Number Theory

Jim Coykendall

September 28, 2011

Chapter 1

Background and Notation

Definition 1.0.1. *A set $(R, +, \cdot)$ is a ring if*

1) $(R, +)$ is an abelian group and for all $r, s, t \in R$:

2) $r(st) = (rs)t$;

3) $r(s + t) = rs + rt$;

4) $(r + s)t = rt + st$.

Additionally, we will usually assume

5) $rs = sr$ (commutativity) and

6) There is a $1_R \in R$ such that $r1_R = 1_R r = r$ for all $r \in R$.

Definition 1.0.2. *Let R be a commutative ring with 1.*

1. *If $R \setminus 0$ is an abelian group, then we say that R is a field.*
2. *If $ab = 0$ implies that $a = 0$ or $b = 0$ then we say that R is an (integral) domain.*

Definition 1.0.3. *A nonempty subset $I \subseteq R$ is said to be an ideal of R if*

1. *$(I, +)$ is an abelain group.*
2. *For all $r \in R$ and $z \in I$, $rz \in I$.*

Definition 1.0.4. *Let R, S be rings. We say that a function $\phi : R \longrightarrow S$ is a ring homomorphism if*

1. *$\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in R$.*
2. *$\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in R$.*
3. *$\phi(1_R) = 1_S$.*

Note that if $\phi : R \longrightarrow S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R and $\text{im}(\phi)$ is a subring of S.

Recall also that if R is a ring and $I \subseteq R$ is an ideal, then R/I is a ring with the additive structure induced by the quotient group and multiplication defined by

$$(x + I)(y + I) = xy + I$$

for all $x, y \in R$.

Here is a list of some common rings that one may encounter.

Definition 1.0.5. *Let R be a ring. We say that:*

1. *R is Euclidean if there is a function $f : R \setminus 0 \longrightarrow \mathbb{N}_0$ such that for all $x, y \in R \setminus 0$, $f(xy) \geq f(y)$ and there exist $q, r \in R$ such that $y = qx + r$ with $r = 0$ or $f(r) < f(x)$.*

2. *R is a PID (principal ideal domain) if every ideal of R is of the form Rx for some $x \in R$.*

3. *R is a UFD (unique factorization domain) if every nonzero nonunit of R can be expressed uniquely as a product of irreducible elements (equivalently, every nonzero nonunit is a product of primes).*

4. *R is atomic if every nonzero nonunit is a product of atoms.*

5. *R is of characteristic n if $n1_R = 0$ and n is the minimal natural number with the property (if no such $n \in \mathbb{N}$ exists, we say that R is of characteristic 0).*

We now produce a definition that highlights some important types of elements in a ring.

Definition 1.0.6. *Let R be a ring and $x \in R$ an element. We say that x is*

1. *A unit if $x^{-1} \in R$ (the units for a group under multiplication denoted by $U(R)$).*

2. *A zero divisor if there is a nonzero $y \in R$ such that $xy = 0$ (note that 0 is a zero divisor in any ring with identity).*

3. *Nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.*

4. *Irreducible if $x = ab$ implies that either a or b is a unit in R (this assumes that R is a domain).*

5. *Prime if x divides ab implies that x divides a or x divides b.*

Now for some types of ideals.

Definition 1.0.7. *An ideal $I \subseteq R$ is said to be*

1. *Prime if $ab \in I$ implies that $a \in I$ or $b \in I$;*
2. *Maximal if given J, an ideal, with the property that $I \subseteq J$ implies that $I = J$ or $J = R$;*
3. *Radical if $x^n \in I$ implies that $x \in I$ (equivalently, I is an intersection of prime ideals).*

Note that Euclidean $\implies$ PID $\implies$ UFD $\implies$ atomic, and maximal $\implies$ prime $\implies$ radical.

Here are some theorems to tie things together.

Theorem 1.0.8. *Let R be a ring and $I \subseteq R$ an ideal.*

1. *I is prime if and only if R/I is a domain.*
2. *I is maximal if and only if R/I is a field.*
3. *I is radical if and only if R/I is reduced (that is, R/I has no nonzero nilpotent elements).*

Proof. Exercise. □

Theorem 1.0.9. *Let F be a field and H a finite subgroup of $F^* = U(F)$, then H is cyclic.*

Proof. Since H is finite (and abelian), we can decompose

$$H \cong C_{m_1} \oplus C_{m_2} \oplus \cdots \oplus C_{m_k}$$

where $m_1 | m_2 | \cdots | m_k$.

Now note that for all $x \in H$, $x^{m_k} = 1$. Hence every element of H satisfies the polynomial

$$z^{m_k} - 1 = 0.$$

But since this equation is over a field, the polynomial $z^{m_k} - 1 = 0$ has at most m_k solutions. Hence $k = 1$ and H is cyclic. □

Corollary 1.0.10. *The multiplicative group of a finite field is cyclic.*

Chapter 2

Elementary number theory and the rational integers $\mathbb{Z}$

2.1 The rational integers

Theorem 2.1.1. *(The Fundamental Theorem of Arithmetic) Any nonzero natural number greater than or equal to 2 is uniquely a product of irreducible (prime) natural numbers.*

From this theorem it follows that $\mathbb{Z}$ is a UFD. A question of fundamental importance is "what rings share this fundamental theorem". For example, the ring $\mathbb{Z}[i]$ is a UFD as is $F[x_1, x_2, \cdots, x_n]$ where F is a field. However neither $F[x^2, x^3]$ nor $\mathbb{Z}[\sqrt{-14}]$ do not.

Example 2.1.2. *In the ring $F[x^2, x^3]$, both x^2 abd x^3 are irreducible but not prime. The same is true of the of 3 and $640 \pm 37\sqrt{-89}$ in $\mathbb{Z}[\sqrt{-89}]$.*

Theorem 2.1.3. *There are infinitely many prime elements of $\mathbb{Z}$.*

Proof. Suppose $p_1, \cdots p_n$ is an exhaustive list of primes if $\mathbb{Z}$. Now consider the element $a = p_1 p_2 \cdots p_n + 1$. This cannot be a "new" prime since the list is exhaustive. Hence p_i divides a for some i. Therefore p_i divides 1, which is the desired contradiction. □

Here is another proof for those that dig Calculus II.

