November 5:

Math 431 Class Lecture Notes

- Factoring primes
- Diophantine equations, continued
- Integer points on an elliptic curve

0.1 Factoring primes

Suppose F is a number field and let $\alpha \in F$. Let p be a rational prime not dividing $[\mathbf{Z}_F : \mathbf{Z}[\alpha]]$. Then a very useful theorem, stated last time, asserts that the principal ideal generated by p factors as

$$(p) := p\mathbf{Z}_F = \prod P_i^{e_i},$$

where $P_i = (p, f_i(\alpha))$ and $m_\alpha \equiv \prod f_i^{e_i} \bmod p$. In addition, the residue class degree of P_i is the degree of f_i, and in fact, $\mathbf{Z}_F/P_i = \mathbf{F}_p[x]/(f_i(x))$.

We outline a proof of this result, mostly by reducing it to a sequence of "elementary" algebra isomorphisms; the reader will have to draw on their abstract algebra brain cells to verify the details.

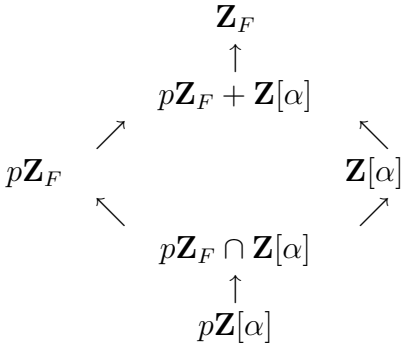
The behavior of p i $\mathbf{Z}_F$ is determined by the structure of the quotient $\mathbf{Z}_F/(p)$ where (p) denotes $p\mathbf{Z}_F$. We start by showing that our hypothesis on the index of $\mathbf{Z}[\alpha]$ in $\mathbf{Z}_F$ implies that this quotient is isomorphic to $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$.

The kernel of the map from $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$ to $\mathbf{Z}_F/p\mathbf{Z}_F$ is $(p\mathbf{Z}_F \cap \mathbf{Z}[\alpha])/p\mathbf{Z}[\alpha]$, and the cokernel (the quotient of the domain by the image) is $\mathbf{Z}_F/(p\mathbf{Z}_F +$

$\mathbf{Z}[\alpha]$). In the language of abstract algebra, we have an exact sequence

$$0 \to \frac{p\mathbf{Z}_F \cap \mathbf{Z}[\alpha]}{p\mathbf{Z}[\alpha]} \to \frac{\mathbf{Z}[\alpha]}{p\mathbf{Z}[\alpha]} \to \frac{\mathbf{Z}_F}{p\mathbf{Z}_F} \to \frac{\mathbf{Z}_F}{p\mathbf{Z}_F + \mathbf{Z}[\alpha]} \to 0.$$

Consider the following diagram of inclusions of abelian groups (in which all upward arrows are inclusions).



The index $a := [\mathbf{Z}_F : p\mathbf{Z}_F + \mathbf{Z}[\alpha]]$ is a divisor both of $[\mathbf{Z}_F : p\mathbf{Z}_F]$, which has order a power of p, and of $[Z_F : \mathbf{Z}[\alpha]]$, which is prime to p by assumption. Therefore $a = 1$. Similarly the index $b := [p\mathbf{Z}_F \cap \mathbf{Z}[\alpha]$ is a divisor of $[p\mathbf{Z}_F : p\mathbf{Z}[\alpha]] = [\mathbf{Z}_F : \mathbf{Z}[\alpha]$ and of $[\mathbf{Z}[\alpha] : p\mathbf{Z}[\alpha]]$ and we conclude that $b = 1$. Thus the kernel and cokernel of the map ϕ are trivial, and the map from $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$ to $\mathbf{Z}_F/p\mathbf{Z}_F$ is an isomorphism, as claimed.

With this in hand, we study the ring $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$. There are natural isomorphisms

$$\frac{\mathbf{Z}[\alpha]}{p\mathbf{Z}[\alpha]} \simeq \frac{\mathbf{Z}[x]}{(p, f(x))} \simeq \frac{\mathbf{F}_p[x]}{\overline{f}(x)} \simeq \bigoplus \frac{\mathbf{F}_p[x]}{\overline{f}_i(x)^{e_i}}.$$

The quotient $\mathbf{F}_p[x]/\overline{f}_i^{e_i}$ is a ring with a unique prime ideal, name the principal ideal $P_i' := (f_i)$. By chasing back through the isomorphisms, one finds that this corresponds to the prime ideal $P_i = (p, f_i(\alpha))$ in $\mathbf{Z}[\alpha]$. Since the prime ideals in a direct sum of rings correspond to prime ideals in each summand, we conclude that the P_i are the unique prime ideals in $\mathbf{Z}[\alpha]$ that contain p. Moreover, the quotient rings $\mathbf{Z}[\alpha]/P_i$ are isomorphic to $\mathbf{F}_p[x]/\overline{f}_i(x)$ so that the residue class degree of P_i is the degree of f_i.

