We have $x^n - 1 = \Phi_n P(x)$, where $P(x)$ is the product of Φ_d for d dividing n and strictly less than n. In particular P is monic with integer coefficients by the induction hypothesis. Let e be the degree of p.

Write $\Phi_n(x) = \sum a_n x^n$ and $P(x) = \sum b_n x_n$. Suppose Φ_n does not have integer coefficients, and let q be the largest integer such that a_q is not an integer. Since $P(x)$ is monic, the coefficient of x^{q+e} in $P(x)\Phi_n$ is $a_q + a_{q+1}b_{e-1} + \cdots + a_{q+e}b_0$; every term except a_q is an integer, so this coefficient is *not* an integer. SInce $P(x)\Phi_n(x) = x^n - 1$ this is impossible. □

In light of this, we can consider Φ_n as a polynomial mod p for various p. In fact, we will show that if p does not divide n, then Φ_n has no repeated roots mod p. In order to do this, we need the notion of the *derivative* of a polynomial with coefficients in an arbitrary field.

Definition 1.4. Let F be a field, and $P = \sum a_n x^n$ a polynomial with coefficients in F. The derivative P' of P is the polynomial $\sum_{n=1}^{d} n a_n x^{n-1}$.

Note that $(P+Q)' = P' + Q'$ and $(PQ)' = P'Q + Q'P$, as one easily checks.

Lemma 1.5. *Suppose P has a double root α in F. Then $(x-\alpha)$ divides both P and P'.*

Proof. Write $P = (x-\alpha)^2 Q$. Then $P' = (x-\alpha)^2 Q' + 2(x-\alpha)Q$. □

Corollary 1.6. *If p does not divide n, then $\Phi_n(x)$ has no repeated roots mod p.*

Proof. Since $\Phi_n(x)$ divides $x^n - 1$, it suffices to show that $x^n - 1$ has no repeated roots mod p. But the derivative of $x^n - 1$ is a nonzero multiple of x^{n-1} (since p does not divide n) and thus has no common factors with $x^n - 1$. □

Theorem 1.7. *Let p be a prime not dividing n, and let a be an integer. Then p divides $\Phi_n(a)$ if, and only if, a has exact order n mod p.*

Proof. Suppose that a has exact order n mod p. Then a is a root of $x^n - 1$ mod p, but is not a root of $x^d - 1$ mod p for any d dividing n. Since $\Phi_d(x)$ divides $x^d - 1$, it follows that a can't be a root of $\Phi_d(x)$ for any d dividing n other than $\Phi_n(x)$. SInce $a^n - 1 = \prod_{d|n} \Phi_d(a)$, we must have $\Phi_n(a) \equiv 0 \pmod{p}$.

Conversely, suppose that $\Phi_n(a) \equiv 0 \pmod{p}$. Then $a^n - 1$ is zero mod p, so the order of a mod p divides n. Let d be this order, and suppose $d < n$. We have $a^d - 1 \equiv 0 \pmod{p}$ which means that $\Phi_e(a)$ is zero for some e dividing d. On the other hand then a is a root of $\Phi_n(x)$ and $\Phi_e(x)$, which are distinct factors of $x^n - 1$. Thus a is a double root of $x^n - 1$ which is impossible by the lemma. Therefore $d = n$ and we are done. □

Corollary 1.8. *Let p be a prime not dividing n, and a an integer. If p divides $\Phi_n(a)$, then $p \equiv 1 \pmod{n}$.*

Proof. The order of a mod p is n by the theorem above. Thus n divides $p-1$ by Fermat's little theorem. □

2. Primes congruent to 1 mod n

We are now in a position to prove:

Theorem 2.1. *Let n be a positive integer. There are infinitely many primes congruent to* 1 *mod n.*

Proof. Let S be a finite set of primes congruent to 1 mod n. Let R be the product of the primes in S, and for each k, let Q_k be the integer $\Phi_n(knR)$. Note that not all Q_k are ± 1, since Φ_n is a nonconstant polynomial. Thus, for some k, there is a prime p dividing Q_k. Since Q_k divides $(knR)^n - 1$, no prime dividing n or R can divide Q_k. Thus p is not in S, and by the corollary p is congruent to 1 mod n. □