Proof. Again suppose that $p_1, \cdots p_n$ is an exhaustive list of primes. Consider now the collection of infinite series

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{p_i}{p_i - 1}.$$

Multiplying these series, we obtain

$$(1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots)(1+\frac{1}{p_2}+\frac{1}{p_2^2}+\cdots)\cdots(1+\frac{1}{p_n}+\frac{1}{p_n^2}+\cdots)=\frac{p_1p_2\cdots p_n}{\prod_{k=1}^{n}(p_k-1)}.$$

We can multiply this out and rearrange at will since the series is absolutely convergent. In particular, we obtain

$$\sum_{k=0}^{\infty}\frac{1}{k}=\frac{p_1p_2\cdots p_n}{\prod_{k=1}^{n}(p_k-1)}$$

in particular, the harmonic series converges, which is our contradiction. □

From a more general point of view we have the following theorem.

Theorem 2.1.4. *(Dirichlet) Let m, r be relatively prime integers. Then there are infinitely many primes in the sequence $\{r+mn\}_{n=0}^{\infty}$.*

Definition 2.1.5. *Let R be a domain and $a, b \in R$.*

1. *The greatest common divisor of a and b ($gcd(a,b)$) (if it exists) is an element $d \in R$ such that $d|a$ and $d|b$ and given $x \in R$ such that $x|a$ and $x|b$ then $x|d$.*

2. *The least common multiple of a and b ($lcm(a,b)$) is an element $m \in R$ such that $a|m$ and $b|m$ and if there exists an element z such that $a|z$ and $b|z$ then $m|z$.*

Theorem 2.1.6. *If R is a PID and $gcd(a,b) = d$, then $d = ra + sb$ for some $r, s \in R$.*

Proof. Consider the ideal (a, b). Since R is a PID, $(a, b) = (x)$. Hence x divides both a abd b. Since $d = \gcd(a, b)$, we must have that $x|d$. Hence $(x) \supseteq (d)$. Since $ra + sb = x$ for some $r, s \in R$, we have that $d|x$ and hence $(x) = (d)$. So x and d are associates, and we are done. □

Corollary 2.1.7. *If R is a PID, $n|mr$, and $gcd(n,m) = 1$, then $n|r$.*

Proof. If R is a PID and $\gcd(n, m) = 1$ then there exist $r, s \in R$ such that $sn + tm = 1$. Hence $snr + tmr = r$ and so $n|r$. □

Theorem 2.1.8. *Let R be a PID and $m, n \in R$ (both nonzero). Then $mn = lcm(m,n)gcd(m,n)$.*

Proof. Exercise. □

2.2 The Chincese remainder theorem and Fermat's little theorem

Theorem 2.2.1. *Let $m = m_1 m_2 \cdots m_t$ with $(m_i, m_j) = 1$ if $i \neq j$, then the system of equations*

$$x \equiv b_i \ mod(m_i)$$

has a solution modulo m and any two solutions differ by a multiple of m.

This theorem follows from the following lemma.

Lemma 2.2.2. *Let $n > 0$ be an integer and consider the ring $\mathbb{Z}/n\mathbb{Z}$.*

1. *$\mathbb{Z}/n\mathbb{Z}$ is a finite ring with n elements.*
2. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*
3. *Any element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor.*
4. *If $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{a_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_t^{a_t}\mathbb{Z}$ (CRT)*

We look at some modular arithmetic applications.

Example 2.2.3. 1. *Find all integral solutions to $x^2 - 10y^2 = \pm 2$.*

2. *Which primes can be written as the sum of two squares?*

Now for the famous Fermat's Little Theorem.

Theorem 2.2.4. *If p is a prime and p does not divide a, then $a^{p-1} \equiv 1 \ mod(p)$.*

This result actually follows from the more general:

Proposition 2.2.5. *If $a \in \mathbb{Z}$ and p is prime, then $a^p \equiv a \ mod(p)$.*

Proof. The case $a < 0$ easily follows once the $a > 0$ is verified (the case $a = 0$ is certainly true). We proceed by induction. The case $a = 1$ is certainly true. Assume the result holds for $a = k$. Now note that

$$(k+1)^p = k^p + (\sum_{i=1}^{p-1} \binom{p}{i} k^i) + 1 \equiv k^p + 1 \equiv k + 1 \bmod(p).$$

□

It is natural to ask about the converse. In particular, if $a^{p-1} \equiv 1 \bmod(p)$ for all $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$, does this imply that p is prime? (The answer is no.)

Here is the final "classic" from this section.

Theorem 2.2.6. *(Freshman's Dream) $(a+b)^{p^n} \equiv a^{p^n} + b^{p^n} \ mod(p)$*

Proof. Exercise. □

Chapter 3

The Legendre Symbol

3.1 The Symbol and Reciprocity

Consider the equation

$$x^2 \equiv a \bmod(p);\ \gcd(a,p) = 1.$$

If this equation has a solution, then we say that a is a quadratic residue modulo p.

Example 3.1.1. *If $p = 2$ then everything is a square. If p is odd, then half the nonzero residues are squares and half are not.*

Definition 3.1.2. *Let p be an odd prime and $a \in \mathbb{Z}/p\mathbb{Z}$. Then $\left(\frac{a}{p}\right)$ is called the Legebdre symbol (mod p) and is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv a \bmod(p) \text{ has a solution,} \\ -1, & \text{if } x^2 \equiv a \bmod(p) \text{ has no solution,} \\ 0, & \text{if } p|a. \end{cases}$$

Example 3.1.3. *The squares mod 5 are $1, 4$ and the quadratic nonresidues are $2, 3$. So $\left(\frac{2}{5}\right) = \left(\frac{7}{5}\right) = -1$.*

Here are some properties of the Legendre symbol.

Lemma 3.1.4. *Let p be an odd prime and $a, b \in U(\mathbb{Z}/p\mathbb{Z})$.*

1. *If a, b are quadratic residues, then so is ab.*
2. *If a is a quadratic residue and b is not, then ab is not a quadratic nonresidue.*
3. *If a, b are quadratic nonresidues, then ab is a quadratic residue.*

Proof. Recall that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic. Quadratic residues are even powers of the generator and nonresidues are odd powers. From this is follows easily. □

Example 3.1.5. *Solve the equation* $4x \equiv 5 \ mod(p)$. *For what values of* A, B *is the equation* $x^2 + Ax + B \equiv 0 \ mod(7)$ *solvable?*

Theorem 3.1.6. *Let* $p > 0$ *be an odd prime (and we define* $\left(\frac{a}{p}\right) = 0$, *if* $p|a$).

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod(p)$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. *If* $a \equiv b \ mod(p)$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. All results are clear if a or b is divisible by p, so we will assume that p does not divide ab.

