(*September 22, 2011*)

Algebraic Number Theory Exercises-discussion 01

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

[number theory 01.1] Prove the Euler product expansion of the zeta function, namely, for $\mathrm{Re}(s) > 1$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

A useful point is that

$$\frac{1}{1-p^{-s}} \;=\; 1 + p^{-s} + (p^2)^{-s} + (p^3)^{-s} + \ldots$$

Often this Euler product expansion is interpreted as a slightly analytic manifestation of the *unique factorization* in $\mathbb{Z}$. Proper care for *convergence* is a non-trivial task, but worth doing once in one's life. Part of the burden is merely notational, but the risks of bad notation are considerable.

[See http://www.math.umn.edu/˜garrett/m/mfms/ex_c/mfms_disc_01.pdf]

[number theory 01.2] Prove that a prime p is expressible as $p = a^2 + ab + b^2$ for integers a, b if and only if $p = 1 \bmod 3$ (or $p = 3$).

Discussion: One direction has an easy, if slightly ugly, argument: looking at the possible values mod 3, taking $a, b = 0, 1, 2$, the only possibilities are $0, 1 \bmod 3$. A more dignified way to see this half also arises in the following discussion of the harder direction of implication.

Let ω be a primitive cube root of unity. The Galois norm $\mathbb{Q}(\omega) \to \mathbb{Q}$ is $N(a \pm b\omega) = a^2 + ab + b^2$ for $a, b \in \mathbb{Q}$. As usual, norms of units of $\mathbb{Z}[\omega]$ must be units in $\mathbb{Z}$, namely, ± 1. The usual trick

$$\mathbb{Z}[\omega]/p \;\approx\; \mathbb{F}_p[x]/\langle x^2 + x + 1\rangle$$

shows that $\mathbb{Z}[\omega]/p$ is a *field* if and only if there is no cube root of unity in $\mathbb{F}_p^\times$, that is, if and only if $p = 2 \bmod 3$. That is, p remains prime in $\mathbb{Z}[\omega]$ if and only if $p = 2 \bmod 3$. For $p = 2 \bmod 3$, no condition $p = N(a + b\omega)$ is possible, or else p would be a product of two non-units, and not prime.

For primes $p = 1 \bmod 3$, where $\mathbb{F}_p$ *does* have primitive cube roots of unity ρ, ρ^2,

$$\mathbb{Z}[\omega]/p \;\approx\; \mathbb{F}_p[x]/\langle x - \rho\rangle \oplus \mathbb{F}_p[x]/\langle x - \rho^2\rangle$$

Thus, (as in the Lemma proven in class), $p \cdot \mathbb{Z}[\omega]$ is a product $p = p_1 p_2$ of two primes p_i in $\mathbb{Z}[\omega]$. Since p is fixed by the Galois group, the non-trivial Galois automorphism can only *interchange* the two factors, so $p = (a = b\omega)(a - b\omega)$ for some $a, b \in \mathbb{Z}$. ///

[number theory 01.3] Let ω be a primitive 7^{th} root of unity, and let $\xi = \omega + \omega^{-1}$. Observe that $\xi^3 + \xi^2 - 2\xi - 1 = 0$. Find the precise congruence relation on primes p for there to be a solution of $x^3 + x^2 - 2x - 1 = 0$ in $\mathbb{Z}/p$.

Discussion: For $p = \pm 1 \bmod 7$, $7 | p^2 - 1$, so by cyclic-ness of $\mathbb{F}_{p^2}^\times$ there is a primitive 7^{th} root of unity ω in $\mathbb{F}_{p^2}$. Then $\xi = \omega + \omega^{-1}$ is at worst in $\mathbb{F}_{p^2}$. It suffices to show that it is *fixed* by the *Frobenius automorphism* $x \to x^p$ of $\mathbb{F}_{p^2}$: letting $p = 7k \pm 1$,

$$\xi^p \;=\; (\omega + \omega^{-1})^p \;=\; \omega^p + \omega^{-p} \;=\; \omega^{7k\pm 1} + \omega^{1\pm 7k} \;=\; \omega^{\pm 1} + \omega^{\mp 1} \;=\; \xi$$

Conversely, when $\xi \in \mathbb{F}_p$, as ω satisfies the quadratic equation $\omega^2 - \xi\omega + 1 = 0$ over $\mathbb{F}_p(\xi) = \mathbb{F}_p$, ω is at most quadratic over $\mathbb{F}_p$. Thus, $\mathbb{F}_{p^2}^\times$ is cyclic of order divisible by 7, so $p = \pm 1 \bmod 7$. ///