LECTURE 27: HIGHER RECIPROCITY LAWS

Given quadratic reciprocity's status as one of the most profound results of 18th century number theory, it's natural to ask what generalizations exist. In particular it's natural to want to study kth powers mod p for integers $k > 2$, and ask if similar reciprocity laws exist for such powers. It turns out that these "higher reciprocity laws" do indeed exist, but there are some new surprises that don't arise in the quadratic situation.

1. Cubic residues

We'll illustrate these ideas with the case $k = 3$.

Definition 1.1. Let p be a prime, and let a be an integer not divisible by p. We say a is a *cubic residue* if there exists an integer n with $n^3 \equiv a \pmod{p}$.

Almost immediately we see that the behavior of these is different than that of the quadratic residues. In particular we have:

Proposition 1.2. *Let p be a prime, and suppose that p is not 1 mod 3. Then every integer not divisible by p is a cubic residue.*

Proof. This is a consequence of the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. At a more fundamental level, we can prove it as follows: consider the map:

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

that takes n to n^3. Its kernel consists of elements of order dividing 3. But since the order of any element in $(\mathbb{Z}/p\mathbb{Z})^\times$ divides $p-1$, if p is not 1 mod 3 then there are no elements of order 3, so the map is injective, and therefore also surjective. □

By constrast, if p is one mod 3, we have:

Proposition 1.3. *Let p be a prime congruent to 1 mod 3. Then there are $\frac{p-1}{3}$ cubic residues mod p. Moreover, these cubic residues are precisely those a for which $a^{\frac{p-1}{3}} \equiv 1 \pmod{p}$.*

Proof. We again consider the homomorphism:

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

that takes n to n^3. Its kernel consists of the roots of the polynomial $n^3 - 1 = (n-1)(n^2+n+1)$. Note that 1 is not a root of n^2+n+1 mod p, and that the discriminant of this quadratic polynomial is -3. When p is 1 mod 3, it follows from quadratic reciprocity that -3 is a square mod p, so that n^2+n+1 has two distinct roots mod 3. Thus the kernel of the map that takes n to n^3 has order 3, so its image (which is the set of cubic residues) has order $\frac{p-1}{3}$.

Now note that if a is a cubic residue (say $a \equiv n^3 \bmod p$) then $a^{\frac{p-1}{3}} \equiv n^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. Conversely, if $a^{\frac{p-1}{3}}$ is 1 mod p, then a is a root of the polynomial $X^{\frac{p-1}{3}} - 1 \bmod p$. We have shown that every cubic residue is a root of this polynomial, and there are $\frac{p-1}{3}$ of those, so every root of this polynomial is a cubic residue (and in particular a is.) □

It is tempting at this point to define a cubic residue symbol, by defining $\left(\frac{a}{p}\right)_3$ to be the class of $a^{\frac{p-1}{3}}$ mod p. This has some nice properties in common with the Legendre symbol; in particular it is clear that

$$\left(\frac{ab}{p}\right)_3 = \left(\frac{a}{p}\right)_3 \left(\frac{b}{p}\right)_3$$

, and that $\left(\frac{a}{p}\right)_3 = 1$ if, and only if, a is a cubic residue mod p.

On the other hand, unlike the Legendre symbol, which takes values in ±1 (and which we can therefore regard as an *integer-valued* symbol), this cubic residue symbol takes values in the three solutions to $n^3 = 1 \bmod p$. Since there is no way to think of these as integers, we have no good way of comparing (for instance) $\left(\frac{p}{q}\right)_3$ and $\left(\frac{q}{p}\right)_3$, and this no way of formulating an analogue of quadratic reciprocity.

We are thus faced with two limitations from this point of view: we can only make sense of $\left(\frac{a}{p}\right)_3$ mod p, and only for primes p that are 1 mod 3. It turns out we can overcome both of these limitations at once, by moving our attention from the integers to a larger ring!