For the proof of 1, we first note that if a is not divisible by p, then $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod(p)$. To see this, note that $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \bmod(p)$.

With this in hand, we recall that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic of (even) order $p-1$, let us say that the generator is z. So there exists $k \in \mathbb{N}$ such that $z^k \equiv a \bmod(p)$

Hence $a^{\frac{p-1}{2}} \equiv z^{\frac{p-1}{2}k} \bmod(p)$ (and since z is a generator $z^{\frac{p-1}{2}} \equiv -1 \bmod(p)$. So $a^{\frac{p-1}{2}} \equiv (-1)^k \bmod(p)$. Hence $a^{\frac{p-1}{2}} \equiv 1 \bmod(p)$ if and only if k is even if and only if a is a square modulo p if and only if $\left(\frac{a}{p}\right) = 1$. Therefore $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod(p)$.

The second statement follows from the first. The third is easy. □

Corollary 3.1.7. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. *Hence* -1 *is a square modulo* p *if and only if* $p \equiv 1 \ mod(4)$.

Here is a big (and awfully handy) theorem.

Theorem 3.1.8. *Let* p, q *be distinct odd primes.*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \ mod(4) \\ -1, & \text{if } p \equiv 3 \ mod(4) \end{cases}$.
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1, 7 \ mod(8) \\ -1, & \text{if } p \equiv 3, 5 \ mod(8) \end{cases}$.
3. *(Quadratic Reciprocity)* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

In the next section, we will prove this theorem. We will begin here with a couple of nice applications for now.

Example 3.1.9. *Evaluate* $\left(\frac{20}{131}\right)$, $\left(\frac{56}{8675309}\right)$, *and* $\left(\frac{30}{257}\right)$.

3.2 The Proof of Quadratic Reciprocity

For completeness, we repeat the relevant theorem.

Theorem 3.2.1. *Let p, q be distinct odd primes.*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \bmod(4) \\ -1, & \text{if } p \equiv 3 \bmod(4) \end{cases}$.

2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1, 7 \bmod(8) \\ -1, & \text{if } p \equiv 3, 5 \bmod(8) \end{cases}$.

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

Proof. Note that the first result follows immediately from the previous. We prove the second statement here (the third statement will require a sequence of lemmas).

Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ and let $\omega \in \overline{\mathbb{F}_p}$ be a primitive 8^{th} root of 1 ($\omega^8 = 1, \omega^k \neq 1, 0 < k < 8$).

Note that $\omega^4 = -1$ and hence $\omega^2 + \omega^{-2} = 0$. Let $z = \omega + \omega^{-1}$. It is easy to verify that $z^2 = 2$. We now consider $z^p = \omega^p + \omega^{-p}$.

In the first case, we consider $p \equiv \pm 1 \bmod(8)$. In this case $z^p = \omega^{\pm 1 + 8k} + \omega^{\mp 1 + 8k} = \omega + \omega^{-1} = z$. Therefore $z^{p-1} = 1$. Now observe that

$$\binom{2}{p} \equiv 2^{\frac{p-1}{2}} \equiv (z^2)^{\frac{p-1}{2}} \equiv z^{p-1} \equiv 1 \bmod(p)$$

hence $\left(\frac{2}{p}\right) = 1$ when $p \equiv \pm 1 \bmod(8)$.

Now in the case where $p \equiv \pm 3 \bmod(8)$, so $z^p = \omega^{\pm 3 + 8k} + \omega^{\mp 3 + 8k} = \omega^3 + \omega^{-3} = -z$. To see the last step (the fact that $\omega^3 + \omega^{-3} = -z$), note that $\omega^3 + \omega^{-3} + z = \omega^3 + \omega^{-3} + \omega + \omega^{-1} = \omega^{-1}(\omega^4 + 1) + \omega^{-3}(\omega^4 + 1) = 0$.

Picking up where we left off, we now see that $z^p = -z$ and hence $z^{p-1} = -1$. Hence

$$\binom{2}{p} \equiv 2^{\frac{p-1}{2}} \equiv (z^2)^{\frac{p-1}{2}} \equiv z^{p-1} \equiv -1 \bmod(p)$$

and so $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \bmod(8)$.

□

We now produce some lemmas that will be useful in establishing quadratic reciprocity. In the sequel, we will denote by ξ a primitive p^{th} root of 1, i.e. $\xi = e^{\frac{2\pi i}{p}}$. Also for our purposes, $\left(\frac{a}{p}\right) = 0$ if $p|a$.

Lemma 3.2.2. $\sum_{n=0}^{p-1} \xi^{an} = \begin{cases} p, & \text{if } a \equiv 0 \bmod(p), \\ 0, & \text{if } a \not\equiv 0 \bmod(p). \end{cases}$

Proof. The result obviously holds if $a \equiv 0 \bmod(p)$. If not then

$$\sum_{n=0}^{p-1} \xi^a n = 1 + \xi^a + \xi^{2a} + \cdots + \xi^{(p-1)a} = \frac{\xi^{pa} - 1}{\xi^a - 1} = 0,$$

and we are done. □

We now establish the following notation. Let

$$\delta(x, y) := p^{-1} \sum_{n=0}^{p-1} \xi^{n(x-y)} = \begin{cases} 1, \text{ if } x \equiv y \bmod(p), \\ 0, \text{ if } x \not\equiv y \bmod(p). \end{cases}$$

Lemma 3.2.3. $\sum_{n=0}^{p-1} \binom{n}{p} = 0$.

Proof. Since p is an odd prime, half the nonzero elements of $\mathbb{Z}/p\mathbb{Z}$ are squares and the other half are not. □

We now define what is called a quadratic Gauss sum.

Definition 3.2.4. $G_a = \sum_{n=0}^{p-1} \binom{n}{p} \xi^{an}$.

Here are some useful properties of the Gauss sum G_a.

Lemma 3.2.5. $G_a = \binom{a}{p} G_1$

Proof. If $a \equiv 0 \bmod(p)$ then $\xi^{an} = 1$ for all n. Hence $G_a = \sum_{n=0}^{p-1} \binom{n}{p} = 0 = \binom{a}{p} G_1$.

If $a \not\equiv 0 \bmod(p)$ then

$$\binom{a}{p} G_a = \binom{a}{p} \sum_{n=0}^{p-1} \binom{n}{p} \xi^{an} = \sum_{n=0}^{p-1} \binom{an}{p} \xi^{an} = \sum_{t=0}^{p-1} \binom{t}{p} \xi^t = G_1.$$

□

We point out at this juncture that if $a \not\equiv 0 \bmod(p)$ then

$$G_a^2 = \binom{a}{p}^2 G_1^2 = G_1^2.$$

This next result is the analogue of the result from the proof of part 2) that showed that $z^2 = 2$.