Moreover, in the quotient $\mathbf{F}_p[x]/\overline{f}$ the product $\prod(P_i')^{e_i}$ vanishes. Chasing back through the isomorphisms, we find that this means that in $\mathbf{Z}[\alpha]$ the product

$$\prod P_i^{e_i}$$

contains the ideal $p\mathbf{Z}[\alpha]$. If $p\mathbf{Z}[\alpha] = \prod P_i^{E_i}$ then by the "$\sum e_i f_i$" theorem, we have

$$n = \sum e_i \deg(f_i) \geq \sum E_i \deg(f_i) = n$$

so equality holds throughout.

Putting all of this together gives us the desired result!

0.2 Diophantine equations, continued

Many applications of algebraic number theory to specific Diophantine equations start by factoring a homogeneous polynomial into two variables into a product of linear forms, with coefficients in an algebraic number field. Typically, the other side of the equation is a perfect power, or a constant times a perfect power.

For instance:

- The parametrization of all Pythagorean triples over $\mathbf{Z}$, can be done by carefully considering the factorization

  $$(x + iy)(x - iy) = z^2,$$

  in $\mathbf{Z}[i]$.

- The integral points of the elliptic curve $y^2 = x^3 - 355$ can be found by factoring $y^2 + 355$ and setting it equal to a perfect cube.

- All solutions to $x^2 + y^2 = z^3$ can be found by factoring the LHS and working in $\mathbf{Z}[i]$.

- As we will see shortly, the nonexistence of nontrivial solutions to $x^3 + y^3 = z^3$ can be proved by writing this as

  $$(x + y)(x + \omega y)(x + \overline{\omega} y) = z^3,$$

  where $\omega = \exp^{2\pi i/3}$, and then working in $\mathbf{Z}[\alpha]$.

The problem of finding which numbers are values of a given homogeneous polynomial sometimes succumbs to the same techniques. For instance, solutions to the equation $x^2 + y^2 = n$ boil down to the question of which integers are norms of elements of $\mathbf{Z}[i]$; the equation has solutions if and only if all primes $p \mid n$, $p \equiv 3 \bmod 4$ have even exponents in the prime factorization of n.

0.3 Integer points on an elliptic curve

One of the famous open conjectures in number theory asserts that the rank of an elliptic curve (the number of independent points of infinite order) is equal to the order of vanishing at $s = 1$ of the L-series of the elliptic curve. This conjecture is due to Bryan Birch and Peter Swinnerton-Dyer. Their conjecture has led to an immense amount of research. It is somehow comforting that this conjecture was originally motivated by calculations on many specific curves.

One of the most famous curves that Birch and Swinnerton-Dyer used was the curve

$$y^2 + m = x^3.$$

As above, this leads naturally to consideration of the field $\mathbf{Q}(\sqrt{-m}) =: F$. To treat a simple general case, let's suppose that $-m \equiv 2$ or $3 \bmod 4$, that m is positive and squarefree, and that $3 \nmid h_F$.

The equation factors as $(y + \sqrt{-m})(y - \sqrt{-m}) = x^3$. Considering this modulo 8 we see that x must be odd; also, $(y, m) = 1$, since if $p \mid y$, $p \mid m$, then $p \mid x$; but then m is not squarefree.

The ideals $y \pm \sqrt{-m}$ are relatively prime. If $IJIK = x^3$ then $y \pm \sqrt{-m} \in I \Rightarrow 2\sqrt{-m}, 2y \in I$. $(y, m) = 1 \Rightarrow (x, m) = 1$. So we have $(y + \sqrt{-m}) = I^3 = (a + b\sqrt{-m})^3$; moving to elements, $y + \sqrt{-m} = (a + b\sqrt{-m})^3$, since we can absorb the unit into a and b. Thus,

$$\begin{aligned} y + \sqrt{-m} &= \pm(a + b\sqrt{-m})^3 && (1) \\ &= (a^3 - 3ab^2m) + (3a^2b - b^3m)\sqrt{-m} && (2) \end{aligned}$$

Now, $(3a^2 - b^2m)b = 1 \Rightarrow b = \pm 1$. So we have $3a^2 - m = \pm 1$ which implies $m = 3a^2 \pm 1$. The conclusion is as follows.

Theorem 1. With the above assumptions on m, the equation

$$y^2 + m = x^3$$

has a solution if and only if m is of the form $m = 3a^2 \pm 1$, in which case we must have $x = (a^2 + m)^3$, and $y = a^3 - 3am$.