2. The Eisenstein integers

Let $\zeta = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ be a cube root of unity; it is the unique solution to $x^2 + x + 1 = 0$ with positive imaginary part. We consider the ring $\mathbb{Z}[\zeta]$; note that $N(a + b\zeta) = a^2 - ab + b^2$. This gives a Euclidean norm on the ring $\mathbb{Z}[\zeta]$, which is also known as the *Eisenstein integers.*

In order to apply this ring to our question about cubic residues, we must study congruences in the ring of Eistenstein integers. If $a, b, x \in \mathbb{Z}[\zeta]$, with $x \neq 0$, we say that $a \equiv b \pmod x$ if x divides $a - b$. Just as for integers, the set of congruence classes of x forms a ring, which we denote $\mathbb{Z}[\zeta]/x\mathbb{Z}[\zeta]$, and there is a surjective "reduction mod x" homomorphism:

$$\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/x\mathbb{Z}[\zeta].$$

One can then show that following:

(1) The ring $\mathbb{Z}[\zeta]/x\mathbb{Z}[\zeta]$ has $N(x)$ elements, for any nonzero $x \in \mathbb{Z}[\zeta]$.
(2) If x is prime in $\mathbb{Z}[\zeta]$, then $\mathbb{Z}[\zeta]/x\mathbb{Z}[\zeta]$ is a field.

(3) If p in $\mathbb{Z}$ is congruent to 2 mod 3, then p remains prime in $\mathbb{Z}[\zeta]$, and $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$ is a field with p^2 elements.

(4) If p in $\mathbb{Z}$ is congruent to 1 mod 3, then p factors as a product qq' of conjugate primes in $\mathbb{Z}[\zeta]$. Moreover, the map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta]$ is an isomorphism of rings. (In other words, every element of $\mathbb{Z}[\zeta]$ is congruent to an integer mod q, and if two integers are congruent mod q then they are congruent modulo p as well.)

We can define cubic residues for $\mathbb{Z}[\zeta]$ exactly as we did for $\mathbb{Z}$: if q is a prime of $\mathbb{Z}[\zeta]$, we say $x \in \mathbb{Z}[\zeta]$ is a cubic residue mod 3 if there exists $y \in \mathbb{Z}[\zeta]$ such that $y^3 \equiv x \pmod{q}$. This turns out to have much more uniform behavior than it does over the integers! The point is that as long as q does not divide 3, we have $N(q) \equiv 1 \pmod{3}$. (You can see this either by considering the integer prime p that q divides, and using (3) and (4) above, or simply by noticing that $N(q)$ is expressible as $a^2 - ab + b^2$ and therefore can never be 2 mod 3.)

Then, exactly as in the integer case, we have:

Proposition 2.1. *Let q be a prime in $\mathbb{Z}[\zeta]$ not dividing 3. Then there are $\frac{N(q)-1}{3}$ cubic residues in $(\mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta])^\times$. Moreover, the cubic residues are precisely those a in $\mathbb{Z}[\zeta]$ such that $a^{\frac{N(q)-1}{3}} \equiv 1 \pmod{q}$.*

The proof is the same as in the integer case, except that we must show that the polynomial $n^3 - 1$ has three distinct roots in $\mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta]$ for any q not dividing 3. This follows from the following lemma:

Lemma 2.2. *Let q be a prime of $\mathbb{Z}[\zeta]$ not dividing 3. Then $1, \zeta, \zeta^2$ are distinct mod q. In particular their classes mod q are the distinct roots of the polynomial $n^3 - 1$.*

Proof. Suppose that $\zeta \equiv 1 \bmod q$. Then q divides $\zeta - 1$. But $N(\zeta - 1) = 3$, so the result follows. The other cases are similar. □

Note that if a is not divisible by q, then $a^{\frac{N(q)-1}{3}}$ is a cube root of 1 mod q, since $(\mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta])^\times$ is a group of order $N(q) - 1$. There is thus a unique element ζ^r of $\{1, \zeta, \zeta^2\} \subset \mathbb{Z}[\zeta]^\times$ such that $a^{\frac{N(q)-1}{3}} \equiv \zeta^r \pmod{q}$. We can thus define $\left(\frac{a}{q}\right)_3$ to be equal to ζ^r. Note that unlike our previous definition, this makes sense as an element of $\mathbb{Z}[\zeta]^\times$, a ring which is independent of q!