Lemma 3.2.6. $G_1^2 = (-1)^{\frac{p-1}{2}} = \binom{-1}{p} p$.

We remark that $G_1^2 = G_a^2$ if $a \not\equiv 0 \bmod(p)$.

Proof. Let $a \not\equiv 0 \bmod(p)$. Then $G_a G_{-a} = \binom{a}{p}\binom{-a}{p} G_1^2 = \binom{-1}{p} G_1^2$. Therefore

$$\sum_{a \not\equiv 0 \bmod(p)} G_a G_{-a} = \binom{-1}{p} G_1^2 (p-1) = \sum_{a \bmod(p)} G_a G_{-a}.$$

Also note that since $G_a = \sum_{x=0}^{p-1} \binom{x}{p} \xi^{ax}$ and $G_{-a} = \sum_{y=0}^{p-1} \binom{y}{p} \xi^{-ay}$, we have that

$$G_a G_{-a} = \sum_{x=0}^{p-1} \binom{x}{p} \xi^{ax} \sum_{y=0}^{p-1} \binom{y}{p} \xi^{-ay} = \sum_x \sum_y \binom{x}{p}\binom{y}{p} \xi^{a(x-y)}.$$

So we now have that

$$\sum_{a \not\equiv 0 \bmod(p)} G_a G_{-a} = \sum_{a \not\equiv 0 \bmod(p)} \sum_x \sum_y \binom{x}{p}\binom{y}{p} \xi^{a(x-y)} =$$

$$= \sum_x \sum_y \Big(\binom{x}{p}\binom{y}{p} \sum_{a \bmod(p)} \xi^{a(x-y)} \Big) = \sum_x \sum_y \binom{x}{p}\binom{y}{p} p\delta(x,y) = p(p-1).$$

From this we see that

$$\binom{-1}{p} G_1^2 (p-1) = p(p-1)$$

and hence

$$G_1^2 = \binom{-1}{p} p = (-1)^{\frac{p-1}{2}} p,$$

and we are done. □

We now‘show quadratic reciprocity. We are working in the appropriate ring of integers modulo q (here p, q are distinct odd primes).

Proof. (Proof of Quadratic Reciprocity).
Note that

$$G_1^{q-1} = (G_1^2)^{\frac{q-1}{2}} = [\binom{-1}{p} p]^{\frac{q-1}{2}} \equiv \binom{p'}{q} \bmod(q)$$

where $p' = \binom{-1}{p}$. Hence

$$G_1^q \equiv G_1 \binom{p'}{q} \bmod(q).$$

But by the Freshman's Dream

$$G_1^q = (\sum_{x=0}^{p-1} \binom{x}{p} \xi^x)^q \equiv \sum_{x=0}^{p-1} \binom{x}{p} \xi^{qx} \equiv G_q \bmod(q)$$

and hence

$$G_1^q \equiv G_q \equiv \left(\frac{q}{p}\right) G_1 \bmod(q).$$

Therefore, $\left(\frac{p'}{q}\right) G_1 \equiv \left(\frac{q}{p}\right) G_1 \bmod(q)$. We now multiply this by G_1. Recalling that $G_1^2 = p'$, we obtain

$$\left(\frac{p'}{q}\right) p' \equiv \left(\frac{q}{p}\right) p' \bmod(q).$$

Since p' and q are relatively prime, we have $\left(\frac{p'}{q}\right)$ and $\left(\frac{q}{p}\right)$ are equivalent modulo q and hence are equal. We now consider

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

This concludes the proof. □

Chapter 4

Algebraic Number Fields

4.1 Motivation and Fermat's Last Theorem

Recall that Fermat's Last Theorem states that if $n \in \mathbb{N}$ is such that $n > 2$ then there is no nontrivial solution to the equation

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

This little ditty confounded many mathematicians over the course of about 350 years. It turns out that this problem would have been solved well over a century ago if all rings of algebraic integers were UFDs (the fact that this is not true is part of the rich tapestry of number theory). We begin with the statement of Fermat's Last Theorem, and then we will highlight some secial relevant cases.

Theorem 4.1.1. *There are no nontrivial solutions to the Diophantine equation*

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

for $n > 2$.

We remark here that if $n = 2$, there are infinitely many solutions (and these solutions can be completely listed). To prove this theorem, it suffices to show that the statement holds for $n = 4$ and $n = p$ where p is an odd prime. We will explore the case $n = 4$ later; for now we restrict to the case $x^p + y^p = z^p$ where p is an odd prime and x, y, z are pairwise relatively prime.

Classically, Fermat's Last Theorem was divided into 2 cases, the first case is the case where p does not divide xyz. The second case is where (precisely) one of the x, y, z is divisible by p. We will concentrate on the first case (where p does not divide xyz).

The case $p = 3$ is fairly easy to establish.

Lemma 4.1.2. *The equation* $x^3 + y^3 = z^3$ *has no solution with* $x, y, z \in \mathbb{Z}$ *if* $3 \nmid (xyz)$

Proof. Reduce modulo 9 and look at the cubes. □

More generally, we will show that if $p > 3$ is an odd prime, then $x^p + y^p = z^p$ has no solution of $p \nmid (xyz)$

We will also make the blanket assumption that the ring $\mathbb{Z}[\xi_p]$ where $\xi_p = e^{\frac{2\pi i}{p}}$ is a UFD (this is true for every prime < 23 and many others after 23).

Lemma 4.1.3. *If $u \in \mathbb{Z}[\xi_p]$ is a unit then $\xi^t u \in \mathbb{R}$ for some $t \in \mathbb{N}$.*

Proof. Note that both u and $\overline{u}$ are units in $\mathbb{Z}[\xi_p]$. We let $v = \frac{u}{\overline{u}}$. Note that $|v| = \frac{|u|}{|\overline{u}|} = 1$.

We first claim that $v = \pm\xi^s$ for some $s \in \mathbb{Z}$. To this end, note that v is a root of the polynomial

$$\prod_{\sigma \in G} (x - \sigma(v)) \in \mathbb{Z}[x]$$

where G is the (cyclic) Galois group of $\mathbb{Q}(\xi_p)$ over $\mathbb{Q}$.