This has the following nice properties:

- $\left(\frac{ab}{q}\right)_3 = \left(\frac{a}{q}\right)_3 \left(\frac{b}{q}\right)_3$,
- $\left(\frac{a}{q}\right)_3 = 1$ if, and only if a is a cubic residue mod q
- If p is a prime congruent to 1 mod 3, that factors as qq' in $\mathbb{Z}[\zeta]$, then for any integer a not divisible by p, there exists $n \in \mathbb{Z}$ with $n^3 \equiv a \pmod{p}$ if, and only if $\left(\frac{a}{q}\right)_3 = 1$.

Moreover, it is now possible to ask if there is a relationship between $\left(\frac{p}{q}\right)_3$ and $\left(\frac{q}{p}\right)_3$ for p, q primes of $\mathbb{Z}[\zeta]$ not dividing 3. There is indeed such a relationship, called the law of cubic reciprocity, which we will formulate below.

3. Cubic Reciprocity

Before we state the law of cubic reciprocity, we will reformulate quadratic reciprocity in a way that makes it clearer how to generalize. Traditionally, the law of quadratic reciprocity states that for p, q odd, we have:

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

For any odd prime p, let p^* denote the element of $\{p, -p\}$ that is congruent to 1 mod 4. Then (using that $\left(\frac{-1}{p}\right)$ is 1 if p is 1 mod 4 and -1 if p is 3 mod 4,) we can rephrase quadratic reciprocity as the statement that, when $p > 0$, we have:

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

The point is that every prime element of $\mathbb{Z}$ comes in a pair $\{p, -p\}$ (the associates of p), and the operation p^* lets us pick a "standard" representative of this pair. In $\mathbb{Z}[\zeta]$, by contrast, the units are $\mathbb{Z}[\zeta]^\times = \{\pm 1, \pm\zeta, \pm\zeta^2\}$, so the associates of a given primes q form a *sextuple* $\{\pm q, \pm\zeta q, \pm\zeta^2 q\}$. In order to formulate cubic reciprocity, we will need to pick a "standard" representative of this sextuple. The key is the following observation, whose proof we omit:

Lemma 3.1. *The group $(\mathbb{Z}[\zeta]/3\mathbb{Z}[\zeta])^\times$ is of order six, and consists of the classes of $\{\pm 1, \pm\zeta, \pm\zeta^2\}$ mod 3. Equivalently, reduction mod 3 gives an isomorphism:*

$$\mathbb{Z}[\zeta]^\times \to (\mathbb{Z}[\zeta]/3\mathbb{Z}[\zeta])^\times.$$

In particular, for any prime q not dividing 3, there is a unique associate q^* of q that is congruent to 1 mod 3.

With q^* as in the lemma, we have the law of cubic reciprocity:

Theorem 3.2. *Let $p, q \in \mathbb{Z}[\zeta]$ be primes not dividing 3. Then:*

$$\left(\frac{p^*}{q}\right)_3 = \left(\frac{q^*}{p}\right).$$

Note that this does not perfectly parallel the quadratic case; in particular there's no condition that $p > 0$ (which indeed makes no sense for Eisenstein integers!), and the $*$ operation appears on both sides. In fact all higher reciprocity laws (cubic and beyond) take a similar form to cubic reciprocity; the quadratic case is a bit of an anomaly. The reason for this anomaly comes from the fact that ±1 are real numbers whereas higher power roots of unity are not.

Together with expressions for $\left(\frac{\zeta}{p}\right)_3$ and $\left(\frac{\sqrt{-3}}{p}\right)_3$ this law suffices, in analogous fashion to the quadratic case, to compute all cubic residue symbols.

4. Higher Reciprocity Laws

Cubic reciprocity gives a clue as to how to formulate k-power reciprocity laws for higher k. The point is that in order to get a well-behaved kth power residue symbol, one should work in a ring containing a primitive kth root of unity $e^{\frac{2\pi i}{k}}$. For $k = 4$ the Gaussian integers $\mathbb{Z}[i]$ suffices. For $k \geq 5$, such a ring will not be quadratic. Moreover, for k sufficiently large unique factorization will fall in such rings, adding further complications. At this point tools from algebraic number theory become essential to formulate (and especially to prove!) the appropriate results.

LECTURE 28: DISTRIBUTION OF PRIMES

1. $\pi(n)$ and the Prime Number Theorem

For an integer n, let $\pi(n)$ denote the number of primes between 1 and n. The problem of accurately estimating $\pi(n)$ was one of the central problems in 19th century number theory.

The strongest statement along these lines that can be simply stated is the Prime Number Theorem, which asserts:

Theorem 1.1. *The function $\pi(n)$ is asymptotic to $\frac{n}{\log n}$, in the sense that $\lim_{n\to\infty} \frac{\pi(n)\log n}{n} = 1$.*

(Put another way, it says that for large n roughly $\frac{1}{\log n}$ of the numbers between 1 and n are prime.)

The Prime Number Theorem was not proven till 1896, and its proof is well beyond the scope of this course. However, it's possible to get at least within a constant factor of proving the prime number theorem with much more elementary techniques, as we will see.

2. Chebyshev's bounds

The results we will prove are due to Chebyshev, and date back to the 1850s. In particular, Chebyshev was able to show:

Theorem 2.1. *There exist constants $c_1, c_2 > 0$ such that for all sufficiently large n, we have:*

$$c_1 \frac{n}{\log n} \leq \pi(n) \leq c_2 \frac{n}{\log n}.$$

Note that as a corollary of this we can deduce that for $d > \frac{c_2}{c_1}$, there is a prime between n and dn for n sufficiently large: Chebyshev's result implies that $\pi(dn) \geq c_1 \frac{dn}{\log n + \log d}$ and $\pi(n) \leq c_2 \frac{n}{\log n}$. We thus have:

$$\pi(dn) - \pi(n) \geq c_1 d \frac{n}{\log n + \log d} - c_2 \frac{n}{\log n}.$$

For n sufficiently large, the log d on the left is negligible, so the fact that $c_1 d > c_2$ implies that this goes to $+\infty$ as n goes to infinity; in particular for some n this becomes, and remains, greater than or equal to 1. (In particular, if one assumes the prime number theorem, then we can take $c_1 = c_2 = 1$ here, so that the result becomes the statement that for every $\epsilon > 0$, and every sufficiently large n, there exists a prime between n and $(1+\epsilon)n$.)

In fact, by getting careful control of c_1 and c_2 (as well as making precise what "sufficiently large" means in the theorem), Chebyshev was able to prove *Bertrand's postulate*, the statement that for *every* n, there is a prime between n and $2n$. The bounds we prove will not be strong enough to do this, however.

3. Binomial Coefficients

For certain (fairly weak) values of c_1 and c_2 there is a very clean way of proving Chebyshev's result by estimating the binomial coefficient $\binom{2n}{n}$. The key idea is to compare a basic "elementary" bound on $\binom{2n}{n}$ with one coming from the factorization of the binomial coefficients. The elementary bounds are easy to deduce:

Lemma 3.1. *We have, for all n:*

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} \leq 2^{2n}.$$

Proof. We have:

$$2^{2n} = (1+1)^{2n} = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k}.$$

On the one hand, $\binom{2n}{n}$ is a summand on the right, so it is less than 2^{2n}. On the other hand, $\binom{2n}{n}$ is the largest of $2n$ summands on the right hand side, so it is greater than the average value of the summands, which is $\frac{2^{2n}}{2n}$. □