When we expand this polynomial, we obtain a polynomial all of whose coefficients are bounded by an appropriate binomial coefficient $\binom{n}{m}$ where $n = |G|$ (recall that $|\sigma(v)| = 1$ for all $\sigma \in G$. Hence there are only finitely many such polynomials and hence only finitely many elements from $\mathbb{Z}[\xi_p]$ that satisfy them.

Now note that every integral power of v satisfies the above conditions. Finiteness assures that there exist integers k, r such that $v^k = v^r$. Since v is nonzero, we have that v is a root of unity and hence $v = \pm\xi^s = \frac{u}{\overline{u}}$.

We now let $\gamma = 1 - \xi$ and we note that $\xi^j \equiv 1 \bmod(\gamma)$ for all j and note that if $\sigma \in G$, $\sigma(\xi) = \xi^k$ for some k.

Writing:

$$u = a_0 + a_1\xi + \cdots + a_{p-3}\xi^{p-3} + a_{p-2}\xi^{p-2}$$

and reducing $\bmod(\gamma)$ we see

$$u \equiv \sigma(u) \bmod(\gamma)$$

and in particular $u \equiv \overline{u} \bmod(\gamma)$.

If $v = -\xi^s$, then $u = -\xi^s\overline{u}$ and $u \equiv -\overline{u} \equiv -u \bmod(\gamma)$. Hence $2u \equiv 0 \bmod(\gamma)$ and this is a contradiction since $2, u$ are both units $\bmod(\gamma)$ (to see that 2 is, assume that $2 = (1 - \xi)r$ and take norms to obtain $2^{p-1} = pN(r)$).

Hence we must assume that $u = \xi^s\overline{u}$. Letting $s \equiv -2t \bmod(p)$, we have that

$$\xi^t u = \xi^{-t}\overline{u} = \overline{\xi^t u}$$

and hence $\xi^t u \in \mathbb{R}$.

□

Lemma 4.1.4. *In $\mathbb{Z}[\xi]$, the element $1 - \xi$ is prime.*

Proof. We will (perhaps prematurely) use the norm. Have a little faith here and all will be tied together later.

Our unproven fact(s) concern properties of the norm. $N(1-\xi) = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1})$. Now since

$$\frac{x^p-1}{x-1} = 1 + x + x^2 + \cdots + x^{p-1} = (x-\xi)(x-\xi^2)\cdots(x-\xi^{p-1})$$

and hence $\prod_{i=1}^{p-1}(1-\xi^i) = p$. Hence $p = N(1-\xi)$ is irreducible (as a norm) and hence $(1-\xi)$ is irreducible (and hence prime since we have an active "UFD" assumption. This concludes the proof. □

Lemma 4.1.5. *If $x^p + y^p = z^p$ with p prime, x, y, z pairwise relatively prime, and $p \nmid (xyz)$ then $x + \xi^i y$ and $x + \xi^j y$ are relatively prime if $i \not\equiv j$ mod(p).*

Proof. Any divisor of $x+\xi^i y$ and $x+\xi^j y$ must divide $\xi^{j-i}-1$, since ξ is a unit and x and y are relatively prime. Without loss of generality, we will say this divisor is $1-\xi$ (use Galois group if necessary) and we recall that this element is prime.

Since

$$\prod_{i=0}^{p-1}(x+\xi^i y) = z^p$$

we must have that $1-\xi$ divides z.

We now note that $(1-\xi)^p \equiv 0 \bmod(p)$ and hence $(1-\xi)^p = p\alpha$ with $\alpha \in \mathbb{Z}[\xi]$. Tying these together, we get that

$$\frac{z^p}{p\alpha} = \beta \in \mathbb{Z}[\alpha].$$

And so

$$\frac{z^p}{p} = \alpha\beta \in \mathbb{Z}[\xi] \bigcap \mathbb{Q} = \mathbb{Z}.$$

Hence p divides z^p in $\mathbb{Z}$ and so $p|z$ and we are done. □

Lemma 4.1.6. *There exist $u, \beta \in \mathbb{Z}[\xi]$ (where u is a real unit) such that $x+\xi y = \xi^s u\beta$ where $\beta \equiv n$ mod(p) for some $n \in \mathbb{Z}$.*

Proof. Since $\prod_{i=0}^{p-1}(x+\xi^i y) = z^p$ and the terms on the left are relatively prime, each $x+\xi^i y$ is a p^{th} power. In particular, there exists $\alpha \in \mathbb{Z}[\xi]$ with $x+\xi y = \epsilon\alpha^p$ with $\epsilon \in U(\mathbb{Z}[\xi])$. By our previous, we can write $\epsilon = \xi^s u$ where u is a real unit in $\mathbb{Z}[\xi]$. Hence the first statement is satified with $\beta = \alpha^p$.

Now writing

$$\alpha = \sum_{i=o}^{p-2} n_i \xi^i,$$

we note that $\alpha^p \equiv \sum_{i=0}^{p-2} n_i \bmod(p)$. □

Lemma 4.1.7. *With notation as above, we have, as elements of* $\mathbb{Z}[\xi]$*:*

$$x + \xi y - \xi^{2s} x - \xi^{2s-1} y \equiv 0 \ mod(p).$$

Proof. In the previous lemma, we had that

$$x + \xi y = \xi^s u \beta$$

and so complex conjugation gives that

$$x + \xi^{-1} y = \xi^{-s} u \overline{\beta}.$$

Hence $\xi^{-s}(x + \xi y) - \xi^s(x + \xi^{-1} y) = u(\beta - \overline{\beta})$. Recalling that $\beta \equiv n \bmod(p)$ for some $n \in \mathbb{Z}$, we reduce modulo p; since $\beta \equiv \overline{\beta} \bmod(p)$ we obtain

$$\xi^{-s}(x + \xi y) - \xi^s(x + \xi^{-1} y) \equiv 0 \bmod(p),$$

and this completes the proof. □

We now tie this machinery together to obtain our desired result.

Theorem 4.1.8. *(Under blanket UFD assumption). The equation*

$$x^p + y^p = z^p$$

has no nontrivial solutions for integers x, y, z *if* $p \nmid (xyz)$.

Proof. By the previous lemma, $x + \xi y - \xi^{2s} x - x i^{2s-1} y \equiv 0 \bmod(p)$.

Since the set $\{1, \xi, \xi^2, \cdots, \xi^{p-2}\}$ is linearly independent over $\mathbb{Q}$, we note that if each power of ξ is distinct in $x + \xi y - \xi^{2s} x - x i^{2s-1} y$ then both x and y must be divisible by p. Hence our only worry is when (at least) two of the powers are the same. We eliminate the cases.

In the case where $\xi^{2s} = 1$, we have that $y(\xi^2 - 1) = y(\xi - 1)(\xi + 1) \in p\mathbb{Z}[\xi]$. Note that since $p = (1 - \xi)(1 - \xi^2) \cdots (1 - \xi^{p-1})$, $(1 - \xi)$ divides p $p - 1$ times and $1 + \xi$ is relatively prime to p. Hence $1 - \xi$ divides y and hence $(1 - \xi)^p$ divides y^p. We conclude that $p | y^p$ and the quotient is an integer. Hence $y | p$ and this case is eliminated.

In the case that $\xi^{2s-1} = \xi$, we have that $x(1 - \xi^2) \in p\mathbb{Z}[\xi]$ and this is the same as the previous.

In the case that $\xi^{2s-1} = 1$, we have that $x - y + (y - x)\xi \in p\mathbb{Z}[\xi]$. Hence $(x - y) \equiv 0 \bmod((1 - \xi)^{p-2})$ and so $x \equiv y \bmod(p)$.

We now rewrite our equation as

$$x^p + (-z)^p = (-y)^p.$$

If we encounter one of the first two cases, we are done. If not, we must conclude that

$$x \equiv -z \bmod(p).$$

Hence

$$0 = x^p + y^p + (-z)^p \equiv x + y - z \equiv 3x \bmod(p).$$

But since p is a prime greater than 3, $p|x$ and we are done. □

Remark 4.1.9. *The so called "second case" where precisely one of x, y, z is divisible by p can be proved by similar (although perhaps harder) techniques similar to the above.*

The really big assumption used was the "blanket assumption" that $\mathbb{Z}[\xi_p]$ is a UFD. We can loosen the blanket assumption to the case where p is a "regular prime" (which means, for further reference, that p does not divide the class number of $\mathbb{Z}[\xi]$ (the class number, which we will see later, is basically a measure of how far one of these domains is from being a UFD...the class number of a UFD is 1).

Kummer showed in 1850 that Fermat's Last Theorem held for any regular prime. The only irregular primes less than 100 are 37, 59, 67. However as of 2011, it is not know if there are infinitely many regular primes (although it has been known since 1915 that there are infinitely many irregular primes).

With this motivation in hand, we move on to study algebraic number fields. We begin our study with the case of quadratic fields (the nuts and bolts of most general phenomena can be seen here).

4.2 Quadratic fields

Definition 4.2.1. *Let d be a square-free integer. A quadratic field is a field of the form*

$$K := \mathbb{Q}(\sqrt{d}).$$

We note that K is the smallest field containing both $\mathbb{Q}$ and $\sqrt{d}$ and is a 2 dimensional vector space over $\mathbb{Q}$. It is also worth noting that every element of K is of the form $a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$.

Theorem 4.2.2. *There are precisely two automorphisms of K: the identity and the conjugation automorphism*

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}.$$

This follows from the more general statement:

Theorem 4.2.3. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial with distinct roots $r_1, r_2, \cdots, r_k\mathbb{C}$. If $K = \mathbb{Q}(r_1, r_2, \cdots, r_k)$ and $\sigma \in Aut(K/\mathbb{Q})$, then $\sigma(r_i) = r_j$. What is more, for all $1 \leq i, j \leq k$, there is a $\sigma \in Aut(K/\mathbb{Q})$ such that $\sigma(r_i) = r_j$.*

Since we have that for all $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ and $f \in \mathbb{Q}[x]$, we have that $f(r_i) = 0$ implies that $\sigma(f(r_i)) = f(\sigma(r_i)) = 0$. Hence $\mathrm{Aut}(K/\mathbb{Q})$ permutes the roots. So we have the first statement. We skip the second.

We remark that $\mathrm{Aut}(K/\mathbb{Q})$ is called the Galois group of K. For our purposes, we say that K is Galois if $K = \mathbb{Q}(\alpha)$ and every root of the minimal polynomial for α is in K. We recall that the Galois group is a transitive subgroup of S_n where n is the degree of the minimal polynomial of α.

We build an analog of $\mathbb{Z}$ inside $\mathbb{Q}(\sqrt{d})$. To this end, we look for elements in $\mathbb{Q}(\sqrt{d})$ with the property that they are roots of a monic polynomial over $\mathbb{Z}[x]$.

Theorem 4.2.4. *Let d be a squarefree integer. The quadratic ring of integers corresponding to the field $\mathbb{Q}(\sqrt{d})$ is given by:*

$$R := \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \ mod(4); \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d \equiv 1 \ mod(4). \end{cases}$$

Proof. Definitely homework. □

Basic question on these quadratic rings of integers.

1. Does R have unique factorization?
2. What elements are prime/irreducible?
3. If $p \in \mathbb{Z}$ is prime, what is the behavior of p in R?
4. If R is not a UFD, what kind of factoriztion properties does it exhibit?
5. What is the structure of $U(R)$?

Before we proceed, let us review some useful concepts from algebra.

Definition 4.2.5. *We say that R is a Euclidean domain if there is a map $\phi : R^* \longrightarrow \mathbb{N}_0$ satisfying:*

1. *$\phi(xy) \geq \phi(x)$ for all $x, y \in R^*$.*
2. *For all $x, y \in R, x \neq 0$, there exists $q, r \in R$ such that $y = qx + r$ with $r = 0$ or $\phi(r) < \phi(x)$.*

The next two results help to clarify the places in the universe of PIDs and UFDs.

Proposition 4.2.6. *Let R be a commutative ring with identity. If I is an ideal that is maximal with respect to being nonprincipal, then I is prime.*

Proof. Suppose that $ab \in I$ with neither a nor b in I. Note that $I \subsetneq (I, a)$ and hence $(I, a) = (y)$. We now let $J = \{z \in R | zy \in I\} = (w)$. We claim that $Jy = I$ (meaning that I is principal and our desired contradiction). The fact that $Jy \subseteq I$ is clear. For the other containment, suppose that $i \in I$. Note that since $(y) \supseteq I$, we can write $i = ry$, but then $r \in J$ by definition. This completes the proof. □

Proposition 4.2.7. *Let R be commutative with identity, I an ideal and S a multiplicative set such that $I \bigcap S = \emptyset$. Then there is a prime ideal $\mathfrak{P}$ containing I with the property that $\mathfrak{P} \bigcap S = \emptyset$.*

Proof. Consider X, the set of ideals of R containing I that miss S. This set of ideals is partially ordered by inclusion. TO show that there is a maximal element, we verify that any chain in X has an upper bound and apply Zorn's lemma. If $\mathfrak{C}$ is a chain in X, it is easy to see that the union of this chain is an upper bound in X.