On the other hand, we can bound $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ by understanding the prime factorization of factorials. For any integer n and prime p, let $\mathrm{ord}_p(n)$ be the largest integer k such that p^k divides n. Then we have:

Lemma 3.2. *Let n be a positive integer. Then*

$$\mathrm{ord}_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \dots$$

(Note that this is actually a finite sum as $\lfloor \frac{n}{p^k} \rfloor = 0$ once $p^k > n$.) The idea behind this lemma is easy: since $n!$ is the product of the integers between 1 and n, the $\lfloor \frac{n}{p} \rfloor$ multiples of p between 1 and n each contribute a factor of p to $n!$. The $\lfloor n \rfloor p^2$ multiples of p^2 contribute an additional factor; the multiples of p^3 contribute at least one more on top of that, and so forth.

Using this, we find that:

$$\mathrm{ord}_p(\binom{2n}{n}) = \sum_{k=1}^{\infty} \lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor.$$

Note that for any real number t, the expression $\lfloor 2t \rfloor - 2\lfloor t \rfloor$ is zero if $t - \lfloor t \rfloor < \frac{1}{2}$ and 1 otherwise. In particular if $p^k > 2n$ the kth term in the sum is zero, and all terms before that are zero or one. Thus if $p^k > 2n$, then $\mathrm{ord}_p(\binom{2n}{n}) < k$. We can rephrase this as saying that if p^k divides $\binom{2n}{n}$ for some prime p, then $p^k < 2n$. (In particular every prime dividing $\binom{2n}{n}$ is less than n.)

We thus have:

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\mathrm{ord}_p(\binom{2n}{n})} \leq \prod_{p \leq 2n} 2n = (2n)^{\pi(2n)}.$$

Combining this with our elementary lower bound on $\binom{2n}{n}$ we find that:

$$(2n)^{\pi(2n)} \geq \frac{2^{2n}}{2n}.$$

Taking logs yields $\pi(2n)\log 2n \geq 2n \log 2 - log 2n$, so that we have:

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

Thus for any $c_1 < \log 2$, and any n sufficiently large, we have $\pi(n) \geq c_1 \frac{n}{\log n}$. (To go from $2n$ to n here we use that $\pi(n)$ and $\frac{n}{\log n}$ are increasing functions.)

The upper bound on $\pi(n)$ takes a bit more work. Returning to the factorization of $\binom{2n}{n}$, we find that if $n < p \leq 2n$, then $\mathrm{ord}_p(\binom{2n}{n}) = 1$. Thus the product of the primes between n and $2n$ dividies $\binom{2n}{n}$. Note that this product is at least $n^{\pi(2n)-\pi(n)}$ (as every prime appearing in it is greater than n, and there are $\pi(2n) - \pi(n)$ such primes.) We thus have:

$$2^{2n} \geq \binom{2n}{n} \geq n^{\pi(2n)-\pi(n)},$$

and taking logs we deduce that:

$$\pi(2n) - \pi(n) \log n \leq 2n \log 2,$$

or equivialently $\pi(2n) - \pi(n) \leq 2 \log 2 \frac{n}{\log n}$.

To turn this into a lower bound on $\pi(n)$, we note that:

$$\begin{aligned}
\pi(n) &= \pi(n) - \pi(\frac{n}{2}) + \pi(\frac{n}{2}) - \pi(\frac{n}{4}) + \dots + \pi(\frac{n}{2^{k-1}}) - \pi(\frac{n}{2^k}) \\
&\leq \log 2[\frac{n}{2\log\frac{n}{2}} + \frac{n}{4\log\frac{n}{4}} + \dots + \frac{n}{2^k \log \frac{n}{2^k}}
\end{aligned}$$

where k is chosen as small as possible such that $\frac{n}{2^k}$ is greater than 1. With some additional work (which we will omit), and taking n sufficiently large, one can bound the right hand side of this by $c_2 \frac{n}{\log n}$ for any constant $c_2 > 2\log 2$, completing the proof of Chebyshev's theorem.