To finish the proof, we merely need to show that such an ideal is prime. Suppose that $\mathfrak{P}$ is maximal with respect to the property that $\mathfrak{P} \bigcap S = \emptyset$. Now suppose that $ab \in \mathfrak{P}$ with neither a nor b in $\mathfrak{P}$. Note that both $(\mathfrak{P}, a)$ and $(\mathfrak{P}, b)$ intersect S nontrivially. Hence there are $p_1, p_2 \in \mathfrak{P}$ and $r_1, r_2 \in R$ such that

$$p_1 + r_1 a = s_1$$

and

$$p_2 + r_2 b = s_2$$

with $s_1, s_2 \in S$.

Multiplying the equations gives

$$p_1 p_2 + p_1 r_2 b + p_2 r_1 a + r_1 r_2 ab = s_1 s_2 \in \mathfrak{P}$$

and this is our desired contradition.

□

Proposition 4.2.8. *Let R be an integral domain. Then R is a UFD if and only if every nonzero principal ideal contains a nonzero prime element.*

Proof. Suppose that R is a UFD, $\mathfrak{P}$ is a nonzero prime ideal, and $0 \neq x \in \mathfrak{P}$. Writing x as a product of primes:

$$x = p_1 p_2 \cdots p_n$$

we see that $p_i \in \mathfrak{P}$ for some i and the first direction is complete.

On the other hand, we consider the set, S, of elements in R that can be expressed as a product of primes (and units). Suppose that a is a nonzero nonunit of R that cannot be written as a product of primes. Since the set of elements that can be written as a product of primes is saturated,$(a) \bigcap S = \emptyset$. Hence there is a prime ideal $\mathfrak{P}$ containing (a) such that $\mathfrak{P} \bigcap S = \emptyset$. But clearly $\mathfrak{P}$ cannot contain a prime element and this is our contradiction. □

Theorem 4.2.9. *Let R be a domain. Then R is Euclidean implies R is a PID implies R is a UFD.*

Proof. To see that any Euclidean domain is a PID, we let I be a nonzero ideal in R and consider the set $\{\phi(x)|0 \neq x \in I\}$, where ϕ is the Euclidean function. It is easy to I is generated by y where y is the minimal element of this set.

To see that PID implies UFD, let $\mathfrak{P}$ be a nonzero prime ideal. Since $\mathfrak{P}$ is principal, it contains a prime. So R is a UFD. □

Before we formally talk about the norm, we delve into some examples.

Example 4.2.10. *$\mathbb{Z}[i]$ is a UFD. To see this we show that it is, in fact, Euclidean. Consider the function defined by*

$$\phi(a+bi) = a^2 + b^2.$$

It is easy to see that $\phi(xy) = \phi(x)\phi(y)$. We let $0 \neq \alpha = a+bi$ and $\beta = c+di$. Note that

$$\frac{\beta}{\alpha} = \frac{c+di}{a+bi} = \frac{ac+bd+i(ad-bc)}{a^2+b^2} = r + si$$

with $r, s \in \mathbb{Q}$.

Now select $m, n\mathbb{Z}$ such that $|r-m| \leq \frac{1}{2}$ and $|s-n| \leq \frac{1}{2}$. Observe that $\phi(\frac{\beta}{\alpha} - (m+ni)) = (r-m)^2 + (s-n)^2 \leq \frac{1}{2}$ Finally let $R = \beta - \alpha(m+ni)$ (hence $\beta = \alpha(m+ni) + R$) and either $R = 0$ or $\phi(R) = \phi(\alpha)\phi(\frac{\beta}{\alpha} - (m+ni)) \leq \frac{1}{2}\phi(\alpha) < \phi(\alpha)$.

Example 4.2.11. *We can now classify the primes (irreducibles) in $\mathbb{Z}[i]$. $p \in \mathbb{Z}$ remains prime if and only if $p \equiv 3$ mod(4). In all other cases, the prime splits into two prime factors (the case $p = 2$ is special as the prime is "ramified".*

Example 4.2.12. *Again, we use the norm to show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.*

Example 4.2.13. *One can use the norm to determine units.*

4.3 Norm and Trace for Quadratic Fields

Definition 4.3.1. *Let d be a square free integer. The norm $N : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}$ is given by*

$$N(a+b\sqrt{d}) = a^2 - db^2$$

and the trace is given by

$$T(a+b\sqrt{d}) = 2a.$$

Theorem 4.3.2. *The norm and trace have the following properties.*

N1) $N(\alpha\beta) = N(\alpha)N(\beta)$.

N2) $N(\alpha) = 0$ if and only if $\alpha = 0$.

N3) $N(\alpha) = \alpha^2$ *if and only if* $\alpha \in \mathbb{Q}$.

T1) $T(\alpha + \beta) = T(\alpha) + T(\beta)$.

T2) $T(\alpha) = 2\alpha$ *if and only if* $\alpha \in \mathbb{Q}$.

Proof. Think of norm and trace as product and sum of conjugates respectively. □

It is worth noting that if $\alpha \in \mathbb{Q}(\sqrt{d})$ then α is a root of $x^2 - T(\alpha)x + N(\alpha)$.

Theorem 4.3.3. *Let R be a ring of algebraic integers. Then $r \in U(R)$ if and only if $N(r) = \pm 1$.*

Proof. Exercise. □

Proposition 4.3.4. *Let R be an imaginary quadratic ring of integers ($d < 0$), and $\omega = \frac{-1+\sqrt{-3}}{2}$. The unit structure of R is given by*

$$U(R) = \begin{cases} \pm 1, \pm i, & \text{if } d = -1; \\ \pm 1, \pm\omega, \pm\omega^2, & \text{if } d = -3; \\ \pm 1, & \text{otherwise.} \end{cases}$$

Proof. An exercise in completing the square. □

We remark here that the real quadratic case is more complicated.

Example 4.3.5. *The existence of the element $1 + \sqrt{2} \in \mathbb{Z}$ shows that the unit group here must be infinite.*

4.4 Pell's Equation (Real Quadratic Units)

Consider the equation

$$x^2 - dy^2 = \pm 1$$

where d is a square free (positive) integer. A motivating question is when does this equation have aa solution. For the case when the right hand side is 1, the answer is always and when the right side is -1 the answer is sometimes. But this is far from obvious. For example the "smallest" solution to the equation $x^2 + 94y^2 = \pm 1$ is $(x, y) = (2143295, 221064)$.

The existence and structure of solutions to Pell's equation has some clear ramifications for the unit structure of the ring of integers of $\mathbb{Q}(\sqrt{d})$ with $d > 0$. We begin on our quest to show that this equation has solutions by introducing some lemmata.

Proposition 4.4.1. *Let γ be an irrational number. Then there are infinitely many rational numbers $\frac{x}{y} \in \mathbb{Q}$, with $gcd(x, y) = 1$ such that $|\frac{x}{y} - \gamma| < \frac{1}{y^2}$.*

Proof. We partition the interval $[0,1)$ by

$$[0,\frac{1}{n})\bigcup[\frac{1}{n},\frac{2}{n})\bigcup\cdots\bigcup[\frac{n-1}{n},1).$$

Recall that the fractional part of the real number z is given by $z-\lfloor z\rfloor$.

Now consider the fractional parts of $0,\gamma,2\gamma,\cdots,n\gamma$. By the pigeonhole principle, 2 of these fractional parts must be in the same subinterval. More precisely, there exist $0\leq k<j\leq n$ such that

$$|j\gamma-\lfloor j\gamma\rfloor-(k\gamma-\lfloor k\gamma\rfloor)|<\frac{1}{n}.$$

Letting $y=k-j$ and $x=\lfloor k\gamma\rfloor-\lfloor j\gamma\rfloor$ we have

$$|x-\gamma y|<\frac{1}{n}$$

(We can go ahead and assume that $\gcd(x,y)=1$ as division by $\gcd(x,y)$ only "helps".)

Note that $0<y=j-k\leq n$ and hence $|\frac{x}{y}-\gamma|<\frac{1}{ny}\leq\frac{1}{y^2}$.

To see that there are infinitely many solutions, choose any $m>\frac{1}{|\frac{x}{y}-\gamma|}$ and note that $\frac{1}{m}<|\frac{x}{y}-\gamma|$.

By our previous work, we can find x_1,y_1 such that

$$|\frac{x_1}{y_1}-\gamma|<\frac{1}{my_1}\leq\frac{1}{y_1^2}.$$

Also note that $(x_1,y_1)\neq(x,y)$ since $|\frac{x}{y}-\gamma|>\frac{1}{m}\geq\frac{1}{my_1}$. Hence we have infinitely many solutions. □

Lemma 4.4.2. *If $d>0$ is a square-free integer then there is a constant N such that $|x^2-dy^2|<N$ has infinitely many solutions.*

Proof. By the previous, there are infinitely many pairs (x,y) of positive relatively prime integers satisfying $|\frac{x}{y}-\sqrt{d}|<\frac{1}{y^2}$ or equivalently

$$|x-y\sqrt{d}|<\frac{1}{y}.$$

By the triangle inequality, we have

$$|x+y\sqrt{d}|+2\sqrt{d}|y|<\frac{1}{y}+2\sqrt{d}|y|,$$

and hence

$$|x^2-dy^2|<|\frac{1}{y}+2\sqrt{d}y|\frac{1}{y}\leq 2\sqrt{d}+1,$$

and this concludes the proof. □

Theorem 4.4.3. *If $d > 0$ is a square-free integer then the equation $x^2 - dy^2 = 1$ has infinitely many integral solutions. What is more, there is a solution (u, v) such that every solution is of the form $\pm((u_n, v_n)$ where $u_n + v_n\sqrt{d} = (u + v\sqrt{d})^n, n \in \mathbb{Z}$.*

Proof. By the previous lemma there is an m such that $x^2 - dy^2 = m$ for infinitely pairs $x > 0, y > 0$ integers. Assume that for all pairs (x, y) the x's are distinct. Note that since there are only finitely many residue classes modulo $|m|$, we can find $(x_1, y_1), (x_2, y_2)$ with $x_1 \neq x_2$ and $x_1 \equiv x_2 \bmod(|m|)$ and $y_1 \equiv y_2 \bmod(|m|)$. We now let $\alpha = x_1 - y_1\sqrt{d}, \beta = x_2 - y_2\sqrt{d}$.

Note now that $N(\alpha\beta) = m^2 = \alpha\overline{\alpha}\beta\overline{\beta}$. We write $\alpha\overline{\beta} = r + s\sqrt{d}, \overline{\alpha}\beta = r - s\sqrt{d}$.

We observe that

$$\alpha\overline{\beta} = (x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 - dy_1y_2 + (x_1y_2 - x_2y_1)\sqrt{d}.$$

Since we have that $x_1 \equiv x_2 \bmod(|m|)$ and $y_1 \equiv y_2 \bmod(|m|)$, both terms of $r \pm s\sqrt{d}$ are divisible by m. We write

$$\alpha\overline{\beta} = m(u + v\sqrt{d})$$

where $N(u + v\sqrt{d}) = 1 = u^2 - dv^2$. (Note that if $v = 0$ then we multiply by β to get $\alpha\overline{\beta}\beta = \pm m\beta = m\alpha$ and hence $\pm\beta = \alpha$. Since $x_1 \equiv x_2 \bmod(|m|)$ we have that $x_1 = x_2$ which is a contradiation. Hence there is a nontrivial solution.

For the second statement, we note that for all solutions (x, y) we consider the corresponding real numbers $x + y\sqrt{d}$. Note that if $x^2 - dy^2 = 1$ then all positive solutions correspond to $x, y > 0$ $(x + y\sqrt{d} > 1)$ and $x > 0, y < 0$ $(0 < x + y\sqrt{d} < 1$, the inverse or conjugate case to the previous). Clearly there is a minimal solution with the property that $x > 0, y > 0$. We claim that any solution in the case $x, y > 0$ is a positive power of this minimal solution, α. Indeed if β is another "positive" solution then there is a positive $n \in \mathbb{N}$ such that $\alpha^n \leq \beta \leq \alpha^{n+1}$. If both inequalities are strict then we consider $1 < \beta\alpha^{-n} < \alpha$ which is a contradiction. All other solutions are $\pm$ a conjugate of this. □

Corollary 4.4.4. *Let R be the ring of integers in $\mathbb{Q}(\sqrt{d})$ (where $d > 0$ is a square-free integer). Then there is a unit $\eta \in R$ such that every unit of R is of the form $\pm\eta^n$, $n \in \mathbb{Z}$.*

Proof. □

Bibliography